Charon-SSP
Virtual Environment (VE)
License Server 1.0
User's Guide

Current product version: 1.0.36

Contents

About this Guide

Contents

Intended Audience

This guide is intended for anyone who needs to install, configure, or manage the Stromasys Charon-SSP Virtual Environment (VE) license server. A general working knowledge of Linux and its conventions is expected.

VE stands for "Virtual Environment". At the time of writing, this term refers to supported cloud environments only. For Charon-SSP products using such licenses, customers must purchase their license from Stromasys. This is different from the cloud-specific Charon-SSP Automatic Licensing (AL) images where licensing is configured automatically when the cloud instance is launched.

This guide covers the **Charon-SSP VE License Server** software**.** This package contains a license server application that can be installed in customer-specific AWS, OCI, GCP and Azure environments (the list of supported platforms may be extended in the future). This licensing option is adapted to the special requirements of a cloud environment and simplifies the process of running Charon-SSP in customer-specific cloud environments. The license server is managed by the customer.

VE licenses provided by a VE license server require a specific variant of the Charon-SSP software (available starting with Charon-SSP version 4.2.x). The examples in this guide were partially created with a pre-release of version 4.2. **For a full description of Charon-SSP version 4.2 aspects that are not related to the specifics of the VE license application, please refer to your Charon-SSP user's guide.**

For additional information about this product, please contact Stromasys at the **regional addresses** below or contact your **Stromasys VAR**.

Structure of this Document

The document contains the following sections:

- Charon-SSP Cloud-based VE License Server Overview: brief overview of license server topologies.
- Installing the VE License Server and the Charon-SSP Packages: installation of the license server software in cloud environments, and installation of the VE-enabled Charon-SSP emulator software.
- Installing a License on the VE License Server: steps for requesting and installing a Charon-SSP product license on the license server.
- Configuring Charon-SSP to Use a VE License Server: steps for configuring Charon-SSP to use the VE license server.
- Operational Information and Logging: information that may be helpful when operating a VE license server. For example, log file locations and samples.
- Updating a VE License: steps for updating a license, for example, when the expiration date approaches.
- Additional Information: supplemental information about installing a Linux cloud instance, about installing and starting the Charon Manager on a Linux or Windows management system, and about cloud-specific firewall considerations.

Please note:

- Cloud providers may change their management GUI without prior warning. Hence, the screenshots in this document may not always reflect the latest GUI appearance of the cloud provider. However, they will still provide an illustration of the described configuration steps.
- In general, the sample outputs in this document may show different versions than the one documented in this manual, but they are still representative of what a user will see.

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 or General Product Information

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.

Obtaining General Product Information

If you require information in addition to what is available on the Stromasys Product Documentation and Knowledge Base and on the Stromasys web site you can contact the Stromasys team using https://www.stromasys.com/contact/, or by sending an email to info@stromasys.com.

For further information on purchases and the product best suited to your requirements, you can also contact your regional sales team by phone:

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

Conventions

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.

Definitions

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 User's Guides and Release Notes

Charon Licensing Overview

The Charon-SSP VE License server provides a new type of licensing for the Charon-SSP product. This is in addition to the already existing licensing models. This section briefly describes the different licensing concepts and products.

Contents

Charon-SSP VE Licenses

The main characteristics of VE (Virtual Environment) licenses are the following:

- Software licenses only.
- Developed by Stromasys.
- Installed on Charon-SSP host or separate license server.
- Require the Charon-SSP VE license server software.
- Require matching Charon-SSP emulator software.
- Currently, the VE license server is only available for cloud environments (at the time of writing: AWS, OCI, Azure, and GCP).
- Currently only available for Charon-SSP products.

This document describes the use of this type of licenses.

Sentinel (Gemalto) HASP Licenses

Sentinel HASP licenses are the "traditional" licensing method for Charon emulator products. Their main characteristics are:

- Software and hardware (dongle) licenses.
- Based on third-party vendor solution.
- Require special third-party license driver software.
- Installed on Charon-SSP host or separate license server.
- Problematic in cloud environments.
- Dongles are flexible and host-hardware independent for on-premises installations (as long as there is a free USB port).

Please refer to the Charon License Handbook (Handbooks) for details about these licenses.

Charon-SSP Automatic Licensing for Cloud Environments

When installing a Charon-SSP Automatic Licensing (AL) image from a supported cloud marketplace (at the time of writing AWS and OCI US), the cloud instance automatically receives a license at first launch. The license server must be reachable via a cloud-specific public IP address. The license server is operated by Stromasys.

Reason for VE Licenses

Other license types have drawbacks that prompted the development of VE licenses:

- USB dongles are by nature not suitable for cloud environments and their use in VMware environments is somewhat complex.
- Sentinel software licenses are easy to install in a cloud or VMware environment. However, their ties to hardware characteristics also make it easy to inadvertently invalidate them in such environments. Hence they are also not suited for use in cloud environments. Other Sentinel software license types do not provide the same level of license security.
- Cloud-based automatic licensing does not allow a customer-specific environment in the cloud without Internet access. This is not suitable for many customers who require a private cloud network environment.

VE licenses are designed to enable the ease-of-use of software licenses while providing a high level of security for licensing Charon-SSP products in virtualized environments. At the time of writing, VE licenses are specific to cloud environments (currently, the VE license server is not supported in an on-premises installation).

Charon-SSP Cloud-based VE License Server Overview

The following image provides an overview of a sample VE license server topology in a cloud environment:

Cloud-based VE License Server Topology Overview
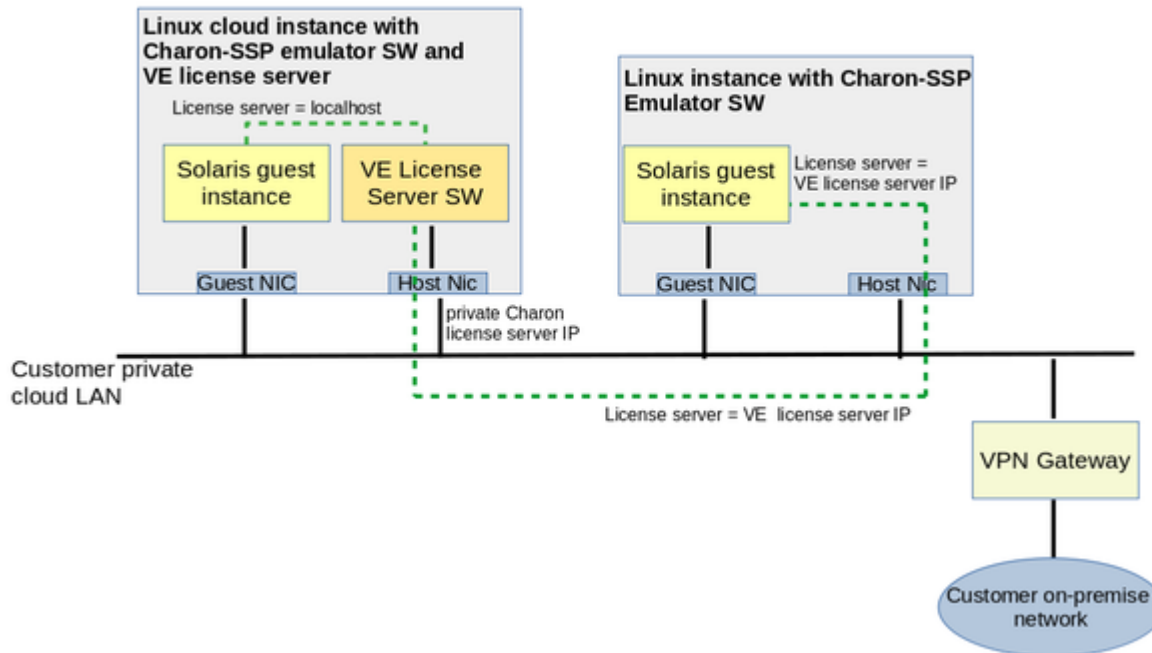
Points to note:

- The license server software can be combined with the matching Charon-SSP emulator software on one instance, or it can run on a separate system.
- The license server must be installed in a supported cloud environment.
- Charon host and license server do not need a public IP address. They communicate across the cloud-internal LAN environment.
- Starting with version 4.1.19, a backup license server is supported.

The decision whether the license server should run on a separate instance depends on the customer's requirements.

Installing the VE License Server and the Charon-SSP Packages

Contents

Prerequisites

The Charon-SSP VE License Server has a number of prerequisites:

- The VE license server package
- A suitable Linux cloud instance in a supported cloud environment to be used as the VE license server
- Correct firewall settings
- The VE-capable Charon-SSP emulator software running on a Charon host with appropriate network access to the VE license server

These items are described below.

VE License Server Package

The Charon-SSP VE License Server package is delivered as an RPM package. Stromasys or your Stromasys VAR will provide you with the software or a download link.

Package name:

```
license-server-<version>.rpm
```

Where *<version>* indicates the version of the software, for example, 1.0.35.

Linux Cloud Instance for License Server

The license server package must be installed on a Linux cloud instance.

Currently supported cloud providers:

- Amazon AWS
- Oracle Cloud Infrastructure (OCI)
- Microsoft Azure
- Google Cloud Platform (GCP)

Please refer to your cloud provider's documentation for configuring and launching an appropriate instance. A description of the basic steps of launching an instance can be found in Additional Information.

Depending on the cloud environment, Stromasys may offer a prepackaged Charon-SSP VE image on the cloud marketplace. This image includes the Charon-SSP emulator software (already installed) and the VE License Server RPM package (can be installed optionally). An instance launched from such a prepackaged image can also be used as a VE license server.

Software requirements for License Server:

Red Hat, CentOS, or Oracle Linux (64-bit) versions 7.x or 8.x

Basic hardware requirements (the shape or instance type capabilities) for running only the license server:

Must be sufficient for the selected Linux operating system.

Additional hardware requirements (the shape or instance type capabilities) for running the emulator software on the same system:

- **If the license server is combined with the Charon-SSP emulator software on the same instance,** the instance used must satisfy the requirements of the Charon-SSP host and all instances that will run on it. If this requirement exists, please refer to your *Charon-SSP user's guide* for details.

Additional general requirements:

- In the AWS cloud, an IAM role allowing the ***ListUsers*** action (IAMReadOnlyAccess in the example below) must be attached to the instance. This can be done during the launch of the instance as shown in the sample below.

Alternatively, the role can be set/changed by selecting the instance, right-clicking on it, and selecting **Security > Modify IAM Role** (in the older AWS console, use the **Action** menu). If such a role has not yet been defined, please refer to Creating and Attaching an AWS IAM Role and to the documentation provided by AWS for additional information.

Firewall Settings

Communication Between License Server and Client System

Any intermediate firewall as well as the cloud-specific subnet and instance security settings must permit the following ports for the appropriate source systems:

- **TCP/8083**: must be permitted on the license server for the client system to enable the use of the license by the client.
- **TCP/8084**: must be permitted by the license server for any system that should access the web interface to display information about licenses and active clients (currently not encrypted, hence should not be run across the Internet without a VPN).

See Cloud-Specific Firewall Information for information about the traffic filtering mechanisms used in the different cloud environments.

Simplified sample commands if firewalld is used on the Linux system:

```
# firewall-cmd --permanent --zone=public --add-port=8084/tcp

# firewall-cmd --permanent --zone=public --add-port=8083/tcp

# firewall-cmd --reload
```

- The default zone name can be found with the command `firewall-cmd --get-default-zone`, a list of all zones can be displayed with the command `firewall-cmd --get-zones`.
- The parameter --*permanent* writes the command to the respective firewalld configuration files. To add the command to the running firewall, re-run it without the parameter --*permanent*.
- The simplified sample above does not limit the source IP address to the addresses of the license clients. This would require a more sophisticated configuration. Please refer to the documentation of your Linux system.

Communication Between License Server and Cloud Infrastructure

The license server must be able to access information provided by the cloud infrastructure. In particular, it must be able to communicate with the following addresses/systems:

- The metadata server of the cloud environment (**169.254.169.254**) on AWS, Azure, OCI, and GCP.
- If running on AWS, the host **iam.amazonaws.com**
- If running on GCP, the host **www.googleapis.com**
- Once support has been implemented for IBM cloud, the license server will need to communicate with the hosts **iam.cloud.ibm.com** and **resource-controller.cloud.ibm.com**.

Any intermediate firewall as well as the cloud-specific subnet and instance security settings must permit communication with these systems for the VE license server to function properly. See Cloud-Specific Firewall Information for information about the mechanisms used in the different cloud environments, and your Linux firewall documentation for any Linux specific questions.

Charon-SSP VE-Capable Emulator and Management Software

The VE license server software requires matching Charon-SSP emulator software. The necessary features are available in Charon-SSP 4.2.x and later. Stromasys or your Stromasys VAR will provide you with the software or a download link. In certain cloud environments, Stromasys may offer a prepackaged Charon-SSP VE image on the cloud marketplace. This image includes the Charon-SSP emulator software (already installed) and the VE License Server RPM package (can be installed optionally). If you use a Charon host in the cloud and the instance was launched from such a prepackaged image, the required VE-capable emulator software is already installed (refer to the respective cloud-specific *Getting Started Guide* for more information).

Please note: The protocol versions used by the emulator software and the license server must be compatible. The software checks for compatible protocol versions and reports an error should there be a mismatch.

The Charon-SSP packages to be installed are the following RPM packages:

- **Management components (not VE-specific)**:
  - charon-agent-ssp-*<version>*-x86_64.rpm
  - charon-director-ssp-*<version>*.rpm
  - charon-manager-ssp-*<version>*.rpm
- **VE-capable emulator software**:
  - charon-ssp-*<architecture>*-*<version>*.ve.el7-x86_64.rpm
  - charon-ssp-*<architecture>*-*<version>*.ve.el8-x86_64.rpm

In the above list, the placeholders have the following meaning:

- *<version>* indicates the software version (e.g., 4.2.5).
- *<architecture>* indicates the type of emulated SPARC covered by the software (currently it can have the values 4m, 4u, 4v, 4u+, or 4v+).
- The string **ve** in the package containing the Charon emulator software indicates that this version of the emulator requires a VE license server.
- The string **el7** denotes packages intended for Red Hat/CentOS/Oracle Linux 7.x.
- The string **el8** denotes packages intended for Red Hat/CentOS/Oracle Linux 8.x.
- Charon Agent, Manager, and Director are not license-model specific.

Please note:

- Unless there is GUI access to the Charon-SSP host system (or an option to use X11-Forwarding via SSH), Charon Manager and Charon Director must be installed on a remote management system that will be used to configure and manage the Charon-SSP software. The Charon-SSP emulator software can also be run from the command-line, in which case Charon Manager and Director are not required.
- The Charon Agent package contains the RPM and Debian packages for the Charon Manager on Linux and a ZIP file for the Charon Manager on Microsoft Windows (charon-manager-ssp-*<version>*.zip).
- The Charon-SSP VE emulator software can run on the same system as the license server or on a separate system with appropriate network access to the VE License Server.

VE License Server Software Installation

If you are not familiar with the installation of RPM packages, please refer to the regular user's guide or your Linux system documentation.

Please note:

- In versions before 1.0.17, the license server will not start automatically after the initial installation. It will be started once a valid license has been installed (see Installing a License on the VE License Server).
- When upgrading to version 1.0.24 from an older version of the license server, a license update is required due to a change in the license schema.
- If you plan to use a primary and a backup license server, the license server software must be installed on both systems.

VE License Server Installation Steps

Perform the following steps to install the VE License Server software:

1. **Copy the license server software package to the cloud instance (if still required)**:
   a. Use **sftp** to connect to the cloud instance.
      `# sftp -i ~/.ssh/`*`<mykey>`* *`<user>`*`@`*`<cloud-instance-ip>`*
      where
          i. *<mykey>* is the private key of the key-pair you associated with your cloud instance
          ii. *<user>* is the user associated with your cloud instance (e.g., *opc* on OCI, or *centos* for a CentOS instance on AWS; for an instance installed from a prepackaged Charon-SSP VE image, use the SFTP user *charon*)
          iii. *<cloud-instance-ip>* the ip address of your cloud instance
   b. Copy the software package to the cloud instance using the following sftp command:
      `> put `*`<local-path-to-license-server-package>`*

2. **Use ssh to log in on the cloud instance**.
   `# ssh-i ~/.ssh/`*`<mykey>`* *`<user>`*`@`*`<cloud-instance-ip>`*
   where
   a. *<mykey>* is the private key of the key-pair you associated with your cloud instance
   b. *<user>* is the user for interactive login associated with your cloud instance (e.g., *opc* on OCI, or *centos* for a CentOS instance on AWS; for an instance installed from a prepackaged Charon-SSP VE image, use *sshuser*)
   c. *<cloud-instance-ip>* the ip address of your cloud instance

3. **As a privileged user (root) go to the directory where you stored the installation package and install the package**:
   a. Become the root user: `# sudo -i`
   b. Go to the package location: `# cd `*`<path-to-package-directory>`*
      On an instance installed from a prepackaged Charon-SSP VE image, the installation package is stored under */charon/storage*)
   c. Install the package:
          i. Linux 7.x: `# yum install license-server*.rpm`
          ii. Linux 8.x: `# dnf install license-server*.rpm`

Below, you find the sample output of an installation:

```
# yum install license-server-1.0.35.rpm
Loaded plugins: fastestmirror, langpacks
Examining license-server-1.0.35.rpm: license-server-1.0.35-1.x86_64
Marking license-server-1.0.35.rpm to be installed
Resolving Dependencies
--> Running transaction check
---> Package license-server.x86_64 0:1.0.35-1 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package           Arch        Version          Repository            Size
================================================================================
Installing:
 license-server    x86_64      1.0.35-1         /license-server-1.0.35   79 M

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

Total size: 79 M
Installed size: 79 M
Is this ok [y/d/N]: y
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : license-server-1.0.35-1.x86_64                        1/1
  Verifying  : license-server-1.0.35-1.x86_64                        1/1

Installed:
  license-server.x86_64 0:1.0.35-1

Complete!
```

Charon-SSP VE-Capable Emulator Software Installation

General Information

The Charon-SSP packages are RPM packages that are installed using the **yum** (Linux 7.x), **dnf** (Linux 8.x), or **rpm** command. They can be copied to the Charon host system using **SFTP** as shown in the example for copying the license server RPM.

At least the required emulator packages (**charon-ssp-4*.rpm**) and the agent (**charon-agent*.rpm**) must be installed for the system to run emulated SPARC systems and to allow remote management by the Charon Manager. If local management with graphical tools is required, then the Charon Manager and the Charon Director packages must also be installed.

For detailed host system requirements and for the management of the Charon-SSP software, please refer to the regular Charon-SSP documentation on the Stromasys Product Documentation and Knowledge Base pages.

Please note: To use the graphical user interface (Charon Manager for SSP) the Charon Manager package typically is installed on your local Linux or Windows PC that will be used for management purposes. Running the Charon Manager in a non-graphical cloud instance and export it via X11-Forwarding is possible, but will require additional configuration and installation steps (with access to a package repository) - this is outside the scope of this document. It is also possible to manage Charon-SSP via the command-line only. This is described in the general Charon-SSP user's guide.

Possible Additional Requirements

Many Linux server instances are missing packages that are typically available on workstation installations. Such packages may have to be installed, for example, if Charon-SSP graphics device emulation or audio emulation are to be used. The same applies to the Charon-SSP Manager, the Server JIT feature, and some non-critical functions of the Charon Agent. On prepackaged Charon-SSP cloud marketplace images, the necessary packages are preinstalled.

The following table provides an overview of the packages that may be missing:

RPM Package	Graphics and audio emulation	Charon Manager*	Server JIT feature	Charon Agent
libX11	x	x		
xorg-x11-server-utils	x	x		
alsa-plugins-pulseaudio	x			
gtk2		x		
xorg-x11-xauth (only required for X11-Forwarding)		x		
libicu (version 50 for Linux 7.x, version 60 for Linux 8.x)			x	
pciutils				x

* If you install the Charon Manager with the **yum** (or **dnf**) command, these packages (except for xorg-x11-xauth) and any dependencies that these packages themselves may have, are resolved automatically if a package repository is available.

If you suspect problems caused by missing packages and the emulator was started via the Charon Manager, check the emulator crash-log file in addition to the emulator log file. If starting the emulator from the command-line, review the command-line output.

The packages above have their own dependencies. Install the above packages with the **yum** (or **dnf**) command in order to have their dependencies automatically installed. If your server does not have access to the standard operating system repositories, refer to this document for instructions on setting up a local repositories.

Sample Installation

Only the Charon-SSP emulator packages (4M, 4U(+), 4V(+)) are specific to the license model used. The packages required for managing Charon-SSP (Charon Agent, Manager, and Director) are the same as in the conventional product of the same version.

For detailed host system requirements and for the management of the Charon-SSP software, please refer to the regular Charon-SSP documentation on the Stromasys Product Documentation and Knowledge Base pages.

The log output below shows a sample Charon-SSP emulator and management package installation on a Linux 7 system:

```
# yum install charon*.rpm

(lines removed)

Resolving Dependencies
--> Running transaction check

(lines removed)

Dependencies Resolved

================================================================================
 Package                 Arch    Version      Repository                 Size
================================================================================
Installing:
 charon-agent-ssp        x86_64 4.2.5-1      /charon-agent-ssp-4.2.5-x86_64 32 M
 charon-director-ssp     x86_64 4.2.5-1      /charon-director-ssp-4.2.5     287 k
 charon-manager-ssp      x86_64 4.2.5-1      /charon-manager-ssp-4.2.5      5.8 M
 charon-ssp-4m           x86_64 4.2.5.ve.el7-1 /charon-ssp-4m-4.2.5.ve.el7-x86_64 6.1 M
 charon-ssp-4u+          x86_64 4.2.5.ve.el7-1 /charon-ssp-4u+-4.2.5.ve.el7-x86_64 54 M
 charon-ssp-4v+          x86_64 4.2.5.ve.el7-1 /charon-ssp-4v+-4.2.5.ve.el7-x86_64 54 M

Installing for dependencies:

(lines removed)

Transaction Summary
================================================================================
Install  6 Packages (+32 Dependent packages)

Total size: 161 M
Total download size: 8.9 M
Installed size: 183 M
Is this ok [y/d/N]: y
Downloading packages:

(lines removed)

Running transaction check
Running transaction test
Transaction test succeeded
Running transaction

(lines removed)

Installed:
  charon-agent-ssp.x86_64 0:4.2.5-1      charon-director-ssp.x86_64 0:4.2.5-1
  charon-manager-ssp.x86_64 0:4.2.5-1    charon-ssp-4m.x86_64 0:4.2.5.ve.el7-1
  charon-ssp-4u+.x86_64 0:4.2.5.ve.el7-1 charon-ssp-4v+.x86_64 0:4.2.5.ve.el7-1

(lines removed)

Complete!
```

Installing a License on the VE License Server

Contents

Important Information to Protect the License Validity

Certain actions can invalidate your license. Therefore, once you have installed your license, please note the following points:

If supported by the cloud provider, the VE license server instance can be moved to a different subnet, as long as the original instance can be moved. It is also possible to backup and restore (to the same instance) the license server data.

However, the following actions will invalidate the license:

- Changing the number of CPU cores of the license server system.
- Copying the license server data to a different instance
- Seriously damaging the root filesystem of the license server system
- Re-installing the license server system

Requesting and Installing a License

Perform the following basic steps to request and install a license:

- Collect the fingerprint (the customer-to-vendor, or C2V, file) on the license server and (if applicable) the backup license server.
- Send the fingerprint data to Stromasys stating license requirements based on your contract with Stromasys (product version, number of concurrent instances, is this the main or the backup license, etc.). Stromasys will send you the license data.
- Install the license data (the vendor-to-customer, or V2C, file) on the license server and (if applicable) on the backup license server.
- Verify the license installation.

These basic steps are described in more detail below.

Collecting the Fingerprint Data on the License Server

The fingerprint is collected on the license server using the **c2v** utility.

Perform the following steps to collect the fingerprint on the license server and (if applicable) the backup license server:

1. Use **ssh** to log in on the license server instance.
   # ssh -i ~/.ssh/`<mykey> <user>@<license-server-ip>`
   where
   a. *<mykey>* is the private key of the key-pair you associated with your cloud instance
   b. *<user>* is the user for interactive login associated with your license server instance (e.g., *opc* on OCI, or *centos* for a CentOS instance on AWS; for an instance installed from a prepackaged Charon-SSP VE image, use *sshuser*)
   c. *<license-server-ip>* is the ip address of your cloud instance
2. Become the privileged user and run the **c2v** program.
   a. Become the root user: **# sudo -i**
   b. Run the c2v program: **# /opt/license-server/c2v --filename** `<my-file>`**.c2v --platform** `<my-platform>`
      where
      i. *<my-file>.c2v* is the path and name under which you want to store the fingerprint; the file type is C2V (customer-to-vendor)
      ii. *<my-platform>* indicates the platform on which the license server runs (possible values: **aws**, **oci, gcp,** or **azure**; the value **ibm** shown in the help output is reserved for future use)
3. Copy the resulting C2V file to your local system (unless you can send email from the license server system).

Sending the C2V File to Stromasys and Receive License Data File

Stromasys or your Stromasys VAR will provide you with an email address to which you should send the C2V file you created in the previous step.

In response, you will receive a so-called V2C (vendor-to-customer) file which contains the license data. The content of the license (type of emulated SPARC, expiration date, number of concurrent instances, etc.) depends on your contract with Stromasys. You may also receive a text file containing the license content in human readable form.

Installing the License Data on the License Server

The license data is installed on the license server using the **v2c** utility.

Perform the following steps to install the license on the license server:

1. Copy the V2C file to the license server (e.g., with SFTP).
2. Use **ssh** to log in on the license server instance.
   # ssh -i ~/.ssh/`<mykey> <user>@<license-server-ip>`
   where
   a. *<mykey>* is the private key of the key-pair you associated with your license server instance
   b. *<user>* is the user for interactive login associated with your cloud instance (e.g., *opc* on OCI, or *centos* for a CentOS instance on AWS; for an instance installed from a prepackaged Charon-SSP VE image, use *sshuser*)
   c. *<license-server-ip>* is the ip address of your cloud instance
3. Become the privileged user and run the **v2c** program.
   a. Become the root user: **# sudo -i**
   b. Run the v2c program: **# /opt/license-server/v2c -f** `<my-file>`**.v2c**
      where *<my-file>.v2c* is the path and name under which you want to store the fingerprint. The file type is V2C (vendor-to-customer).

After the installation of the V2C file, the license server will be restarted.

Please note:

- Starting with version 1.0.35, a previously installed license will be cleanly removed once a new license is installed with the **v2c** command.
- In versions before 1.0.17, the license server will not start until a valid license has been installed.

The following example shows the installation of a V2C file:

```
$ sudo /opt/license-server/v2c -f mylicense.v2c
<<V2C>> Going to import "mylicense.v2c" ...
<<V2C>> Imported "mylicense.v2c" successfully.
<<V2C>> Restarting license server ...
<<V2C>> Done
```

Verifying the License Installation

Using the license_viewer Program

The license server provides a license_viewer program to view the content of the license. To run it, use the following command (as the privileged user):

```
# /opt/license-server/license_viewer
```

The following sample shows the output of an active license:

```
# /opt/license-server/license_viewer
<<License Viewer>> Current license:
KEYSEC
K_FINGER=58ca76281dd3d99b49252b2c877c88329691c328240156615db293f545055359
K_LICENSE_ID=01.00000001.002.044
K_TYPE=NORMAL
K_CUSTOMER=Stromasys/Testing
K_PLATFORM=amazon.aws
K_R_DATE=1593308781
K_INTERVAL=60
KEYEND
PRODSEC
P_NAME=Charon-SSP/4U,Charon-SSP/4U+,Charon-SSP/4V,Charon-SSP/4V+
P_CODE=test
P_RLSD=31-DEC-2020 23:55:00
P_MAJV=4
P_MINV=2
P_CPU_NUM=4
P_MAX_MEM=4096MB
P_INSTANCE=4
PRODEND
PRODSEC
P_NAME=Charon-SSP/4M
P_CODE=test
P_RLSD=31-DEC-2020 23:55:00
P_MAJV=4
P_MINV=2
P_CPU_NUM=4
P_MAX_MEM=512MB
P_INSTANCE=4
PRODEN
```

Important product-specific license parameters:

- P_RLSD is the expiration date.
- P_MAJV and P_MINV are the major and minor product versions.
- P_CPU_NUM defines the maximum number of CPUs in an emulated SPARC system.
- P_MAX_MEM defines the maximum amount of RAM in an emulated SPARC system.
- P_INSTANCE defines the maximum number of concurrently running emulated SPARC systems.

Important key-specific license parameters:

- K_PLATFORM: the platform for which the license has been created.
- K_LICENSE_ID: in older versions, the license ID changed if the license server software was reinstalled; in newer versions, it will remain unchanged as long as the license server host instance is not re-installed.
- K_TYPE: possible values are *NORMAL* (time-limited or perpetual license) or *COUNTDOWN* (limited to a certain number of emulator runtime hours).
- K_EXPIRED: configured number of emulator runtime hours. The remaining hours can be seen in the web interface of the license server and the emulator log file.
- K_INTERVAL: configured license check interval.

Using the Web Interface

The license server provides a web interface to display important license characteristics and a list of currently connected client systems and emulator instances.

Prerequisite: access to TCP port 8084 of the license server must be possible.

The following image shows sample output of a **backup license** with 179 hours and 57 minutes of runtime remaining:

VE License Server: v1.0.35, Build time: Dec 19 2020 10:49:07

License ID: 03.00000003.001.003, Platform: amazon.aws

Product Section	Expiration	Product Name	Product Code	Major Version	Minor Version	Maximum CPUs	Maximum Memory (MB)	Maximum Instances
1	179 Hours and 57 Minutes	Charon-SSP/4M,Charon-SSP/4U,Charon-SSP/4U+,Charon-SSP/4V,Charon-SSP/4V+	Charon-SSP/Full VAR	4	2	64	4194304	3

Client List:

No.	Client IP	Client OS	Product Name	Version	CPU Number	Memory (MB)	Login Time	Product Section
1	127.0.0.1	CentOS Linux release 7.6.1810 (Core)	CHARON-SSP/4U	v4.2.5	1	1024	2020-12-21 16:12:17	1

The following image shows sample output of a **regular license with an expiration date and one client attached**:

VE License Server: v1.0.35, Build time: Dec 17 2020 19:15:00

License ID: 01.00000001.002.112, Platform: ms.azure

Product Section	Expiration	Product Name	Product Code	Major Version	Minor Version	Maximum CPUs	Maximum Memory (MB)	Maximum Instances
1	01-Mar-2021(UTC)	Charon-SSP/4M	test	4	2	4	512	4
2	01-Mar-2021(UTC)	Charon-SSP/4U,Charon-SSP/4U+	test	4	2	4	10240	4
3	01-Mar-2021(UTC)	Charon-SSP/4V,Charon-SSP/4V+	test	4	2	8	10240	4

Client List:

No.	Client IP	Client OS	Product Name	Version	CPU Number	Memory (MB)	Login Time	Product Section
1	127.0.0.1	CentOS Linux release 7.7.1908 (Core)	CHARON-SSP/4M	v4.2.5	1	64	2020-12-17 18:14:44	1

The first section of the samples shows the characteristics of the license. The second section shows the client running a Charon-SSP instance that is connected to the license server. In this example, client and license server are installed on the same system and the client uses product section 1 (4M) of the three product sections on the license.

Configuring Charon-SSP to Use a VE License Server

Contents

Charon-SSP License Server Configuration

The license server address must be configured on the Charon-SSP host system for every emulated system that is to use the license server. This configuration is normally performed via the Charon Manager. On host systems that allow command-line access, it can also be performed by editing the configuration file.

Configuring the License Server Address Using the Charon Manager

To configure the license server address using the Charon Manager, perform the following steps:

1. Start the Charon Manager and log in to your Charon-SSP host system. Please refer to the user's guide of your Charon-SSP product for details.
2. Select the emulated SPARC system from the list of VMs on the left and click on **Edit Virtual Machine** to open the configuration window:
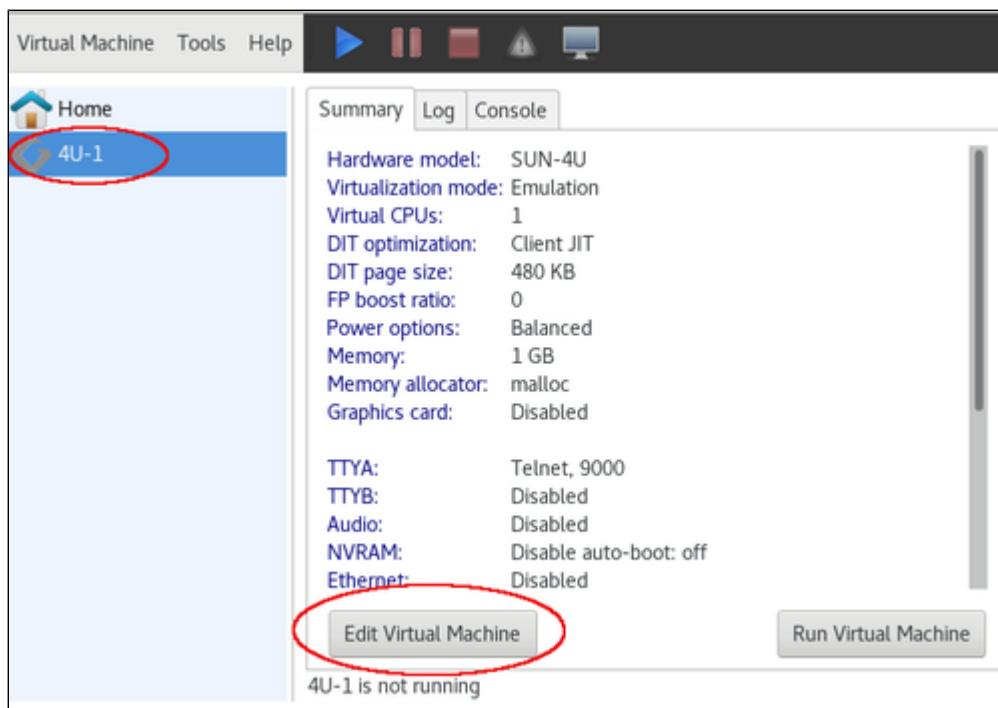
3. In the configuration window select the license configuration section and enter the IP address of the license server in the field **Primary license server** in the **Private cloud** section (use *localhost* or 127.0.0.1 if the license server runs on the same system as the emulator). If you have a backup license server (supported in Charon-SSP version 4.1.19 or later), add the IP address of the backup server in the field **Backup license server**. The backup server provides a license limited to a certain number of runtime hours should the primary server become unavailable. With the introduction of the backup server feature, the grace period should the license become unavailable will be reduced from 24 hours to 2 hours (starting with version 4.1.21). The grace period is the time period the emulator continues to run after its license has been lost or removed. If there is no valid license after the grace period ends, the emulator will stop.
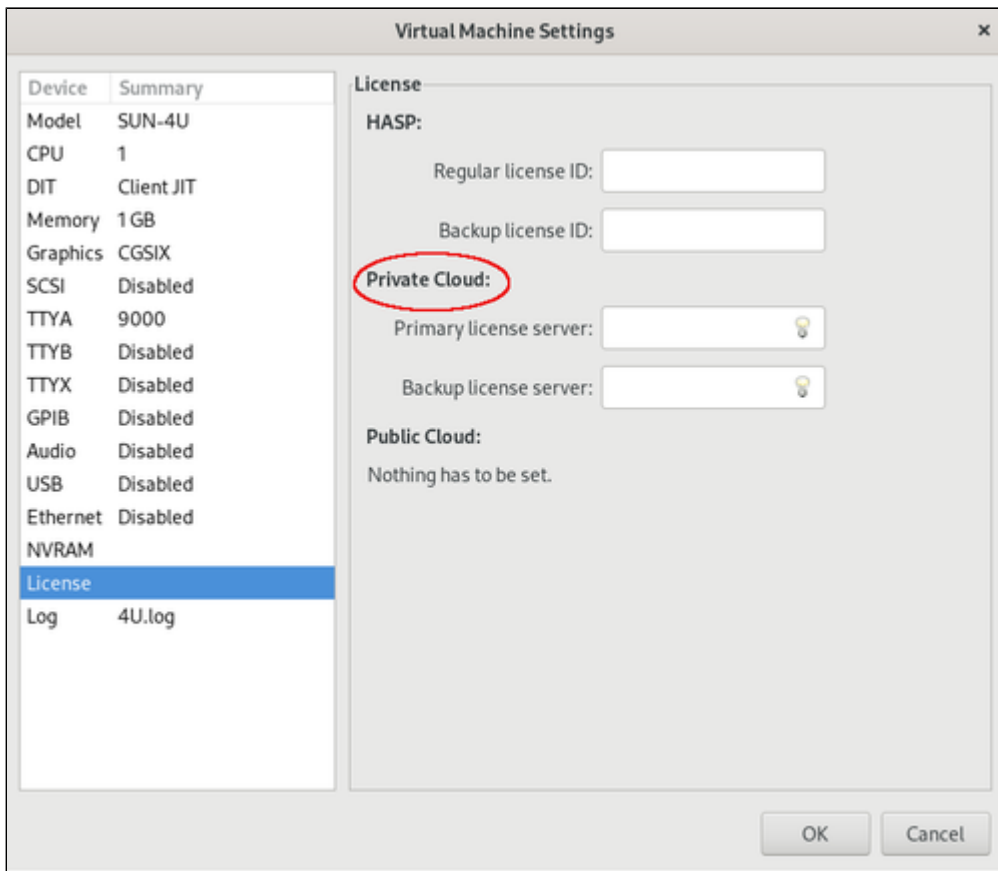
4. Click on **OK** to save the configuration. It will become active at the next start of the emulator.

Configuring the License Server Address in the Configuration File

If your Charon-SSP host system allows command-line access, you can manually edit the configuration file of an emulated SPARC system. This section only describes the license server address parameter. Please refer to your general Charon-SSP user's guide for a full documentation of the configuration file options.

Configuration File Location

The default location for the configuration files is in **/opt/charon-agent/ssp-agent/ssp/***<architecture>***/***<vmname>***/***<vmname>***.cfg**.

In the above path

- *<architecture>* stands for sun-4m, sun-4u, or sun-4v,
- *<vmname>* stands for the name of the emulated SPARC.

However, if the Charon-SSP system is managed without the GUI, the user can decide where to store the emulator configuration files.

Adding the License Server Address to the Configuration File

To add the license server IP address to the configuration file, perform the following steps:

1. Log in to the system as the privileged user.
2. Open the configuration file with a text editor.
3. Locate the **[license]** section.
4. Add the parameter
   server = *<license-server-ip-address>*
   to the section, where
   <license-server-ip-address> is the IP address of the license server.
5. Optionally, add the parameter
   backup_server = *<backup-license-server-ip-address>*
   to the section, where
   <backup-license-server-ip-address> is the IP address of the backup license server.
   The backup server provides a license limited to a certain number of runtime hours should the primary server become unavailable.
6. Save the configuration file
7. At the next restart of your emulator instance, the configuration becomes active.

Additional Information

Depending on your Charon-SSP product, the Charon Manager will show additional license management tools. In particular the following:

- Primary and backup license configuration under HASP in the license configuration section.
- HASP Tools in the Tools menu.

Please note: These tools are not relevant for Charon-SSP VE licenses. The same is true for the license management command-line tools **hasp_srm_view** and **hasp_update** that are installed with the Charon Agent.

Operational Information and Logging

This section describes some information that could become relevant during the operation of a VE license server and the corresponding Charon-SSP emulator products.

Contents

Sentinel/Gemalto License Tools not Applicable to the VE License Server

In Charon-SSP, the Sentinel/Gemalto-specific license tools and configuration options are available when installing the management packages for the VE-capable Charon-SSP emulator packages. These tools and options are in particular the following:

- HASP Viewer, HASP Updater, and HASP Manager in the **Tools > HASP Tools** menu of the Charon Manager
- The Regular and Backup License parameter in the emulator license configuration section
- The command-line tools in */opt/charon-agent/ssp-agent/utils/license*

The above tools cannot be used for managing Charon-SSP VE licenses. Please ignore them if you have a VE license.

Actions that can Invalidate a VE License

If supported by the cloud provider, the VE license server instance can be moved to a different subnet, as long as the original instance can be moved. It is also possible to backup and restore (to the same instance) the license server data.

However, the following actions will invalidate the license:

- Changing the number of CPU cores of the license server system.
- Copying the license server data to a different instance
- Seriously damaging the root filesystem of the license server system
- Re-installing the license server system

Starting and Stopping the License Server

Please note: In versions before 1.0.17, the license server can only be started if a valid license is installed.

The license server is a systemd service that is controlled via **systemctl**:

- Starting the license server: **# systemctl start licensed**
- Stopping the license server: **# systemctl stop licensed**
- Restarting the license server: **# systemctl restart licensed**

Primary and Backup License Server

General Information

Charon-SSP for VE licenses supports a backup license server to ensure service continuity should the primary license server become temporarily unavailable. Backup licenses are typically limited to a certain number of emulator runtime hours.

The example below shows the output of such a license:

```
# /opt/license-server/license_viewer
<<License Viewer>> Current license:
KEYSEC
K_FINGER=123db1ec91a1526c40da028b9e68e5abaadc70c62719af0f6ef1f2cfd2c85bba
K_LICENSE_ID=01.00000001.002.045
K_TYPE=COUNTDOWN
K_EXPIRED=100
K_CUSTOMER=Stromasys/Testing
K_PLATFORM=amazon.aws
K_R_DATE=1593308906
K_INTERVAL=60
KEYEND
PRODSEC
P_NAME=Charon-SSP/4U,Charon-SSP/4U+,Charon-SSP/4V,Charon-SSP/4V+
P_CODE=test
P_MAJV=4
P_MINV=2
P_CPU_NUM=4
P_MAX_MEM=4096MB
P_INSTANCE=4
PRODEND
PRODSEC
P_NAME=Charon-SSP/4M
P_CODE=test
P_MAJV=4
P_MINV=2
P_CPU_NUM=4
P_MAX_MEM=512MB
P_INSTANCE=4
PRODEND
```

Note the parameters K_TYPE=COUNTDOWN and K_EXPIRED=100. They indicate that this is a backup license with 100 hours of emulator runtime.

Backup License Server Operation

Should the primary license server become unavailable, the emulator tries to connect to the backup license server. If this succeeds, the emulator continues to run without interruption. If no connection to a valid license can be established within 2 hours, the emulator will stop.

Please note: If you do not have a valid backup license and the primary license server is unavailable for more than 2 hours, make sure to shut down the Solaris guest operating system cleanly before the end of the grace period. Failure to do so may cause data loss or corruption.

If the primary license server becomes available again after the emulator has switched to the backup server, the emulator will automatically switch back to the primary server to avoid unnecessary depletion of the backup license runtime hours.

Log Files

Log files provide important information about the operation of the license server and the Charon-SSP software. In case of problems, this is the first place to check.

License Server Log File

Log File Location

The license server log file is stored under **/opt/license-server/license_log**

The log file is called *license.log*. At every license server start, a new version of the log file is created and the previous file is rotated to *license.log.1*. Other existing versions are rotated accordingly.

Log File Samples

Normal startup:

```
2020-01-16 09:00:43 INFO    MAIN     Build time: Jan 16 2020 10:54:15
2020-01-16 09:00:44 INFO    MAIN     License server is ready to serve.
```

No valid license installed:

```
2020-01-10 12:17:19 INFO    MAIN     Build time: Jan 10 2020 17:22:12
2020-01-10 12:17:19 ERROR   License  license is not available.
2020-01-10 12:17:19 INFO    MAIN     The program is terminated.
```

Client connection log (new in 1.0.28):

```
2020-10-02 21:46:29 INFO    MAIN     License server is ready to serve.
2020-10-03 01:31:09 INFO    Server   CHARON-SSP/4U v4.1.32 has logged in from 127.0.0.1:40704.
2020-10-03 01:45:21 INFO    Server   CHARON-SSP/4U v4.1.32 from 127.0.0.1:40704 has been disconnected
```

Charon-SSP Emulator Log Files

Log File Location

The default emulator log file location is **/opt/charon-agent/ssp-agent/ssp/**<*architecture/<vm-name>/*.

- *<architecture>* can be sun-4m, sun-4u, or sun-4v.
- *<vm-name>* is the name of the emulated SPARC system.

The log file is called *<vm-name>.log*. At every emulator start, a new version of the log file is created and the previous file is rotated to *<vm-name>.log.1*. Other existing versions are rotated accordingly. The number of retained files is determined by the log configuration of the emulated SPARC system.

Please note: The log file path can be changed by the user to a non-default value.

Log File Samples

Working license found during emulator start:

```
2020-07-16 21:25:10 INFO  VE      Trying to login to license server: 127.0.0.1
2020-07-16 21:25:13 INFO  VE      Connected with license server: 127.0.0.1
2020-07-16 21:25:13 INFO  VE      Found available license ID: 01.00000001.002.044.
2020-07-16 21:25:13 INFO  VE      Customer name: Stromasys/Testing.
2020-07-16 21:25:13 INFO  VE      Virtual hardware model Charon-SSP/4M is licensed.
2020-07-16 21:25:13 INFO  VE      Maximum concurrent instances are limited to 4.
2020-07-16 21:25:13 INFO  VE      Maximum allowed virtual CPU(s) are 4.
2020-07-16 21:25:13 INFO  VE      Maximum allowed virtualized memory is 512 MB.
2020-07-16 21:25:13 INFO  VE      Major allowed version number is 4.
2020-07-16 21:25:13 INFO  VE      Minor allowed version number is 2.
2020-07-16 21:25:13 INFO  VE      Expiration UTC time: 2020-12-31 15:55:00.
```

Connection to license server lost temporarily and then restored:

```
(License loss detected)

2020-07-16 22:25:56 ERROR VE      Failed to connect with the license server!
2020-07-16 22:25:56 WARN  VE      Charon will be terminated within 2 hours!

(License server connection restored)

2020-07-16 23:26:01 INFO  VE      Connected with license server: 127.0.0.1
2020-07-16 23:26:01 INFO  VE      Found available license ID: 01.00000001.002.044.
2020-07-16 23:26:01 INFO  VE      Customer name: Stromasys/Testing.
2020-07-16 23:26:01 INFO  VE      Virtual hardware model Charon-SSP/4M is licensed.
2020-07-16 23:26:01 INFO  VE      Maximum concurrent instances are limited to 4.
2020-07-16 23:26:01 INFO  VE      Maximum allowed virtual CPU(s) are 4.
2020-07-16 23:26:01 INFO  VE      Maximum allowed virtualized memory is 512 MB.
2020-07-16 23:26:01 INFO  VE      Major allowed version number is 4.
2020-07-16 23:26:01 INFO  VE      Minor allowed version number is 2.
2020-07-16 23:26:01 INFO  VE      Expiration UTC time: 2020-12-31 15:55:00.
2020-07-16 23:26:01 INFO  VE      Local UTC time: 2020-07-16 15:26:01.
2020-07-16 23:26:01 INFO  VE      The license is verified, back to normal operation.
```

Please note: The output shows a 2 hour grace-period. This is applicable to Charon-SSP versions 4.1.21 and later. In earlier versions the grace-period was 24 hours. This is no longer needed because a backup license server can now be configured (since Charon-SSP version 4.1.19). If a valid license has not become available before the end of the grace period, the emulator will be stopped.

Switch to backup license server:

```
2020-06-29 18:08:25 ERROR VE     Failed to connect with the license server!
2020-06-29 18:08:25 INFO  VE     Trying to login to license server: 127.0.0.1
2020-06-29 18:08:34 ERROR VE     Failed to connect with the license server!
2020-06-29 18:08:43 WARN  VE     Charon will be terminated within 2 hours!
2020-06-29 19:08:57 INFO  VE     Connected with license server: 172.31.40.62
2020-06-29 19:08:57 INFO  VE     Found available license ID: 01.00000001.002.045.
```

License Server version mismatch:

The following message is logged in older versions. Newer versions may have a more descriptive error message.

```
2020-01-16 11:24:38 WARN  VE  Failed to get data from license server!
```

Please note: The software checks for for compatible protocol versions between license server and emulator software. It logs an error if the versions are not compatible. Compatible versions are required for the emulator to verify the license and to run.

Updating a VE License

An update to a license may become necessary due to

- the expiration date being reached,
- Charon-SSP product upgrade,
- additional Charon-SSP instances,
- etc.

To update your license, perform the following steps:

1. Create a new C2V file on the license server.
2. Send the output to Stromasys.
3. Install the received V2C file on the license server. This will automatically remove the previously installed license (starting with version 1.0.35).

Please refer to Installing a License on the VE License Server for a detailed description of these steps.

VE License Server Software Upgrade

Please note:

- If you are not familiar with the installation of RPM packages, please refer to the regular user's guide or your Linux system documentation.
- You do not need to stop running emulator instance before upgrading the license server.
- Please refer to the general Charon-SSP user's guide for information on how to upgrade the Charon-SSP emulator software.

To upgrade the license server package, perform the following steps:

1. Use **sftp** to connect to the cloud instance.
   `# sftp -i ~/.ssh/`*<mykey>* *<user>*@*<cloud-instance-ip>*
   where
   a. *<mykey>* is the private key of the key-pair you associated with your cloud instance
   b. *<user>* is the user associated with your cloud instance (e.g., *opc* on OCI, or *centos* for a CentOS instance on AWS; for an instance installed from a prepackaged Charon-SSP VE image, use the SFTP user *charon*)
   c. *<cloud-instance-ip>* the ip address of your cloud instance

2. Copy the software package to the cloud instance using the following sftp command:
   `> put `*<local-path-to-license-server-package>*

3. Use ssh to log in on the cloud instance.
   `# ssh -i ~/.ssh/`*<mykey>* *<user>*@*<cloud-instance-ip>*
   a. *<mykey>* is the private key of the key-pair you associated with your cloud instance
   b. *<user>* is the user for interactive login associated with your cloud instance (e.g., *opc* on OCI, or *centos* for a CentOS instance on AWS; for an instance installed from a prepackaged Charon-SSP VE image, use *sshuser*)
   c. *<cloud-instance-ip>* the ip address of your cloud instance

4. As a privileged user (root) go to the directory where you stored the installation package and update the package. If you used the VE image and copied the file using SFTP to user charon, the file will be in the hierarchy under **/charon/storage**.
   a. Become the root user: `# sudo -i`
   b. Go to the package location: `# cd `*<path-to-package-directory>*
   c. Install the package:
      i. Linux 7.x: `# yum update license-server*.rpm`
      ii. Linux 8.x: `# dnf update license-server*.rpm`

Normally, the license server will restart and continue to work normally. To check the status, perform the following steps:

- Look at the license server log: **/opt/license-server/license_log/license.log**
- Use the ps command to check that the server is running:
  `# ps -ef |grep license-server`

About an hour after the installation check the emulator log files of any active instances to verify that no unexpected problem has been caused by the new version.

🔶 VE License Server Software Deinstallation

Please note:

- If you are not familiar with the deinstallation of RPM packages, please refer to the regular user's guide or your Linux system documentation.
- Before you deinstall a VE license server, make sure that no active emulator guest system depends on this license server.
- Please refer to the general Charon-SSP user's guide for information on how to remove the Charon-SSP emulator software.

To uninstall the license server package, perform the following steps:

1. Use ssh to log in on the cloud instance.
   `# ssh -i ~/.ssh/<mykey> <user>@<cloud-instance-ip>`
   a. *<mykey>* is the private key of the key-pair you associated with your cloud instance
   b. *<user>* is the user for interactive login associated with your cloud instance (e.g., *opc* on OCI, or *centos* for a CentOS instance on AWS; for an instance installed from a prepackaged Charon-SSP VE image, use *sshuser*)
   c. *<cloud-instance-ip>* is the ip address of your cloud instance

2. As a privileged user (root) perform the deinstallation command:
   a. Become the root user: `# sudo -i`
   b. Remove the VE license server package:
      i. Linux 7.x: `# yum erase license-server`
      ii. Linux 8.x: `# dnf erase license-server`

VE License Server Command-Line Utilities

The License Server kit contains the following command-line utilities:

- C2V Utility
- V2C Utility
- license_viewer Utility

All License Server utilities are located in **/opt/license-server**.

C2V Utility

The C2V (Customer-to-Vendor) utility enables the user to collect the initial fingerprint of the license server system and later collect C2V data for license updates.

Usage: `c2v [options]`

The options are described in the table below:

Option	Description
`-f,--filename` *name*	Specifies the name of the file in which the C2V data will be stored.
`-p, --platform` *platform*	VE platform on which the license server runs: • **aws**: to run on Amazon Cloud • **oci**: to run on Oracle Cloud • **azure**: to run on Microsoft Azure • **gcp**: to run on Google Cloud Platform • **ibm**: reserved for future use
`-d, --debuglog`	Print a debug log.
`-h, --help`	Print the usage information. Default if no parameter is selected.

V2C Utility

The V2C utility enables the user to install the initial license and subsequent license updates.

Usage: `v2c [options]`

The options are described in the table below:

Option	Description
`-f,--filename` *name*	Specifies the name of the file containing the V2C data.
`-d, --debuglog`	Print a debug log.
`-h, --help`	Print the usage information. Default if no parameter is selected.

license_viewer Utility

The license_viewer utility enables the user to displayed installed licenses.

Usage: `license_viewer`

This utility does not have any parameters.

Additional Information

This section provides additional information to support the installation of the license server and the emulator packages.

Contents

- Creating and Attaching an AWS IAM Role
- Setting Up a Linux Instance in AWS
- Setting up a Linux Instance in OCI
- Setting up a Linux Instance on Azure
- Setting up a Linux Instance on GCP
- Installing the Charon Manager
- Starting the Charon-SSP Manager
- Cloud-Specific Firewall Information

Please note: cloud providers may change their management GUI without prior warning. Hence, the screenshots in this document may not always reflect the latest GUI appearance. However, they will still provide an illustration of the described configuration steps.

Creating and Attaching an AWS IAM Role

The Charon-SSP VE License Server on AWS requires that an IAM role that allows at least the *ListUsers* action is attached to the instance. This section provides an overview of how to create such a role if required. Please refer to the AWS documentation for details.

The basic steps to create and attach a new IAM role definition are the following:

1. Go to the IAM service section.
2. Define a policy with the required permission if it does not already exist.
3. Define a role including the policy with the required permissions.
4. Attach the new IAM role to your instance during instance creation or to an existing instance.

These steps are described in more detail below.

Step 1: Go to the IAM service section:

Open the services overview and search for IAM or open it from the Recently Visited list:
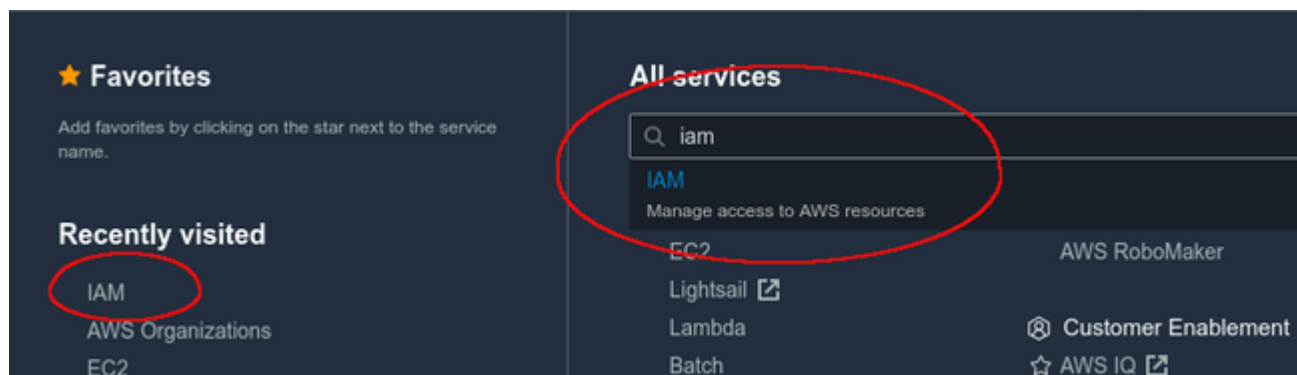
This will open the IAM dashboard.

Step 2: Define a policy with the required permissions (if it does not already exist):

Select **Policies** in the IAM dashboard:
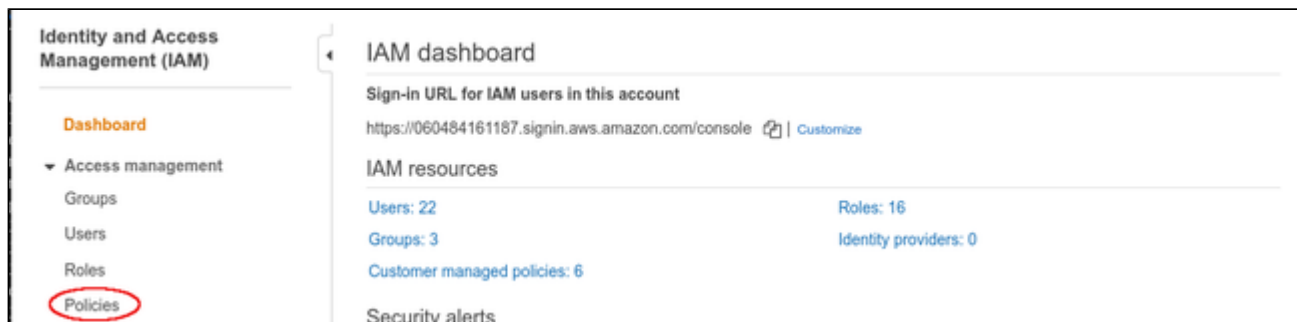
This will open a list of existing policies. If the required policy does not already exist, click on **Create policy** to create a new one as shown below:
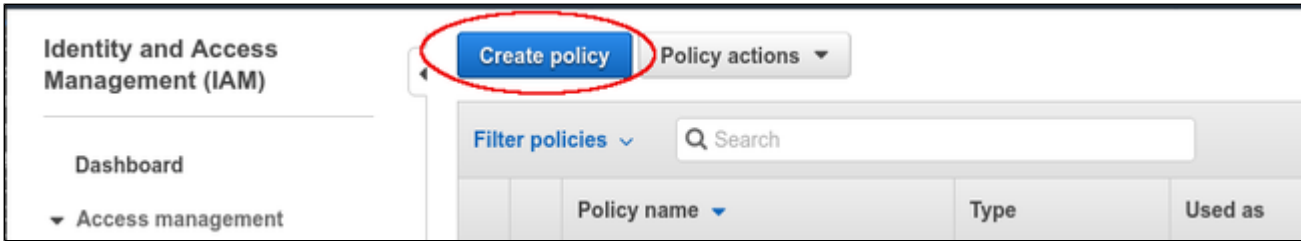
The **Create policy** window opens.

- At the top of the page click on **Choose a service** and select **IAM**.
- Use the filter field to search for the list options.
- Select the **ListUsers** option.
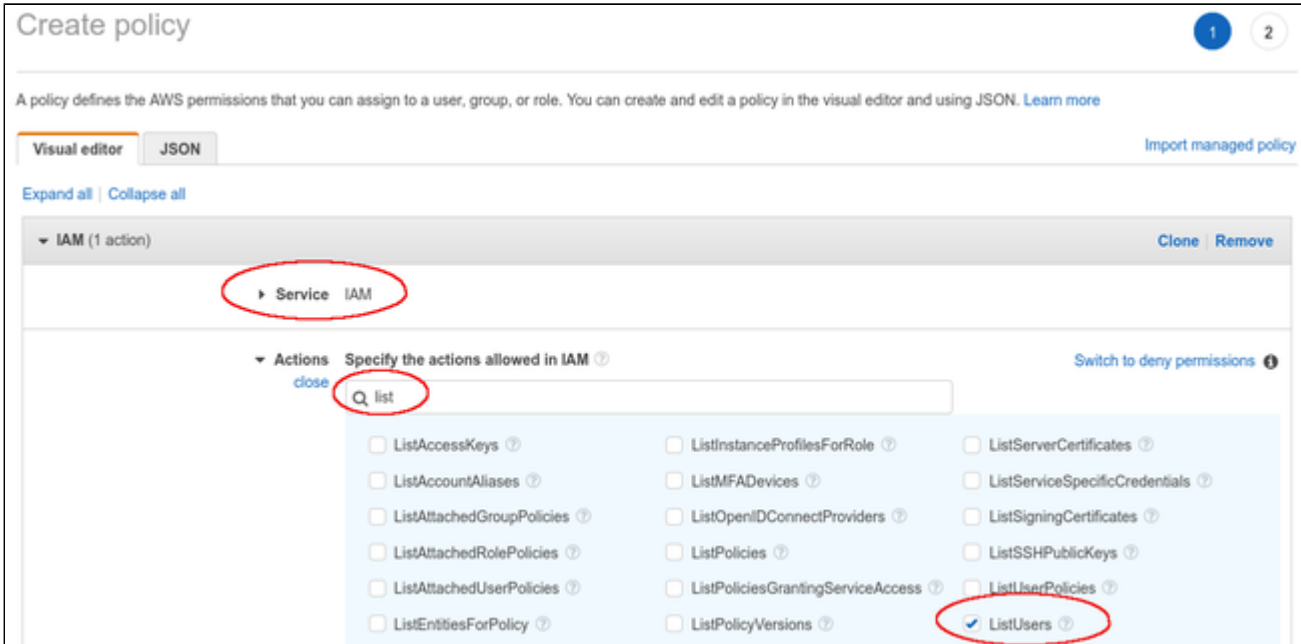
At the bottom of the page click on **Review policy**.

The review page opens:
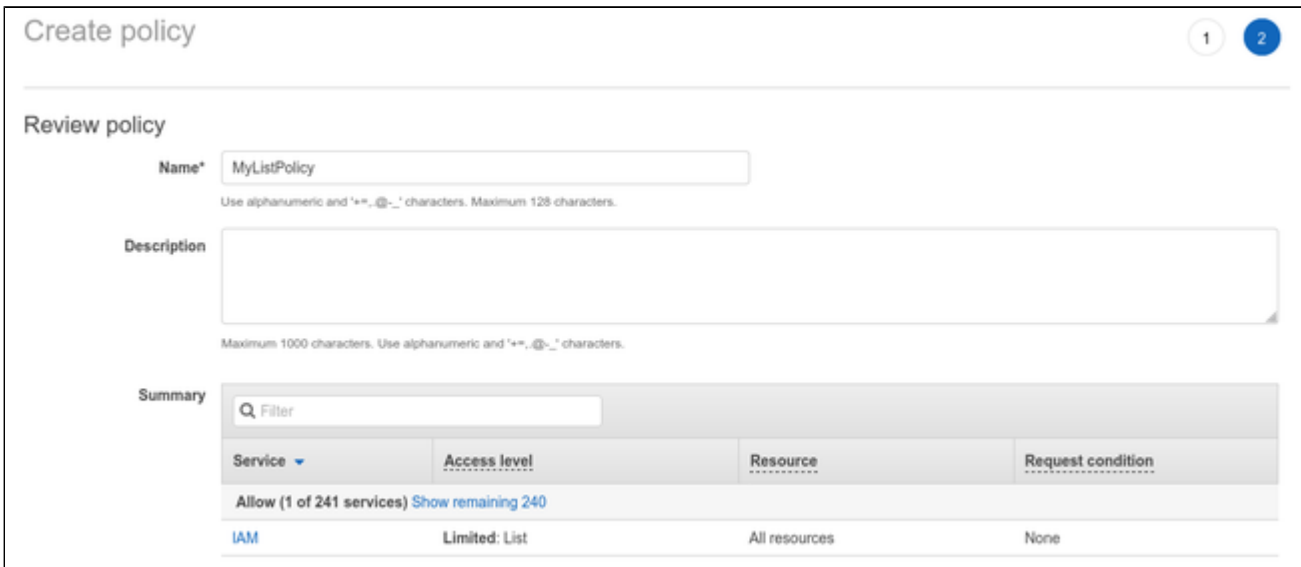
Add a name for the policy and click on **Create policy** at the bottom of the page.

Step 3: Define a role including the policy with the required permissions:

Select **Roles** on the sidebar of the IAM service section (for example on the IAM dashboard):
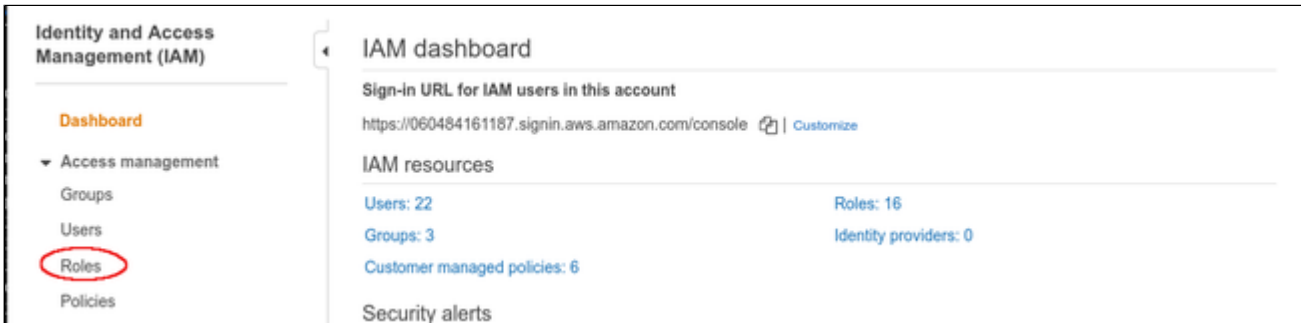
This will open a list of existing roles. To create a new role, click on **Create role**.
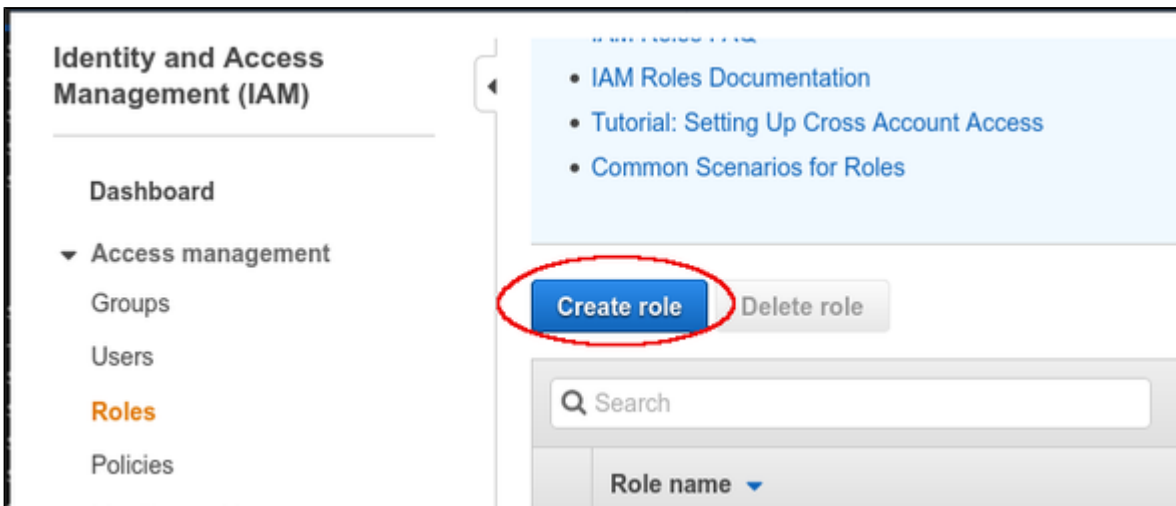
The Create role window opens. Select

- the AWS service, and
- the EC2 use case.
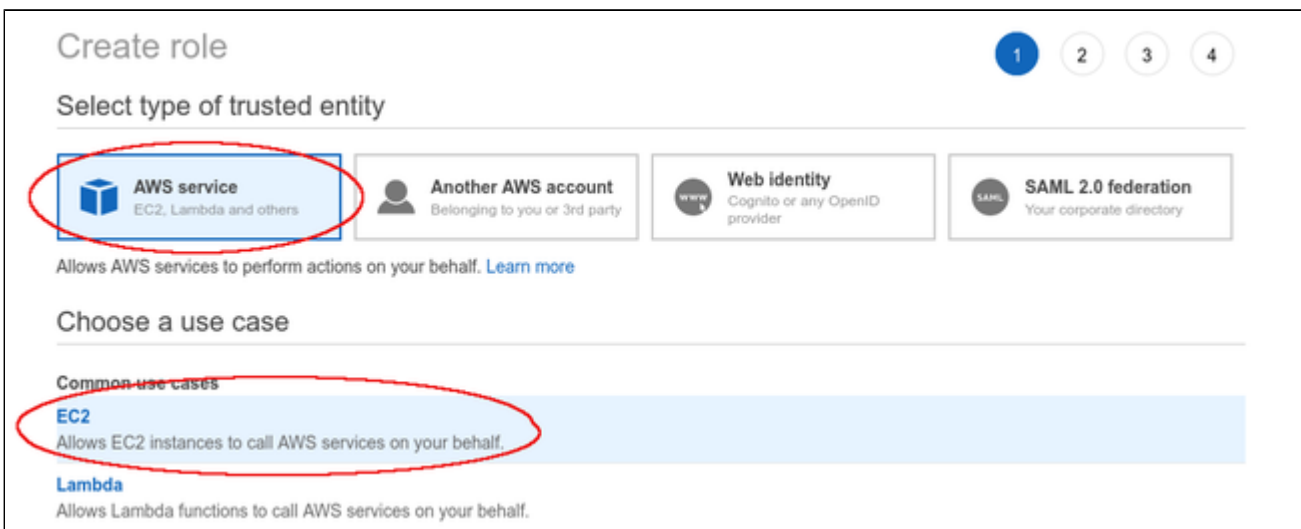
Then click on **Next: Permissions** at the bottom of the window.

The permissions window opens and allows you to select the appropriate policy. Use the filter field to find your policy and select it.

Create role

- Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy

Filter policies ∨   Q My   Showing 1 result

	Policy name ▾	Used as
✓ ▸	MyIAMListUsers	Permissions policy (1)

Click on **Next: Tags** and optionally add tags to your rule. Then click on **Next: Review** to open the review window. Assign a name to your new role as shown in the sample below:

Create role

Review

Provide the required information below and review this role before you create it.

Role name*   MyIAMListRule

Use alphanumeric and '+=,.@-_' characters. Maximum 64 characters.

Role description   Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Trusted entities   AWS service: ec2.amazonaws.com

Policies   MyIAMListUsers ☒

Permissions boundary   Permissions boundary is not set

No tags were added.

Then click on **Create role** at the bottom of the window to complete the creation of your role.

The sample below shows the JSON code created for the rule:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "iam:ListUsers",
            "Resource": "*"
        }
    ]
}
```

Step 4: Attach the new IAM role to your instance during instance creation or to an existing instance.

To attach the role to an instance during instance creation, use the IAM role option in the **Configure Instance Details** window, as shown in the sample below.
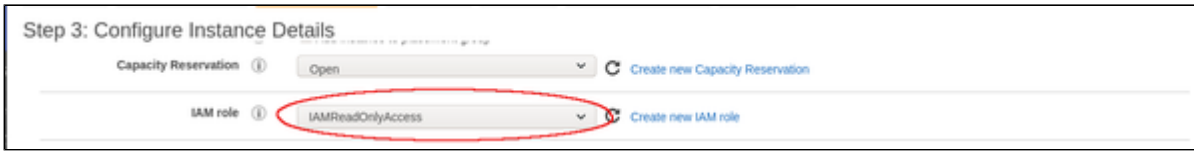
Alternatively, the role can be set/changed by selecting the instance, right-clicking on it, and selecting **Security > Modify IAM Role** (in the older AWS console, use the **Action** menu). Please note that if the instance is stopped, you have to detach an existing role before you can add a new one. On a running instance, you can replace the existing role without removing it first. **If you replace an existing IAM role, ensure that this will not impact other functionality of your instance.**

Setting Up a Linux Instance in AWS

This chapter describes how to set up a Linux instance in AWS. The purpose for which the instance is created will determine the prerequisites for image and instance type used.

Contents

- Prerequisites
- AWS Login and New Instance Launch
- New Instance Configuration
- Initial Access to the Instance
    - SSH Interactive Access
    - File Transfer with SFTP

Prerequisites

As this description shows the basic setup of a Linux instance in AWS, it does not list specific prerequisites. However, depending on the use case, the following prerequisites should be considered:

- To set up a Linux instance in AWS, you need an Amazon AWS account.
- If this instance is to be used as a Charon host system, refer to the user's guide of your Charon product to determine the exact hardware and software prerequisites that must be taken into account for the Linux instance. The **image** you use for your instance and the **instance type** you chose determine which hardware and software your cloud instance has.
- If this instance is to be used as a Charon host system, a product **license** is required to run emulated systems. Contact your Stromasys representative or Stromasys VAR for details.
- Certain legacy operating systems that can run in emulated systems provided by Charon emulator products require a license of the original vendor of the operating system. The user is responsible for any licensing obligations related to the legacy operating system and has to provide the appropriate licenses.

AWS Login and New Instance Launch

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications such as Charon emulator products or the Charon VE license server.

To start the creation of a new cloud instance using a general purpose Linux image, perform the following steps:

1. **Log in** to your AWS management console.

2. Find and select the **EC2 service**. You can use the search window or find it in the recently used services.
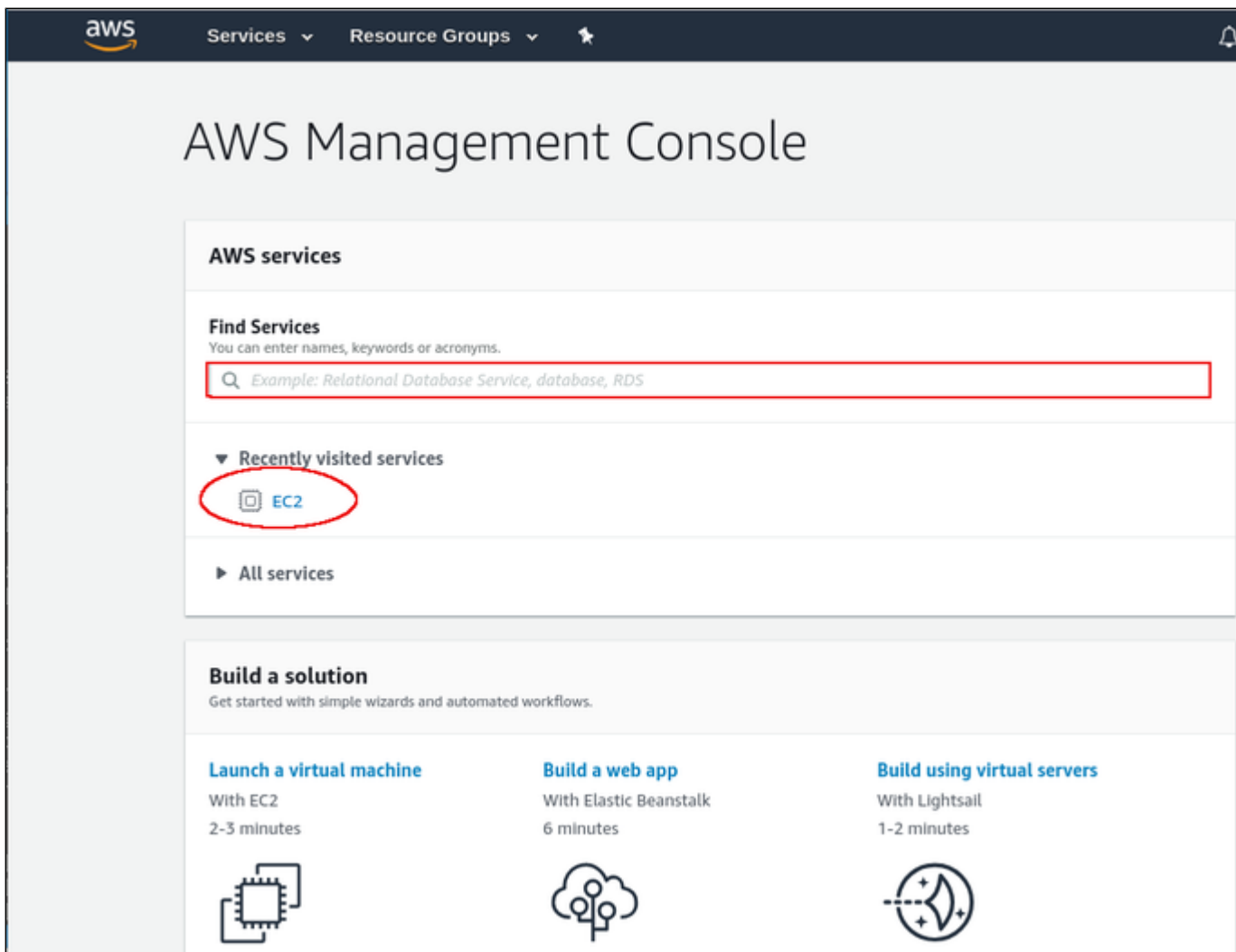
This will open the E2C dashboard.

Please note: The following sample image shows the old E2C dashboard. The new dashboard looks somewhat different, but still has the **Launch instance** button.

3. On the EC2 dashboard click on the **Launch Instance** button.
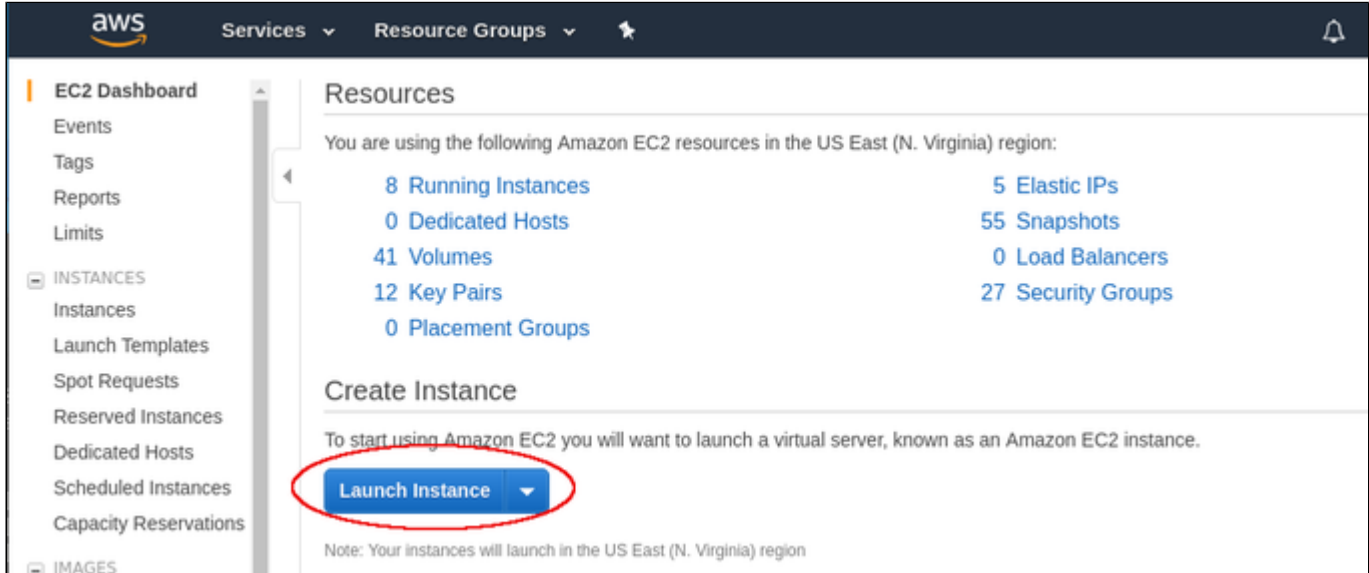
This will initiate the instance creation process consisting of seven steps:

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Groups
7. Review, launch and select/create key-pair for access.

These steps are described in the next section.

New Instance Configuration

The instance creation and configuration process will guide you through a number of configuration steps and allow you to start the new instance when done.

1. Choose AMI:

This example shows the search for **centos** and the results in Marketplace. Depending on your environment, the image may also be in one of the other sections (e.g., My AMIs).
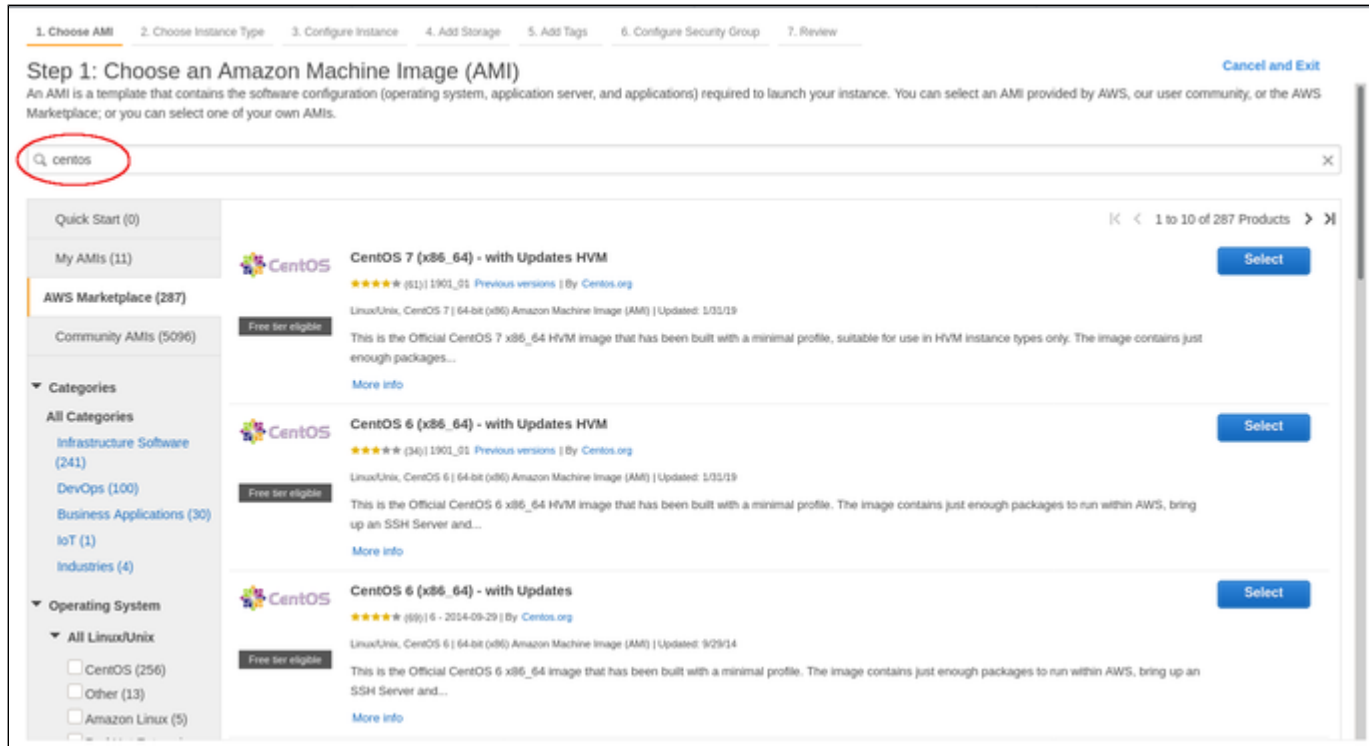
Clicking on one of the categories above will display a list of images. Select the appropriate Linux AMI (a supported Linux version or - if appropriate - a prepackaged Charon-SSP VE marketplace image).

This will take you to the next step, the instance type selection.

2. Choose Instance Type:

Amazon EC2 offers instance types with varying combinations of CPU, memory, storage, and networking capacity. Depending on the image selected, not all instance types may be offered.

Select an instance type that matches the requirements of the planned use of the instance.

When done, continue by clicking on the **Next: Configure Instance** button.

3. Configure Instance:

In this section, you can set up the details of your instance configuration.
For example,

- you can select the VPC **subnet** your instance should be in, and
- whether an interface should automatically be assigned a **public IP address**.

Please note: Automatic assignment of a public IP address only works if there is only one network interface attached to the instance.

You can also assign the required IAM role (allowing the *ListUsers* action) to the instance.

Once you have selected all desired configuration options, click on **Next: Add storage** to continue.

4. Add Storage:

The size of the root volume depends on the minimum size for the Linux system plus any additional products you plan to install. You can add more storage later to provide space, for example for virtual disk containers (if this is a Charon host) and other storage requirements.

Please note: It is recommended to create separate storage space (using AWS EBS volumes) for any application data. If required, such volumes can later easily be migrated to another instance.

Once you are done, again click on the **Next: Add tags** button.

5. Add Tags:

Tags allow you to add information to your instance, for example, an easily remembered name as shown in the example below:

After adding tags as required, continue to the next step (**Configure Security Groups**).

6. Configure Security Groups:

A security group is similar to a firewall. It defines which traffic is allowed to flow to and from the instance. You must at least enable SSH access to the system. This will allow you to access the management interface and to transfer files from/to the cloud instance. You can select an existing group or create a new one. If you create a new one, you can enter an name and an appropriate description. An example of a security group is shown below.

The warning shown alerts the user to the fact that the source IP addresses are not restricted, i.e., any system is allowed to use SSH to access the instance. Restrict the source address range if possible.

Once you have set up your security group, continue to the next step (**Review and Launch**).

7. Review:

Here you can review the configuration of your instance and edit the individual sections if required. The image below shows a sample:

If you are satisfied with the settings, click on the **Launch** button to start your instance for the first time.

8. Launch and select/create key-pair for access:

When starting the instance for the first time, you will be shown a window asking you to create a new key-pair or to use an existing one. When creating a new key-pair, you must download the **private key** to your local system and store it in a safe place. It is required to access your instance. The **public key** is stored in the newly created Linux system, in the **authorized_keys** file of the management user. The name of the management user depends on the selected image and should be shown in its description. For a CentOS image it often is **centos**. The sample below shows the window when the creation of a new key-pair was selected:

You cannot start the instance without downloading the key. If you select to re-use an existing key-pair, you have to confirm that you are in possession of the private key before you can launch the instance.

Verify that instance is running:

After starting your instance for the first time, you will see it in the initializing state in the list of your AWS instances. It will take a bit of time to get to the running state. After this, important information, for example, the public IP address and public DNS name (marked in red) of the instance will also be displayed. The following image shows an example:

The following sections will show you how to access the instance and how to perform additional storage and network configurations.

If you select your instance, the bottom of the screen will show a detailed description and status information of your instance.

Initial Access to the Instance

Once you have access to the instance, you can create the access you require for your applications. This section just shows the basic steps for initial access to the instance.

SSH Interactive Access

To connect to the instance interactively, you must connect as the management user of your instance. Use the following command:

> **$ ssh -o ServerAliveInterval=30 -i** *<path-to-your-private-key>* *<management-user-name>*@*<cloudhost-IP-address>*

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

Please note:

- Depending on the type of connection, you will have to use either the public IP address of the cloud system or its address in a customer-specific VPN.
- The management user account normally allows sudo access to privileged commands (use **sudo -i**).

File Transfer with SFTP

SFTP enables file transfers to and from the cloud instance. Use the management user of your instance. The security rules must allow SSH access to allow SFTP access to the cloud instance.

Please note: Depending on the type of connection, you will have to use either the public IP address of the cloud system or its address in a customer-specific VPN.

To connect to the instance, use the following command:

$ sftp -i *<path-to-your-private-key>* *<management-user>*@*<cloudhost-IP-address>*

Setting up a Linux Instance in OCI

This chapter describes how to set up a basic Linux instance in OCI.

Contents

- Prerequisites
- OCI New Instance Launch
- Initial Access to the Instance
    - SSH Interactive Access
    - File Transfer with SFTP

Prerequisites

As this description shows the basic setup of a Linux instance in OCI, it does not list specific prerequisites. However, depending on the use case, the following prerequisites should be considered:

- To set up a Linux instance in OCI, you need an OCI account.
- If this instance is to be used as a Charon host system, refer to the user's guide of your Charon product to determine the exact hardware and software prerequisites that must be taken into account for the Linux instance. The **image** you use for your instance and the **instance type** you chose determine which hardware and software your cloud instance has.
- If this instance is to be used as a Charon host system, a product **license** is required to run emulated systems. Contact your Stromasys representative or Stromasys VAR for details.
- Certain legacy operating systems that can run in emulated systems provided by Charon emulator products require a license of the original vendor of the operating system. The user is responsible for any licensing obligations related to the legacy operating system and has to provide the appropriate licenses.

OCI New Instance Launch

Please note: 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 Linux cloud instance in 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.
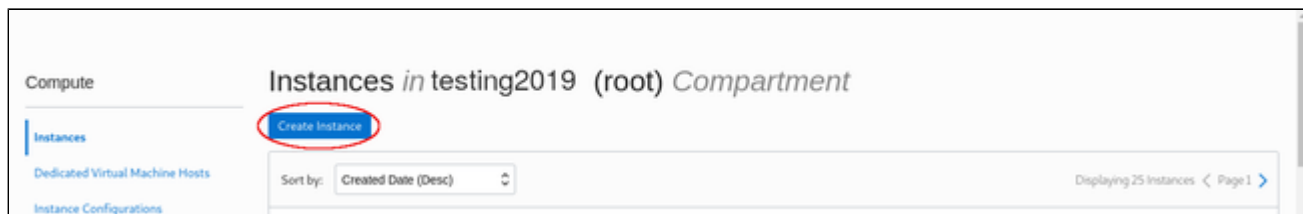
This opens the **Create Compute Instance** window.

Step 3: on the first part of **Create Compute Instance** window, name your instance and select an appropriate Linux image for it.

To select the correct image, select **Change Image**. This will allow you to browse the different available categories.

The image below shows an example of the image selection screen (choose a supported Linux version or - if appropriate - a prepackaged Charon-SSP VE marketplace image):

Optionally, change the compartment. Select the correct image and confirm your selection by clicking on **Select Image** at the bottom of the page. This will take you back to the **Create Compute Instance** window.

Step 4: in the middle part of the **Create Compute Instance** window, select the appropriate **shape** (i.e., the virtual Charon host hardware), the **subnet** membership of the instance and whether to assign a **public IP address**. If required, you can also create a new virtual cloud network or a new subnet here.

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.

Instance type

Virtual Machine	Bare Metal Machine
A virtual machine is an independent computing environment that runs on top of physical bare metal hardware. ✓	A bare metal compute instance gives you dedicated physical server access for highest performance and strong isolation.

Shape series

AMD Rome	Intel Skylake	Specialty and Legacy
AMD Customizable OCPU count. For general purpose workloads.	(intel) Fixed OCPU count. Latest generation Intel Standard shapes. ✓	Earlier generation AMD and Intel Standard shapes. Always Free, Dense I/O, GPU, and HPC shapes.

	Shape Name	OCPU	Memory (GB)	Local Disk	Network Bandwidth (Gbps)	Max. Total VNICs
☐	VM.Standard2.1	1	15	Block Storage Only	1	2
☐	VM.Standard2.2	2	30	Block Storage Only	2	2
☐	VM.Standard2.4	4	60	Block Storage Only	4.1	4
☐	VM.Standard2.8	8	120	Block Storage Only	8.2	8
☐	VM.Standard2.16	16	240	Block Storage Only	16.4	16
☐	VM.Standard2.24	24	320	Block Storage Only	24.6	24

0 Selected   Showing 6 Items

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

Select Shape   Cancel

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

Step 5: on the bottom of the **Create Compute Instance** window create a new SSH key-pair or upload the public SSH key of an existing key-pair that you will use to access your instance. If you create a new key-pair, you must download the private key and store it in a save place for later use. You can also download the public key.

Add SSH keys

Linux-based instances use an SSH key pair instead of a password to authenticate remote users. Generate a key pair or upload your own public key now. When you connect to the instance, you will provide the associated private key.

○ GENERATE SSH KEYS   ○ CHOOSE SSH KEY FILES   ○ PASTE SSH KEYS   ○ NO SSH KEYS

ⓘ Download the private key so that you can connect to the instance using SSH. It will not be shown again.

↓ Save Private Key   ↓ Save Public Key

Step 6: optionally define non-default parameters (including the size) for the boot volume.

The boot volume section allows you to configure the boot volume of your instance with additional non-default parameters. For example, you can configure disk encryption parameters and a non-default system disk size (recommended minimum system disk size: 30GB).

Configure boot volume

Your boot volume is a detachable device that contains the image used to boot your compute instance.

☐ SPECIFY A CUSTOM BOOT VOLUME SIZE
Volume performance varies with volume size. Default boot volume size: 46.6 GB

☐ USE IN-TRANSIT ENCRYPTION
Encrypts data in transit between the instance, the boot volume, and the block volumes.

☐ ENCRYPT THIS VOLUME WITH A KEY THAT YOU MANAGE
By default, Oracle manages the keys that encrypt this volume, but you can choose a key from a vault that you have access to if you want greater control over the key's lifecycle and how it's used. Learn more about managing your own encryption keys

Step 7 (supported starting with Charon-SSP marketplace images version 4.2.2 and VE license server 1.0.33): support an IMDSv2 authorization header for applications relying on the IMDS service to improve security. For this, open the additional options by clicking on **Show Advanced Options** at the bottom of the instance creation page, select the **Management** tab, and activate the authorization header, as shown below:

On existing instances, this parameter can be changed, by editing the instance metadata service settings for the instance (go to **Instance Details** and click on **Edit** in the line **Instance Metadata Service**).
Only change the configuration to IMDSv2 if the image you launched the instance from supports it. Otherwise, you may not be able to connect to your instance. **Please note**: at the time of writing, the official CentOS 7 image on OCI did not support the new feature. If you create an instance to be used as a host for a manual VE license server or Charon-SSP VE installation, verify the capabilities of the image used before you enable the new IMDSv2 feature.

Step 8 (**only for Charon-SSP versions before 4.1.32**): the correct networking type selection is important. Charon-SSP disables offloading parameters on the Ethernet interfaces it uses. This is required for proper functionality and good performance of the emulator. To allow this configuration to be correctly reflected in the underlying cloud instance NICs for Charon-SSP versions before 4.1.32, the correct networking type (HARDWARE ASSISTED (SR-IOV) NETWORKING) must be chosen for the instance. For this, open the additional options section by clicking on **Show Advanced Options** at the bottom of the instance creation page and select the **Networking** tab as shown below:

On this tab select **HARDWARE ASSISTED (SR-IOV) NETWORKING** (after creation, the instance will display the NIC Attachment Type VFIO). Please observe the warning displayed: not all shapes support this type properly.

Step 8: Click on **Create** to create your instance.

Step 9: verify that your instance is running.

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

Initial Access to the Instance

Once you have access to the instance, you can create the access you require for your applications. This section just shows the basic steps for initial access to the instance.

SSH Interactive Access

To connect to the instance interactively, you must connect as the management user of your instance. Use the following command:

> **$ ssh -o ServerAliveInterval=30 -i** *<path-to-your-private-key>* *<management-user-name>***@***<cloudhost-IP-address>*

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

Please note:

- Depending on the type of connection, you will have to use either the public IP address of the cloud system or its address in a customer-specific VPN.
- The management user account normally allows sudo access to privileged commands (use **sudo -i**).

File Transfer with SFTP

SFTP enables file transfers to and from the cloud instance. Use the management user of your instance. The security rules must allow SSH access to allow SFTP access to the cloud instance.

Please note: Depending on the type of connection, you will have to use either the public IP address of the cloud system or its address in a customer-specific VPN.

To connect to the instance, use the following command:

$ sftp -i *<path-to-your-private-key>* *<management-user>***@***<cloudhost-IP-address>*

Setting up a Linux Instance on Azure

Contents

Prerequisites

As this description shows the basic setup of a Linux instance in Azure, it does not list specific prerequisites. However, depending on the use case, the following prerequisites should be considered:

- To set up a Linux instance in Azure, you need a Microsoft Azure subscription.
- If this instance is to be used as a Charon host system, refer to the user's guide of your Charon product to determine the exact hardware and software prerequisites that must be taken into account for the Linux instance. The **image** you use for your instance and the **instance size** you chose determine which hardware and software your cloud instance has.
- If this instance is to be used as a Charon host system, a product **license** is required to run emulated systems. Contact your Stromasys representative or Stromasys VAR for details.
- Certain legacy operating systems that can run in emulated systems provided by Charon emulator products require a license of the original vendor of the operating system. The user is responsible for any licensing obligations related to the legacy operating system and has to provide the appropriate licenses.

Azure Login and New Instance Launch

Log in to your Azure account

To log in perform the following steps:

- Go to **portal.azure.com**. You will see a Microsoft Azure login screen.
- Enter your login credentials.
- Upon successful login, the Azure home screen will be displayed as shown in the example below:
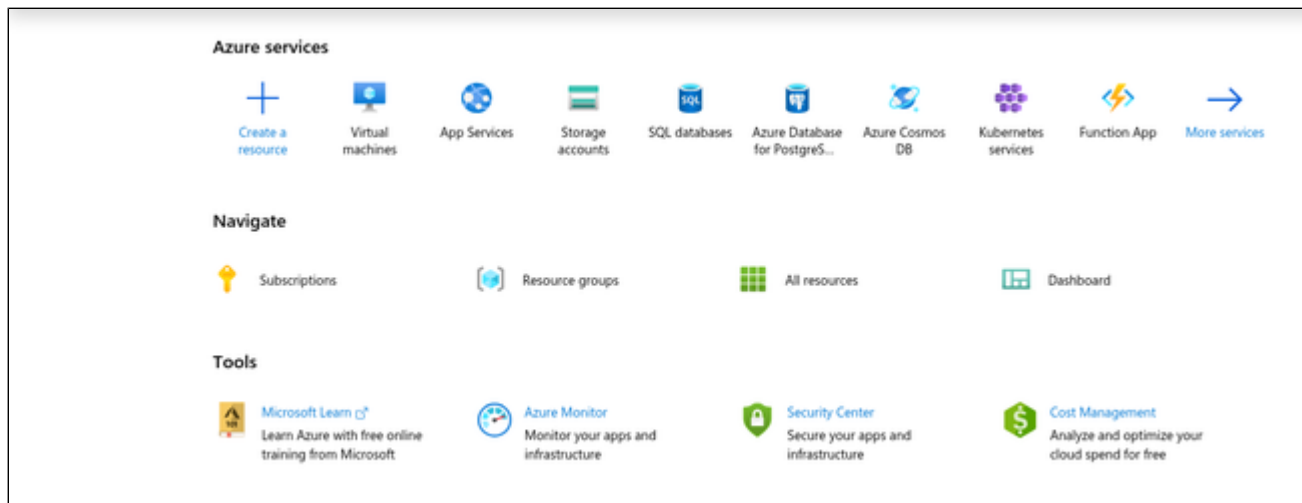
Create a Virtual Machine

Step 1: Click on the Virtual machines icon on the home page.
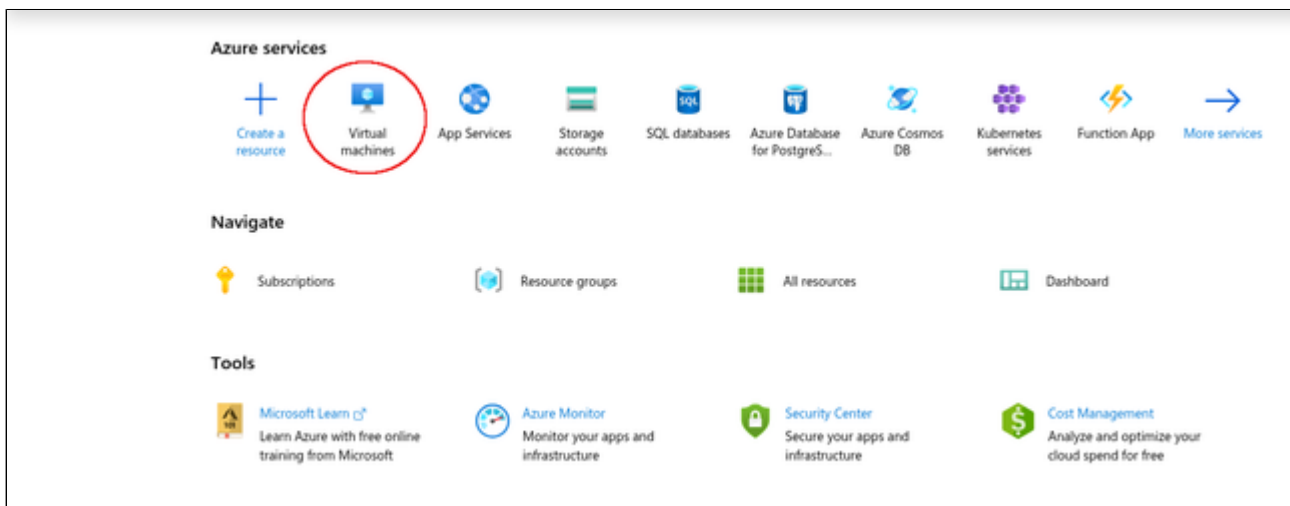
This opens the virtual machines overview list.

Step 2: Click on the Add icon in the overview list.
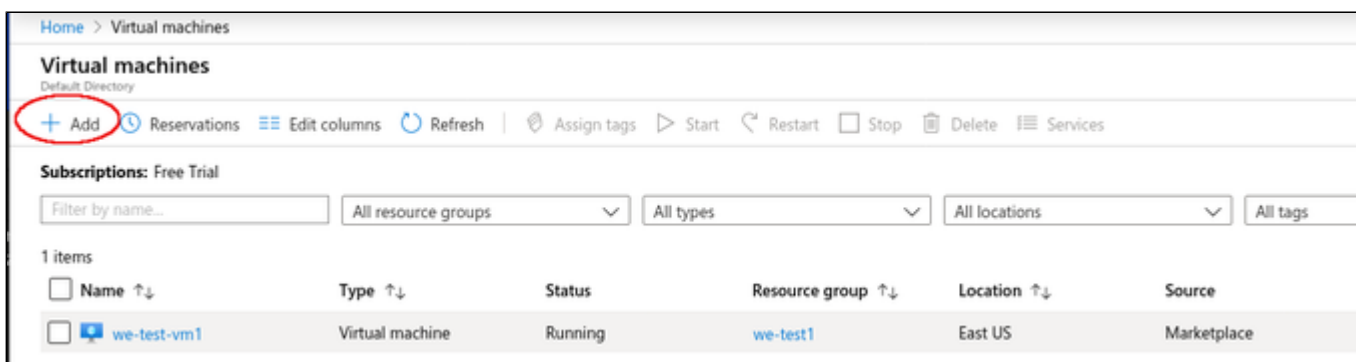
This opens the **Basics** tab of the **Create a Virtual Machine** window.

Step 3: Enter your data on the **Basics** tab. Mandatory data are, for example:

- Your subscription
- Existing resource group (or click on **Create new**)
- Virtual machine name
- Region for the virtual machine
- Linux image (choose a supported Linux version or - if appropriate - a prepackaged Charon-SSP VE marketplace image)
- Size of your VM (click on **Select size** to see a list of available sizes)
- User name for the administrative user of the VM
- Authentication type (SSH or password). Then either paste the public key of the key-pair to use into the field provided, or enter and confirm your password.

Basics tab **upper part** sample:

Basics tab **lower part** sample:

- Enter the name of the administrative user.
- Select **SSH public key** authentication. You can then use **one of the following** steps to install your SSH public key.
  - Let Azure create a new key-pair for you.
  - Use the public key from a key-pair on your computer. As shown in the example below, you will have to past your public key into the field provided.
  - Use a key-pair previously created on Azure.
- The default allowed inbound port will allow SSH connections without limiting the source IP range. Remember to adapt it to your requirements after creating the instance or in the Networking tab (advanced) during the creation of the instance.

Click on **Next: Disks**. This will open the **Disks** tab of the VM creation window.

Step 4: Define the disks for your VM.

Please note: By default, Azure VMs have one operating system disk and a temporary disk for short-term storage (mounted on /mnt/resource and not persistent). You can attach existing additional data disks, or create new disks and attach them.

Disks tab sample:

Click on **Next: Networking**. This will open the **Networking** tab of the VM creation window.

Step 5: Enter the necessary information in the **Networking** tab.

On this tab, you can define the network configuration of your VM:

- Virtual Network (existing or new)
- Subnet (default or other subnet)
- Whether a public IP should be assigned or not
- Basic security settings (which ports are open for access to the VM).

Networking tab sample:

Optionally, you can proceed to the Management, Advanced, and Tags tabs to configure additional details of your VM. However, for a basic test, this is not required.

Click on **Review + Create** to proceed to the review screen.

Step 6: Check the data on the Review + Create screen and create VM.

Verify that the checks passed successfully and click on **Create** to create the VM.

Sample **Review+Create** screen:

If key-pair was newly created, download private key:

If you chose to let Azure create a new SSH key-pair, you will be asked to download the private key after clicking on the Create **button**, this step is very important as this is the only opportunity to download the private key, which is required to access your VM. The image below shows a sample of this prompt:
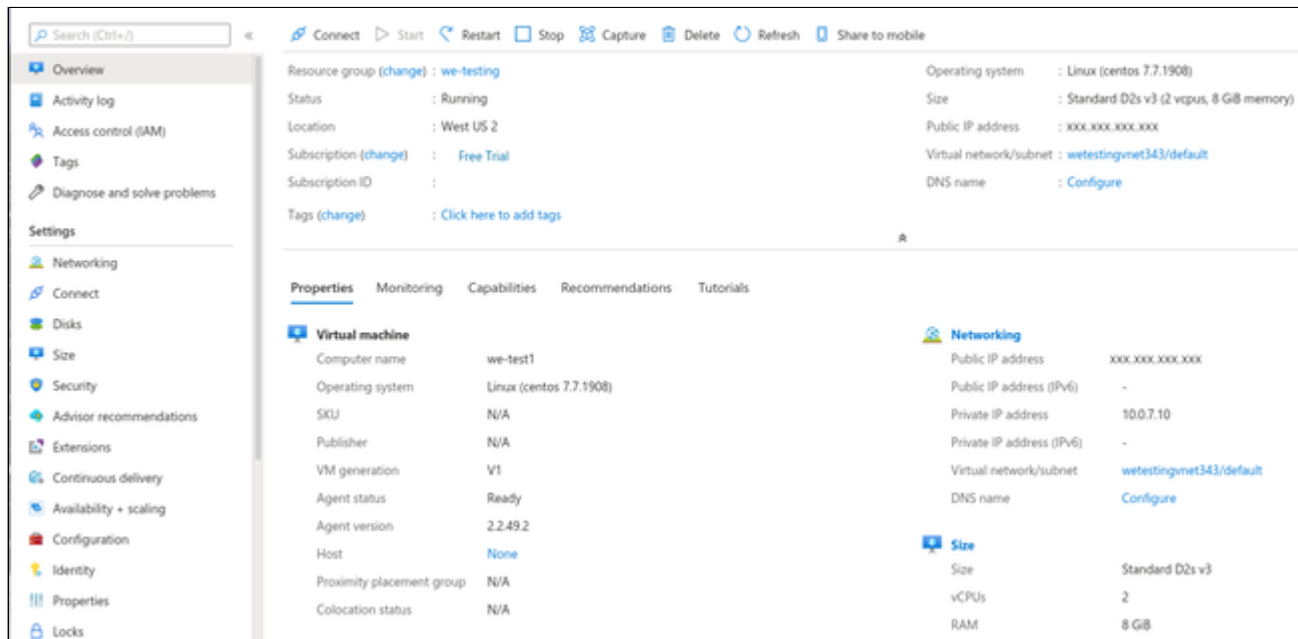
The Deployment page:

Create will take you to the **Deployment** page (possibly after downloading the private SSH key) where the current status of the deployment is displayed. Once the VM has been fully deployed, the **Deployment Complete** screen will be displayed.

Sample **Deployment Complete** screen:
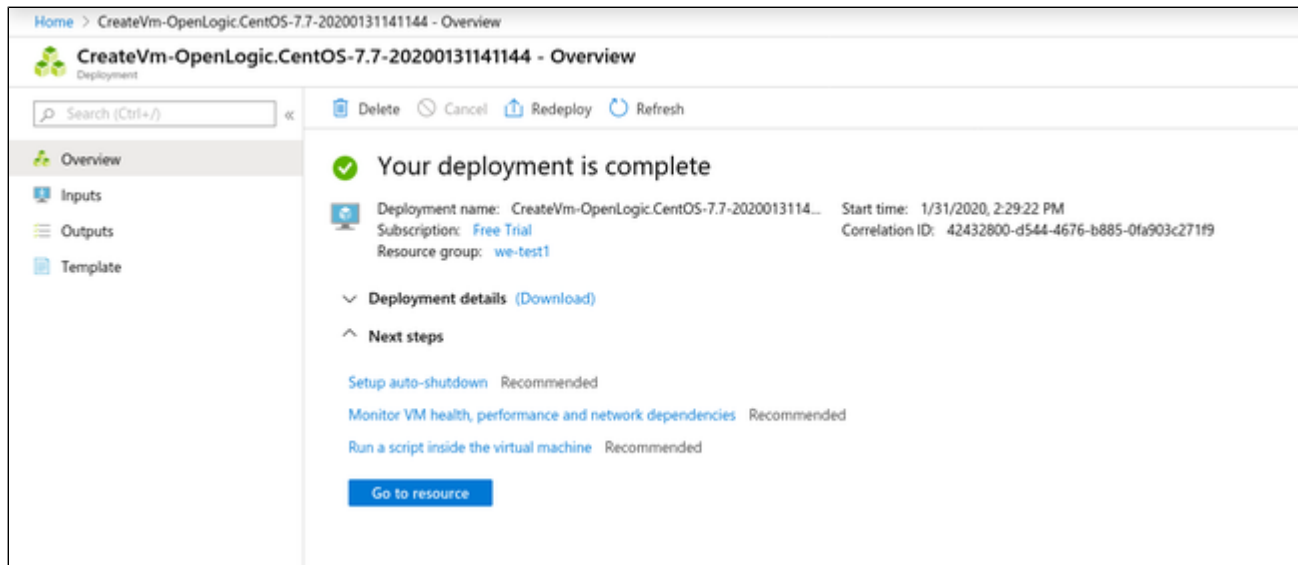
Click on **Go to resource** to get to the details page of the newly created VM. The image below shows a sample of a detail page:

Initial Access to the Instance

Once you have access to the instance, you can create the access you require for your applications. This section just shows the basic steps for initial access to the instance.

SSH Interactive Access

To connect to the instance interactively, you must connect as the management user of your instance. Use the following command:

> **$ ssh -o ServerAliveInterval=30 -i** *<path-to-your-private-key> <management-user-name>@<cloudhost-IP-address>*

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

Please note:

- Depending on the type of connection, you will have to use either the public IP address of the cloud system or its address in a customer-specific VPN.
- The management user account normally allows sudo access to privileged commands (use **sudo -i**).

File Transfer with SFTP

SFTP enables file transfers to and from the cloud instance. Use the management user of your instance. The security rules must allow SSH access to allow SFTP access to the cloud instance.

Please note: Depending on the type of connection, you will have to use either the public IP address of the cloud system or its address in a customer-specific VPN.

To connect to the instance, use the following command:

$ sftp -i *<path-to-your-private-key> <management-user>@<cloudhost-IP-address>*

Setting up a Linux Instance on GCP

Contents

Prerequisites

As this description shows the basic setup of a Linux instance on the GCP, it does not list specific prerequisites. However, depending on the use case, the following prerequisites should be considered:

- To set up a Linux instance on the GCP, you need a Google Cloud account.
- If this instance is to be used as a Charon host system, refer to the user's guide of your Charon product to determine the exact hardware and software prerequisites that must be taken into account for the Linux instance. The **image** you use for your instance and the **machine type** you chose determine which hardware and software your cloud instance has.
- If this instance is to be used as a Charon host system, a product **license** is required to run emulated systems. Contact your Stromasys representative or Stromasys VAR for details.
- Certain legacy operating systems that can run in emulated systems provided by Charon emulator products require a license of the original vendor of the operating system. The user is responsible for any licensing obligations related to the legacy operating system and has to provide the appropriate licenses.

GCP Login and New Instance Launch

Logging in to GCP

To log in perform the following steps:

- Go to https://console.cloud.google.com. You will see the login screen.
- Enter your login credentials.
- Upon successful login, a Google cloud dashboard screen will be displayed similar to the example below:
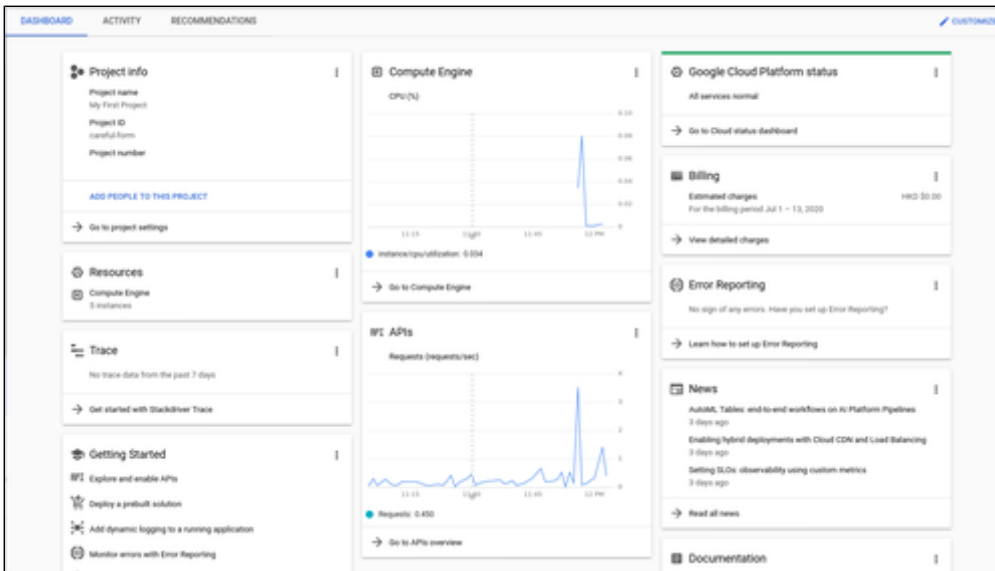
Preparation

Select or Create Project

A project organizes all your Google Cloud resources. To organize all resources for a certain application purpose, you can group them in their own project. So before you start creating resources, select or create the appropriate project.

To select or create a project, select the project list from the top of the Google cloud console window, as shown below:
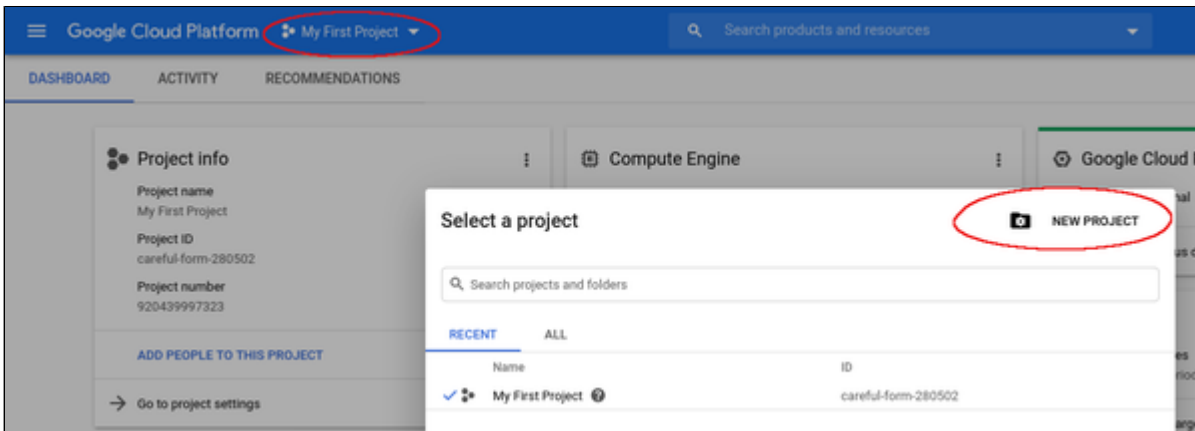
Either select the correct project or create a new one by clicking on the **New Project** button.
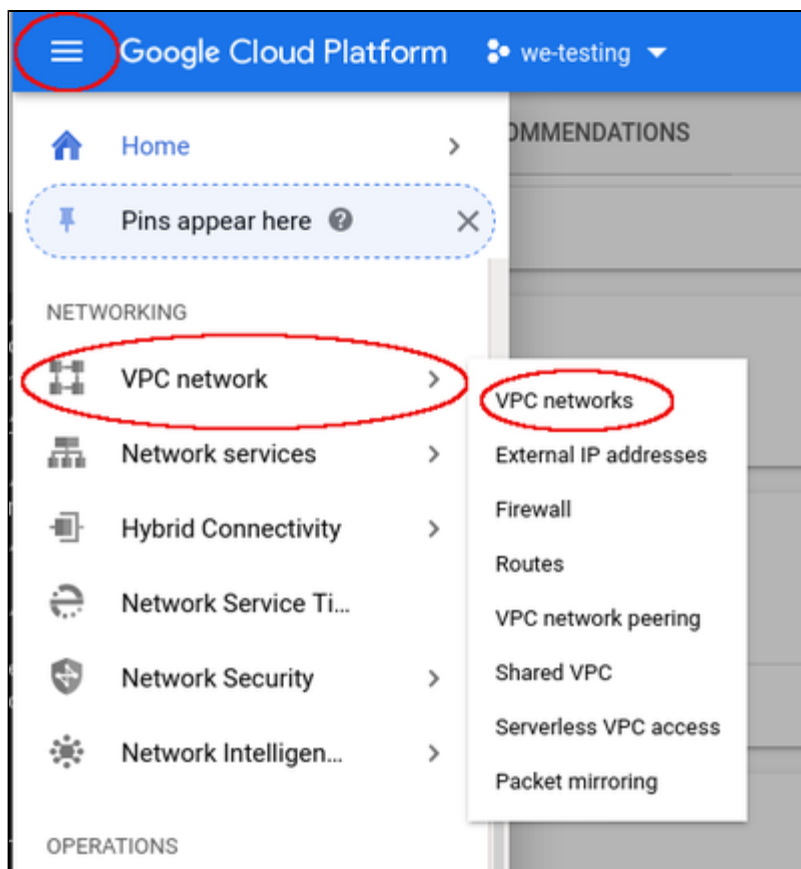
Create VPCs and Subnets for Instance

Important rules for Google cloud instances with respect to network interfaces:

- Interfaces can only be added during instance creation.
- Each network interface configured in a single instance must be attached to a different VPC network.
- The additional VPC networks that the multiple interfaces will attach to must exist before an instance is created. See Using VPC Networks for instructions on creating additional VPC networks.
- You cannot delete a network interface without deleting the instance.
- IP forwarding can only be enabled when the instance is created.
- The VPC network has a maximum transmission unit (MTU) of `1460` bytes for Linux images and Windows Server images. Operating system images provided by Compute Engine are already configured with the appropriate MTU. For custom images, set the MTU to `1460` for custom Linux images and Windows Server images to avoid the increased latency and packet overhead caused by fragmentation.

Therefore the required VPCs and subnets must exist before the instance is created.

To create additional VPCs (if required), perform the following steps.

Step 1: Open the VPC network section by clicking on the Navigation menu, then selecting VPC network, and clicking on VPC networks - as illustrated below.

This will open the VPC overview page with the already existing VPCs. If all required VPCs and subnets already exist, continue with creating the new VM instance. Otherwise, continue with step 2.

Step 2: If you need to create a new VPC, click on CREATE VPC NETWORK at the top of the VPC overview list.

This opens the VPC configuration window.

Step 3: Create VPC and subnets.

In the VPC configuration window, enter

- the VPC name, and
- the subnet name, region and address.

Click on **Create** at the bottom of the window to create the VPC.

The new VPC should appear in the VPC overview list. Selecting the VPC in the overview list will open the detail information window. Example:

Step 4: Create firewall rules for the VPC.

With the detail information open, click on Firewall. This will allow you to define the required firewall rules for the VPC.

An example of a small set of firewall rules that allow incoming SSH and ICMP is shown below:

Creating a New VM Instance

Step 1: Go to the VM instance overview page.

Open the Navigation menu, click on Compute Engine and then on VM Instances as illustrated below:
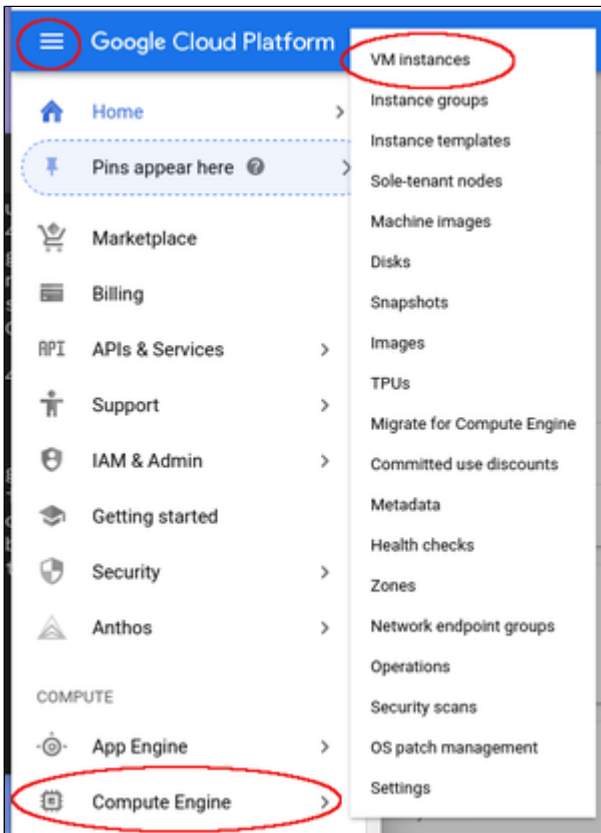
This will open the list of already existing VM instances.

Step 2: Click on Create Instance at the top of the overview list.
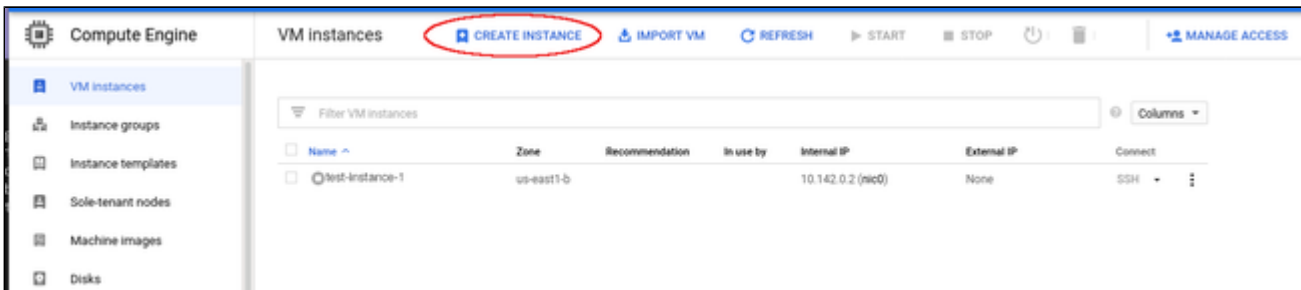
This will open the VM creation window as shown below.

Step 3: Configure the basic information of your new VM instance.

In the main configuration window set the following information at a minimum:

- **Name** of the instance (permanent setting)
- Correct **Machine family** and **Machine type** to match the Charon-SSP host and guest requirements
- **Boot disk** type and size, and the image to use as the operating system. To change the image, press the **Change** button and select the correct image (a supported Linux version or - if appropriate - a prepackaged Charon-SSP VE marketplace image).

The following image illustrates the basic settings:

Step 4: Add you SSH key for remote access to the cloud instance.

Open the advanced settings at the bottom of the VM creation window by clicking on **Management, security, disks,...** at the bottom of the page:

The advanced settings allow you to create and add disks and network interfaces during the creation of a VM.

Please note: network interfaces can only be added during the creation of a VM instance.

The advanced settings also allow you to add your public SSH key for accessing the VM once started. To do this,

- select the tab **Security** in the advanced settings section,
- paste your **public key** into the field provided.

You can collapse the section again by clicking on **Less**.

Step 5: Optionally, configure additional NICs and/or IP forwarding

To add an **additional network interface**, perform the following steps:

- Open the advanced settings at the bottom of the VM creation window by clicking on **Management, security, disks,...** at the bottom of the page.
- Select Networking from the advanced settings section.
- Click on **Add network interface**.
- Select the correct subnet.
- Set the information about internal and external IP address (static or ephemeral) as required.

After adding all the required information, click on **Done**.

To enable **IP forwarding,** perform the following steps:

- Open the advanced settings at the bottom of the VM creation window by clicking on **Management, security, disks,...** at the bottom of the page.
- Select Networking from the advanced settings section.
- Select the edit option for the default NIC.
- Enable IP forwarding
- Click on **Done**.

Step 6: Create the VM.

Once you filled in all the required data, create the VM by pressing the **Create** button at the bottom of the page:

This will create the VM, start it and show it in the VM instances list.

Step 7: Verify the settings of the newly created cloud instance.

After successful creation, the new instance will be shown in the VM instances list:
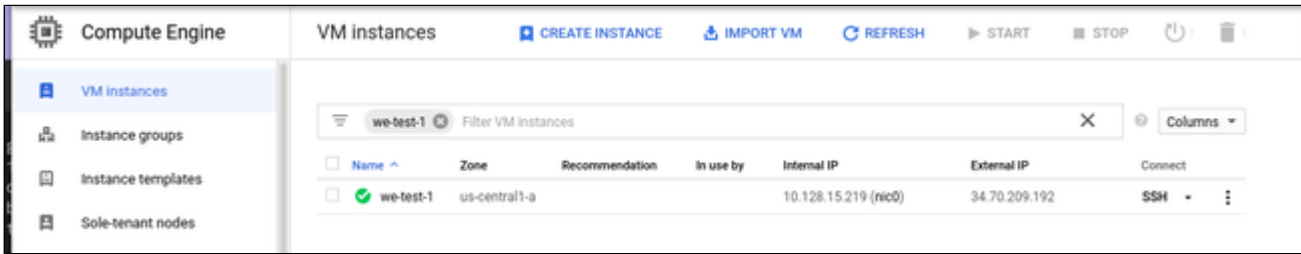
By clicking on it, you will see the details of the cloud instance, as shown in the example below:

Initial Access to the Instance

Once you have access to the instance, you can create the access you require for your applications. This section just shows the basic steps for initial access to the instance.

SSH Interactive Access

To connect to the instance interactively, you must connect as the management user of your instance. Use the following command:

$ ssh -o ServerAliveInterval=30 -i *<path-to-your-private-key>* *<management-user-name>*@*<cloudhost-IP-address>*

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

Please note:

- Depending on the type of connection, you will have to use either the public IP address of the cloud system or its address in a customer-specific VPN.
- The management user account normally allows sudo access to privileged commands (use **sudo -i**).

File Transfer with SFTP

SFTP enables file transfers to and from the cloud instance. Use the management user of your instance. The security rules must allow SSH access to allow SFTP access to the cloud instance.

Please note: Depending on the type of connection, you will have to use either the public IP address of the cloud system or its address in a customer-specific VPN.

To connect to the instance, use the following command:

$ sftp -i *<path-to-your-private-key>* *<management-user>*@*<cloudhost-IP-address>*

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 cloud host. Therefore, the Charon-SSP Manager must be installed on every system that will be used to manage the Charon instances running on the Charon-SSP cloud host. Configuring and managing Charon-SSP instances from the command-line is also possible, but outside the scope of this Getting Started Guide. Please refer to the general Charon-SSP User's Guide for information about using the command-line.

Typically, the Charon Manager is installed on a system on customer premises and used via an encrypted connection to manage the Charon host in the cloud. The Charon Manager can also be installed on the Charon host itself and the be accessed via X11-Forwarding across an SSH connection. The latter currently requires additional package installation (via standard or local repository) on the Charon host.

Stromasys provides Charon-SSP Manager installation packages for the following operating systems:

- **Linux distributions and versions**:
    - Oracle Linux, Red Hat Enterprise Linux, and CentOS: 7.x or higher (64-bit versions only)
    - Ubuntu 17 or higher (64-bit)
- **Microsoft Windows:** versions 7, 8, and 10

Installation Packages

Installation packages are available in RPM or Debian package formats for Linux and as a ZIP-file for Microsoft Windows:

- RPM package: **charon-manager-ssp-**<version>**.rpm**
- Ubuntu package: **charon-manager-ssp-**<version>**.deb**
- Microsoft Windows package: **charon-manager-ssp-**<version>**.zip**

There are different ways to obtain the Charon-SSP Manager installation packages. They are briefly described below:

a) For installation on a management system on customer premises if using a prepackaged marketplace image:

The packages are included in the Charon-SSP cloud-specific image. Once a new instance has been launched, you can download the Charon-SSP Manager packages from the running instance:

- Connect to the public IP address of the instance via SFTP using the private key assigned during launch and the user **charon**:
  `$ sftp -i <path-to-private-key> charon@<public-ip-of-cloud-instance>`
- Download the required package:
  `sftp> get charon-manager-ssp-<version>.[rpm | deb | zip]`

b) For installation on the Charon host in the cloud if using a prepackaged marketplace image: the packages are located in the */charon/storage/* directory.

c) For installation on a Charon host in the cloud where a conventional RPM installation was performed: the packages can be downloaded from a Stromasys server.

Charon-Manager Installation on Linux

Prerequisites

When the Charon Manager is installed on a Linux host with a graphical user environment, the prerequisites are often already fulfilled. However, when installing the Charon Manager on the Charon-SSP host in the cloud or on a Linux server without graphics (for example to display it via a remote X11-connection) instead of on a local management system, additional packages may have to be installed that normally are already available in a workstation environment.

In particular, the Charon-SSP Manager requires the following packages:

- libX11
- xorg-x11-server-utils
- gtk2
- xorg-x11-xauth (only required for X11-Forwarding)

If you install the Charon Manager with the **yum** command, these packages (with the exception of xorg-x11-xauth) and any dependencies that these packages themselves may have, are resolved automatically if a package repository is available. The xorg-x11-xauth package must be installed separately (also with yum). If your server does not have access to the standard operating system repositories, refer to this document for instructions on setting up a local repositories.

Please note:

- The exact list of additionally required packages depends on what is already installed on the server.
- To install dependencies on Ubuntu, please refer to your Linux documentation.

Installation Steps on Linux

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

Step	Description
1	Installation on a Linux management system on customer premises (typical installation): • Log in to the Linux management system as the **root** user (denoted by the **#** prompt). • Copy the installation package to your local Linux management system (as described above). Installation on the Charon-SSP host system in the cloud (optional): • Log in and become the root user on the Charon host in the cloud using the following commands: **$ ssh -i** *<path-to-private-key>* **sshuser@***<ip-address-of-cloud-instance>* **# sudo -i** • **Please note:** if the Charon host was not installed using a prepackaged marketplace image, the username may be different and the installation package will have to be copied to the Charon host in a separate step.
2	Go to the directory where the package has been stored: **# cd** *<package-location>*
3	**Installing the package:**
	For systems with RPM package management (Red Hat, CentOS, Oracle Linux): **# yum install** *<filename-of-package>* (For an installation on the cloud host system, check if xorg-x11-xauth is already installed if X11-Forwarding is planned.)
	For systems with Debian package management (Ubuntu): **# dpkg -i** *<filename-of-package>*

Example (RPM installation with yum command recursively resolving package dependencies):

```
# yum install charon-manager-ssp*.rpm
Loaded plugins: fastestmirror, langpacks
Examining charon-manager-ssp-4.2.5.rpm: charon-manager-ssp-4.2.5-1.x86_64
Marking charon-manager-ssp-4.2.5.rpm to be installed
Resolving Dependencies
--> Running transaction check
---> Package charon-manager-ssp.x86_64 0:4.2.5-1 will be installed

<lines removed>

Dependencies Resolved

================================================================================
 Package               Arch    Version        Repository            Size
================================================================================
Installing:
 charon-manager-ssp    x86_64 4.2.5-1      /charon-manager-ssp-4.2.5  5.8 M
Installing for dependencies:

<lines removed>

Transaction Summary
================================================================================
Install  1 Package (+42 Dependent packages)

Total size: 14 M
Total download size: 9.5 M
Installed size: 37 M
Is this ok [y/d/N]: y
Downloading packages:

< lines removed >

Running transaction check
Running transaction test
Transaction test succeeded
Running transaction

< lines removed >

Installed:
  charon-manager-ssp.x86_64 0:4.2.5-1

Dependency Installed:
  atk.x86_64 0:2.28.1-1.el7
  cairo.x86_64 0:1.15.12-4.el7
  dejavu-fonts-common.noarch 0:2.33-6.el7
  dejavu-sans-fonts.noarch 0:2.33-6.el7

<lines removed>

  xorg-x11-server-utils.x86_64 0:7.7-20.el7

Complete!
```

Installation Steps on Microsoft Windows

The Charon-SSP Manager for Windows software is shipped as a zipped archive package. To complete the installation, use the following instructions.

1. **Right-click** on the zip archive charon-manager-ssp-{version}.zip and select **Extract All**.
2. A window titled **Extract Compressed (Zipped) Folders** opens. In this window:
    a. Click on the **Show extracted files when complete** checkbox.
    b. Click on the **Extract** button.
3. A new Windows Explorer window opens showing the extracted packages.
4. **Double-click** on the **setup.exe** executable to begin the installation.
5. If you are presented with an **Open File - Security Warning** window, click on the **Run** button.
6. You should now see the Charon-SSP Manager Setup Wizard. To proceed with the installation, click on the **Next** button. If the Windows Installer reports that Charon-SSP Manager for Windows is already installed, you must deinstall the currently installed software before you can install a different version. Normally, several versions can coexist.
7. To accept the default installation options, simply click on **Next** without modifying any options. Alternatively, the following installation options can be adjusted:
    a. Click on **Browse** to select an alternative installation target.
    b. Click the appropriate radio button, **Everyone** or **Just for Me**, to specify system-wide or private installation respectively (the system-wide installation will prompt for the administrator password if you are not using the administrator account).
    c. To determine the approximate disk usage after the installation, click on the **Disk Cost** button.
    d. Once all options have been set, click on **Next**.
8. Proceed with the installation by clicking on **Next**.
9. Once the installation has completed, click on **Close** to exit the SSP-Manager Setup Wizard.
10. The installation process creates:
    a. A Charon Manager icon on the desktop
    b. A Charon Manager entry in the Start menu (folder Stromasys)

Starting the Charon-SSP Manager

Contents

General Information

To use the management GUI for Charon-SSP and the emulated SPARC systems, you must connect to the Charon-SSP cloud instance with the Charon-SSP Manager. The Charon-SSP Manager is the main interface to all important functions of the Charon-SSP software. Managing Charon-SSP via the command-line is possible but outside the scope of this document (please refer to the user's guide of the conventional product for more information).

Prerequisites:

- Typically, **Charon-SSP Manager** is installed on a system on customer premises. **This is the use-case described in this section**. Other configurations are possible. For example, the Charon Manager could be installed on the Charon host itself and be displayed on a remote system using X11-Forwarding via an SSH connection.
- **For access via the public IP address of the Charon host instance**:
    - The **security configuration** on your Charon host instance 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 additional ports. However, if the connection runs over the Internet without a general 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 host instance in the cloud. To determine this address, refer to the instance information displayed on the cloud management console.
    - 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 or another VPN solution**:
    - Active SSH-based VPN (see *SSH VPN - Connecting Charon Host and Guest to Customer Network* in the Charon-SSP User's Guide) or other active VPN solution
    - Private IP address of the Charon-SSP host in the VPN

Information about the initial management password configuration:
Before connecting to the Charon-SSP host in the cloud with the Charon Manager for the first time after the initial installation you must set the 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 on Linux and to open the Charon Manager login window, use the following command:

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

To start the Charon-SSP Manager on Microsoft Windows, click on the Desktop icon or use the entry in the Start menu.

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

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

- Enter the public IP address or the private VPN IP address of your Charon-SSP host instance in the **IP address** field.
- Leave the **Password** field empty.
- Enable the SSH tunnel configuration (select **ON**) unless connected to localhost.
- 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 in the **IP address** field.
- 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
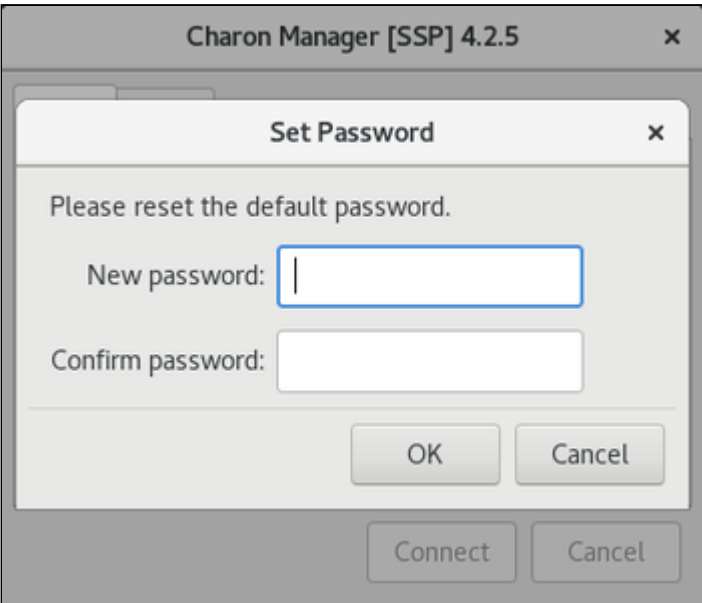
If you use the integrated SSH tunnel, perform the following steps:

- Enter the Charon-SSP user in the **Username** field. For prepackaged images, use **charon** or **sshuser**; for RPM installations use the user for whom the correct public key has been installed.
- Enter the path to the private key file (click on the three dots next to the **Private key** field to open a file browser). You typically associated your cloud instance with this key-pair during instance creation.
- Enter the passphrase for the private key if required.
- Adjust the server port (default 22) if required.

Please note: the public key of the key-pair must be in the `.ssh /authorized_keys` file of the user entered above (**sshuser** and **charon** for prepackaged images).
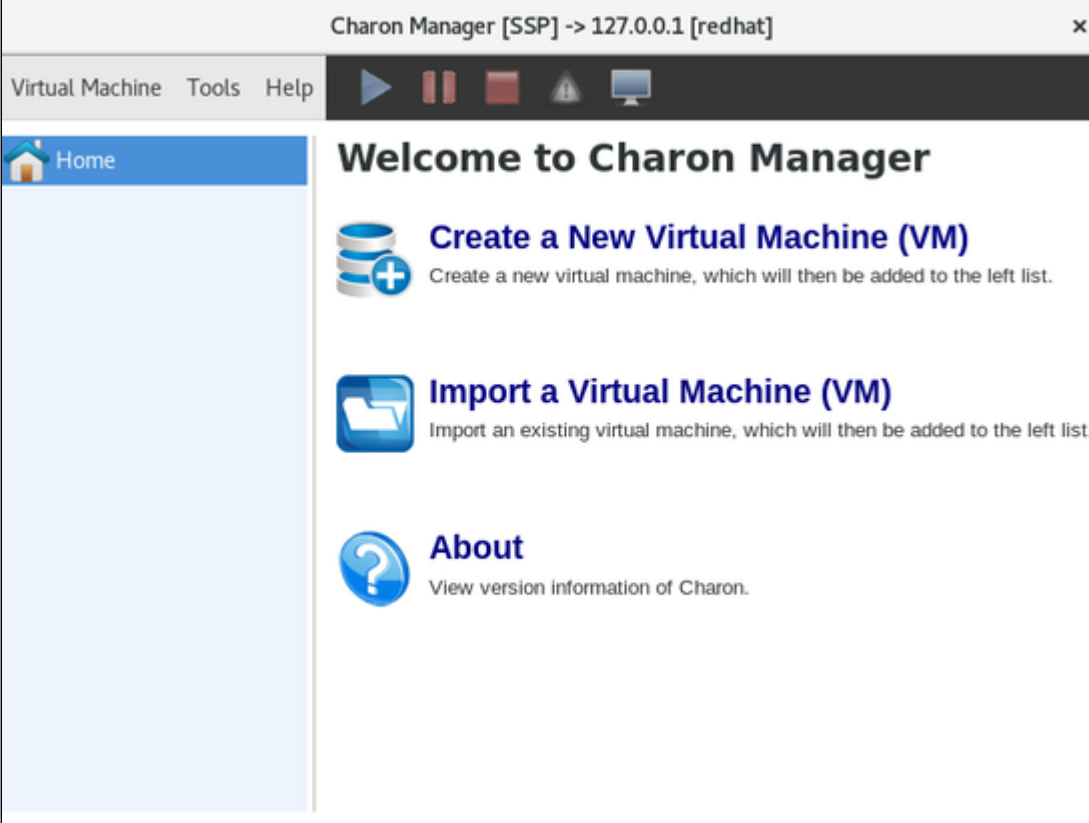
Step 3: connecting to the Charon host system

After entering all the required information, click on **Connect** to connect to the Charon-SSP instance. **If the management password still needs to be set,** you will receive a prompt to enter the new password:

- Enter the desired password in the **New password** field and confirm it in the **Confirm password** field.
- Then click on **OK**.
- The login process continues.

After a connection has been successfully created, the Charon Manager welcome screen opens. Example of the Charon Manager welcome page:

Please note: the **title bar** of this screen indicates the managed system type in square brackets (conventional Red Hat installation in the example).

Cloud-Specific Firewall Information

Contents

OCI Firewall Information

Access to an OCI cloud instance can be controlled by

- an external firewall,
- the operating system firewall of the instance (see Installing the VE License Server and the Charon-SSP Packages),
- security list of the subnet to which the instance belongs, and
- VNIC-specific Network Security Groups.

The different firewall levels must be configured to permit at least TCP port 8083 to enable a license client to access a VE license server. If the web interface is to be used, TCP port 8084 must also be allowed.

Security Lists

Security lists form the original type of virtual firewall offered by the Oracle cloud network service.

A security list acts as a virtual firewall for an instance. It has ingress and egress rules that specify the types of traffic allowed in and out. Security lists are defined **at the subnet level**. Therefore, all VNICs in a given subnet are subject to the same set of security lists.

You can associate multiple security lists with a subnet. Each list can have multiple rules. Traffic is allowed if **any rule in any of the lists** allows the traffic. Traffic is also allowed if it is the response traffic of a permitted tracked connection.

If you don't specify one or more other security lists during the creation of a subnet, a default security list will be associated with it.

Please see the relevant Oracle documentation for more information and configuration details.

Network Security Groups

Network Security Groups (or NSGs) form another type of virtual firewall. Unlike a security list, an NSG does not apply to all VNICs in a subnet, but is assigned to specific VNICs connected to the subnet. This allows a more granular access control. By default, no NSG is assigned to a VNIC.

Please see the relevant Oracle documentation for more information and configuration detail.

Please note: Traffic is allowed if **any rule in any of the relevant lists and groups** allows the traffic. Traffic is also allowed if it is the response traffic of a permitted tracked connection. In addition to allowing SSH access, at least TCP port 8083 must be allowed to enable a license client to access a VE license server. If the web interface is to be used, TCP port 8084 must also be allowed.

AWS Firewall Information

Access to an AWS cloud instance can be controlled by

- an external firewall,
- the operating system firewall of the instance,
- AWS security groups, and
- AWS network ACLs.

In addition to allowing SSH access, the different firewall levels must be configured to permit at least TCP port 8083 to enable a license client to access a VE license server. If the web interface is to be used, TCP port 8084 must also be allowed.

Network ACLs

A network ACL applies to a subnet as a whole. Only one network ACL per subnet is allowed. The rules in a network ACL are stateless (i.e., return traffic must be explicitly allowed). Rules are evaluated starting from the lowest rule number. After the first match the search is terminated.

Please note: Security groups cannot allow more than what is permitted in a Network ACL.

Security Groups

A security group can be seen as a virtual firewall that controls the traffic for one or more instances. When you launch an instance, you must assign a security group to the instance. If no custom security group is specified, a default security group will be created and associated with the instance. You can add rules to each security group that allow traffic to or from its associated instances. The rules of a security group can be modified at any time, and the modifications are automatically applied to all instances that are associated with the security group. If there is more than one security group associated with an instance, the rules of all groups are combined.

Security groups in a VPC are associated with network interfaces. Changing an instance's security groups changes the security groups associated with the primary network interface (eth0). Additional security groups can associated with any other network interfaces added to an instance.

Points to note:

- By default, all outbound traffic is allowed.
- Rules in a security group always define what is permitted. They cannot be used to deny specific traffic.
- Response traffic to traffic that was permitted by a rule is always allowed (connection tracking).

Please see the relevant AWS documentation for more information and configuration details.

Azure Firewall Information

Access to an Azure cloud instance can be controlled by

- an external firewall,
- the operating system firewall of the instance,
- Azure Network Security Groups (NSGs).

In addition to allowing SSH access, the different firewall levels must be configured to permit at least TCP port 8083 to enable a license client to access a VE license server. If the web interface is to be used, TCP port 8084 must also be allowed.

Network Security Groups

Network Security Groups can be associated to interfaces or subnets. Security rules in network security groups enable you to filter the type of network traffic that can flow in and out of virtual network subnets and network interfaces. When a cloud instance is created, you can assign a default security group to its interface (allowing SSH). Please refer to the following tutorial for more information: https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic.

GCP Firewall Information

Access to an GCP cloud instance can be controlled by

- an external firewall,
- the operating system firewall of the instance,
- GCP Firewall

In addition to allowing SSH access, the different firewall levels must be configured to permit at least TCP port 8083 to enable a license client to access a VE license server. If the web interface is to be used, TCP port 8084 must also be allowed.

Google Cloud Firewall Rules

In addition to firewall rules created by the customer, there are other rules that can affect incoming or outgoing traffic:

- Certain IP protocols, such as GRE, are not allowed within a VPC network. For more information, see always blocked traffic.
- Communication between a VM instance and its corresponding metadata server (`169.254.169.254`). Is always allowed.
- Every network has two implied firewall rules that permit outgoing connections and block incoming connections. Firewall rules that you create can override these implied rules.
- The default network is pre-populated with firewall rules that can be deleted or modified.

VPC firewall rule characteristics:

- Each rule is either for incoming or outgoing traffic. It can allow or deny traffic.
- Only IPv4 traffic is supported.
- Firewall rules are stateful (return traffic for an established connection is allowed).
- If TCP traffic is fragmented, a rule is only applied to the first fragment of a packet.