Charon-SSP/4M OCI
Getting Started Guide

Contents

About this Guide

Contents

Intended Audience

This guide is intended for anyone who needs to install, configure, or manage the Stromasys Charon-SSP processor/platform virtualization software. A general working knowledge of PC operating systems and their conventions is expected.

This getting-started guide covers the **Charon-SSP/4M for OCI** distribution. This appliance package contains the full software set including the underlying Linux host operating system. The document provides a first introduction to the product. For more detailed information, please refer to the Charon-SSP/4M sections of the general Charon-SSP user's guide.

If you require additional information about this product, please contact Stromasys at the regional addresses below or at **Team.Support.OCI@Stromasys.com**, or contact your Stromasys VAR.

Obtaining documentation

The latest released version of this manual and other related documentation are available on the Stromasys support website at Product Documentation and Knowledge Base.

Obtaining technical assistance

Several support channels are available to cover the Charon virtualization products.

If you have a support contract with Stromasys, please visit http://www.stromasys.com/support/ for up-to-date support telephone numbers and business hours. Alternatively, the support center is available via email at support@stromasys.com.

If you purchased a Charon product through a Value-Added Reseller (VAR), please contact them directly.

For further information on purchases and the product best suited to your requirements, please contact your regional sales team:

Region	Email address	Phone	Address
Australasia-Pacific	apac.sales@stromasys.com	+852 3520 1030	Room 1113, 11/F, Leighton Centre 77 Leighton Road, Causeway Bay, Hong Kong, China
Americas	ams.sales@stromasys.com	+1 919 239 8450	2840 Plaza Place, Ste 450 Raleigh, NC 27612 U.S.A.
Europe, Middle-East and Africa	emea.sales@stromasys.com	+41 22 794 1070	Avenue Louis-Casai 84 5th Floor 1216 Cointrin Switzerland

Throughout the document(s) these conventions are followed

Notation	Description
$	The dollar sign in interactive examples indicates an operating system prompt for VMS. The dollar sign can also indicate non superuser prompt for UNIX / Linux.
#	The number sign represents the superuser prompt for UNIX / Linux.
>	The right angle bracket in interactive examples indicates an operating system prompt for Windows command (cmd.exe).
`User input`	Bold monospace type in interactive examples indicates typed user input.
`<`**`path`**`>`	Bold monospace type enclosed by angle brackets indicates command parameters and parameter values.
`Output`	Monospace type in interactive examples, indicates command response output.
[ ]	In syntax definitions, brackets indicate items that are optional.
...	In syntax definitions, a horizontal ellipsis indicates that the preceding item can be repeated one or more times.
`dsk0`	Italic monospace type, in interactive examples, indicates typed context dependent user input.

The following definitions apply

Term	Description
Host	The system on which the emulator runs, also called the Charon server
Guest	The operating system running on a Charon instance, for example, Tru64 UNIX, OpenVMS, Solaris, MPE or HP-UX

Related Documents

- CHARON-SSP V3.0.2 for Linux
- CHARON-SSP V2.0.5 for Linux
- CHARON-SSP V1.4.1 for Linux
    - Charon-SSP V1.4.5 for Linux - Patch Notes - August 2017
- CHARON-SSP V1.0.36 for Linux
- CHARON-SSP V1.0.34 for Linux
- CHARON-SSP V1.0.26 for Linux
    - CHARON-SSP V1.0.26 for Linux - User's Guide

Introduction to Charon-SSP

In 1987, Sun Microsystems released the SPARC V7 processor, a 32-bit RISC processor. The SPARC V8 followed in 1990 – a revision of the original SPARC V7, with the most notable inclusion of hardware divide and multiply instructions. The SPARC V8 processors formed the basis for a number of servers and workstations such as the SPARCstation 5, 10 and 20. In 1993, the SPARC V8 was followed by the 64-bit SPARC V9 processor. This too became the basis for a number of servers and workstations, such as the Enterprise 250 and 450.

Due to hardware obsolescence and lack of spare or refurbished parts, software and systems developed for these older SPARC-based workstations and servers have become harder to maintain. To fill the continuous need for certain, end-of-life SPARC-based systems, Stromasys S.A. developed the Charon-SSP line of virtual machine products. The following products are software-based, virtual machine replacements for the specified native-hardware SPARC systems. A general overview of the emulated hardware families is shown below:

Charon-SSP/4M emulates the following SPARC hardware:

- **Sun-4m family (for example Sun SPARCstation 20)**: Originally, a multiprocessor Sun-4 variant, based on the MBus processor module bus introduced in the SPARCServer 600MP series. The Sun-4m architecture later also encompassed non-MBus uniprocessor systems such as the SPARCstation 5, utilizing SPARC V8-architecture processors. Supported starting with SunOS 4.1.2 and by Solaris 2.1 to Solaris 9. SPARCServer 600MP support was dropped after Solaris 2.5.1.

Charon-SSP/4U(+) emulates the following SPARC hardware:

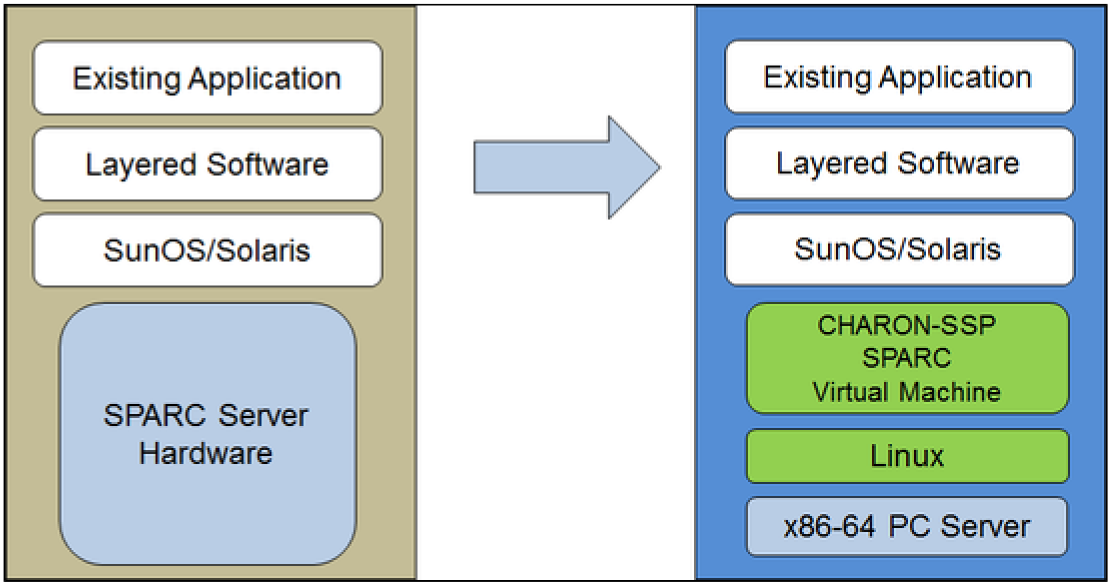
- **Sun-4u family (for example Sun Enterprise 450)**: (U for UltraSPARC) – this variant introduced the 64-bit SPARC V9 processor architecture and UPA processor interconnect first used in the Sun Ultra series. Supported by 32-bit versions of Solaris starting from version 2.5.1. The first 64-bit Solaris release for Sun-4u was Solaris 7. UltraSPARC I support was dropped after Solaris 9. Solaris 10 supports Sun-4u implementations from UltraSPARC II to UltraSPARC IV.

Charon-SSP/4V(+) emulates the following SPARC hardware:

- **Sun-4v family (for example SPARC T2)**: A variation on Sun-4u which includes hypervisor processor virtualization; introduced in the UltraSPARC T1 multicore processor. Selected hardware was supported by Solaris version 10 starting from release 3/05 HW2 (most models - including the hardware emulated by Charon-SSP - require newer versions of Solaris 10). Several Solaris 11 versions are also supported.

⚠ For up-to-date information about supported features and versions refer to Virtual Hardware and Guest OS Supported by Charon-SSP/4M for OCI and to the release notes of your product.

The image below shows the basic concept of migrating physical hardware to an emulator:



The Charon-SSP virtual machines allow users of Sun and Oracle SPARC-based computers to replace their native hardware in a way that requires little or no change to the original system configuration. This means you can continue to run your applications and data without the need to switch or port to another platform. The Charon-SSP software runs on commodity, Intel 64-bit systems ensuring the continued protection of your investment.

Charon-SSP/4U+ supports the same virtual SPARC platforms as Charon-SSP/4U, and **Charon-SSP/4V+** the same as Charon-SSP/4V. However, the 4U+ and 4V+ versions take advantage of Intel's VT-x/EPT hardware assisted virtualization technology in modern Intel CPUs to offer end users better virtual CPU performance. Charon-SSP/4U+ and Charon-SSP/4V+ require Intel CPUs with VT-x/EPT capability and **must** be installed on a dedicated Intel-based host. Running these product variants in a VM is **not supported**.

ℹ Unless otherwise mentioned, the terms Charon-SSP/4U and Charon-SSP/4V also include Charon-SSP/4U+ and Charon-SSP/4V+.

Virtual Hardware and Guest OS Supported by Charon-SSP/4M for OCI

Contents

Supported Virtual Hardware

The different families of Charon-SSP virtual machines support a number of different hardware devices. The table below describes the device features and maximum number supported by Charon-SSP/4M for OCI:

Charon-SSP/4M for OCI Supported Virtual Hardware	
	Charon-SSP/4M for OCI
SPARC V8 (32-bit)	Y
SPARC V9 (64-bit)	n/a
Max. number of CPUs	4
Max. RAM	64MB to 512MB
Ethernet controllers	2 (controller type le)
SCSI controllers	1
SCSI target IDs	7 (1)
Serial ports	2
Graphics controllers	1 (CGTHREE or CGSIX)
Audio controllers	1 (DBRIe)

(1) Each SCSI target ID can have up to 8 LUNs. Therefore, the overall number of SCSI devices can be larger than the number of target IDs. The exact number depends on the emulated hardware, the guest operating system version, and the SCSI devices used

Supported Guest Operating Systems

The Charon-SSP/4M virtual machines support the following guest operating system releases:

- SunOS 4.1.3 - 4.1.4
- Solaris 2.3 to Solaris 9

Setting up a Charon-SSP/4M OCI Instance

This chapter describes how to set up a basic Charon-SSP/4M for OCI instance.

Contents

Prerequisites

General Prerequisites

To access and use Charon-SSP/4M for OCI, you need an Oracle Cloud account.

Licensing

Charon-SSP/4M for OCI requires a license to run emulated SPARC systems. Such licenses can be software or network-enabled hardware licenses.

Please contact your Stromasys representative or your Stromasys VAR for information about the available licensing options. For contact information see About this Guide.

⚠ The user is responsible for any Solaris licensing obligations and has to provide the appropriate licenses.

OCI Shape Prerequisites (Hardware Prerequisites)

By selecting a shape in OCI, you select the virtual hardware that will be used for Charon-SSP. Therefore, the selection of an instance type determines the hardware characteristics of the Charon-SSP virtual host hardware (e.g., how many CPU cores and how much memory your virtual Charon host system will have).

Minimum requirements for Charon-SSP:

- Minimum number of host system CPU cores:
  - At least one CPU core for the host operating system.
  - **For each emulated SPARC system:**
    - One CPU core for each emulated CPU of the instance.
    - At least one additional CPU core for I/O. If server JIT optimization is used, add an additional I/O CPU for improved translation speed.
- Minimum memory requirements:
  - At least 2GB of RAM for the host operating system.
  - **For each emulated SPARC system:**
    - The configured memory of the instance.
    - 2GB of RAM (6GB of RAM if server JIT is used) to allow for DIT optimization, emulator requirements, run-time buffers, SMP and graphics emulation.
- One or more network interfaces, depending on customer requirements.
- Charon-SSP/4U+ and Charon-SSP/4V+ must run on hardware supporting VT-x (not applicable to Charon-SSP/4M).

⚠ Please note that the sizing guidelines above—in particular regarding number of host CPU cores and host memory—show the minimum requirements. Every use case has to be reviewed and the actual host sizing has to be adapted as necessary. For example, the number of I/O CPUs may have to be increased if the guest applications produce a high I/O load. Also take into consideration that a system with many emulated CPUs in general is also able to create a higher I/O load and thus the number of I/O CPUs may have to be raised.

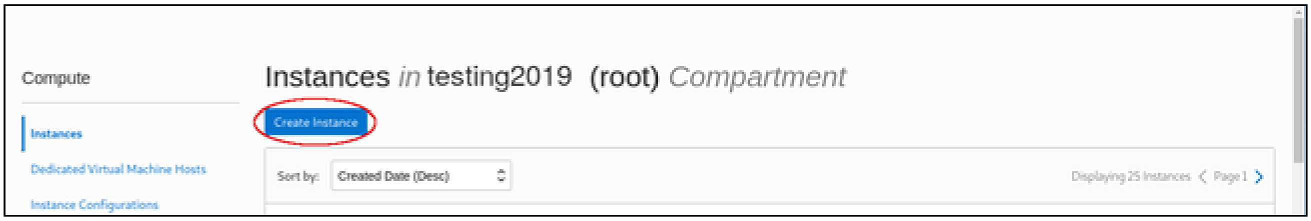
OCI New Instance Launch

⚠ This section only shows a very basic example. Please refer to the Oracle Cloud documentation for more detailed information.

To start the creation of a new cloud instance using Charon-SSP/4M for OCI, perform the following steps:

Step 1: log in to your Oracle Cloud environment.

Step 2: go to the instance list in the compute section and select to create an instance.



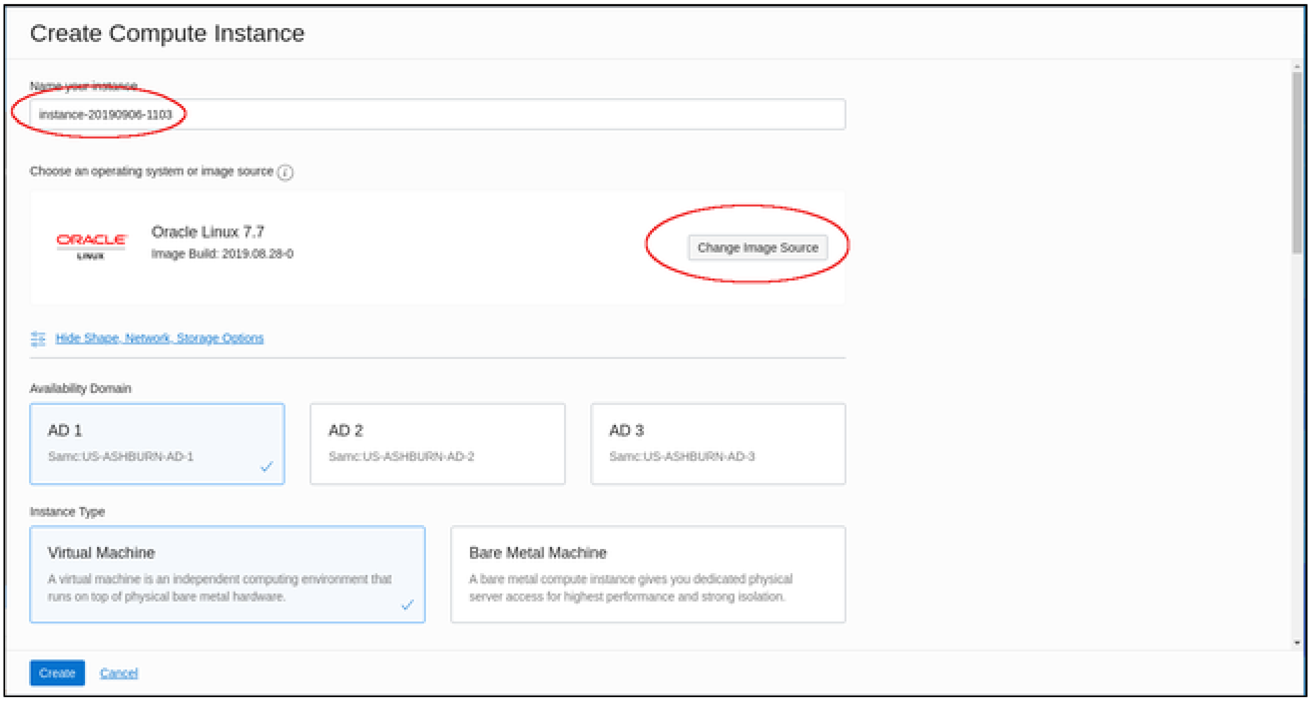
Instances *in* testing2019 (root) *Compartment*

Sort by: Created Date (Desc)

Displaying 25 Instances Page 1

This opens the **Create Compute Instance** window.

Step 3: on the first part of **Create Compute Instance** window, name your instance and select the Charon-SSP image for it.



Create Compute Instance

Name your instance: instance-20190906-1103

Choose an operating system or image source: Oracle Linux 7.7, Image Build: 2019.08.28-0

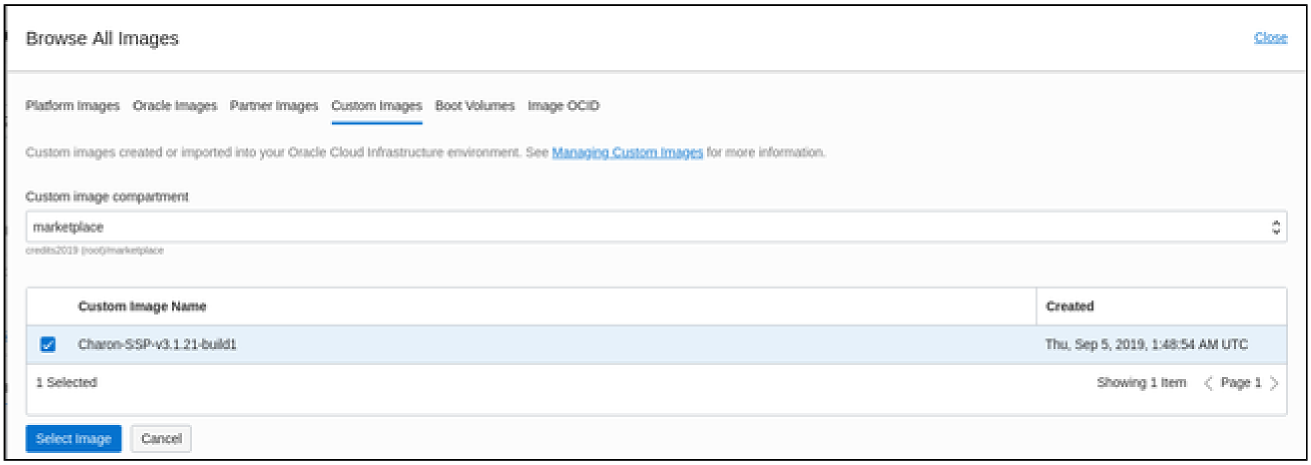
Availability Domain: AD 1 Samc:US-ASHBURN-AD-1 ✓

Instance Type: Virtual Machine ✓

ORACLE LINUX
Change Image Source
Hide Shape, Network, Storage Options
AD 2
Samc:US-ASHBURN-AD-2
AD 3
Samc:US-ASHBURN-AD-3
A virtual machine is an independent computing environment that runs on top of physical bare metal hardware.
Bare Metal Machine
A bare metal compute instance gives you dedicated physical server access for highest performance and strong isolation.
Create
Cancel

To select the correct image, select **Change Image Source**. This will allow you to browse the different available categories for the Charon-SSP/4M image.

The image below shows an example:



Browse All Images

Close

Platform Images Oracle Images Partner Images Custom Images Boot Volumes Image OCID

Custom images created or imported into your Oracle Cloud Infrastructure environment. See Managing Custom Images for more information.

Custom image compartment: marketplace

credits2019 (root)/marketplace

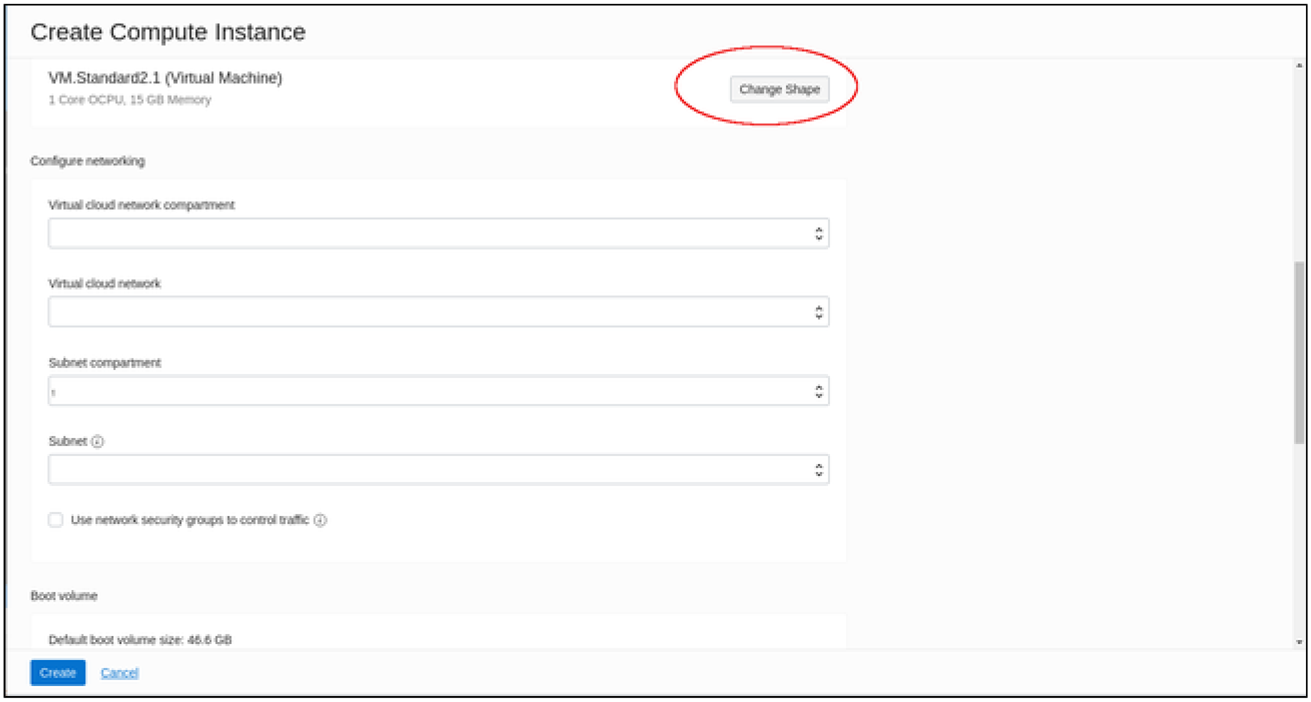
	Custom Image Name	Created
☑	Charon-SSP-v3.1.21-build1	Thu, Sep 5, 2019, 1:48:54 AM UTC

1 Selected — Showing 1 Item — Page 1

Select Image Cancel

Selecting the image and confirming your selection will take you back to the **Create Compute Instance** window.

Step 4: on the middle part of the **Create Compute Instance** window, select the appropriate shape (i.e., the virtual Charon host hardware) and the subnet membership.



Create Compute Instance

VM.Standard2.1 (Virtual Machine)

1 Core OCPU, 15 GB Memory

Change Shape

Configure networking

Virtual cloud network compartment

Virtual cloud network

Subnet compartment

Subnet

□ Use network security groups to control traffic

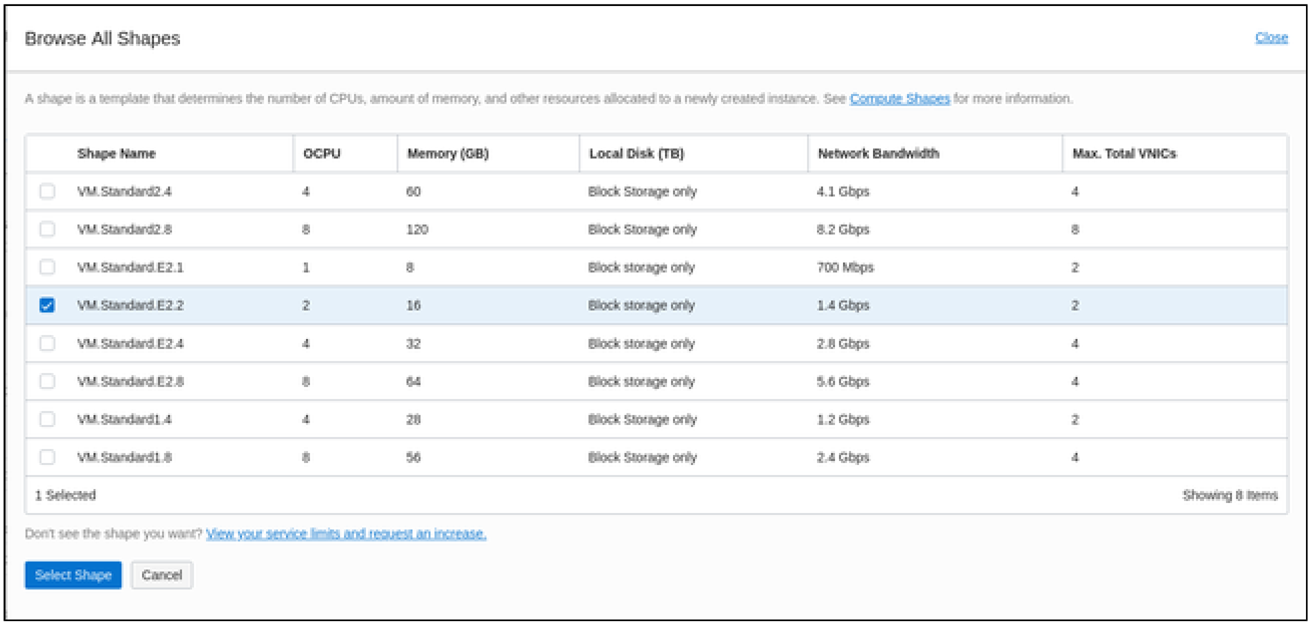
Boot volume

Default boot volume size: 46.6 GB

Create Cancel

To select an appropriate shape conforming to the hardware requirements of the emulated SPARC system, click on **Change Shape**.

This will open a window where you can select the correct system type.



Browse All Shapes

A shape is a template that determines the number of CPUs, amount of memory, and other resources allocated to a newly created instance. See Compute Shapes for more information.

	Shape Name	OCPU	Memory (GB)	Local Disk (TB)	Network Bandwidth	Max. Total VNICs
□	VM.Standard2.4	4	60	Block Storage only	4.1 Gbps	4
□	VM.Standard2.8	8	120	Block Storage only	8.2 Gbps	8
□	VM.Standard.E2.1	1	8	Block storage only	700 Mbps	2
☑	VM.Standard.E2.2	2	16	Block storage only	1.4 Gbps	2
□	VM.Standard.E2.4	4	32	Block storage only	2.8 Gbps	4
□	VM.Standard.E2.8	8	64	Block storage only	5.6 Gbps	4
□	VM.Standard1.4	4	28	Block Storage only	1.2 Gbps	2
□	VM.Standard1.8	8	56	Block Storage only	2.4 Gbps	4

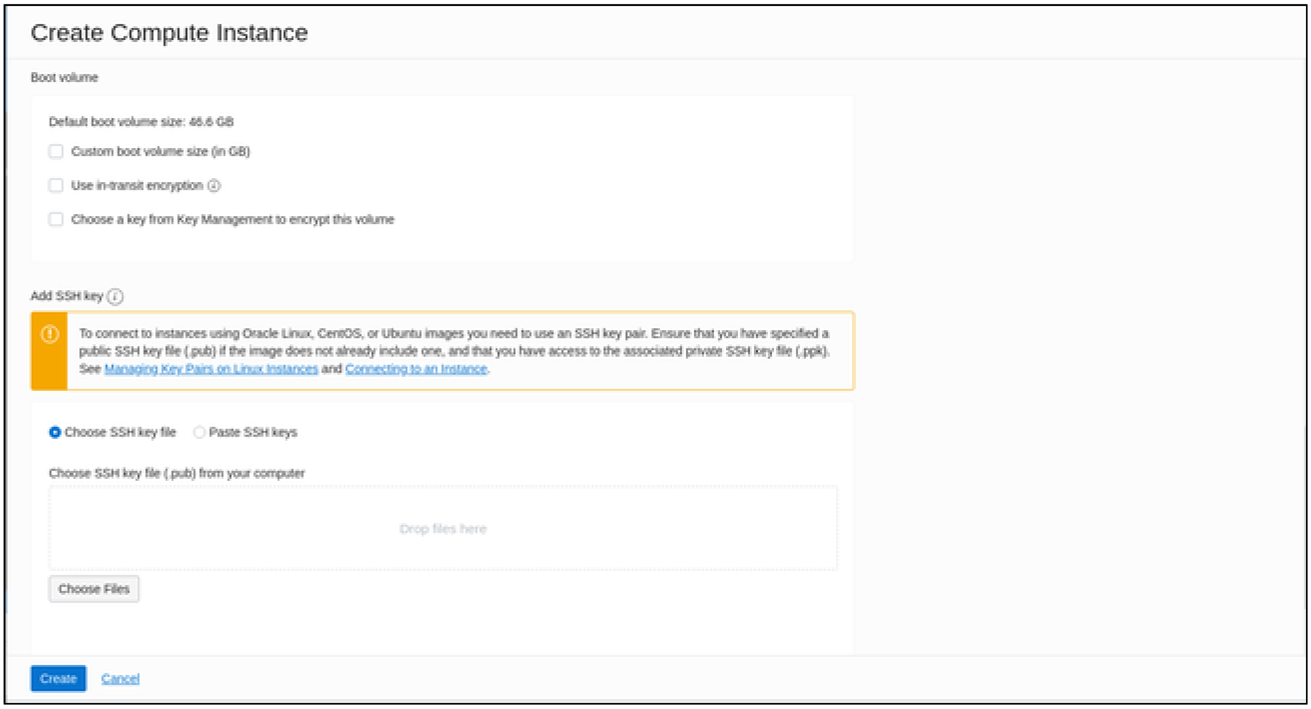
1 Selected

Showing 8 Items

Don't see the shape you want? View your service limits and request an increase.

Confirming you selection will take you back to the **Create Compute Instance** window.

Step 5: on the bottom of the **Create Compute Instance** window configure your boot device as required and upload the public SSH key of the key-pair you will use to access your instance.



Create Compute Instance

Boot volume

Default boot volume size: 46.6 GB

□ Custom boot volume size (in GB)

□ Use in-transit encryption

□ Choose a key from Key Management to encrypt this volume

Add SSH key

To connect to instances using Oracle Linux, CentOS, or Ubuntu images you need to use an SSH key pair. Ensure that you have specified a public SSH key file (.pub) if the image does not already include one, and that you have access to the associated private SSH key file (.ppk). See Managing Key Pairs on Linux Instances and Connecting to an Instance.

● Choose SSH key file ○ Paste SSH keys

Choose SSH key file (.pub) from your computer

Click on **Create** to create your instance.

Step 6: verify your instance is running.

Your instance should now be visible in the list of compute instances.

Installing the Charon Manager

Contents

Overview

The Charon-SSP Manager is the main interface for managing the emulated SPARC systems running on a Charon-SSP host. Therefore, the Charon-SSP Manager must be installed on every local system that will be used to manage the Charon instances running on the Charon-SSP cloud host.

Stromasys provides Charon-SSP Manager installation packages for the following Linux distributions and versions:

- Versions 7.x or higher of Oracle Linux (64 bit) version, Red Hat Enterprise Linux (64 bit), or CentOS (64 bit).

Support for Charon Manager on Microsoft Windows is planned for a later date.

Installation Packages and Installation Steps

Installation Packages

Installation packages are available in RPM package format:

- RPM package: **charon-manager-ssp-<*version*>.rpm**

Obtaining the installation packages:

Please contact your Stromasys representative or Stromasys VAR to obtain the installation package or the correct download location for your version.

Installation Steps on Linux

The following table describes the installation steps for Charon-SSP Manager:

Step	Details
1	Log-in to the local Linux system as the **root** user (denoted by the **#** prompt).
2	Copy the installation package to the local Linux system
3	Go to the directory where the package has been stored: `# cd <package-location>`
4	**Install package:**

	For systems with RPM package management (Oracle Linux, Red Hat, CentOS):
	`# yum install <package-name>`

Example (RPM):

```
# yum install /media/sf_vmshare/charon-manager-ssp-3.1.8.rpm
Loaded plugins: langpacks, product-id, search-disabled-repos, subscription-manager
Examining /media/sf_vmshare/charon-manager-ssp-3.1.8.rpm: charon-manager-ssp-3.1.8-1.x86_64
Marking /media/sf_vmshare/charon-manager-ssp-3.1.8.rpm to be installed
Resolving Dependencies
--> Running transaction check
---> Package charon-manager-ssp.x86_64 0:3.1.8-1 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
Package Arch Version Repository Size
================================================================================
Installing:
charon-manager-ssp x86_64 3.1.8-1 /charon-manager-ssp-3.1.8 4.2 M

Transaction Summary
================================================================================
Install 1 Package

Total size: 4.2 M
Installed size: 4.2 M
Is this ok [y/d/N]: y
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Warning: RPMDB altered outside of yum.
Installing : charon-manager-ssp-3.1.8-1.x86_64 1/1
Verifying : charon-manager-ssp-3.1.8-1.x86_64 1/1

Installed:
charon-manager-ssp.x86_64 0:3.1.8-1

Complete!
```

Accessing the Charon-SSP Cloud Instance

There are several ways to access your Charon-SSP cloud instance. Some of them are described below:

Contents

SSH Command-Line Access

Contents

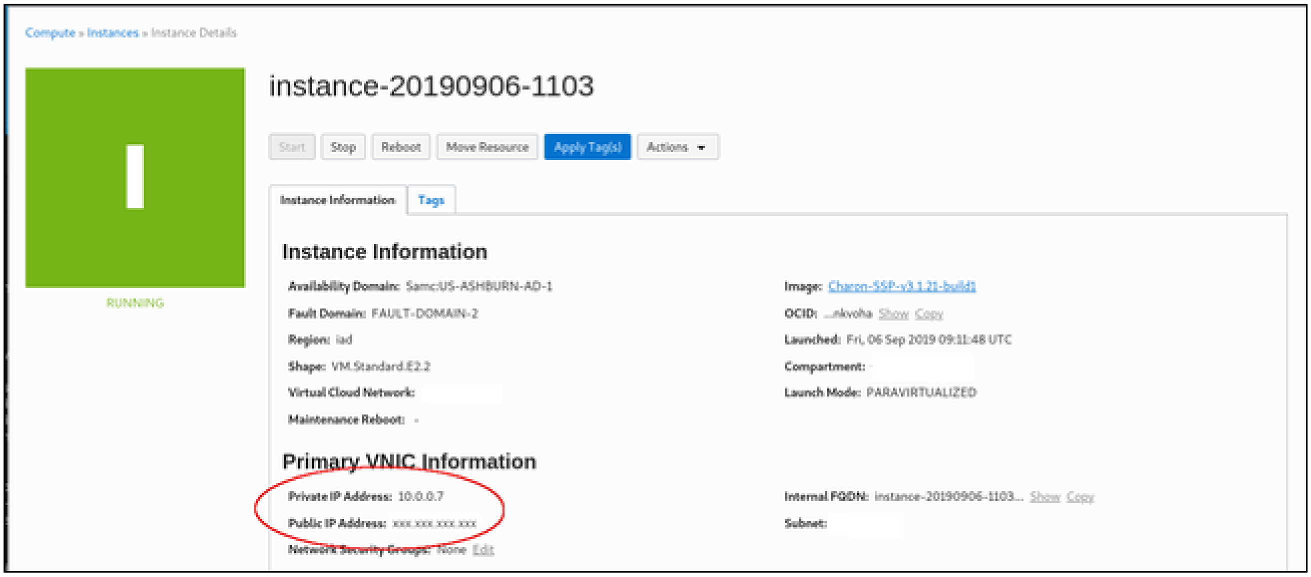
General Information

Access to your instance is controlled through several different methods:

- Firewall of the instance
- Security list of the subnet to which the instance belongs
- VNIC-specific Network Security Groups

Note that if both, a security list and a Network Security Group are assigned to a VNIC, the rules of both are combined. Please refer to the Oracle documentation for details.

With the default subnet security list, and without custom Network Security Groups installed, SSH from the command-line or from a tool such as PuTTY can be used to access the command-line of the **sshuser** user on the Charon-SSP instance. If you select your instance in the instance list and then click on the name, you will see details about your instance including its public IP address as shown below.



instance-20190906-1103

Instance Information

Availability Domain: Samc:US-ASHBURN-AD-1

Fault Domain: FAULT-DOMAIN-2

Region: iad

Shape: VM.Standard.E2.2

Virtual Cloud Network:

Maintenance Reboot: -

Image: Charon-SSP-v3.1.21-build1

OCID: ...nkvoha

Launched: Fri, 06 Sep 2019 09:11:48 UTC

Compartment:

Launch Mode: PARAVIRTUALIZED

Primary VNIC Information

Private IP Address: 10.0.0.7

Public IP Address: xxx.xxx.xxx.xxx

Network Security Groups: None

Internal FQDN: instance-20190906-1103...

Subnet:

To connect to the instance, you need the private key corresponding to the public key uploaded during the launch of the instance.

The file permissions of the private key file must be set such that the file is only readable by the user.

General Login Steps

To connect to the instance interactively, you must connect as the user **sshuser**. Use the following command:

```
$ ssh -o ServerAliveInterval=30 -i <path-to-your-private-key> sshuser@<OCI-public-IP-address>
```

The parameter `ServerAliveInterval` will protect the connection from timing out.

Below, you see sample output of a login:

```
$ ssh -o ServerAliveInterval=30 -i .ssh/mykey.pem sshuser@<public-ip-address>
Last login: Tue May 21 05:34:33 2019 from myhost.example.com
[sshuser@ip-172-31-38-252 ~]$ pwd
/home/sshuser
```

⚠ Note that this account allows root access to a limited subset of commands (use **`sudo -i`**). In particular, commands that are required to create more complex network configurations are allowed.

Setting the Management Password

⚠ **Initial management password configuration:** before connecting to the Charon-SSW host with the Charon Manager for the first time after the initial installation of your instance you must set the management password. This can either be done via the Charon Manager itself (see Connecting with the Charon-SSP Manager) or via the command line as shown below.

Steps to set the management password:

- Log in to the Charon host using SSH as show above.
- Become the root user (**`sudo -i`**).
- Change to the Charon Agent utilities directory (**`cd /opt/charon-agent/ssp-agent/utils`**).
- Run the charon-password script (**`./charon-passwd`**).
- Enter and confirm the new management password when prompted.

After this has been completed, you can connect to the host using the Charon Manager with the new management password.

Below, you see sample output of the steps:

```
$ ssh -i .ssh/mykey.pem  sshuser@<public-ip-address>
[root@ip-172-31-35-32 ~]# cd /opt/charon-agent/ssp-agent/utils
[root@ip-172-31-35-32 utils]# ./charon-passwd
Enter new Charon password:
Retype new Charon password:
Password updated successfully.
Changing password for user charon.
passwd: all authentication tokens updated successfully.
Changing password for user sshuser.
passwd: all authentication tokens updated successfully.
sh: /home/charon/.vnc/passwd: No such file or directory
[root@ip-172-31-35-32 utils]#
```

SFTP File Transfer

SFTP enables file transfers to and from the Charon-SSP instance. The user for file transfers is the **charon** user. Firewalls and security lists must allow SSH access to allow SFTP access to the Charon-SSP instance.

To connect to the instance as the user **charon**, use the following command:

```
$ sftp -i <path-to-your-private-key> charon@<OCI-public-IP-address>
```

Below you see sample output of a connection:

```
$ sftp -i .ssh/mykey.pem charon@<public-ip-address>
Connected to storage@3.81.64.139.
sftp> ls
media             ssp-snapshot
```

Connecting with the Charon Manager

Contents

General Information

To manage Charon-SSP and the emulated SPARC systems, you must connect to the Charon-SSP instance with the Charon-SSP Manager. The Charon-SSP Manager is the main interface to all important functions of the Charon-SSP software.

Prerequisites:

- The **Charon-SSP Manager** must be installed on your local system.
- **For access via the public IP address of the Charon host instance**:
  - The combination of **firewall, security lists, and network security groups** on your system must at least allow SSH access. This allows the **built-in SSH tunneling** of the Charon-SSP Manger to work. Should you not use SSH tunneling, you must open up any additionally required ports. However, if the connection runs over the Internet without a VPN, Stromasys strongly recommends to use SSH tunneling to protect your Charon-SSP cloud instance and any emulated systems running on it.
  - You must have the public IP address of the Charon-SSP cloud instance. To determine this address refer to the instance information displayed on the Oracle Cloud compute instance details.
  - To use the Charon Manager integrated SSH tunnel, you need the private SSH key of the key-pair associated with your instance.
- **For access via an SSH-based VPN**:
  - Active SSH-based VPN (see Appendix: SSH VPN - Connecting Charon Host and Guest to Customer Network)
  - Private IP address of the Charon-SSP host in the VPN

⚠ **Initial management password configuration**: before connecting to the Charon-SSW cloud host with the Charon Manager for the first time after the initial installation you must change the default management password. This can either be done via the command line (see SSH Command-Line Access) or via the Charon Manager as described below.

Starting the Charon Manager and Login to Charon Host

Starting the Charon Manager

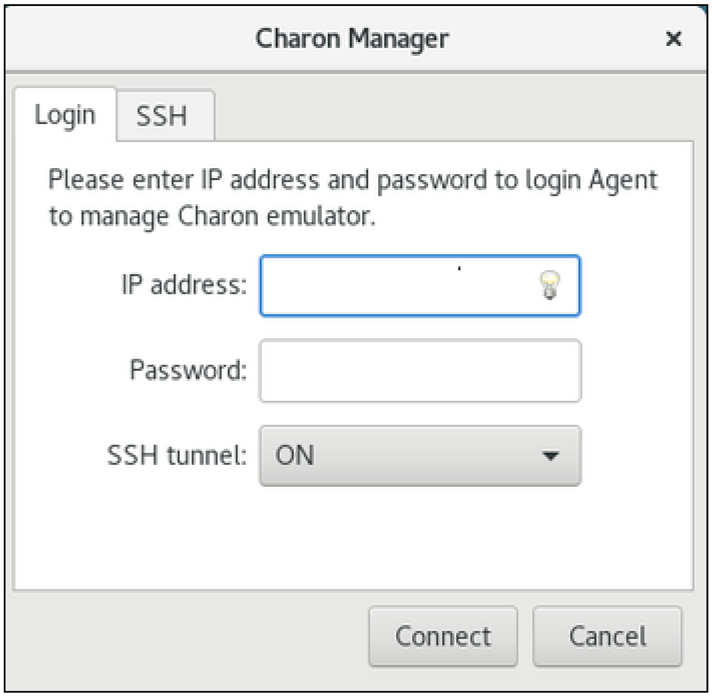
To start the Charon-SSP Manager and to open the Charon Manager login window, log in on your Linux management system and use the following command:

```
$ /opt/charon-manager/ssp-manager/ssp-manager
```

The steps above will open the Charon Manager login window which has **two tabs**.

Entering Charon Manager Login Information and Connecting to Charon Host

Step 1: the Charon Manager **Login** tab



Please enter IP address and password to login Agent to manage Charon emulator.

IP address:

Password:

SSH tunnel: ON

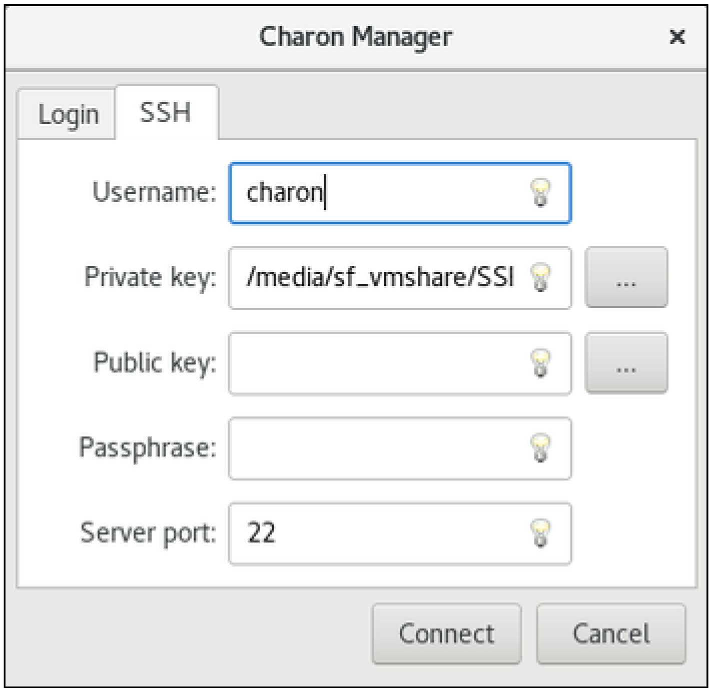
If the management password has not yet been set, perform the following steps:

- Enter the **public** IP address of your Charon-SSP host instance.
- Enter the default management password (**stromasys**).
- Enable the SSH tunnel configuration (select **ON**).
- Change to the SSH tab to fill in the required information there.

If the management password has already been set, perform the following steps:

- Enter the public IP address or the private VPN IP address of your Charon-SSP instance.
- Enter the Charon-SSP management password.
- Enable the SSH tunnel configuration for communication across a public network unless you use a secure VPN connection.
- If the SSH tunnel is enabled, change to the SSH tab to fill in the required information there.

Step 2: the Charon Manager **SSH** tab



Username: charon

Private key: /media/sf_vmshare/SSI

Public key:

Passphrase:

Server port: 22

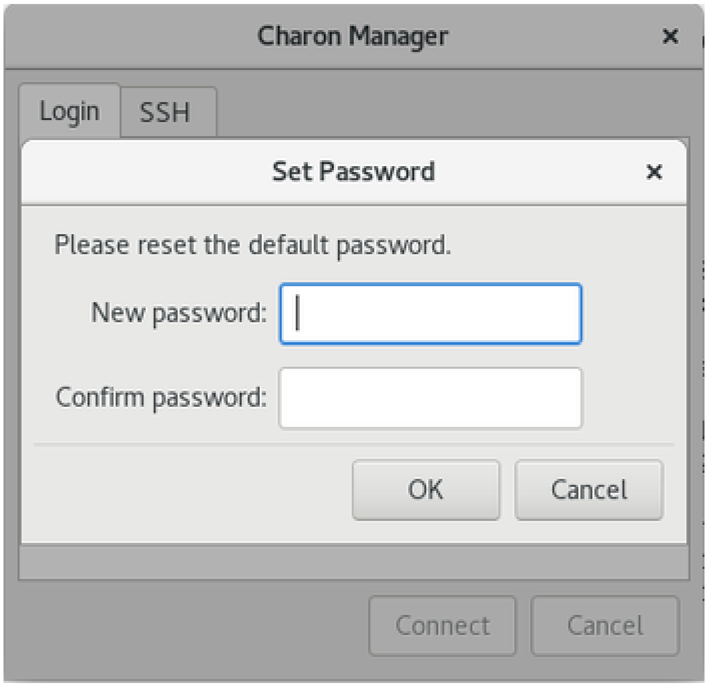
If you use the integrated SSH tunnel, perform the following steps:

- Enter the Charon-SSP user (**charon** or **sshuser**).
- Enter the path to the private key file (click on the three dots to open a file browser),
- In rare cases, you may need to add the path to the public key on the local system.
- Enter the passphrase for the private key if required.
- Adjust the server port (default 22) if required.

Step 3: connecting to the Charon host system

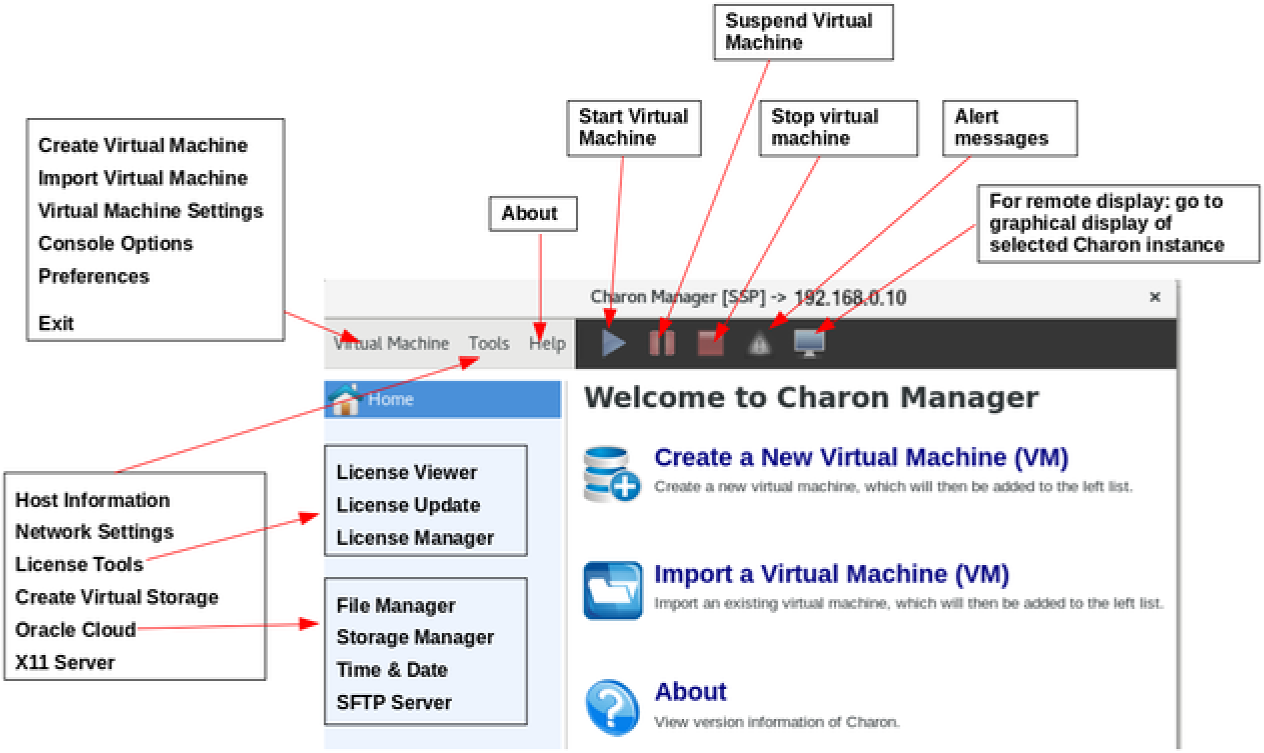
After entering all the required information, click on **Connect** to connect to the Charon-SSP cloud instance.

If the management password still needs to be set, you will receive a prompt to enter the new password:

 Please reset the default password. New password: Confirm password: Charon Manager Login SSH Set Password OK Cancel Connect Cancel	- Enter the desired password and confirm it. - Then click on **Save**. - The login process continues.

After a connection has been successfully created, the Charon Manager welcome screen opens.

The image below shows a sample of the Charon Manager welcome page with an overview of the different menus:



Welcome to Charon Manager

Create a New Virtual Machine (VM)

Create a new virtual machine, which will then be added to the left list.

Import a Virtual Machine (VM)

Import an existing virtual machine, which will then be added to the left list.

About

View version information of Charon.

Next Steps with Charon-SSP/4M for OCI

Now that you have launched your cloud instance and learned how to access it, you can continue with the next steps.

⚠ This chapter only provides a brief outline of how to continue. For more information, please refer to the Oracle Cloud documentation and the general CHARON-SSP documentation provided by Stromasys.

Contents

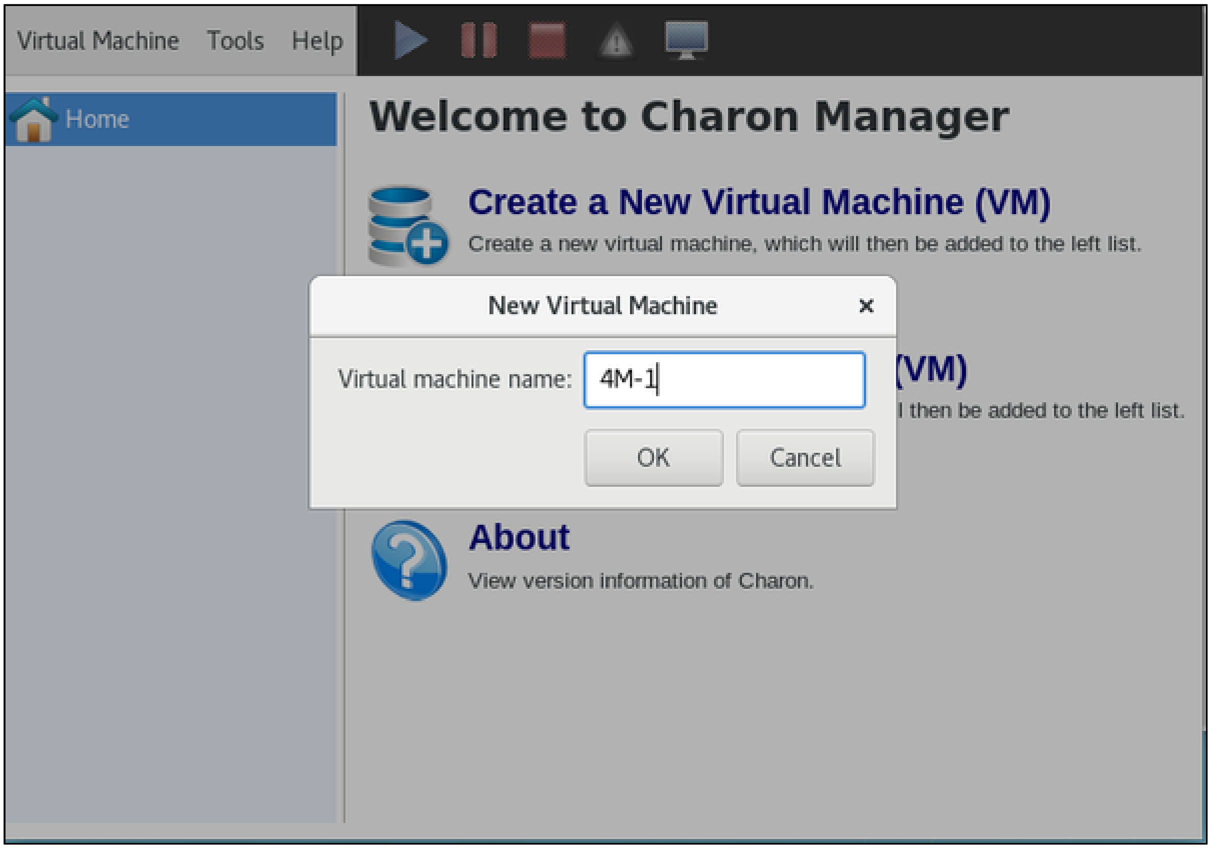
Obtaining a Charon-SSP License

Charon-SSP/4M for OCI contains the license drivers and license management tools. However, you need to obtain an appropriate product license from either your Stromasys representative or your Stromasys VAR. They will help you to select the appropriate license option and provide you with a license.

The Charon Manager provides tools to install, view, and update licenses in **Tools > License Tools**. The license management chapter in the general Charon-SSP user's guide provides details.

Creating an Emulated SPARC System

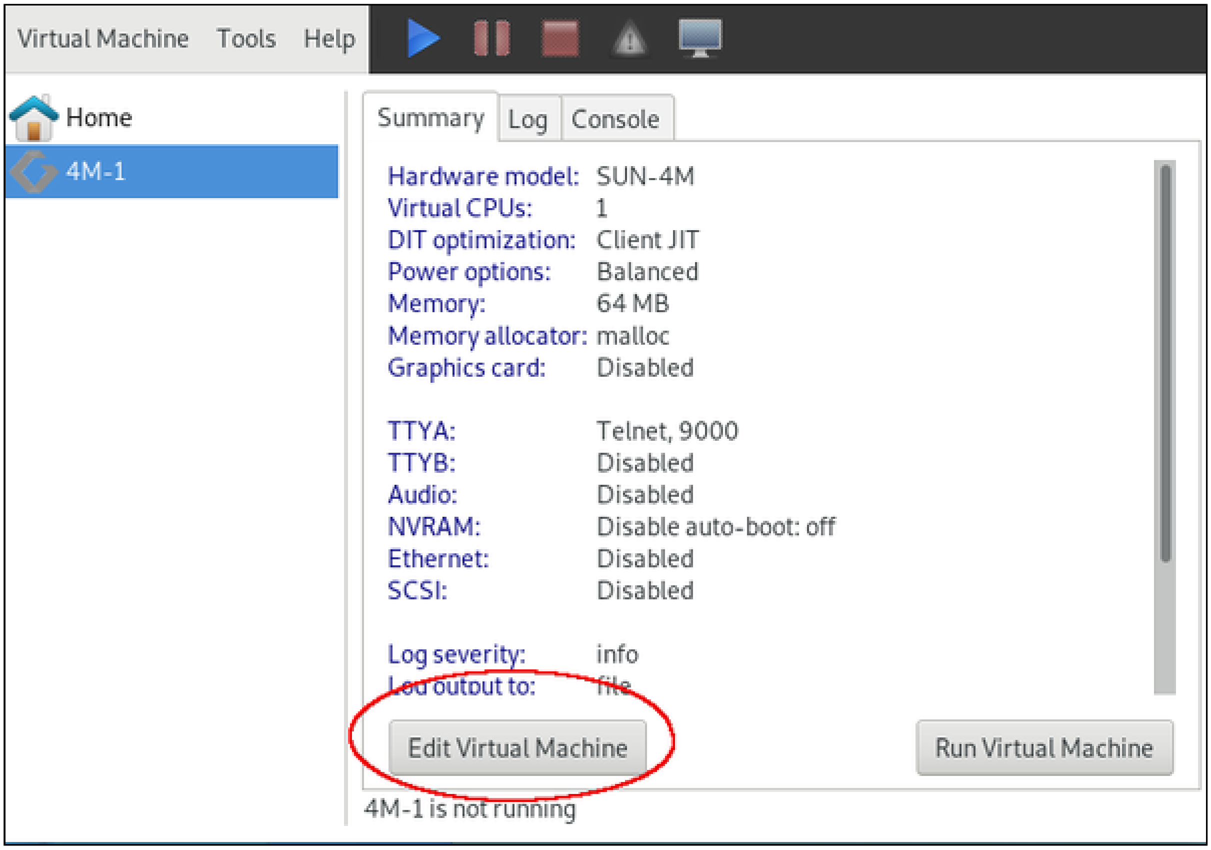
To create your emulated SPARC system, open the Charon Manager and click on **Create a New Virtual Machine (VM)** on the welcome screen. This will allow you to enter a name for your emulated SPARC system and confirm the creation of the virtual machine as shown below:


Virtual Machine
Tools
Help
Home
Welcome to Charon Manager
Create a New Virtual Machine (VM)
Create a new virtual machine, which will then be added to the left list.
New Virtual Machine
Virtual machine name: 4M-1
OK
Cancel
(VM)
l then be added to the left list.
About
View version information of Charon.

Configuring the Emulated System

The newly created system has only a template configuration. Therefore, you have to configure the virtual hardware as required before using the emulated system.

Select your virtual SPARC in the manager and click on **Edit Virtual Machine** on the **Summary** tab as illustrated below.



```
Hardware model:    SUN-4M
Virtual CPUs:      1
DIT optimization:  Client JIT
Power options:     Balanced
Memory:            64 MB
Memory allocator:  malloc
Graphics card:     Disabled

TTYA:              Telnet, 9000
TTYB:              Disabled
Audio:             Disabled
NVRAM:             Disable auto-boot: off
Ethernet:          Disabled
SCSI:              Disabled

Log severity:      info
Log output to:     file
```

4M-1 is not running

This will open the configuration window. Please refer to the general Charon-SSP user's guide for configuration details and how to start and stop the emulated system.

Copying Installation Media and Data Backups for Migration to the Instance

There are different methods to copy files to the Charon cloud instance. One way is to use SFTP as described in SFTP File Transfer.

Creating a VPN Connection between Your Internal Network and the Cloud Instance

There are different VPN options. The customer is responsible for ensuring that any VPN solution meets the requirements of his or her company's security guidelines. The example shown in the Charon documentation is only for illustrative purposes.

Charon Manager provides support for setting up a simple SSH based VPN tunnel between the Charon host in the cloud and a remote Linux system in the customer network. This connection can be used, for example, to transfer files, to access applications on the guest system running in the emulated SPARC, or for accessing a network-enabled license located in the customer network.

The appendix provides an introduction to this configuration.

Appendix: SSH VPN - Connecting Charon Host and Guest to Customer Network

Contents

Overview

If the connection between the Charon-SSP host system, including the configured Charon-SSP guest systems, and the rest of the customer's network runs over a public network as is the case for Charon-SSP cloud instances, it is necessary to secure the traffic against unauthorized access.
The example in this section describes how to configure a bridged SSH-based VPN tunnel between the Charon-SSP cloud host and a remote Linux system across a public network. Topologies that are more complicated will require other, more sophisticated, solutions.

⚠ The customer is responsible for ensuring that any VPN solution meets the requirements of his or her company's security guidelines. The example in this chapter is only for illustrative purposes.

ℹ The advantage of a bridged connection is that L2 protocols are also supported.

Once the sample configuration has been set up, it can be used for

- communication between host and guest system,
- communication between customer network and guest system.

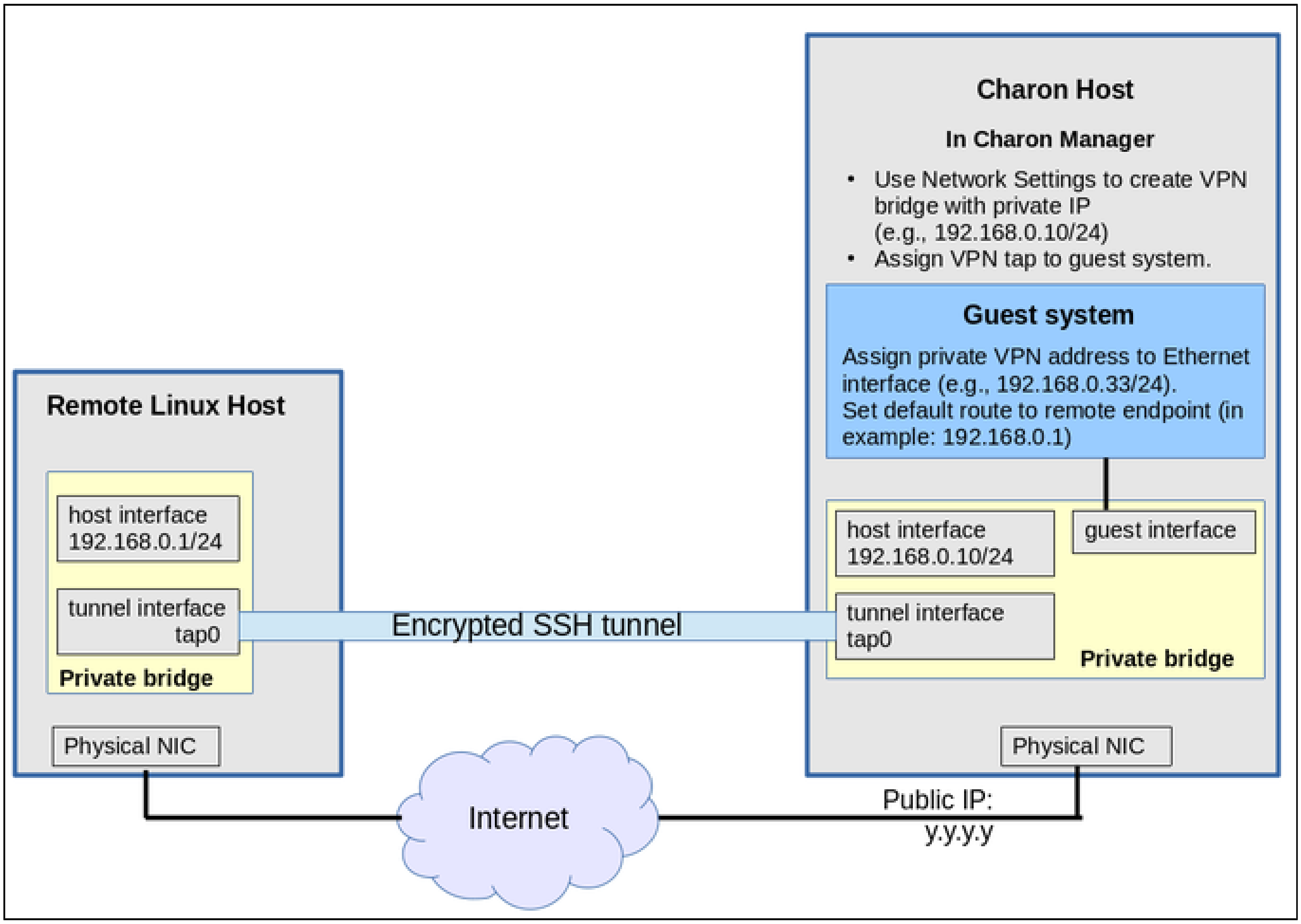
Prerequisites

The example shows how to use the Charon Manager on the Charon-SSP host and a set of commands on the remote Linux System to create an SSH VPN tunnel. For this configuration to work, the following prerequisites must be met:

- The remote Linux system must have access to the public IP address and the SSH port of the Charon-SSH host.
- The private key necessary to access the instance must be available on the remote Linux system.
- The *bridge-utils* and *autossh* packages must be installed on the remote Linux system.

Setting up the VPN Tunnel

The image below shows a sample setup. This section describes how to configure this sample setup.


Charon Host
In Charon Manager
• Use Network Settings to create VPN bridge with private IP (e.g., 192.168.0.10/24)
• Assign VPN tap to guest system.
Guest system
Assign private VPN address to Ethernet interface (e.g., 192.168.0.33/24).
Set default route to remote endpoint (in example: 192.168.0.1)
host interface 192.168.0.10/24
guest interface
tunnel interface tap0
Private bridge
Physical NIC
Remote Linux Host
host interface 192.168.0.1/24
tunnel interface tap0
Private bridge
Physical NIC
Encrypted SSH tunnel
Internet
Public IP: y.y.y.y

Steps on the Charon-SSP Host System

Creating a VPN Bridge

To configure the SSH VPN connection, you must setup a private VPN bridge (called a virtual network in the Charon context) using the Charon Manager. Use the following steps to perform this task:

1. Open the Charon-SSP Manager and log in to the Charon-SSP host.

2. In the Charon Manager, open the Network Settings window by clicking on **Tools > Network Settings**. This will open the **Network Settings** window.

3. Click on **Add** and then on **Virtual Network** to open the virtual network configuration window. This will open the **Add Virtual Network** configuration window as shown below.

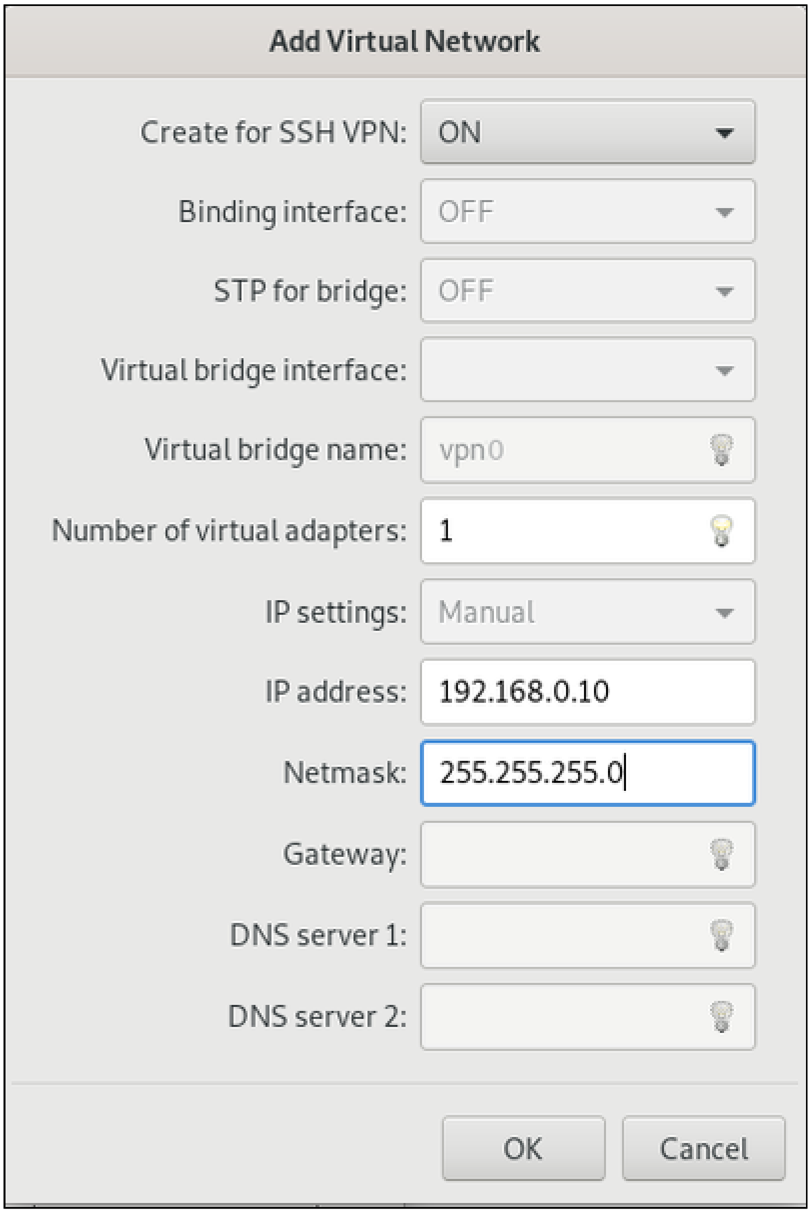
4. Enter the required information as shown below:

Perform the following steps to configure a VPN bridge,

- Set **Create for SSH VPN** to **ON.**
- Enter the **Number of virtual adapters** (TAP interfaces) required. These interfaces will be assigned to the emulated SPARC systems as Ethernet interfaces.
- Configure the **IP address** for the bridge interface.
- Set the **Netmask**.

⚠ This interface and the interface on the remote Linux system must be in the **same IP subnet.**

Click on **OK** to save your configuration.



Add Virtual Network

Create for SSH VPN: ON

Binding interface: OFF

STP for bridge: OFF

Virtual bridge interface:

Virtual bridge name: vpn0

Number of virtual adapters: 1

IP settings: Manual

IP address: 192.168.0.10

Netmask: 255.255.255.0

Gateway:

DNS server 1:

DNS server 2:

To learn more about the virtual network configuration options, refer to section Host System Network Configuration.

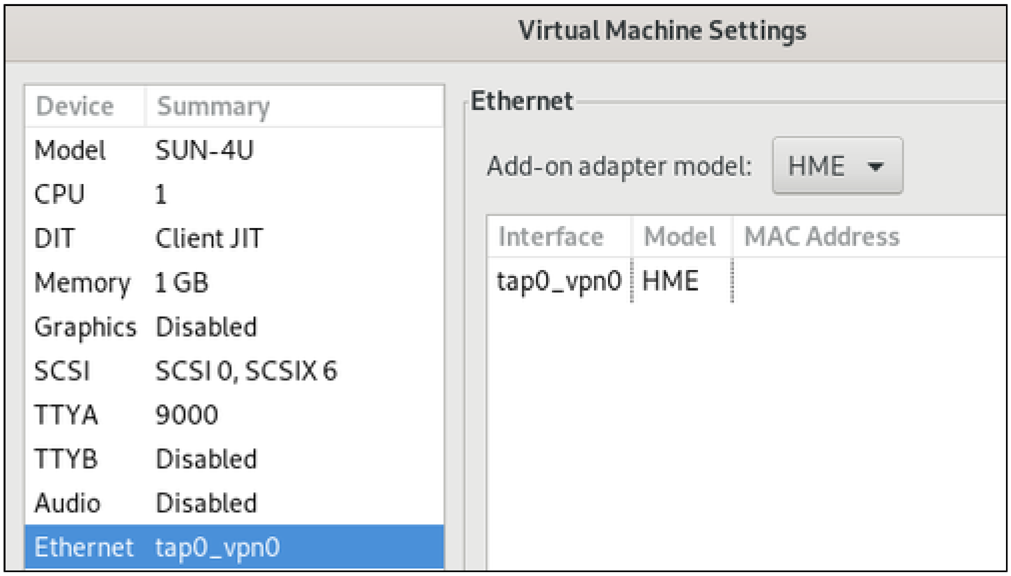
Assigning the Guest Ethernet Interface

One of the TAP interfaces created in the step above, must be assigned to the Solaris guest system to add it to the LAN that will be tunneled across SSH to the remote Linux system.

Perform the following steps:

1. Open the Charon-SSP Manager and log in to the Charon-SSP host.

2. In the Charon Manager, select the guest system and then the **Ethernet** configuration category on the left. Assign one of the created TAP interfaces to the guest (see example below).



Virtual Machine Settings

Device	Summary
Model	SUN-4U
CPU	1
DIT	Client JIT
Memory	1 GB
Graphics	Disabled
SCSI	SCSI 0, SCSIX 6
TTYA	9000
TTYB	Disabled
Audio	Disabled
Ethernet	tap0_vpn0

Ethernet

Add-on adapter model: HME

Interface	Model	MAC Address
tap0_vpn0	HME	

Click on **OK** to save the configuration change.

ℹ If the emulated instance is currently running, the guest must be shut down and the emulated instance must be restarted for the change to become active.

Steps on the Remote Linux System

⚠ The steps on the Charon-SSP host must be performed first.

As the user **root** on the remote Linux system, perform the following steps to set up the VPN tunnel according to the overview image above:

Action	Command
Create TAP interface	**# ip tuntap add dev *tap0* mod tap**
Enable TAP interface	**# ip link set *tap0* up**
Create bridge	**# ip link add name *br_vpn0* type bridge**
Enable bridge interface	**# ip link set *br_vpn0* up**
Define IP address for bridge	**# ip addr add *192.168.0.1/24* dev *br_vpn0***
Add TAP interface to bridge	**# ip link set *tap0* master *br_vpn0***
Start the SSH tunnel **autossh** is a program to start a copy of **ssh** and monitor it, restarting it as necessary should it die or stop passing traffic. Once started, you can move the program to the background.	**# autossh -M 9876 -o ServerAliveInterval=60 -o Tunnel=ethernet ** **-w 0:0 -t -i** *<path-to-private-key>* **-NCT sshuser@***<public-cloud-instance-IP>* **-M** defines the monitoring port autossh uses to monitor the connection **-o** sets SSH options (bridged tunnel and keepalive) **-i** denotes the path to the private key matching the public key copied to the host system. **-w** denotes the number of the local and remote tunnel interfaces for tunnel device forwarding (e.g., the 0 in interface tap0). **-N** denotes that no remote command should be executed **-T** disables pseudo-terminal allocation **-C** requests data compression

Possible additional steps:

- Enable IP forwarding on the remote Linux system if it is to act as a router between the tunnel connection and other systems in the customer network:
  ```
  # /sbin/sysctl -w net.ipv4.ip_forward=1
  ```
  (to make permanent: add the setting to /etc/sysctl.conf)
- Add static or dynamic routes to distribute the tunnel subnet to other systems in the customer network that need to communicate with the Solaris guest system across the VPN..
- Adapt the firewall on the remote Linux system as required to allow the VPN traffic to pass.

Steps on the Solaris Guest System

Set the IP address on the Ethernet interface to an address within the VPN subnet. To follow the example above, you would set the address to 192.168.0.33/24. To permanently change the IP address on the Solaris system, change the address in **/etc/hosts** for the hostname specified in **/etc/**<*interfacename*>**.hostname**.
On Solaris 11, use the commands **`ipadm create-ip net`***`X`* and **`ipadm create-addr -T static -a`** *`<ip-address>`***`/`***`<netmask>`* **`net`***`X`***`/v4`**.

Stopping the SSH Tunnel

To stop the SSH tunnel, perform the following steps on the remote Linux system:

Action	Command
Terminate the autossh process	**`# kill -9`** *`<autossh-pid>`*
Terminate remaining SSH tunnel connections	**`# kill -9`** *`<tunnel-ssh-pid>`*
Delete the bridge	**`# ip link delete`** ***`br_vpn0`***
Delete the TAP interface	**`# ip link delete`** ***`tap0`***

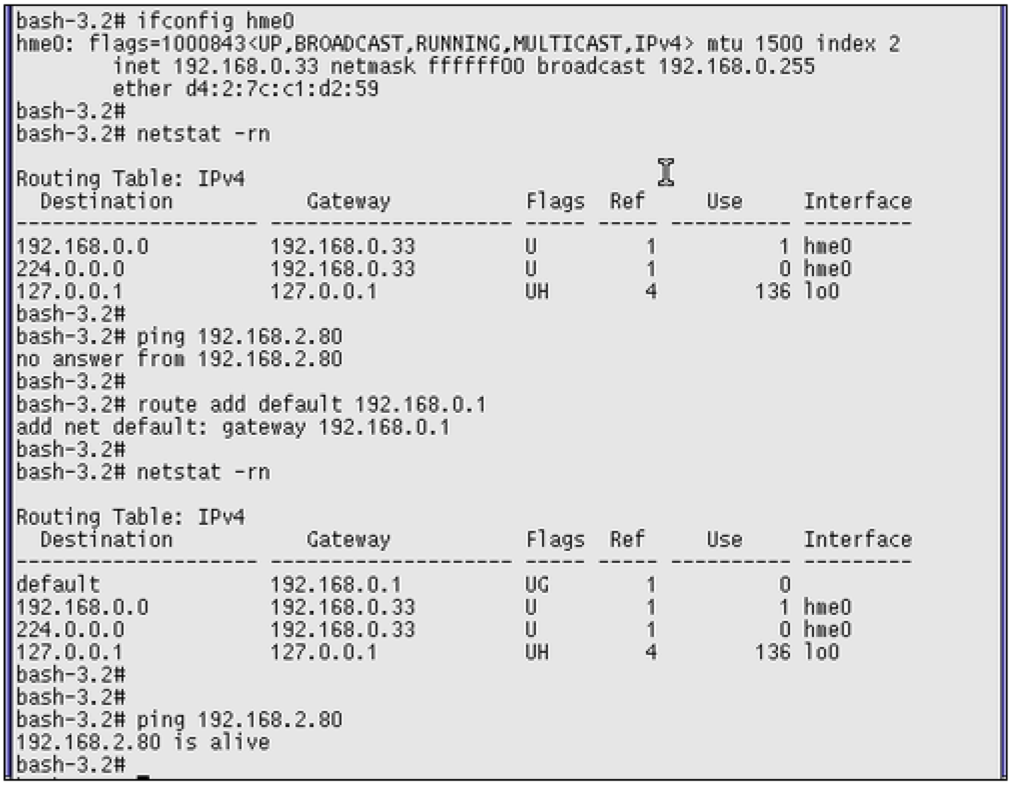
Routing to/from Solaris Guest

After following the description above, the Solaris guest system can be reached from the systems that are also connected to the virtual bridge (in the example: remote Linux system and host system). To enable the Solaris guest system to **communicate with other systems** in the customer network (or the Internet) over the VPN connection, perform the following steps:

- Add the VPN address of the remote Linux system as the default gateway for the Solaris guest system.
- Propagate the IP network used for the SSH VPN within the customer network, as required.
- Enable IP forwarding on the remote Linux system and allow forwarded packages through the firewall.

The screenshot below illustrates the Solaris guest system behavior (after the VPN network has been made known within the customer LAN and the remote Linux host has been set up as a router):

- The interface address shows that the Solaris system is in the 192.168.0.0/24 network using the **ifconfig** command.
- The **`netstat -rn`** command shows the routing table without a default route.
- The ping to an IP address outside the SSH VPN fails.
- The **`route add default <gateway>`** command adds the remote Linux host as the default gateway.
- The **`netstat -rn`** command now shows the default route.
- The ping to an IP address outside the SSH VPN succeeds.



```
bash-3.2# ifconfig hme0
hme0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 192.168.0.33 netmask ffffff00 broadcast 192.168.0.255
        ether d4:2:7c:c1:d2:59
bash-3.2#
bash-3.2# netstat -rn

Routing Table: IPv4
  Destination           Gateway           Flags  Ref     Use     Interface
-------------------- -------------------- ----- ----- ---------- ---------
192.168.0.0          192.168.0.33         U         1          1 hme0
224.0.0.0            192.168.0.33         U         1          0 hme0
127.0.0.1            127.0.0.1            UH        4        136 lo0
bash-3.2#
bash-3.2# ping 192.168.2.80
no answer from 192.168.2.80
bash-3.2#
bash-3.2# route add default 192.168.0.1
add net default: gateway 192.168.0.1
bash-3.2#
bash-3.2# netstat -rn

Routing Table: IPv4
  Destination           Gateway           Flags  Ref     Use     Interface
-------------------- -------------------- ----- ----- ---------- ---------
default              192.168.0.1          UG        1          0
192.168.0.0          192.168.0.33         U         1          1 hme0
224.0.0.0            192.168.0.33         U         1          0 hme0
127.0.0.1            127.0.0.1            UH        4        136 lo0
bash-3.2#
bash-3.2#
bash-3.2# ping 192.168.2.80
192.168.2.80 is alive
bash-3.2# _
```

To make the entry permanent

- on Solaris 10: use the **`route -p`** command (stores routes in */etc/inet/static_routes*).
- on older Solaris versions: add the address of the default gateway to */etc/defaultrouter*.