Charon Virtual Environment (VE) License Server 2.2 to 2.4 User's Guide

Applicable to product versions v2.1.3 and higher

Contents

About this Guide

Contents

Introduction

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

VE stands for "Virtual Environment" denoting Charon emulators and the environment in which they run. At the time of writing, the VE license server is supported in selected cloud and VMware environments, and on physical servers.

A VE license server can run in one of **two basic modes of operation**:

- **General VE license server mode**: license server for one or more emulator instances. Customers must purchase their license from Stromasys, and use a VE-enabled emulator product. The license is based on number of emulator instances and the emulator model configuration required, and typically valid for a certain period of time (it has an expiration date), or for a defined number of runtime hours.
- **AutoVE mode (selected cloud environments only)**: AutoVE is an extension of the cloud-specific Charon Automatic Licensing (AL) where licensing is configured automatically when the cloud instance is launched. The Charon host instance must be launched from a **supported, cloud-specific marketplace image**. The customer is billed by the cloud provider per instance launched, but the AutoVE license server is managed by the customer and part of the customer cloud environment.

This guide covers the **Charon VE License Server** software**.** This package contains a license server application that can be installed in customer-specific AWS, OCI, GCP, Azure, IBM, Nutanix and VMware environments, and on physical servers. This licensing option is adapted to the special requirements of virtualized environments and simplifies the process of running Charon emulator products in supported cloud and VMware environments. The license server is managed by the customer.

Please note:

- VE licenses provided by a VE license server require **VE-enabled Charon emulator software**. This support is available in the following products:
  - Charon-SSP (starting with Charon-SSP version 4.2.x)
  - Charon-PAR (starting with Charon-PAR version 3.0.6 and VE license server version 1.1.19)
  - Charon-AXP/VAX (planned to start with version 4.12 - Linux versions only!)
- At the time of writing, **AutoVE mode** was available for the following products:
  - VE license server starting with 1.1.21
  - Charon-SSP AL marketplace images version 5.3.8 and above in selected cloud environments. Please check with your Stromasys representative for availability details of Charon-SSP AL images in your cloud environment.
- Starting with VE license server version 2.1.3, a new certificate and user configurable certificates for the communication between license server and license client (emulator host) were introduced. Using this new feature requires a matching version of the Charon emulator product. At the time of writing, this feature was supported by Charon-SSP version 5.5.5 and higher. Please refer to the release notes of your product and to Certificates Used by the VE License Server for more information.
- For a full description of the Charon emulator product configuration and management aspects that are not related to the specifics of the VE license application**, please refer to the Charon user's guides of you product and version**:
  - Charon-SSP: see the Charon-SSP user's guides.
  - Charon-PAR: see the Charon-PAR user's guides.
  - Charon-AXP/VAX: see the Charon-AXP and the Charon-VAX guides.

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 VE License Server Topology: brief overview of license server topologies.
- Installing VE License Server and Charon Emulator: installation of the license server software, and installation of the VE-enabled Charon emulator software.
- Installing a License on the VE License Server: steps for requesting and installing a Charon product license on the license server.
- Configuring a Charon Emulator for a VE License Server: steps for configuring the Charon emulator to use the VE license server.
- Transferring a License to Another Server: move a license from one license server to another.
- Removing a License from a VE License Server: removing a license from a license server.
- Additional Configuration Options - the config.ini File: additional configuration options to customize communication ports.
- Certificates Used by the VE License Server: description of the different scenarios of using and configuring the certificates used between license server and license clients.
- VE License Server Web-based Management GUI: description of the interface and the actions provided by the web-based GUI of 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.
- VE License Server Software Upgrade, VE License Server Software Deinstallation: steps to upgrade or uninstall the VE license server software.
- VE License Server Command-Line Utilities: summary of the available command-line utilities with their options.
- Additional Information: supplemental information about installing a Linux cloud instance, about installing and starting the Charon-SSP 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 y ou 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
Americas	+1 919 239 8450	Stromasys LLC 871 Marlborough Ave, suite 100, Riverside CA 92507 USA
Europe, Middle-East and Africa	+41 22 794 1070	Avenue Louis-Casai 84 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-PAR User's Guides and Release Notes
- Charon-AXP and Charon-VAX User's Guide and Release Notes
- VE license server release notes in Virtual Environment (VE) License Server Documentation

Charon Licensing Overview

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

Contents

Charon VE Licenses

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

- Software licenses only.
- Developed by Stromasys.
- Installed on the Charon host or a separate license server.
- Require the Charon VE license server software.
- Require matching VE-capable Charon emulator software.
- Different modes of operation:
  - For **general VE mode**, the customer is billed by Stromasys depending on the number and type of the emulated systems allowed by the installed license(s). The license server software itself is free of charge.
  - **AutoVE mode** is an extension of automatic licensing and introduces metered billing (by the cloud-provider) for VE licenses in cloud environment. It defines how many Charon emulator cloud instances can be run based on the respective license. The number of emulated systems on each host instance is limited by the host resources, not the license.
  - The license server for both modes is managed by the customer.
- Support at the time of writing:
  - **VE license server availability**: supported clouds (at the time of writing: AWS, OCI, Azure, GCP, IBM, and Nutanix), supported VMware environments, and physical servers.
  - **AutoVE support**:
    - VE License server starting with version 1.1.21.
    - Charon-SSP AL (Automatic Licensing) marketplace images version 5.3.8 or higher in selected clouds. Please contact your Stromasys representative for availability details in your cloud environment.
  - **Charon emulator product support**: Charon-SSP and Charon-PAR (starting with Charon-PAR version 3.0.6 and VE license server version 1.1.19). Support for Charon-AXP/VAX is planned starting with version 4.12.

The present document describes the use of Virtual Environment 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 host or separate license server.
- Problematic in cloud environments and somewhat difficult to use in VMware environments.
- Dongles are a flexible and host-hardware independent solution for on-premises installations (as long as there is a free USB port).
- The customer is billed by Stromasys depending on the number and type of the emulated systems allowed by the installed license(s). The license driver software itself is free of charge.

Please refer to the Charon License Handbook (Licensing Documentation) 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, 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. The customer is billed by the cloud provider depending on the type, configuration, and active use of the Charon host instance. See also **AutoVE** mode which allows a customer to run their own license server for an instance launched from such a marketplace image. Please contact your Stromasys representative for availability details in your cloud environment

Rationale for VE Licenses

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

- USB dongles are 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 not suited for use in cloud environments and difficult to use in VMware environments. Other Sentinel software license types do not provide the same level of license security.
- Cloud-based automatic licensing (without AutoVE) does not allow a customer-specific environment in the cloud without access to the public Internet. This is not suitable for many customers who require a private cloud network environment complying with their own security and management policies.

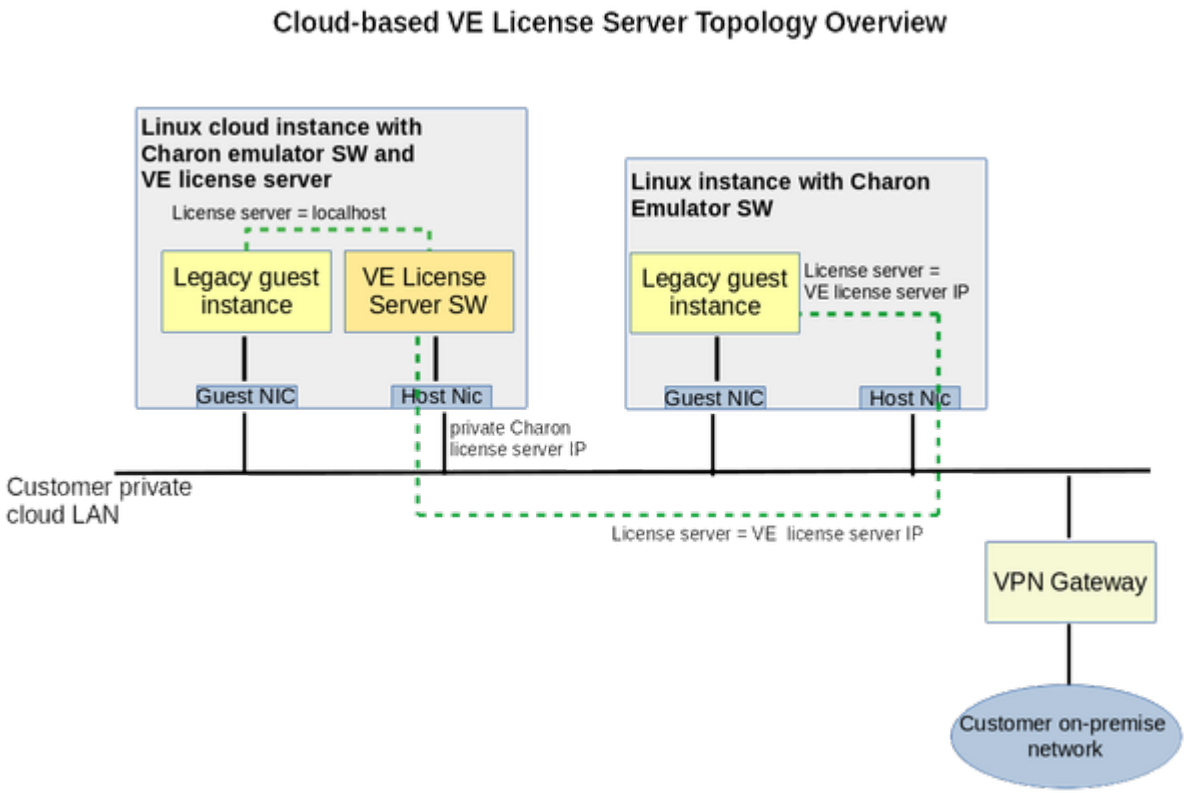
VE licenses are designed to enable the ease-of-use of software licenses while providing a high level of security for licensing Charon products in virtualized environments.

Charon VE License Server Topology

Contents

Cloud-based VE License Server Overview

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



Points to note:

- The license server software can be combined with the Charon emulator software on one instance, or it can run on a separate system. However, it is recommended to run the VE license server on a **dedicated system** to avoid license invalidation caused by changes to the system which are more likely to occur on a system used for other purposes as well, for example, to run a Charon emulator. It is also recommended to install a backup license server to ensure continued operation in case of a failure or invalidation of the primary license.
- The license server typically is installed in the same cloud environment.
- Charon host and license server do not need a public IP address. They communicate across the cloud-internal LAN environment.
- Starting with Charon-SSP version 4.1.19, and with Charon-PAR and Charon-AXP/VAX from initial VE support, a backup license server has been supported.
- Important points for **AutoVE deployments**:
  - The AutoVE license server address must be configured prior to the first launch of the instance from a supported AL marketplace image. Otherwise, the public license servers will be used.
  - License server and Charon host must be in the same cloud environment.

VMware-based VE License Server Overview

The following images provides an overview of sample VE license server topologies in a VMware environment.

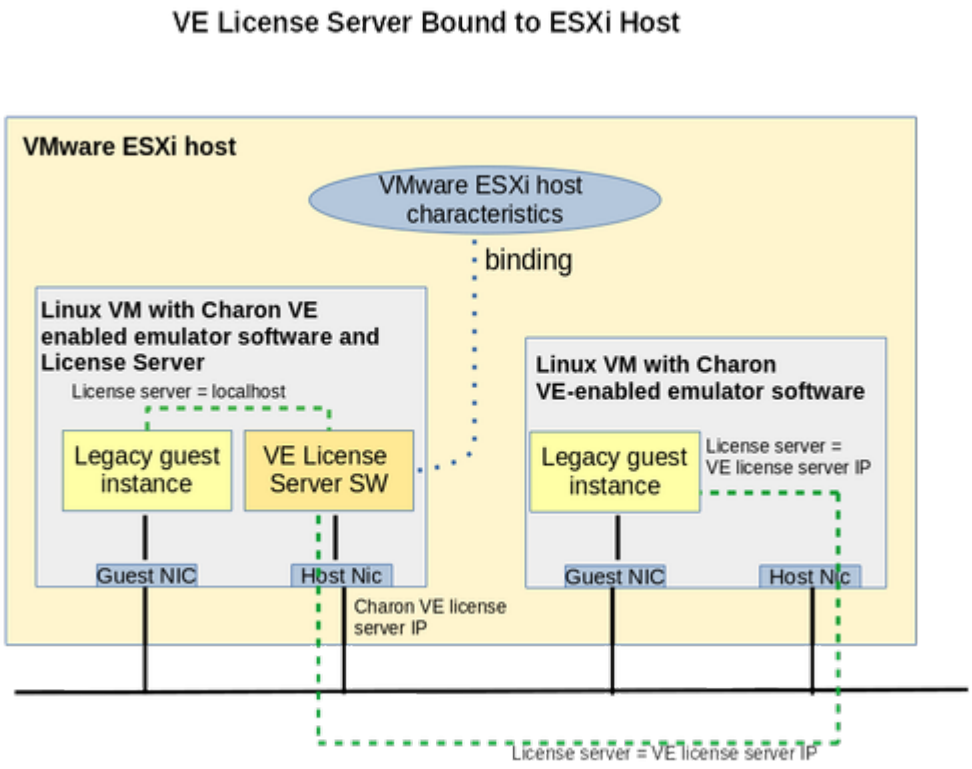
There are two basic options:

1. **The license server binds to the ESXi host** on which the license server VM runs. In this case, any Charon emulator using the VE license server must run either on the same VM as the VE license server or on a VM running on the same ESXi host.
2. **The license server binds to the vCenter Server** that manages the ESXi host on which the license server VM runs. In this case, any Charon emulator using the VE license server must run either on the same VM as the VE license server or on a VM on an ESXi host managed by the same vCenter Server.

Please note: each VE license server instance can only **bind to one ESXi host or one vCenter server**. For example, if a license server is needed in two separate vCenter installations, at least two license server instances are required.

VE License Server Binding with ESXi Host

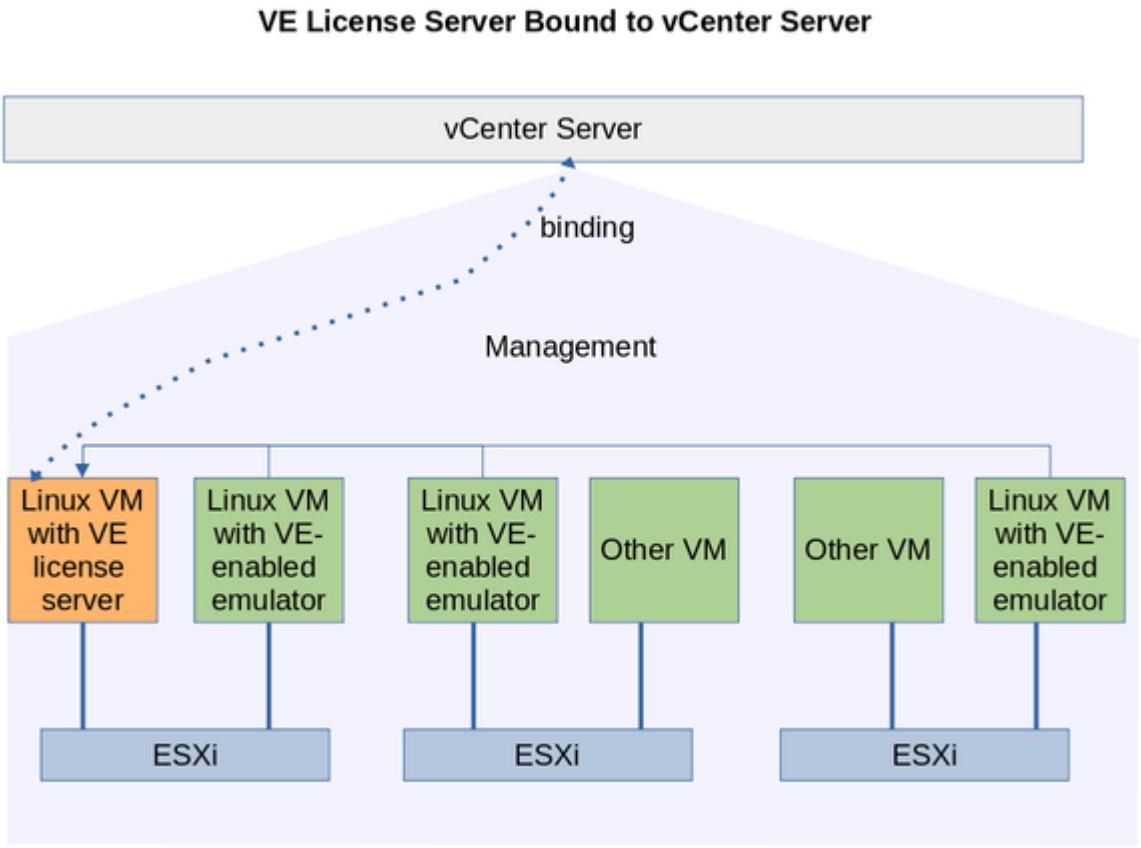
The following image illustrates a topology where the VE license server binds to the ESXi host on which the VM with the license server runs. It shows one VM with license server and emulator software, and another VM on the same ESXi host with the emulator software configured to use the license server via the network.



Please note: vMotion of a VE license server VM to a different ESXi server is only possible if binding to a vCenter Server (see below) is used. vMotion of a license server VM when binding to the ESXi server will invalidate the installed licenses.

VE License Server Binding with vCenter Server

The following image illustrates a topology where the VE license server binds to the vCenter Server managing the ESXi host on which the VM with the license server runs. It shows one VM with license server and several other VMs on ESXi hosts managed by the same vCenter Server using the license server across the network.



Please note: vMotion of a VE license server VM to a different ESXi server is possible if the target server is managed by the same vCenter Server.

Installing VE License Server and Charon Emulator

Contents

VE License Server - Prerequisites

The use of a Charon VE License Server has a number of prerequisites:

1. The **VE license server itself**
   a. VE license server package
   b. A suitable Linux instance to be used as the VE license server. This instance must run
      i. in a supported cloud environment,
      ii. in a supported VMware environment, or
      iii. on a supported physical server.
2. Correct **firewall settings**
3. The **VE-capable Charon emulator software**
   a. For general VE mode: must run on a Charon host with appropriate network access to the VE license server (see restrictions for VMware environments in the section *Charon VE-Capable Emulator and Management Software* below).
   b. For AutoVE mode: a Charon instance launched from a compatible Automatic Licensing marketplace image. AutoVE server and clients must be in the same cloud environment. Please note that the AutoVE definitions must be added before the first launch of such an instance.

These requirements are described in more detail below.

VE License Server Package

The Charon 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. If an instance is created based on a Stromasys-provided emulator marketplace images, the installation kit is in the */charon/storage* directory.

The packaging is different based on the VE license server version:

- VE license server version 2.2.3 and older: **`license-server-`**<*`version`*>**`.rpm`**
  RPM package for installation on a supported Linux system.
- VE license server version 2.2.4 and higher: **`license-server-`**<*`version`*>**`.rpm.sh`**
  Self-extracting archive containing the end-user license agreement (EULA) and the RPM package.

In both cases <*version*> indicates the version of the software, for example, 2.2.1

Linux Instance for the License Server

The license server package must be installed on a supported Linux instance. This instance can run in a supported cloud, in a supported VMware environment, or on a physical host. It is recommended to run the VE license server on a **dedicated system** to avoid license invalidation caused by changes to the system which are more likely to occur on a system used for other purposes as well, for example, to run a Charon emulator. It is also recommended to install a backup license server to ensure continued operation in case of a failure or invalidation of the primary license.

Currently Supported Cloud Providers

At the time of writing, the following cloud providers are supported by the VE license server:

- Amazon AWS
- Oracle Cloud Infrastructure (OCI)
- Microsoft Azure
- Google Cloud Platform (GCP)
- IBM cloud
- Nutanix AHV

Please refer to your cloud provider's documentation for configuring and launching an appropriate instance. A description of the basic steps of launching a cloud instance can be found in Additional Information and the cloud-specific Getting Started guides on the Charon-SSP documentation pages.

Depending on the cloud environment, Stromasys may offer prepackaged Charon VE images on selected cloud marketplaces. Such images include the Charon VE-enabled emulator software (already installed) and the VE License Server RPM package (can be installed optionally). An instance launched from a prepackaged image can also be used as a VE license server. Newer versions of Charon-SSP AL marketplace images also contain the VE License Server RPM that can be installed optionally.

Currently Supported VMware Platforms and Requirements

Below are the VMware Platforms supported by the VE license server at the time of writing, and the associated requirements:

Requirements for direct ESXi host binding

- The VE license server must run **in one of the VMs on the ESXi serve**r.
- Any Charon emulator using the VE license server must run either **on the same VM as the VE license server or on a VM running on the same ESXi host**.
- ESXi/vSphere version 6.5 and above.
- Valid license that supports the **vSphere API** feature (the free license does not support this feature). Otherwise the license server fails to start with one of the following messages
  - **Older license server versions:** *Failed to detect ESXi/vCenter Server*
  - **Newer license server versions**: *Current license or ESXi version prohibits execution of the requested operation*
- Ports **443** (TCP) and **902** (TCP, UDP) on the ESXi system must be accessible to the VE license server host.
- 100 MB of free disk space on the ESXi server to be used by the VE license server host.
- User and password on the ESXi/vSphere host used for the binding between license server and ESXi/vSphere host.

The user used in the esxi_bind command must have at least the following **permissions** that are assigned via a **custom role** definition (**please note** that the permission paths/names can be slightly different depending on the vSphere version). **The permissions must not be limited to a specific VM - they must be global**:

- Datastore > Allocate Space
- VirtualMachine > Config > AddNewDisk
- VirtualMachine > Config > RemoveDisk

Requirements for vCenter Server binding

- The VE license server must run in a VM on one of the ESXi systems managed by the vCenter Server.
- Any Charon emulator using the VE license server must run either **on the same VM as the VE license server or on a VM on an ESXi host managed by the same vCenter Server**.
- vCenter Server version 6.5 and above.
- Valid license that supports the **vSphere API** feature. Otherwise the license server fails to start with the message **Failed to detect ESXi/vCenter Server**.
- Ports **443** (TCP) and **902** (TCP, UDP) on the vCenter system must be accessible to the VE license server host.
- 100 MB of free disk space on the vCenter Server to be used by the VE license server host.
- User and password on the vCenter Server used for the binding between license server and vCenter Server.

The user used in the esxi_bind command must have at least the following **permissions** that are assigned via a **custom role** definition (**please note** that the permission paths/names can be slightly different depending on the vSphere version). **The permissions must not be limited to a specific VM - they must be global**:

- Datastore > Allocate Space
- VirtualMachine > Config > AddNewDisk
- VirtualMachine > Config > RemoveDisk

Please note: vMotion for the virtual machine running the VE license server **can only be used** if the license server binds to the vCenter Server. The target system must be managed by the same vCenter Server.

The VE license server for VMware environments has also been tested successfully in a Google GCVE (Google Cloud VMware Engine) environment. Please contact Stromasys to discuss your requirements if you need this product combination.

Currently Supported Physical Servers

At the time of writing, the following physical platforms are supported by the VE license server:

- Modern Intel x86 or AMD platform with sufficient resources for the required Linux operating system

Linux Host Requirements for the VE License Server

The Linux system on which the VE license server runs must fulfill the requirements described below.

Please note: the VE license server software can run on the same system as the Charon emulator. However, using a **dedicated system** with stable hardware and software configuration as the VE license server is the recommended configuration. This will reduce the risk of invalidating the license by a non-supported hardware or software change. Please see Operational Information and Logging for more information about such changes and also about the operation of a backup license server to ensure continued operation of critical applications.

Linux Host Hardware and Software Requirements

Operating System Requirements for the VE License Server

- Red Hat, CentOS, or Oracle Linux (64-bit) versions 7.x or 8.x
- Rocky Linux 8.x
- Red Hat, Oracle Linux, and Rocky Linux 9.x
- Support for Amazon Linux 2023 is planned to start with VE license server version 2.4.1.

Only 64-bit operating systems are supported.

Other Software Requirements for the VE License Server

Please note the following additional requirements:

- The Btrfs file system is **not supported** as a root file system for a VE license server.
- To unpack the shell archive containing the installation kit, the following utilities are required: **gzip**, **md5sum**, **cksum**, **gpg**, **tar**, and **openssl**

Hardware Requirements for the VE license server

Dedicated System for the License Server (recommended)

If the system is dedicated to running the license server, its hardware configuration must satisfy the requirements of the selected Linux operating system.

License Server Combined with Charon Emulator Software (not recommended)

If the license server is combined with the Charon emulator software on the same instance, the instance used must satisfy the requirements of the Charon emulator host and all instances that will run on it. Please refer to your product-specific documentation for more information:

- For **Charon-SSP**, refer to the Charon-SSP user's guide of your emulator version for details (see Charon-SSP for Linux).
- For **Charon-PAR**, refer to the Charon-PAR user's guide of your emulator version for details (see Charon-PAR documentation).
- For **Charon-AXP/VAX**, refer to the user's guides for Charon-AXP or Charon-VAX.

Please note, that a dedicated license server system is the recommended configuration.

Additional Linux Host Requirements for AWS cloud

VE License Server Installation on Amazon Linux 2023

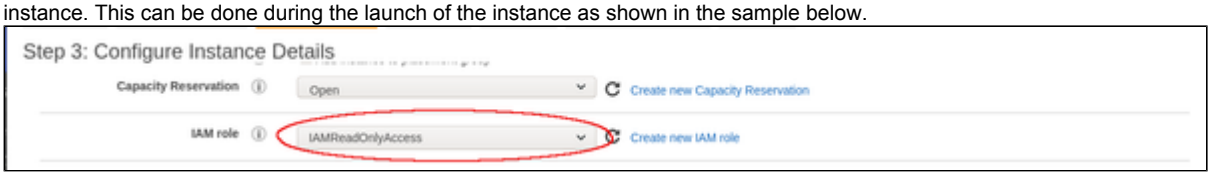
Only for VE license server 2.4.1 and higher (older versions are not supported to be run on Amazon Linux).

By default, Amazon Linux only installs a minimal **gnupg** package. This is not sufficient to unpack the VE license server kits archive. An attempt to unpack the archive will result in the error *gpg: uncompressing failed: Unknown compression algorithm*. To swap the minimal for the full package, use the following command:

```
# dnf swap gnupg2-minimal gnupg2-full
```

VE license server versions earlier than 1.1.23 only - IAM role requirement

In the AWS cloud, an IAM role allowing the ***ListUsers*** action (IAMReadOnlyAccess in the example below) must be attached to the VE license server 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 (versions < 1.1.23 only) and to the documentation provided by AWS for additional information.

Additional Linux Host Requirements for IBM cloud

For the VE license server to work properly in the IBM cloud, an API key must be created and installed. Please refer to Creating and Installing an IBM API Key.

Firewall Considerations

Communication Between License Server and Client Systems

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

- **Basic license operation**
  The TCP port that is used by the license client to access the license must be permitted on the license server, and by any intermediate firewall.
  Default: **TCP/8083**; an alternative port can be configured in */opt/license-server/config.ini*.
- **Access to license server web interface**
  - The TCP port used by remote systems to web-based management interface must be permitted on the license server, and by any intermediate firewall.
    Default: **TCP/8084**; an alternative port can be configured in */opt/license-server/config.ini*.
  - **TCP port 80** must be available to the license server to redirect HTTP requests to HTTPS. For remote connections, the port must also be permitted through intermediate firewalls. Starting with version 1.1.25, redirection (and thereby use of TCP port 80) can be enabled or disabled in */opt/license-server/config.ini*.
  - **Important**: at the time of writing, the web-server component of the license server applications will not start if a port required by the web server is already used by another application. This will also prevent the licensing component from starting.

See Additional Configuration Options - the config.ini File.

See Cloud-Specific Firewall Information for an overview 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=80/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 Primary and Backup AutoVE License Servers

When AutoVE mode is used, the primary and backup license servers can synchronize their database of registered clients. The TCP port for this synchronization must be permitted on both servers. **Default**: **TCP/8085**; an alternative port can be configured in */opt/license-server/config.ini*.

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 a **VE license server version before 1.1.23** on AWS, the host **iam.amazonaws.com**
- If running on GCP there are the following additional requirements:
  - Access to the host **www.googleapis.com**.
  - Service account and role assigned to the instance that allow access to the API and metadata server.
    This is normally provided by the **Compute Engine default service account** and the **Default access** scope in the **Identity and API access** section. Do not change the default assignment unless know how to assign the required permissions in a custom configuration. If the permissions are not correct, the fingerprint creation will fail with *Failed to retrieve instance document*.
- If running on the IBM cloud, 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 an overview about the mechanisms used in the different cloud environments, and your Linux firewall documentation for any Linux specific questions. The license server system must have an appropriate DNS configuration to look up the IP addresses of the hostnames listed above.

Communication Between License Server and ESXi Host / vCenter Server

The license server must be able to access the following ports on the ESXi host or vCenter Server it binds to: ports **443** (TCP) and **902** (TCP and UDP).

Charon VE-Capable Emulator and Management Software

The VE license server software requires matching Charon emulator software.

Please note:

- The requirements are **different for the two modes of a VE license server** (general VE or AutoVE). They are described below.
- 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 VE-capable 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. However, there are restrictions in a VMware environment.
- **Restrictions for VMware environments**:
  - **If the license server binds to the ESXi host** on which the license server VM runs, any Charon emulator using the VE license server must run either on the same VM as the VE license server or on a VM running on the same ESXi host.
  - **If the license server binds to the vCenter Server** that manages the ESXi host on which the license server VM runs, any Charon emulator using the VE license server must run either on the same VM as the VE license server or on a VM on an ESXi host managed by the same vCenter Server.

Charon Emulator Packages for VE Licenses (General VE Mode)

The VE licenses are supported by the following products:

- **Charon-SSP** 4.2.x and later
- **Charon-PAR** 3.0.6 and later
- **Charon-AXP/VAX** planned for version 4.12 (Linux versions only)

Stromasys or your Stromasys VAR will provide you with the software or a download link. In certain cloud environments, Stromasys may offer prepackaged Charon VE images on selected cloud marketplaces. 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).

For detailed information about the relevant installation packages, please refer to the product documentation specific to your emulator product and version:

- For **Charon-SSP**, refer to the Charon-SSP user's guide of your emulator version for details (see Charon-SSP for Linux).
- For **Charon-PAR**, refer to the Charon-PAR user's guide of your emulator version for details (see Charon-PAR documentation).
- For **Charon-AXP/VAX**, refer to the user's guides for Charon-AXP or Charon-VAX.

Charon Automatic Licensing Marketplace Images (AutoVE Mode)

If the VE license server is used in AutoVE mode, the license client must be an instance launched from a compatible marketplace Automatic Licensing image. **At the time of writing AutoVE was only supported by Charon-SSP AL marketplace images. For up-to-date availability information, please contact your Stromasys representative.**

- The AutoVE license server must be defined for the instance before first launch (see Configuring AutoVE Information on the Charon AL Host).
- This support was added in Charon-SSP version 5.3.8 and later images in selected clouds.

VE License Server - Installation

If you are not familiar with the installation of RPM packages, please refer to the general Charon user's guide of your product, 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 or above 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

In the description below, the placeholders used have the following meaning:

- *<mykey>* is the private key of the key-pair you associated with your cloud instance
  (for an on-premises VMware installation or an installation on a physical system where logging in with username/password is allowed, this is not needed).
- *<user>* is the user associated with your license server instance (e.g., *opc* on OCI, *centos* for a CentOS instance on AWS, or the custom user on your VMware virtual machine;
  for an instance installed from a Stromasys-provided Charon AL or VE emulator marketplace image, use user *charon* for SFTP and user *sshuser* for interactive login.
- *<linux-ip>* is the ip address of your license server system.

Please note: if an instance was installed from a prepackaged Charon emulator marketplace image, the installation package is already stored in */charon/storage*. Please check, if there are newer versions available that would be preferable for your environment.

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

1. **Copy the license server software package to the license server host (if needed)**:
   a. For example, use **sftp** to connect to the VE license server system.
      `# sftp -i ~/.ssh/<mykey> <user>@<linux-ip>`
   b. Copy the software package to the license server system using the following SFTP command:
      `> put <local-path-to-license-server-package>`

2. **Use ssh to log in on the license server host**.
   `# ssh-i ~/.ssh/<mykey> <user>@<linux-ip>`

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>`
      If you used SFTP to copy the package to an instance installed from a prepackaged Charon marketplace image, the home directory of the *charon* user and the default location for file transfers is */charon/storage.*
   c. For VE license server 2.2.4 and above, unpack the archive and agree to the end-user license agreement:
      i. `# sh ./license-server-<version>.rpm.sh`
         This will display the EULA. After agreeing to it, for version 2.2.4, the RPM installation package will be unpacked in the current directory. For version 2.2.5 and later, the EULA and the RPM package will be unpacked in a subdirectory (*license-server-<version>.rpm*) of the current working directory.
   d. Install the package:
      i. Go to the directory in which the RPM package is located.
      ii. Linux 7.x: `# yum install license-server*.rpm`
      iii. Linux 8.x and 9.x: `# dnf install license-server*.rpm`

Below, you find the sample output of an installation (version 8.x of the supported Linux distributions; assuming that the RPM is in the current working directory):

```
# dnf install license-server-2.0.1.rpm
Last metadata expiration check: 0:19:36 ago on Di 03 Mai 2022 13:20:02 CEST.
Dependencies resolved.
================================================================================
 Package              Architecture  Version          Repository           Size
================================================================================
Installing:
 license-server       x86_64        2.0.1-1          @commandline         53 M

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

Total size: 53 M
Installed size: 85 M
Is this ok [y/N]: y
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                        1/1
  Running scriptlet: license-server-2.0.1-1.x86_64                          1/1
  Installing       : license-server-2.0.1-1.x86_64                          1/1
  Running scriptlet: license-server-2.0.1-1.x86_64                          1/1
Created symlink /etc/systemd/system/multi-user.target.wants/licensed.service  /etc/systemd/system/licensed.service.

  Verifying        : license-server-2.0.1-1.x86_64                          1/1

Installed:
  license-server-2.0.1-1.x86_64

Complete!
```

VE License Server Post-Installation Tasks

After the installation, it is strongly recommended to change the default password of the web GUI. Please refer to VE License Server Web-based Management GUI for more information.

Charon VE-Capable Emulator Software Installation

The Charon emulator software can be installed as a standard installation based on installation packages provided by Stromasys, or (in supported cloud environments) be provided as a marketplace image from which a Charon emulator host instance can be launched.

The detailed host requirements, the installation, and the management of the Charon emulator software are described in the user's guides of the respective products and versions.

For a **standard Charon emulator installation,** please refer to the following resources on the Stromasys product documentation page:

- For **Charon-SSP**, refer to the Charon-SSP user's guide of your emulator version for details (see Charon-SSP for Linux).
- For **Charon-PAR**, refer to the Charon-PAR user's guide of your emulator version for details (see Charon-PAR documentation).
- For **Charon-AXP/VAX**, refer to the Charon-AXP/VAX user's guides of your emulator version for details (see Charon-AXP and Charon-VAX documentation).

To launch a Charon emulator host instance from a **prepackaged VE or AutoVE enabled marketplace image**, please refer to the cloud-specific information in the appendix or your cloud-specific *Getting Started* guide.

- A prepackaged **VE image** will provide a Charon emulator host suitable to use a VE license server operating in general VE license mode.
- A prepackaged **AL (Automatic Licensing) image** will provide a Charon emulator host suitable to use a VE license server operating in AutoVE mode.
- **Please note**: not every cloud environment will offer one or both types of prepackaged marketplace images. Please refer to the cloud-specific *Getting Started* guide of your product, or contact your Stromasys representative to check the availability.

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:

For cloud deployments: 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. **Please note that is not possible to use such a backup to revert to a previous license version**.

However, the following actions will **invalidate the license**:

1. All supported VE license server platforms:
   - 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.
   - Copying the virtual machine on which the license server runs. This includes cloning a virtual machine, or recovering a backup into a new virtual machine.
   - Changing the number of CPU cores of the license server system.
2. VMware VE license server platforms:
   - Restrictions from point 1 above.
   - If the license server is bound to the ESXi host: using vMotion on the VM in which the VE license server runs.
   - If the license is bound to a vCenter server:
     - Using vMotion to move the VM in which the license server runs to a system not controlled by the same vCenter.
     - Restoring the license server from a backup or snapshot and rebinding the restored license server to a new vCenter server (e.g., DR case).
   - Changes to the API interface of the ESXi host or vCenter Server.
   - The license can become temporarily unavailable if the user credentials or address information recorded by esxi_bind are changed. In this case, esxi_bind must be run again to define the correct user credentials and address information.
3. AutoVE license server platforms:
   - Restrictions from point 1 above.
   - Charon emulator host instance register with their license server only once at start.
     This is recorded on the license server in **/opt/license-server/instances.db**.
     If this file is lost, the license is not invalidated from the license server's point of view, but it can no longer be used from the Charon host instances as they will not register a second time. The Charon host instances would have to be recreated (fresh instance launch from a supported marketplace instance). Therefore, it is very important to backup up the instance database file. If a peer license server is used, the databases are synchronized between the two servers providing another level of data backup.
   - If the virtual hardware of the Charon emulator host is changed significantly (for example, the number of CPUs), then the registration of the Charon emulator host with the license server will be invalidated requiring that a new instance to be launched.
   - AutoVE server and Charon host instance must be in the same cloud and the Charon host instance must be launched from a supported AL marketplace image.
4. Physical VE license server platforms:
   - Restrictions from point 1 above.
   - Replacing the boot disk (i.e., the disk on which the operating system is installed).

If your license is invalidated for whatever reason and you cannot revert the action that caused the invalidation, **you must request a new license from Stromasys**. Therefore, planning your license infrastructure should include a **backup license server** to insure continuity until you received your new primary license.

Overview - Requesting and Installing a License

Overview of the basic steps to request and install a license:

- **VMware only**: for the first license request in a VMware environment, or if the binding data has changed, use the **esxi_bind** command to bind the license server to its ESXi host or vCenter Server.
- 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.
- Stromasys will send you a license. This is a **V2C file** with the license data and a text file with human readable license content.
- 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.

License Installation Using the Command-Line

The following sections will show how to perform a license installation on the VE license server. Alternatively, you can use the web-based GUI (see VE License Server Web-based Management GUI)

Running the *esxi_bind* Command (VMware environment only)

The **esxi_bind** command sets up the necessary communication connection between the VE license server and the ESXi host / the vCenter Server.

It must be run on the license server (and the backup license server, if applicable):

- **once** before the first license is requested, **and**
- **again** should the user credentials, the password, or the address data for the access to the ESXi host / the vCenter Server change. Please make sure that the password of the selected user account does not automatically expire after a certain time period. This would cause disruptions in the license server operation and make it impossible for clients to receive their license.

Perform the following steps:

1. Use **ssh** to log in on the license server instance (assuming that username/password login is possible for an on-premises VMware installation).
   `# ssh <user>@<license-server-ip>`
   where
   a. *<user>* is the user for interactive login associated with your license server system
   b. *<license-server-ip>* is the ip address of your license server system
2. Become the privileged user on the license server and run the **esxi_bind** program.
   a. Become the root user: `# sudo -i`
   b. Run the **esxi_bind** program:
   `# /opt/license-server/esxi_bind -a <address> -u <username> -p <password>`
   where
      i. *<address>* is the IP address of the ESXi host or vCenter Server
      ii. *<username>* is a user on the ESXi host or vCenter Server (**see notes below**).
      iii. *<password>* is the password of the user
3. If the command is successful, it will create the file */opt/license-server/config.ini* containing the connection data (the password is encrypted).

Important notes regarding the user on the ESXi host or the vCenter Server:

1. The **username on the vCenter Server** can take different forms:
   - Simple username
     esxi_bind parameter example: `-u myusername`
   - Username includes a domain name in one of the following two formats:
     - *<domain>\<username>*
       esxi_bind parameter example (quotes are mandatory): `-u 'mydomain\myusername'`
     - *<username>@<domain>*
       esxi_bind parameter example: `-u myusername@mydomain`
2. The user must have at least the following **global permissions** (i.e. the permissions cannot be limited to a specific VM):

- Datastore > Allocate Space
- VirtualMachine > Config > AddNewDisk
- VirtualMachine > Config > RemoveDisk

Please note: if username and/or password contain Unix shell meta-characters, these characters must be escaped (enclose the string in single quotes, or add a backslash character in front of the meta-character).

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
      (for an on-premises VMware installation where login with username/password is allowed, it is not needed)
   b. *<user>* is the user for interactive login associated with your license server instance (e.g., *opc* on OCI, *centos* for a CentOS instance on AWS, or the custom user on your VMware virtual machine or your physical server;
      for an instance installed from a prepackaged Charon supported marketplace image, use *sshuser* for Charon-SSP and *centos* for Charon-PAR)
   c. *<license-server-ip>* is the ip address of your license server system
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 [-a] --filename <my-file>.c2v --platform <my-platform>`
      where
      i. The optional **-a** parameter creates the fingerprint for a AutoVE license. General VE mode and AutoVE mode are **mutually exclusive**.
      ii. *<my-file>.c2v* is the path and name under which you want to store the fingerprint. The file type is C2V (customer-to-vendor)
      iii. *<my-platform>* indicates the platform on which the license server runs (possible values: **physical**, **aws**, **oci, gcp, azure**, **ibm**, **nutanix**, or **esxi;** for AutoVE: **aws, oci, gcp, azure**)
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.

Please also indicate the following:

- License requirements based on your contract with Stromasys (product version, number of concurrent instances, is this the main or the backup license, etc.).
- In case of a license update, **specify clearly what should be changed and what should remain the same**.
- Do you require a license with or without a passphrase (can be configured per product section)?
  - The use of a passphrase requires VE license server versions 1.1.x and higher.
  - The use of a passphrase requires Charon-SSP emulator versions 4.3.x and higher.
  - For Charon-PAR, a passphrase is mandatory. It is required to identify the correct license section.
- Do you require an AutoVE license?
  - Available starting with VE license server version 1.21 for supported cloud-specific Automatic Licensing marketplace images.

In response, you will receive two files:

- The so-called **V2C (vendor-to-customer) file** which contains the license data. The content of the license (type of emulated hardware, expiration date, number of concurrent instances, etc.) depends on your contract with Stromasys.
- A **text file** containing the license content in human readable form. Starting from November 2023, the text file will contain the checksum of the V2C file for integrity checking. **Please review the text file carefully before installing the license to make sure the content is what you expected**.

It is strongly recommended to keep the V2C and text files to have a record of licenses received and updated over time.

Installing the License Data on the License Server

Please review the text file carefully before installing the license to make sure the content is what you expected.

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 (if a backup license server is to be used, it needs its own license):

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
      (for an on-premises VMware installation where login with username/password is allowed, it is not needed)
   b. *<user>* is the user for interactive login associated with your license server instance (e.g., *opc* on OCI, *centos* for a CentOS instance on AWS, or the custom user on your VMware virtual machine or you physical server;
      for an instance installed from a prepackaged Charon supported marketplace image, use *sshuser* for Charon-SSP and *centos* for Charon-PAR)
   c. *<license-server-ip>* is the ip address of your license server system
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 of the V2C (vendor-to-customer) file.
      Starting with VE license server version 1.1.23, the v2c tool will show the difference between old and new license for a license update and require confirmation. Please review the differences carefully before confirming.

After the installation of the V2C file, the license server will be restarted. This restart will not affect running emulators. However, depending on the emulator product, it could be that the license server does not correctly display the license usage (`license_viewer -u` output and license server log file) until the emulators connect to the license server again after the next check interval has expired (default 1 hour).

Please note:

- Please note that to install a license with a new license ID (or another changed static parameter - see below), the old license must first be removed in an additional step (see *Removing a License from a VE License Server* in the applicable *VE License Server Guide*).
- In versions before 1.0.17, the license server will not start until a valid license has been installed.

The following example shows the **initial** 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
```

Please note:

- If the V2C file installed is an **update** to an existing license, the **v2c** command will first **show the difference** between old and new license and wait for the user confirmation before proceeding with the update. Please review the differences carefully before confirming. If absolutely necessary, this behavior can be suppressed using the `-s` option.
- To import the same license repeatedly will not cause a problem. In this case, the user will not be asked to confirm the import.
- The difference between old and new license is shown as a side-by-side list of the old and new license parameters. This list uses short parameter names to keep the old and new parameter on one line.

Verifying License Installation and License Content

Checking the License Server Log file

Check the license server log file to see if the server started successfully or reported an error. Use the following command (as the privileged user):
`# cat /opt/license-server/log/license.log`

The log should indicate that the license server is ready to serve licenses.

Using the license_viewer Program to Display the Content of a License

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 table shows examples for several different license types and platforms (please note that the output may vary depending on platform and software version) :

Regular VE license on AWS

```
<<License Viewer>> Current license:
License Fingerprint: 07792211fc8ce3fdc085 <truncated>
Customer Name: Stromasys
License ID: 01.00000001.002.020
Key Type: NORMAL
Platform: amazon.aws
Release Date: 2021-06-17 13:08:01
Grace Period: 120 minutes
License Check Interval: 60 minutes

Virtual Hardware: Charon-SSP/4M,Charon-SSP/4U
Product Code: Charon-SSP/ALL
Expiration Date: 2021-12-22 23:55:00
Major Version: 5
Minor Version: 3
Maximum CPU: 64
Maximum Virtual Memory: 1048576MB
Instances Allowed: 3
```

Regular VE license on physical server

```
<<License Viewer>> Current license:
License Fingerprint: 07792211fc8ce3fdc085 <truncated>
Customer Name: Stromasys
License ID: 03.00000003.002.006
Key Type: NORMAL
Platform: physical.machine
Release Date: 2021-12-08 13:18:32
Grace Period: 120 minutes
License Check Interval: 60 minutes

Virtual Hardware: Charon-PA9-64-L1
Product Code: CHPA9-64-L1-IP
Expiration Date: 2022-06-08 23:55:00
Major Version: 3
Minor Version: 0
Maximum CPU: 1
Maximum Virtual Memory: 2048MB
Instances Allowed: 10
Passphrase: 77U8-HXR9-VUFK-1B9V
```

Countdown license on physical server

```
<<License Viewer>> Current license:
License Fingerprint: 5f9d9f13f390e3b071 <truncated>
Customer Name: Stromasys
License ID: 01.00000001.002.194
Key Type: COUNTDOWN
Expiration Date: 240 hour(s)
Platform: physical.machine
Release Date: 2021-07-29 09:06:15
Grace Period: 480 minutes
License Check Interval: 60 minutes


Virtual Hardware: Charon-SSP/4U
Product Code: test
Major Version: 5
Minor Version: 3
Maximum CPU: 4
Maximum Virtual Memory: 10240MB
Instances Allowed: 4
```

AutoVE license on AWS

```
<<License Viewer>> Current license:
License Fingerprint: 5aaa364f9fc602323eaab2c   <truncated>

Customer Name: Stromasys
License ID: 03.00000003.002.007
Key Type: NORMAL
Expiration Date: 2022-02-14 23:55:00
Platform: amazon.aws
Release Date: 2021-07-27 10:42:44
Grace Period: 1440 minutes
Instances Allowed: 3
Passphrase:
Auto License: true
```

The license contains a key-specific section and one or more product-specific sections. Please note that the product-specific section is mostly not applicable to AutoVE licenses as this license is based on the number and configuration of the cloud-based host instances.

Important key-specific license parameters:

Parameter	Explanation
Platform	The platform for which the license has been created. This parameter cannot be changed by a license update.
Release Date	Date on which the license has been issued.
Customer Name	The owner of the license. This parameter cannot be changed by a license update. If a change is required, the existing license must be removed before creating a new fingerprint.
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. Once a license has been installed, this parameter cannot be changed by a license update. It also cannot be removed by reinstalling the license server software. If a change is required, the existing license must be removed using the transfer option (`-t`) before creating a new fingerprint.
Key Type	Possible values: • *NORMAL* - time-limited or perpetual license • *COUNTDOWN* - limited to a certain number of emulator runtime hours. The countdown starts, when the first emulator logs in to the license, and stops again when the last emulator disconnects from the license.
Expiration Date	Possible values: • License expiration date (for Key Type = NORMAL) • Configured number of emulator runtime hours (for Key Type = COUNTDOWN). The remaining hours can be seen in the web interface of the license server and the emulator log file. The number of hours refers to how long the license can be used by one or more emulators (up to the number of instances allowed by the license). The countdown process is independent of how many of the allowed instances are active.
Grace Period	Time in minutes the emulator can run after the license used by the emulator has timed out or disappeared. Configured by Stromasys when creating the license (default: 2 hours for general VE, 24 hours for AutoVE).
License Check Interval	Frequency with which the emulator will check the license availability and validity (1 hour).

Important product-specific license parameters (most parameters not applicable to an AutoVE license):

Parameter	Explanation
Virtual Hardware	The emulated hardware covered by this product section.
Product Code	The product code covered by the license.
Expiration Date	The expiration date.
Major Version and Minor Version	The major and minor product versions.
Maximum CPU	Defines the maximum number of CPUs in an emulated system (emulated SPARC in the example).
Maximum Virtual Memory	Defines the maximum amount of RAM in an emulated system.
Instances Allowed	**General VE mode**: defines the maximum number of concurrently running emulated systems. **AutoVE mode**: defines the maximum number of concurrently active AL cloud instances using the AutoVE license server.

Passphrase	For **general VE mode**, this defines the passphrase that must be configured on the license client system. This is optional for Charon-SSP and Charon-AXP/VAX, but mandatory for Charon-PAR. If a passphrase is configured on either side (client or server), there must be a matching passphrase on the other side - otherwise the emulator start will fail. A license update (modification to an existing product section) will not change the passphrase. In the case of **AutoVE mode**, the passphrase can be used to authenticate to the peer server.

License Verification Using the Web Interface

The license server provides a web interface to display important license characteristics, to display license client systems, and to enable license updates.

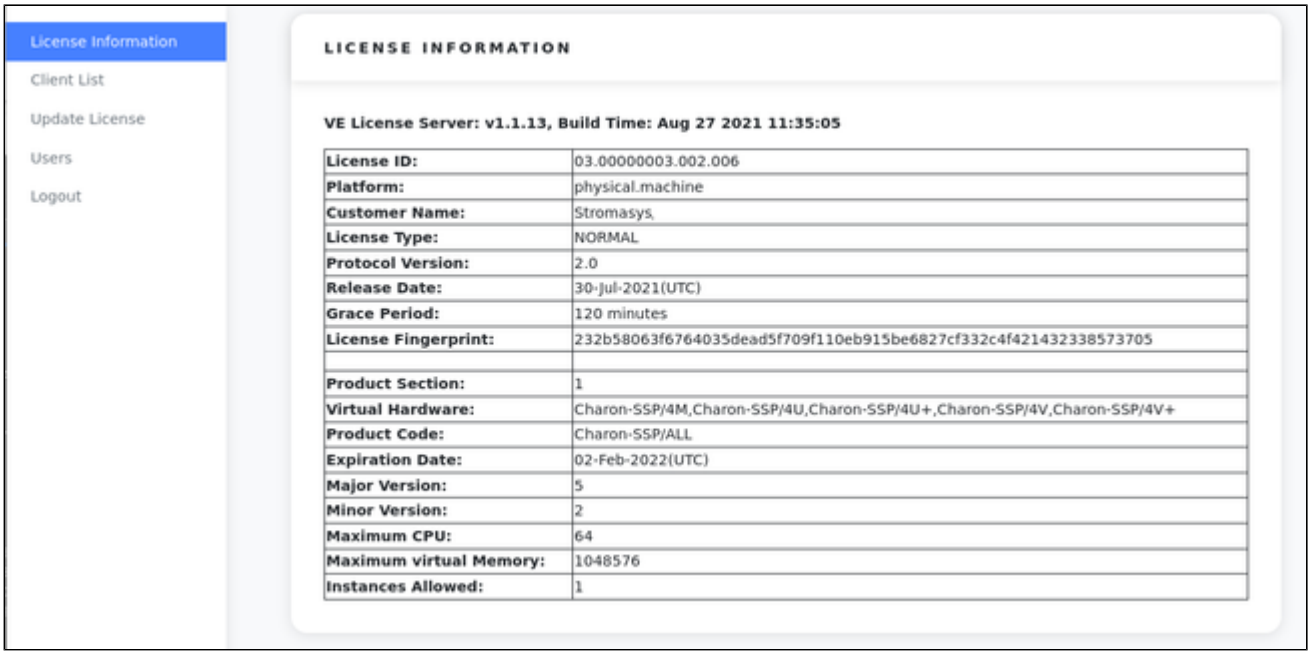
It is accessed using the URL **`https://`**<*`license-server-ip`*>**`:`**<*`web-gui-port`*> where

- *license-server-ip* is the address or the name of the VE license server, and
- *web-gui-port* is the port on which the web-server runs (default 8084).

Using just **`http://<license-server-ip>`** will cause a redirection to the configured HTTPS port (access to TCP port 80 required).

Prerequisite: access to TCP port 8084 of the license server (or an alternative port configured in the file */opt/license-server/config.ini* file) must be possible.

The following image shows sample output of a general VE license for SSP:



The first section of the samples shows the basic characteristics of the license. The Product Section shows the licensed products and their characteristics.

See VE License Server Web-based Management GUI and Additional Configuration Options - the config.ini File for more information.

Configuring a Charon Emulator for a VE License Server

Contents

The Charon host (for AutoVE) or the Charon emulator (for general VE) must be configured with the information needed to find the VE server(s).

The license server address, and optionally, a passphrase must be configured on the Charon host system:

- **General VE mode**: this configuration must be made for every emulated system that is to use the license server. This configuration can be performed via the configuration file or (for Charon-SSP) via the Charon Manager.
- **AutoVE mode**: this configuration must be made for the Charon host system before the first launch of the instance. This is currently only available for Charon-SSP cloud instances launched from supported AL marketplace images (Charon-SSP version 5.3.8 or higher).

The following sections describe this configuration.

VE License Server - General VE Mode

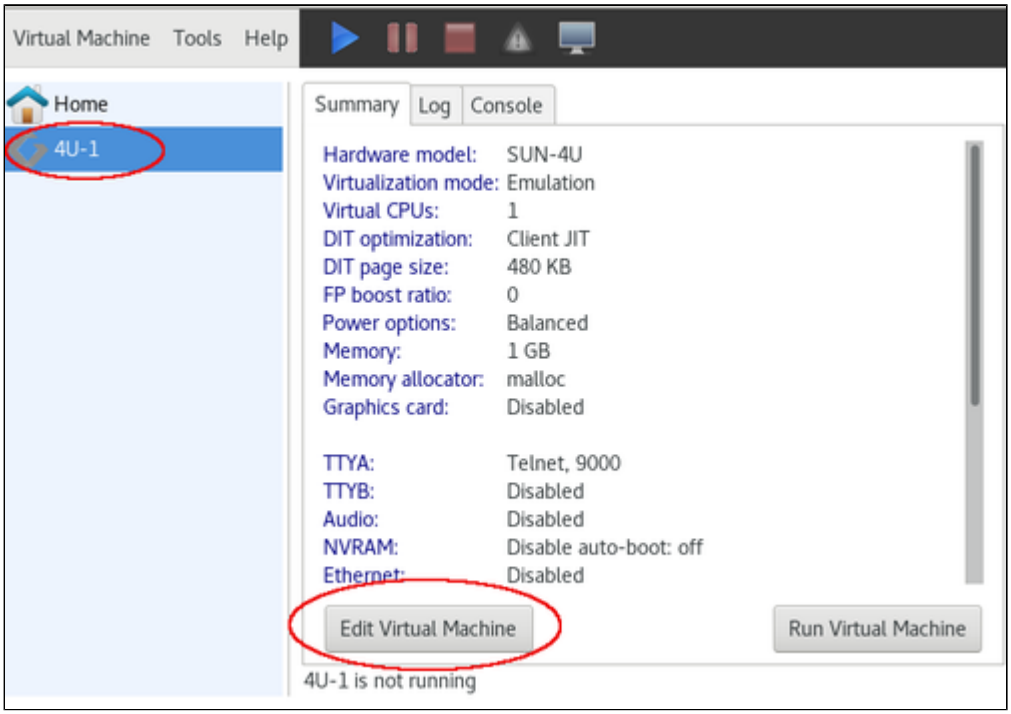
Every VE-enabled Charon emulator must be configured with the information how to reach the primary VE license server and - if applicable - also the backup license server (exactly one backup server can be configured). If the license is protected by a passphrase, this passphrase must also be configured. These steps are described in the following sections:

Charon-SSP Configuration

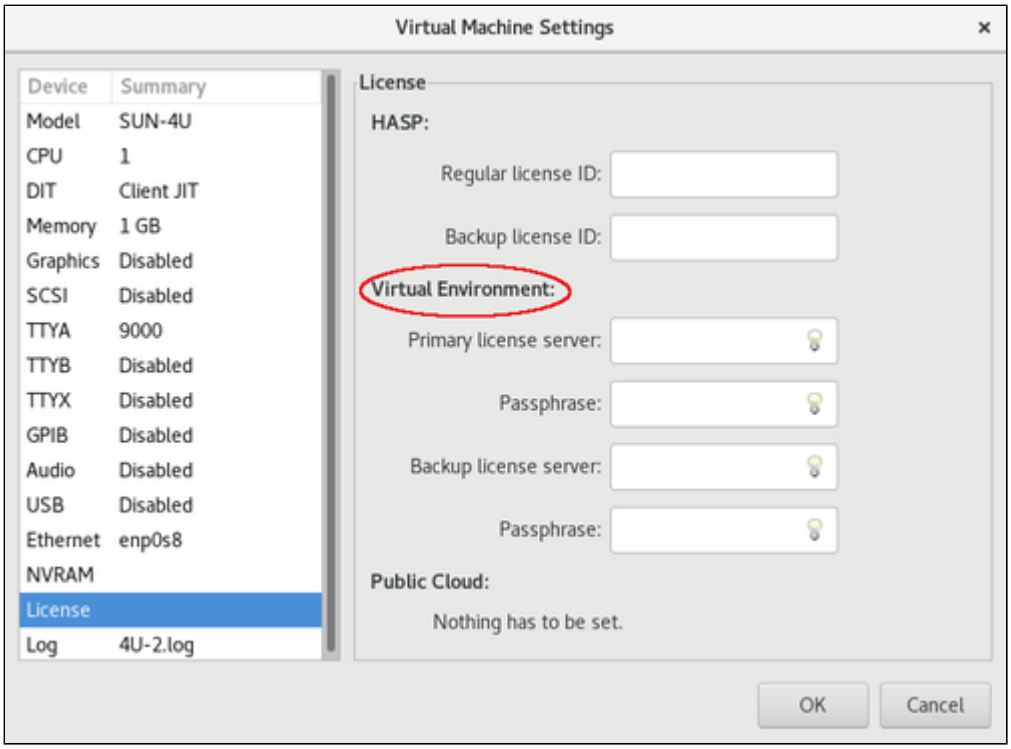
Configuring the License Server Details Using the Charon Manager

To configure the license server details 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:



Enter the following data into the **Virtual Environment** section of the license configuration pane:

- **Primary license server**: the format of this field is *<ip-address>*[*:<port>*]. Where
  - *<ip-address>* is the name or address of the primary license server (use localhost or 127.0.0.1 if the license server is on the same system as the emulator),
  - *<port>* is the TCP port on which the license is served (if not specified, the default port 8083 will be used).

- **Backup license server**: if you have a backup license server (supported in Charon-SSP version 4.1.19 or later), add the **IP address**, and, **if not-default, the TCP port** of the backup server in this field. The format is the same as for the primary license server. The backup server typically provides a license limited to a certain number of runtime hours should the primary server become unavailable. If all valid licenses are lost or removed while an emulator is running, there is a grace period (configured on the license; default: 2 hours). The grace period is the time period during which 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 (this could cause data loss for a running guest system).

- **Passphrase** fields: the passphrase authenticates the license client to the the license server. It is defined when the license is created by Stromasys. Please let Stromasys know if you require a license with or without a passphrase (can be selected per product section); passphrases are supported in emulator versions 4.3.x and higher. If your license was created with a passphrase, enter the passphrase in the corresponding fields. You will find the passphrase on the license server in the output of the **license_viewer** program. If the license contains more than one product section, there will be a passphrase for each product section. Select the one defined for the product section the emulator instance will use.

4. Click on **OK** to save the configuration. It will become active at the next start of the emulator.

Configuring the License Server Details 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 parameters. 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 Details 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
   (the default location is in /opt/charon-agent/ssp-agent/ssp/<*emul-architecture*>/<*emul-sparc-name*>/) where
   <*emul-architecture*> stands for **sun-4m**, **sun-4u**, or **sun-4v**.
3. Locate the **[license]** section (if it does not exist, add it).
4. Add the parameter
   server = <*license-server-ip-address*>[:<*port*>]
   to the section, where
   a. <*license-server-ip-address*> is the IP address of the license server, and
   b. <*port*> is the TCP port on which the license is served (if not specified, the default port 8083 will be used).
5. Optionally, add a backup license server (max. one backup server). The backup server typically provides a license limited to a certain number of runtime hours should the primary server become unavailable.
   Relevant parameter:
   backup_server = <*backup-license-server-ip-address*>*[:<port>]*
   to the section, where
   a. <*backup-license-server-ip-address*> is the IP address of the backup license server, and
   b. <*port*> is the TCP port on which the license is served (if not specified, the default default port 8083 will be used).
6. If defined on the license, add the license passphrase. The passphrase provides an authentication of license client to license server. The correct values for <*primary-license-server-passphrase*> and <*backup-license-server-passphrase*> can be found in the **license_viewer output** of the license server. If there are several product sections on the same license, be careful to select the passphrase associated with the correct product section. Relevant parameters:
   a. **server_key =** <*primary-license-server-passphrase*>
   b. **backup_server_key =** <*backup-license-server-passphrase*>
7. Save the configuration file.
8. 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_viev** and **hasp_update** that are installed with the Charon Agent.

Charon-PAR Configuration

For Charon-PAR, the configuration of primary and (optionally) backup license server must be entered into the emulator configuration file using a text editor.

Relevant parameter:

`license_key_id "VE://`*`<license-server-IP>`*`[:<port>]/<passphrase>/"`**

Where the following parameters are used:

- *<license-server-IP>*: the IP address of the VE license server (127.0.0.1 if the VE license server is on the same host).
- *<port>:* the TCP port on which the license is served (if not specified, the default port 8083 will be used).
- *<passphrase>*: the passphrase of the correct product section on the license. This is required for the emulator to identify the correct section.

To configure a **backup license server,** repeat the line, but with the address and passphrase of the backup license server. The first line is treated as the primary server, the second as the backup server. Only **one** backup server can be configured. The backup server typically provides a license limited to a certain number of runtime hours should the primary server become unavailable. If all valid licenses are lost or removed while an emulator is running, there is a grace period (configured on the license; default: 2 hours). The grace period is the time period during which 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 (this could cause data loss for a running guest system).

Please note: the parameter **`license_id "`***`<product-license-number>`*`"`** which is used by Sentinel HASP licensing to identify the correct product section is not supported by the VE license server. If it is in the configuration file, comment it out.

Charon-AXP/VAX Configuration

For Charon-AXP/VAX, the configuration of primary and (optionally) backup license server must be entered into the emulator configuration file using a text editor.

Relevant parameter:

`set session license_key_id = "VE://`*`<license-server-IP>`*`[:<port>]/[<passphrase>/]"`**

Where the following parameters are used:

- *<license-server-IP>*: the IP address of the VE license server (127.0.0.1 if the VE license server is on the same host).
- *<port>:* the TCP port on which the license is served (if not specified, the default port 8083 will be used).
- *<passphrase>*: the passphrase of the correct product section on the license (optional). The parameter may be required for the emulator in some cases to identify the correct section.

To configure a **backup license server,** add the backup license server information to the same line after the primary license server information:

`set session license_key_id = "VE://`*`<primary-licserv-IP>`*`[:<port>]/<passphrase>/, VE://`***`<backup-licserv-IP>`**`[:<port>]/<passphrase>/"`**

Only **one** backup server can be configured. The backup server typically provides a license limited to a certain number of runtime hours should the primary server become unavailable. If all valid licenses are lost or removed while an emulator is running, there is a grace period (configured on the license; default: 2 hours). The grace period is the time period during which 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 (this could cause data loss for a running guest system).

Charon Host System - Configuring the AutoVE Server Information

The AutoVE mode is an extension of the Automatic Licensing configuration available for selected cloud marketplaces.

Important restrictions:

- At the time of writing, AutoVE mode for Charon products is only available when using an **Automatic Licensing (AL) Charon-SSP marketplace image on AWS, GCP, OCI, or Azure (minimum version 5.3.8)** to create a Charon host instance. Please contact your Stromasys representative to get details on the availability of such marketplace images in your cloud environment.
- The AutoVE license server information must be configured before the Charon host instance is first launched. The information can be changed later, **bu t once the host system has connected to a public license server in the selected cloud, it cannot be reconfigured to use an AutoVE server (and vice-versa).**

Changed license server selection in Charon-SSP AL images starting with SSP version 5.6.8:

Starting with version 5.6.8, the license server selection in cloud-specific AL images has changed to simplify the operation of the SSP Amazon Linux AMI used in the new AWS service.

Case 1: **user provides no license server information** in the instance user data at initial instance launch:

a) If the file */opt/charon-license-server* exists and contains valid AutoVE server information, the cloud instance will use the AutoVE license servers specified in the file. This file exists by default in the SSP Amazon Linux AMI where it points to the public, Stromasys-operated AutoVE license servers specific to this AWS service. Such public AutoVE servers are only available in AWS at the time of writing.

b) If the file does not exist, the cloud instance will use the public, Stromasys-operated license servers (AL mode).

Case 2: **user provides AutoVE license server information** in the instance user data at initial instance launch.

The cloud instance will use the private, customer-operated AutoVE license servers.

The following sections will discuss the AutoVE configuration for a Charon host system:

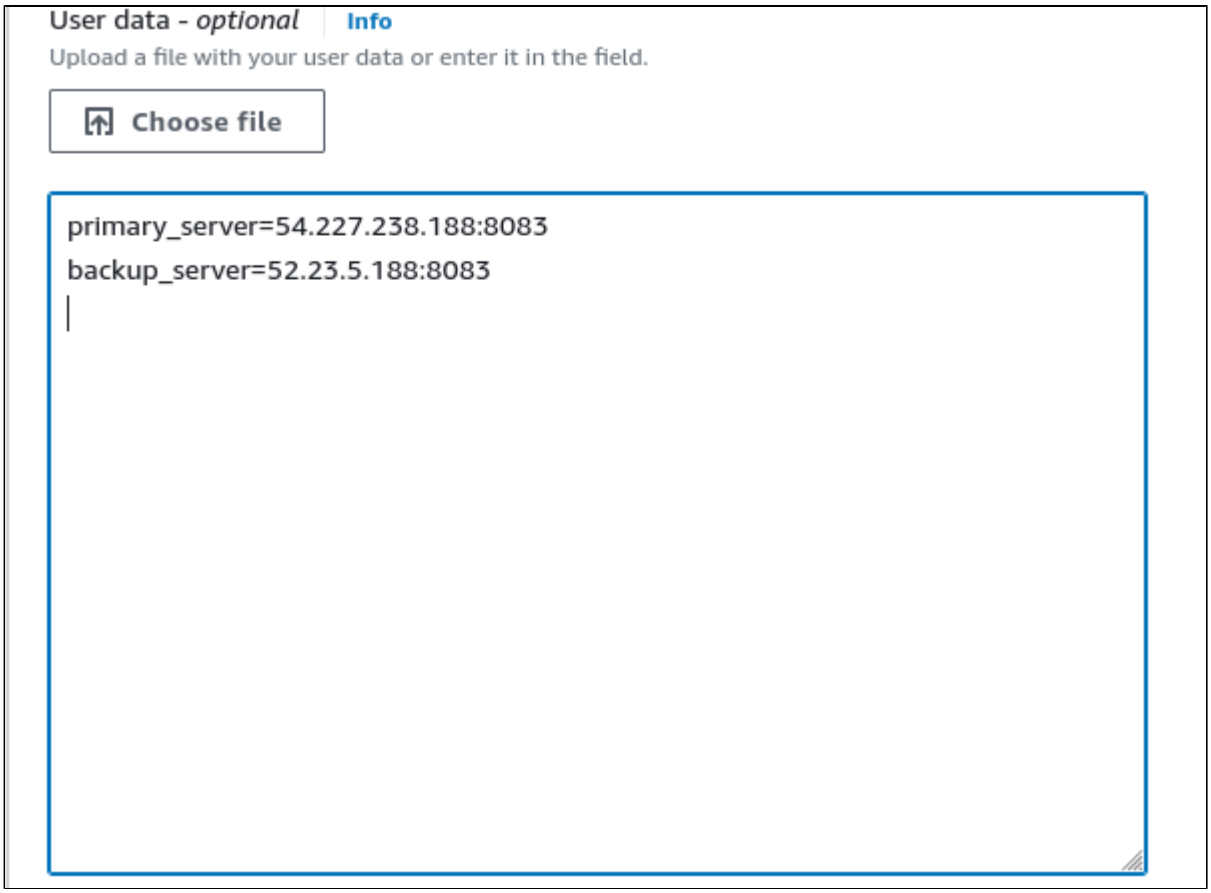
Charon AL Host Instance on AWS

Configuring the AutoVE Server Information at AWS Instance Launch

Please note:

- Should you use the SSP Amazon Linux AMI with **SSP version 5.6.8 or higher** as provided by the *AWS Mainframe Modernization - Virtualization for SPARC* service, the instance will by **default** connect to the **public, Stromasys-operated AutoVE license servers** (defined in */opt/charon-license-server*). You only need the **user data definition for older versions or to override the default** with your private AutoVE servers.
- The example below shows the appearance of the AutoVE license server information that is entered as **User Data** in the **Advanced Details** configuration section at the bottom of the **Launch an Instance** window during the initial configuration of an instance. **Scroll down** to the bottom of the configuration window to open and display the user data section in the **Advanced Details**.
- In the older GUI version, the **Advanced Details** section is part of the **Configure Instance** window - the layout is somewhat different, but the configuration options are the same.

Enter the information for the AutoVE license server as shown in the example below (it shows the public AutoVE servers):



Valid User Data configuration options:

- **`primary_server=`**`<ip-address>[:<port>]`
- **`backup_server=`**`<ip-address>[:<port>]`

where

- *<ip-address>* stands for the IP address of the primary and the backup server as applicable, and
- *<port>* stands for a non-default TCP port used to communicate with the license server (default: TCP/8083).

Please note: at least one license server must be configured at initial launch to enable AutoVE mode. This can be via the */opt/charon-license-server* file with the default public servers (SSP 5.6.8 or higher) or via the manual user data configuration. **Otherwise, the instance will bind to one of the public AL license servers operated by Stromasys.**

Changing the AutoVE Server Configuration After AWS Instance Launch

Once an instance has been launched, the AutoVE server information in the User Data can be changed. To do this, use the following steps:

- If the instance is running, it must be stopped (cleanly shut down any guest systems running in the Charon emulator before).
- Select your instance from the instance list, **right-click** on it and select **Instance settings > Edit user data.**
- Modify the AutoVE configuration in the user data as needed and click on **Save**.
- Activate the changes:
  - Restart the emulator instances and any required guest systems. It can take a minute or two until the change becomes active.
  - If changes are made to the VE license server configuration (e.g., changing the port numbers), the VE license server must also be restarted.

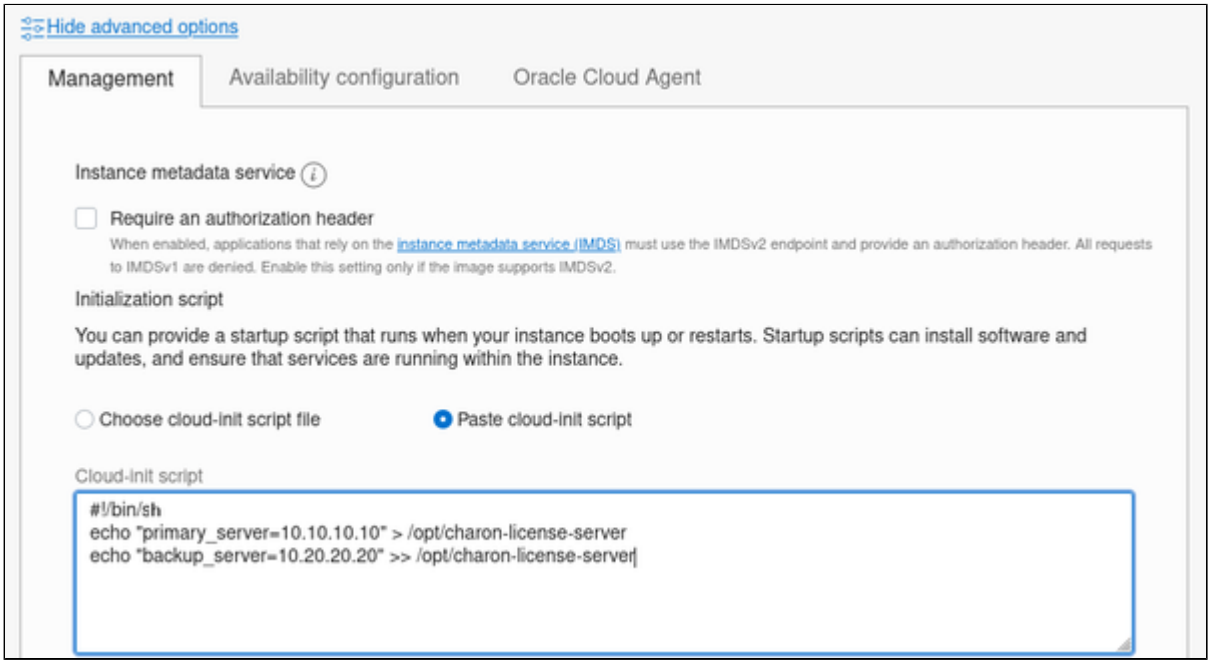
Please note: removing the AutoVE server configuration completely will **not** enable the instance to connect to the public license server

Charon AL Host Instance on OCI

Configuring the AutoVE Server Information at OCI Instance Launch

For OCI, you have to enter a cloud-init script at instance configuration in the **Advanced Options** section.

The following image shows an example:



Valid User Data configuration options:

- **`primary_server=`**`<ip-address>[:<port>]`
- **`backup_server=`**`<ip-address>[:<port>]`

where

- *<ip-address>* stands for the IP address of the primary and the backup server as applicable, and
- *<port>* stands for a non-default TCP port used to communicate with the license server (default: TCP/8083).

Please note: at least one license server must be configured at initial launch to enable AutoVE mode. **Otherwise, the instance will bind to one of the public license servers operated by Stromasys.**

Changing the AutoVE Server Configuration After OCI Instance Launch

Once an instance has been launched, the AutoVE server information in the User Data can be changed. To do this, use the following steps:

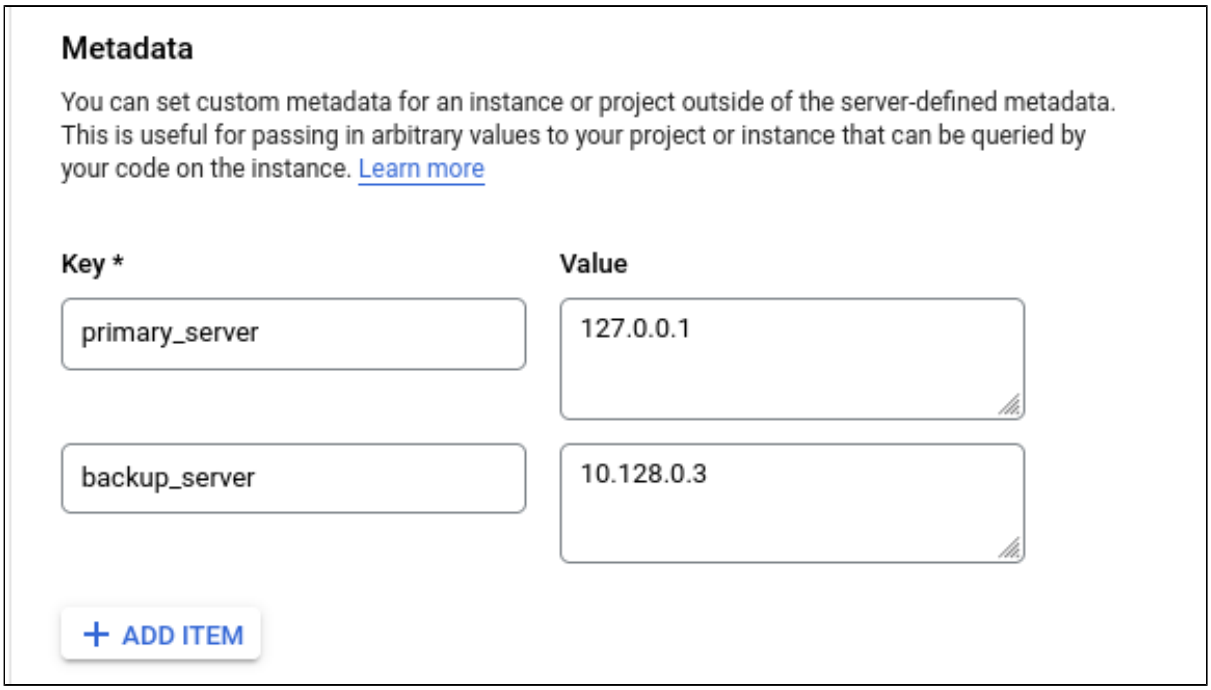
- The Charon host instance must be running.
- Log in to the Charon host instance as the **root** user.
- Open the file **/opt/charon-license-server** with a text editor.
- Modify the AutoVE configuration as needed and save the file.
- Activate the changes:
  - After cleanly shutting down any running guest operating systems, restart the emulator instances and any required guest systems. It can take a minute or two until the change becomes active.
  - If changes are made to the VE license server configuration (e.g., changing the port numbers), the VE license server must also be restarted.

Please note: removing the AutoVE server configuration completely will **not** enable the instance to connect to the public license server.

Charon AL Host Instance on GCP

Configuring the AutoVE Server Information at GCP Instance Launch

The AutoVE license server information is entered as **Custom Metadata**. In the initial instance configuration window, go to the bottom where the **NETWORKING, DISKS, SECURITY, MANAGEMENT...** configuration section is located. Open it and select the **Management** section. Add the Custom Metadata as shown in the example below:



Valid User Data configuration options:

- **`primary_server`** *<ip-address>*`[:`*<port>*`]`
- **`backup_server`** *<ip-address>*`[:`*<port>*`]`

where

- *<ip-address>* stands for the IP address of the primary and the backup server as applicable, and
- *<port>* stands for a non-default TCP port used to communicate with the license server (default: TCP/8083).

Please note: at least one license server must be configured at initial launch to enable AutoVE mode. **Otherwise, the instance will bind to one of the public license servers operated by Stromasys.**

Changing the AutoVE Server Configuration After GCP Instance Launch

Once an instance has been launched, the AutoVE server information in the Custom Metadata section can be changed. To do this, use the following steps:

- In the GCP management console, open the details window of your Charon host instance.
- Click on the **Edit** symbol at the top of the page.
- Scroll down to the Custom Metadata section.
- Modify the AutoVE configuration as needed and click on **Save** at the bottom of the page.
- Activate the changes:
  - After cleanly shutting down any running guest operating systems, restart the emulator instances and any required guest systems. It can take a minute or two until the change becomes active.
  - If changes are made to the VE license server configuration (e.g., changing the port numbers), the VE license server must also be restarted.

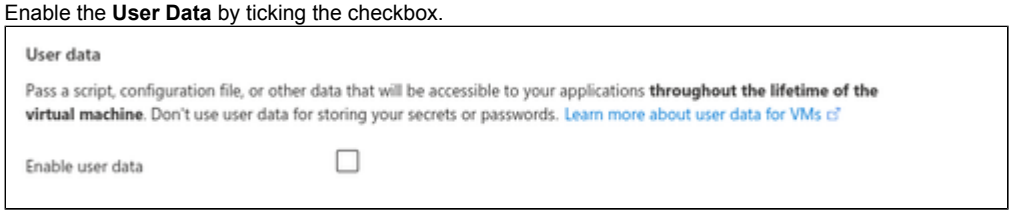
Please note: removing the AutoVE server configuration completely will **not** enable the instance to connect to the public license server.

Charon AL Host Instance on Azure

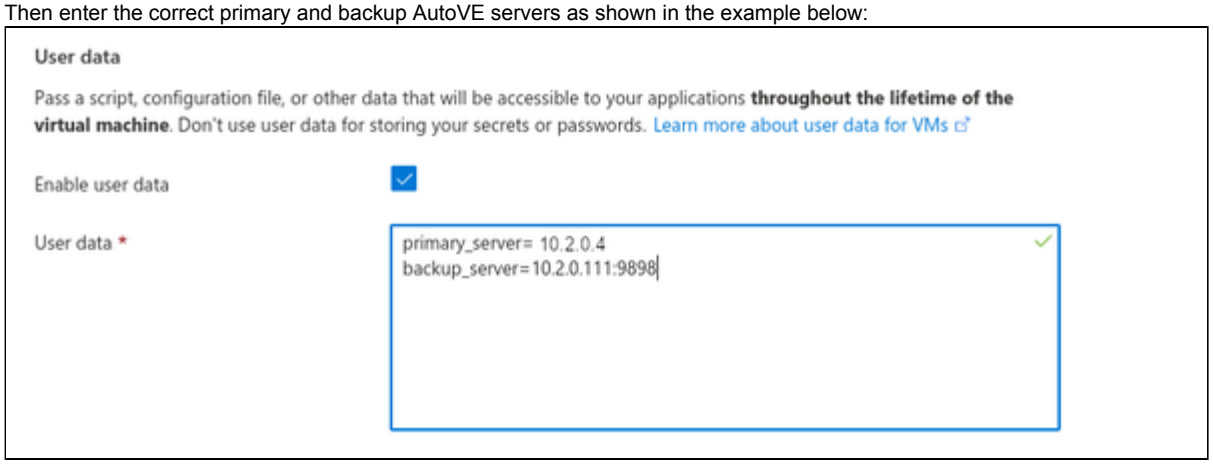
Configuring the AutoVE Server Information at Azure Instance Launch

The AutoVE license server information is entered as instance **User Data**. In the initial instance configuration window, go to the **Advanced** section.

- Open it and scroll down to the **User Data** section.
- Enable the **User Data** by ticking the checkbox.



- Then enter the correct primary and backup AutoVE servers as shown in the example below:



Valid User Data configuration options:

- **`primary_server=`**`<ip-address>[:<port>]`
- **`backup_server=`**`<ip-address>[:<port>]`

where

- *<ip-address>* stands for the IP address of the primary and the backup server as applicable, and
- *<port>* stands for a non-default TCP port used to communicate with the license server (default: TCP/8083).

Please note: at least one license server must be configured at initial launch to enable AutoVE mode. **Otherwise, the instance will bind to one of the public license servers operated by Stromasys.**

Changing the AutoVE Server Configuration After Azure Instance Launch

Once an instance has been launched, the AutoVE server information in the User Data section can be changed. To do this, use the following steps:

- In the Azure management console, open the **Overview** window of your Charon host instance.
- Find the **Configuration** option in the left-hand pane and open it.
- Scroll down to the **User Data** section and tick the checkbox that enables editing the data.
- Modify the AutoVE configuration as needed and click on **Save** at the top of the page.
- Activate the changes:
  - After cleanly shutting down any running guest operating systems, restart the emulator instances and any required guest systems. It can take a minute or two until the change becomes active.
  - If changes are made to the VE license server configuration (e.g., changing the port numbers), the VE license server must also be restarted.

Please note: removing the AutoVE server configuration completely will **not** enable the instance to connect to the public license server.

Transferring a License to Another Server

Contents

General Information

If required, a VE license can be transferred from one license server to another.

Please note:

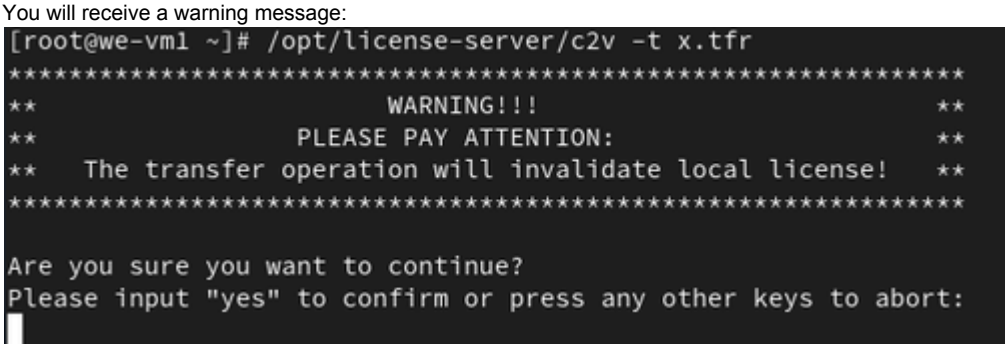
- This action will remove the license from the original license server.
- The transfer operation will fail for an expired license.
- The transfer operation can only be executed once per license.

Steps to Transfer a License

The steps below describe the license transfer to another server:

1. Become the **root** user on the license server.
2. Export the transfer license from the **original license server**:
   `# /opt/license-server/c2v -t <export-file>.tfr`

   You will receive a warning message:

   Confirm by entering the string **yes**, or abort by entering any other input (submit the input using the RETURN key).

3. Create a C2V file on the **destination license server** (this step is required even if source and destination server are the same):
   `# /opt/license-server/c2v -f <destination>.c2v -p <platform>`

4. Send **both files** (the TFR and the C2V file) to Stromasys (email address will be provided by Stromasys).

5. You will receive a V2C file.

6. Import the V2C file on the **destination license server**:
   `# /opt/license-server/v2c -f <new-v2c>.v2c`

7. If the address and/or passphrase of the license server has changed, adapt the configuration of the license client with the new license server data.

For more information about creating a C2V file and installing a V2C file, please refer to Installing a License on the VE License Server.

Removing a License from a VE License Server

Sometimes, it may be necessary to remove a license from a VE License Server.

Important note:

- Once a license has been installed on a license server, **the license id will remain the same** until the operating system of the license server host is reinstalled, or the license is transferred away from the system.
- Reinstalling the license server software (RPM) and/or deleting the directory */opt/license-server* will stop the system from being a license server, but not remove the original license id.
- After reinstalling the license server software (RPM), only the original license (V2C with the same license ID) can be installed to restore the former license server state.
- Any C2V file created without first completely removing the license (see below) will contain the original license ID making it impossible for Stromasys to create a new license.

Completely removing a license from a VE license server system:

This step is necessary in the following cases:

- Cleanly erasing the license from the current license server system for any reason.
- Transferring the license to a different system.
- Preparing the current system for the installation of a completely new license (new license ID or new license owner).

For such cases, you must use the C2V transfer option: **`c2v -t`** *<filename>*

Please note:

- The transfer option does not work for expired licenses.
- A transfer can only be executed once per license. A second attempt will produce an error message.
- Once a license has been transferred out from a license server, it can only be installed again on the same system if the transfer file is sent to Stromasys together with a new C2V from the system.
- For additional information about the transfer option, please refer to Transferring a License to Another Server

Additional Configuration Options - the config.ini File

The file **/opt/license-server/config.ini** offers additional configuration options for the VE License Server.

There are samples of the options in **/opt/license-server/config.ini.sample**.

The file currently has three sections:

- **[esxi]**: the parameters in this section are set up by the esxi_bind program. **Do not modify them manually**.
- **[peer]**: contains the configuration of a peer license server when running in **AutoVE mode**. If a peer has been defined, the two license servers can synchronize their client databases and act as primary and backup AutoVE servers. It contains the following parameters:
  - **address**: IP address of the peer license server
  - **port**: TCP port used to contact the peer server
  - **passphrase**: used to authenticate to the peer server (must be the same as configured on the the license installed on the peer). This use of the passphrase is different from the client/server authentication when the license server runs in general VE mode.
- **[general]**: used to define non-default ports for the VE server operation:
  - **port**: TCP port used to serve the license to license client systems. Default: 8083.
  - **http_port**: TCP port on which the web interface can be accessed. Default: 8084.
  - **http_redirect**: available starting with version 1.1.25. Enables (= on) or disables (= off) HTTP to HTTPS redirection. Default: on. If HTTP redirection is enabled, TCP port 80 must be accessible to the license server. If another application uses port 80, redirection has to be disabled.
  - **sync_port**: local TCP port for communicating with the peer server. Default: 8085. **Relevant for AutoVE mode.**

Please note:

- After parameters in this file have been changed, the **license server must be restarted** to activate the changes (**`# systemctl restart licensed`**).
- After the web server port has been changed, the **browser cache** should be cleared to avoid problems.
- If the **ports required by the web GUI are not accessible** to the license server's integrated web server, the **license server will not start**.

Certificates Used by the VE License Server

Contents

Certificate Usage Overview

The VE license server uses certificates for different purposes:

- **License server operation**: encrypted communication between license server and license clients (emulators)
- **Web-based management GUI**: encrypted (HTTPS) communication between the integrated license server web server and web browsers

This section provides an overview of the different scenarios and user options.

Certificates Used for License Server Operation

The communication between license server and license client (emulator) is encrypted. This encryption is based on TLS and requires matching certificates on sever and client sides.

Starting with VE License Server version 2.1.3, it is possible to use **certificates created by the user**, or **certificates the user obtained from an official certificate authority** (CA). This requires a matching emulator version. Currently, this is supported in Charon-SSP starting with version 5.5.5.

Older versions of the VE License Server and older versions of Charon emulator products use built-in certificates that cannot be changed.

Default Operation and Backward Compatibility

By default, the VE license server and the license clients use their built-in certificate when configured for general VE mode. No action on the user's side is required in this case. However, there are some aspects to be considered:

AL Marketplace Images with Stromasys-operated Public License Servers

- Charon host instances based on **marketplace image versions using the old certificate scheme**: the Stromasys-operated public license servers offer the **old certificate on port 8080** as before. The Charon instances will continue to run normally using their built-in certificates. This applies, for example to Charon-SSP images before version 5.5.5.
- Charon host instances based on **marketplace image versions using the new certificate scheme**: the Stromasys-operated public license servers offer the **new certificate on port 8081**. The Charon instances will use their built-in certificate and automatically connect to port 8081 of the public license server. This applies, for example, to Charon-SSP images of versions 5.5.5 and higher.
- Custom certificates are not possible if the public license servers are used.
- At the time of writing, AL marketplace images are only available for Charon-SSP.

AL Marketplace Images with Customer-operated AutoVE License Servers

- Emulator hosts that use AutoVE license servers are created from AL marketplace images. These images (if the feature is supported by the respective version) use the new certificates by default. The AutoVE license server must also support the new certificates for the configuration to work. An attempt to use a marketplace image including the new certificate version with a AutoVE server running a version not supporting the new certificates will lead to a registration failure and a **Bad Certificate** error in a network traffic trace.
- Emulator hosts based on AL marketplace images supporting the new certificates cannot register with an AutoVE server not supporting the new certificates. This means, for example, that Charon-SSP instances based on marketplace instances with SSP version 5.5.5 or higher **are not compatible** with AutoVE servers running a VE license server version before 2.1.3.
- A VE license server supporting the new certificates and running in AutoVE mode will **always use the new certificate**. Therefore, all Charon emulator hosts connecting to it must also use the new certificate.
- AutoVE peer servers must use compatible certificates (the same or based on the same root CE). Otherwise, the synchronization will fail.
- At the time of writing, AL marketplace images are only available for Charon-SSP.

General VE mode

- **License server side**: the VE license server will be initially installed using the old certificates. So backward compatibility to Charon emulator products using the old certificate is maintained.
  New certificates created by Stromasys are available in **/opt/license_server/certs** (file names **.sample*). However, they will not become active until they are renamed such that the string *.sample* is removed from the name. This must be followed by a restart of the license server. Customers can also create their own certificates or obtain certificates from an official CA instead of using the certificates provided by Stromasys (described later in this document).
- **License client (emulator) side**: after the new certificates have been enabled on the license server, license clients must also use the new certificates. For this, the certificates provided by Stromasys with the installation kit (e.g. for SSP/4U: **/opt/charon-ssp/ssp-4u/certs/*.sample**) must again be renamed to remove the string *.sample* from the name and the emulator must be restarted. Customers can also create their own certificates or obtain certificates from an official CA instead of using the certificates provided by Stromasys (described later in this document).
- The **.sample* certificates included in the kits cannot be used for AL or AutoVE environments.

Enabling New Certificates on License Server and Emulator

By default, the VE license server will use the old certificates to maintain compatibility. This section shows how to activate the new certificates.

Please note: all commands shown in this section are executed as the **root user**.

Activating the Certificates Provided by Stromasys

As part of certain RPM packages, Stromasys provides sample certificates for enabling the new certificates:

Product	Version	Sample certificate file names

VE license server	Starting with version 2.1.3	`/opt/license-server/certs/ca.crt.sample`
		`/opt/license-server/certs/ca.key.sample`
		`/opt/license-server/certs/server.crt.sample`
		`/opt/license-server/certs/server.key.sample`

Charon-SSP (emulator **RPMs for VE licensing**)	Starting with SSP version 5.5.5 (**example for 4U**)	`/opt/charon-ssp/ssp-4u/certs/ca.crt.sample`
		`/opt/charon-ssp/ssp-4u/certs/ssp.crt.sample`
		`/opt/charon-ssp/ssp-4u/certs/ssp.key.sample`

	Starting with SSP version 5.6.2 (**example for 4U**)	`/opt/charon-ssp/ssp-4u/certs/ca.crt.sample`
		`/opt/charon-ssp/ssp-4u/certs/charon.crt.sample`
		`/opt/charon-ssp/ssp-4u/certs/charon.key.sample`

Please note: Charon-SSP marketplace images for licensing by Stromasys-operated public license servers (AL) or customer-operated AutoVE license servers **do not contain these sample certificates**. New versions of these marketplace images always use the new certificates.

To activate the preconfigured certificates, perform the following steps:

	Step Description	Examples

1	Should there be active Charon emulators, cleanly shut down the guest systems and stop the emulators.	
2	Create a backup of the preconfigured certificates.	VE license server: **# mkdir /opt/license-server/certs/Backup** **# cp /opt/license-server/certs/*.sample /opt/license-server/certs/Backup/**
		SSP/4U emulator host (replace ssp-4u with ssp-4v or ssp-4m as appropriate): **# mkdir /opt/charon-ssp/ssp-4u/certs/Backup** **# cp /opt/charon-ssp/ssp-4u/certs/*.sample /opt/charon-ssp/ssp-4u/certs /Backup/**
3	Rename the preconfigured certificates on the **VE license server.**	**# cd /opt/license-server/certs** **# rename -v .sample '' *.sample**
4	Rename the preconfigured certificates on the **emulator host.**	SSP/4U emulator host (replace ssp-4u with ssp-4v or ssp-4m as appropriate): **# cd /opt/charon-ssp/ssp-4u/certs/** **# rename -v .sample '' *.sample**
5	Restart the license server.	**# systemctl restart licensed**
6	Restart emulators and guest systems.	

Please note: if the above steps were completed with an SSP version before 5.6.2 (old *ssp.key* and *ssp.crt* filenames used), and there is an upgrade to Charon-SSP to 5.6.2 or later, the old names will still be recognized.

Creating Custom Certificates

Please note:

- Customers can obtain certificates from an official CA or create self-signed certificates.
- Customers are **solely responsible** for obtaining or creating certificates in accordance with their organization's requirements. Any scripts and documentation provided by Stromasys are for **illustrative purposes only**.
- The different SSP emulator types (4M/4U/4V) can use different certificates, but the certificates must all be issued from the same root CA as the root CA used by the VE license server.

Special Considerations for Custom Certificates in AutoVE mode

The Charon AL marketplace images require special considerations with respect to custom certificates if they are to use a **customer-operated AutoVE server**:

- Please review the general certificate information above regarding AutoVE mode.
- AL marketplace images do not have a **certs subdirectory** in the */opt/charon-ssp/ssp-[4m|4u|4v]* directory. To use non-default certificates for AutoVE, the **certs** directory must be created manually.
- If an instance is configured to use an AutoVE license server using non-default certificates, the initial registration at instance launch will fail. To allow a successful registration, perform the following steps **after the initial launch**:
  - If necessary create the Charon certificates at the license server using the **make-ssp-cert.sh** or **make-charon-cert.sh** script as described above.
  - Copy the **resulting files** and the **ca.crt** from the license server to */opt/charon-ssp/ssp-[4m|4u|4v]/certs* of the Charon cloud instance.
  - Restart the instance and verify in the license server log file (*/opt/license-server/log/license.log*) that the registration at the AutoVE server was successful (message example: *Register from instance i-xxxxxxxxx: success*.)

Using the Sample Scripts

The VE license server kit contains the following sample scripts in **/opt/license-server/certs/tools** for creating self-signed certificates for the license server and the Charon emulator host:

- **make-root-cert.sh**: sample script used to create a self-signed root certificate. Result: **ca.key** and **ca.crt**.
- **make-server-cert.sh**: sample script used to create the license server certificate. Result: **server.key** and **server.crt**.
- Sample script used to create the certificate for the Charon emulator host.
  - VE license server starting with version 2.1.3 but before version 2.2.2: **make-ssp-cert.sh** (result: **ssp.key** and **ssp.crt)**.
  - VE license server starting with version 2.2.2: **make-charon-cert.sh** (result: **charon.key** and **charon.crt)**.

Please note: in some environments, the sample scripts will log a warning message (*Warning: ignoring -extensions option without -extfile*). This message can normally be ignored. It is due to different OpenSSL versions supporting different parameters.

To use the sample scripts for updating the certificates used in your Charon environment, perform the following steps:

	Step Description	Examples
1	Should there be active Charon emulators, cleanly shut down the guest systems and stop the emulators.	
2	If applicable, make a backup of the currently used certificates.	VE license server: **# mkdir /opt/license-server/certs/Backup** **# cp /opt/license-server/certs/*.crt /opt/license-server/certs/Backup/** **# cp /opt/license-server/certs/*.key /opt/license-server/certs/Backup/**
		SSP/4U emulator host (replace ssp-4u with ssp-4v or ssp-4m as appropriate): **# mkdir /opt/charon-ssp/ssp-4u/certs/Backup** **# cp /opt/charon-ssp/ssp-4u/certs/*.crt /opt/charon-ssp/ssp-4u/certs/Backup/** **# cp /opt/charon-ssp/ssp-4u/certs/*.key /opt/charon-ssp/ssp-4u/certs/Backup/**
3	Modify the scripts according to your needs.	
4	Run the provided scripts on the VE license server:	**# cd /opt/license-server/certs/tools** **# ./make-root-cert.sh** **# ./make-server-cert.sh** **# ./make-ssp-cert.sh** or **make-charon-cert.sh** (depending on the license server version)
5	Copy the new certificates to the correct location:	Example for the license server: **# cp /opt/license-server/certs/tools/ca.??? /opt/license-server/certs/** **# cp /opt/license-server/certs/tools/server.??? /opt/license-server/certs/** **Please note:** if the license server operates in **AutoVE mode**, the certificates must be copied to **/opt/license-server/certs/autove.**
		Example for a Charon-SSP/4U emulator host (replace ssp-4u with ssp-4v or ssp-4m as appropriate): a) Depending on the license server version: **# scp /opt/license-server/certs/tools/ssp.??? ** **root@**<*charon-emulator-host-ip*>**:/opt/charon-ssp/ssp-4u/certs/** or **# scp /opt/license-server/certs/tools/charon.??? ** **root@<*charon-emulator-host-ip*>:/opt/charon-ssp/ssp-4u/certs/** b) **# scp /opt/license-server/certs/tools/ca.crt ** **root@**<*charon-emulator-host-ip*>**:/opt/charon-ssp/ssp-4u/certs/** **Please note:** • If the emulator host is based on a **Charon marketplace image** and you did not change the default user configuration, you must copy the certificates first to the **charon** user account using **sftp**, and then move the files to the correct certs directory using the interactive login via the **sshuser**.
6	Restart the VE license server.	**# systemctl restart licensed**
7	Restart emulators and guest systems.	

License Server Log File Information

The license server shows whether the default certificates or custom certificates are being used.

AutoVE license server using default certificates:

```
************************************************************

   VE License Server v2.1.4
   Copyright (C) 1998-2022 Stromasys S.A. All Rights Reserved.

************************************************************

2022-10-05 09:18:14 INFO  MAIN     Build time: Sep 30 2022 15:04:22
2022-10-05 09:18:14 INFO  LICENSE  Web server will use default certificate: web-server.pem.default.
2022-10-05 09:18:15 INFO  LICENSE  Default SSL certificates are used.
2022-10-05 09:18:15 INFO  MAIN     license server (AutoVE) is ready to serve on port 8083.
```

VE license server in general VE mode using external server certificates, but the default web server certificate:

```
************************************************************

   VE License Server v2.1.4
   Copyright (C) 1998-2022 Stromasys S.A. All Rights Reserved.

************************************************************

2022-09-30 15:55:37 INFO  MAIN     Build time: Sep 30 2022 15:04:22
2022-09-30 15:55:37 INFO  LICENSE  Web server will use default certificate: web-server.pem.default.
2022-09-30 15:55:37 INFO  MAIN     license server (VE) is ready to serve on port 9093.
2022-09-30 15:55:37 INFO  LICENSE  External SSL certificates are used.
```

VE license server in general VE mode using external server certificates and custom web server certificate:

```
************************************************************

   VE License Server v2.1.4
   Copyright (C) 1998-2022 Stromasys S.A. All Rights Reserved.

************************************************************

2022-10-05 15:25:30 INFO  MAIN     Build time: Sep 30 2022 15:04:22
2022-10-05 15:25:30 INFO  LICENSE  Web server will use custom certificate: web-server.pem
2022-10-05 15:25:30 INFO  MAIN     license server (VE) is ready to serve on port 9093.
2022-10-05 15:25:30 INFO  LICENSE  External SSL certificates are used.
```

Certificates Used for Web-GUI Operation

When connecting to the VE license server web-based management GUI for the first time, the web browser will issue a warning and inform the user that the connection is not private. This is due to the fact that Stromasys, when creating the installation kit, cannot foresee the actual customer environment. Thus, the SSL certificate included with the license server kit includes a dummy hostname that does not match the real hostname of the customer license server system, and it also contains Stromasys as the certificate authority which is unknown to web-browsers by default.

It is possible to override the warning and connect to the page. Otherwise, users must

- **either** obtain a certificate for the host from one of the **commercial certificate authorities**, **or**
- they must create **their own self-signed certificate** and add it to the web browser.

The default certificate is named *web-server.pem.default* and is located in */opt/license-server/certs*. It is used by the license server web GUI unless there is a custom certificate named *web-server.pem* in the same directory. It will be overwritten by an update or a reinstallation of the license server.

Steps to create a **self-signed certificate**:

- Log in as the root user.
- Go to */opt/license-server/certs/tools*.
- Create your private copy of the **make-web-server-pem.sh** (e.g., *my-make-web-server-pem.sh*).
- Edit your private copy of the script to include the correct hostnames for your license server in the CN and DNS fields.
- Run the script, e.g., **my-make-web-server-pem.sh** script.
- This will create the files **web-server.pem** and **web-ca.cer**.
- Move or copy the file **web-server.pem** to the */opt/license-server/certs/* directory.
- Restart the license server (**`# systemctl restart licensed`**).
- Import the root CA (**web-ca.cer**) into your browser's Trusted Root Certification Authorities Certificate Store.

VE License Server Web-based Management GUI

Starting with VE license server version 1.1.13, the previous information-only web interface has been changed to a management interface. It provides the following functions:

Prerequisites:

- The TCP port used by remote systems to web-based management interface must be permitted on the license server, and by any intermediate firewall. **Default**: **TCP/8084**; an alternative port can be configured in */opt/license-server/config.ini*.
- **TCP port 80** must be available to the license server to redirect HTTP requests to HTTPS. For remote connections, the port must also be permitted through intermediate firewalls. Starting with version 1.1.25, redirection (and thereby use of TCP port 80) can be enabled or disabled in */opt/license-server/config.ini*.
- **Important**: at the time of writing, the web-server component of the license server applications will not start if a port required by the web server is already used by another application. This will also prevent the licensing component from starting.

Accessing the Management GUI and Logging in

The web-based management GUI is provided by the license server on TCP port 8084 by default (the port can be changed in */opt/license-server/config.ini*; see also Additional Configuration Options - the config.ini File).

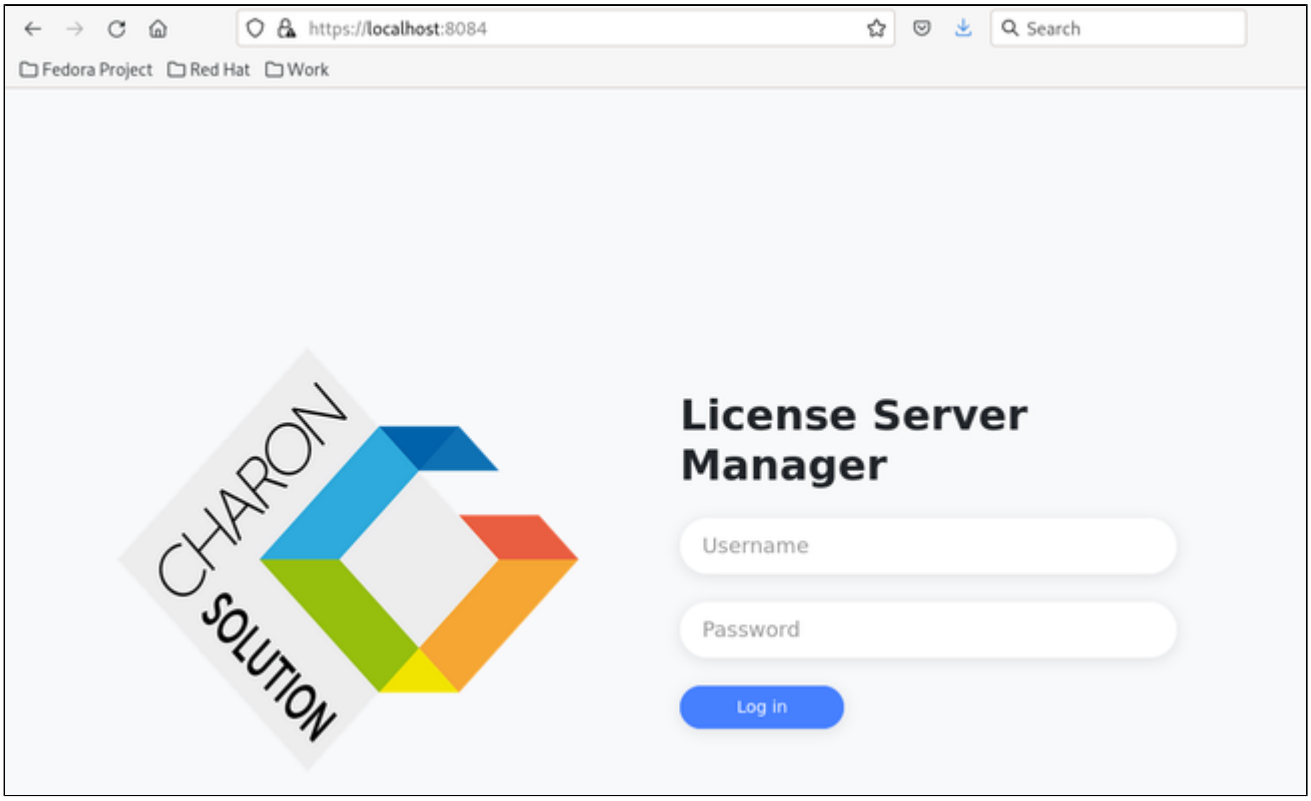
Use the following URL in any web browser to access the management GUI:
`https://``<host>`**`:`**`<port>`**`/`** where

- *host* is the name or address of the VE license server, and
- *port* is the TCP port (8084 by default).

Use *localhost* as the hostname for accessing the GUI of a license server running on the local system. Example: **`https://localhost:8084`**. Using just **`http://<license-server-ip>`** will redirect to the configured HTTPS port.

Please note: any intermediate firewall must allow the TCP ports used for the management GUI.

Upon connecting to the URL, a login screen will be displayed.



Default credentials:

- Username: **charon**
- Password: **stromasys**

After logging in, you will be presented with a list of menu options on the left pane of the screen and the content of the selected option on the right hand. **Please change the default password immediately**.

Certificate Warning when Connecting to the Management GUI

When connecting to the VE license server web-based management GUI for the first time, the web browser will issue a warning and inform the user that the connection is not private. This is due to the fact that Stromasys, when creating the installation kit, cannot foresee the actual customer environment. Thus, the SSL certificate included with the license server kit includes a dummy hostname that does not match the real hostname of the customer license server system, and it also contains Stromasys as the certificate authority which is unknown to web-browsers by default.

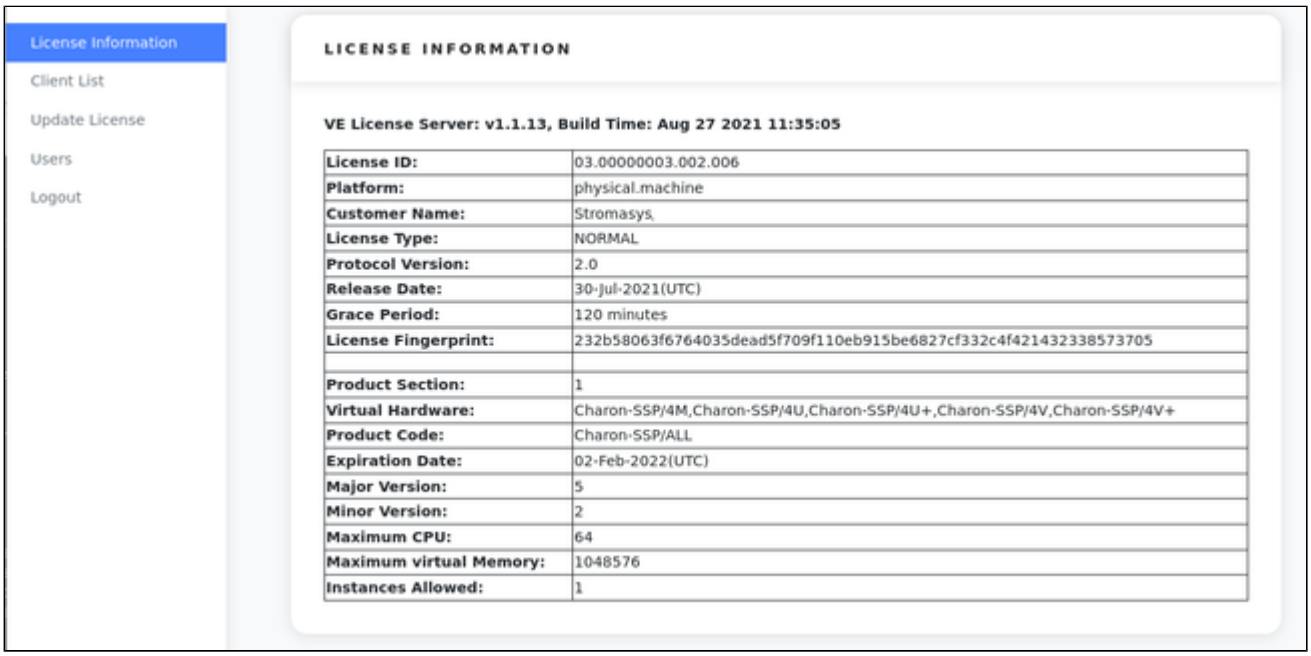
It is possible to override the warning and connect to the page. Otherwise, users must

- **either** obtain a certificate for the host from one of the **commercial certification authorities**, **or**
- they must create **their own self-signed certificate** and add it to the web browser.

See Certificates Used by the VE License Server for more information.

Displaying the License Information

The first screen after login is the license information screen similar to the one shown below:



It can be selected via the menu on the left (**License Information**).

Displaying the List of Connected Clients

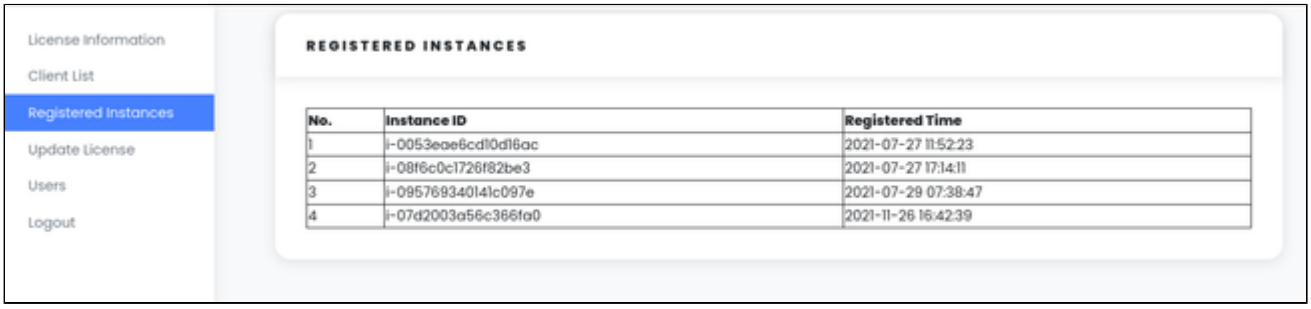
The client list can be displayed by selecting the **Client List** option on the left pane. A sample with one connected client is displayed below:

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	CHARON-SSP/4M	v5.2.8	1	64	2021-12-13 11:52:18	1
2	127.0.0.1	CentOS Linux release 7.7.1908	Charon-PA9-64-L4	v3.0.21905	-	-	2021-12-13 12:02:19	5

Please note: Charon-PAR license clients cannot inform the license server about the configured number of CPUs and amount of memory. Hence, for these clients, the corresponding fields in the display will be empty.

Displaying the List of Registered Clients (AutoVE mode)

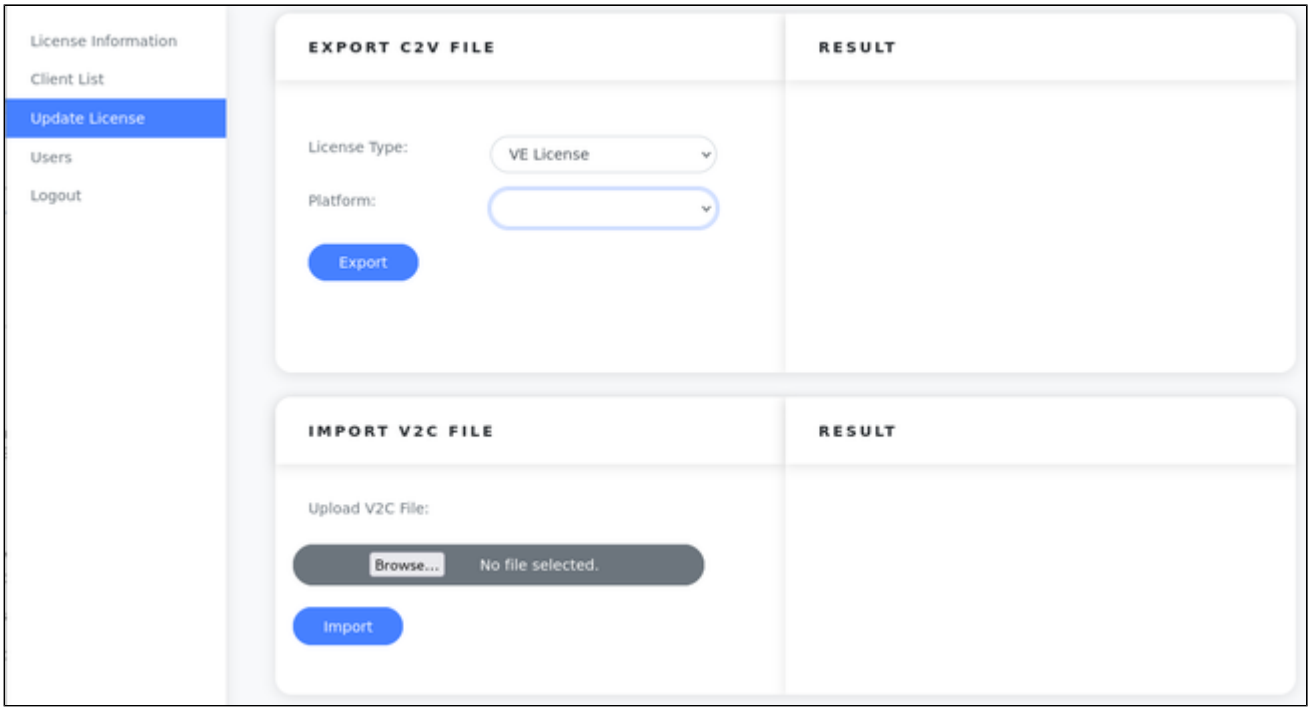
This option shows clients registered with the AutoVE license servers independent of whether the instance is active.



No.	Instance ID	Registered Time
1	i-0053eae6cd10d16ac	2021-07-27 11:52:23
2	i-08f6c0c1726f82be3	2021-07-27 17:14:11
3	i-095769340141c097e	2021-07-29 07:38:47
4	i-07d2003a56c366fa0	2021-11-26 16:42:39

Updating a License

The license management section can be opened by selecting **Update License** on the left pane. This will open the license management screen as shown below:



The license management section includes two options:

- Exporting a C2V file (the fingerprint of the license server system)
- Importing a V2C file (the license file created by Stromasys after receiving the C2V file)

The result panes show the result of the operation including any errors that may have occurred.

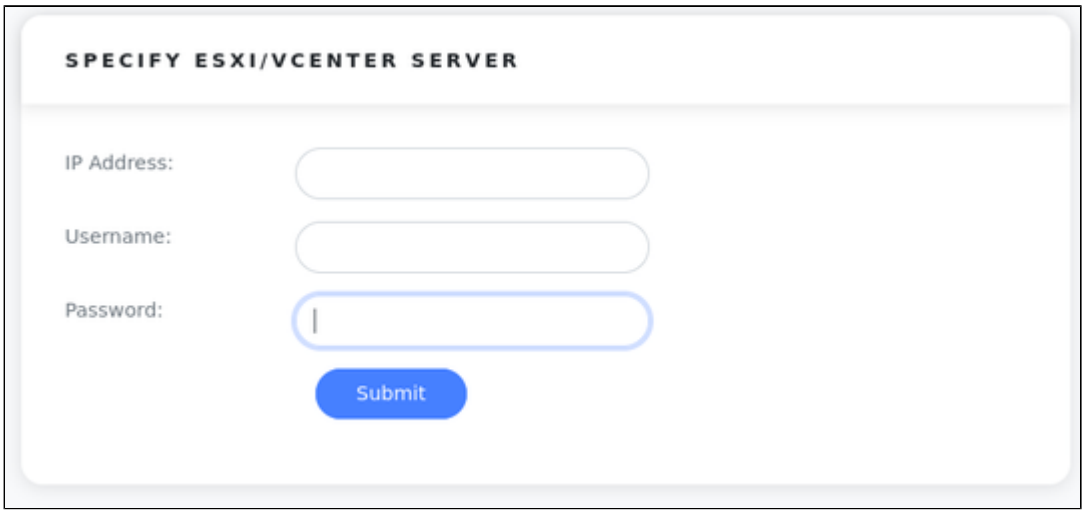
Exporting a C2V File

As an alternative to the command-line program for C2V export, you can create your C2V file via the management GUI. The section for C2V export has two input fields described below:

Field	Description
License Type	Options: • **VE License**: select if the license server operates in general VE license mode. • **AutoVE License**: select if the license server operates in AutoVE mode. General VE license mode and AutoVE mode are mutually exclusive.
Platform	Drop-down menu to select platform on which the license server runs. This list is different depending on the mode in which the VE license server runs: Platforms supported by general VE license mode: • Amazon AWS • Oracle OCI • Microsoft Azure • Google GCP • IBM Cloud • Nutanix AHV • VMware ESXi • Physical Machine The platform selected must match the platform on which the license server host system runs.
	Platforms supported by AutoVE mode: • Amazon AWS • Oracle OCI • Microsoft Azure • Google GCP The platform selected must match the platform on which the license server host system runs.

Steps to export a C2V file:

1. Enter the correct **License Type**.
2. Select the correct **Platform**.
   a. If the chosen platform is **VMware ESXi**, there will be an additional menu indicated by **three dots**. Click on this option to open the esxi_bind configuration window.



   Enter the IP address and the login information of the ESXi host or vCenter Server to which the license server should bind.
   Then press **Submit**.

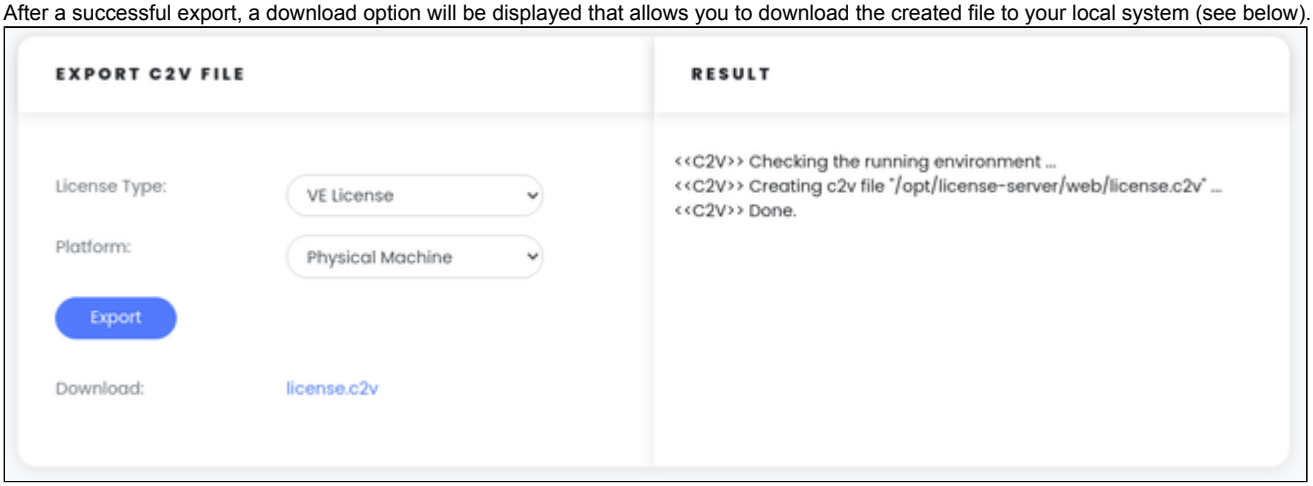
   Important notes regarding the user on the ESXi host or the vCenter Server:

   i. The **username on the vCenter Server** can take different forms:
      - Simple username
        example for web-GUI: `myusername`
        example for esxi_bind command: `-u myusername`
      - Username includes a domain name in one of the following two formats:
        - *<domain>**<username>*
          example for web-GUI: `mydomain\myusername`
          example for esxi_bind command: `-u 'mydomain\myusername'`
        - *<username>*@*<domain>*
          example for web-GUI: `myusername@mydomain`
          example for esxi_bind command: `-u myusername@mydomain`

   ii. The user must have at least the following **global permissions** (i.e. the permissions cannot be limited to a specific VM):
      - Datastore > Allocate Space
      - VirtualMachine > Config > AddNewDisk
      - VirtualMachine > Config > RemoveDisk

   Please note: if username and/or password contain Unix shell meta-characters, these characters must be escaped (enclose the string in single quotes, or add a backslash character in front of the meta-character).
3. Click on **Export** to create the C2V file.

4. After a successful export, a download option will be displayed that allows you to download the created file to your local system (see below).



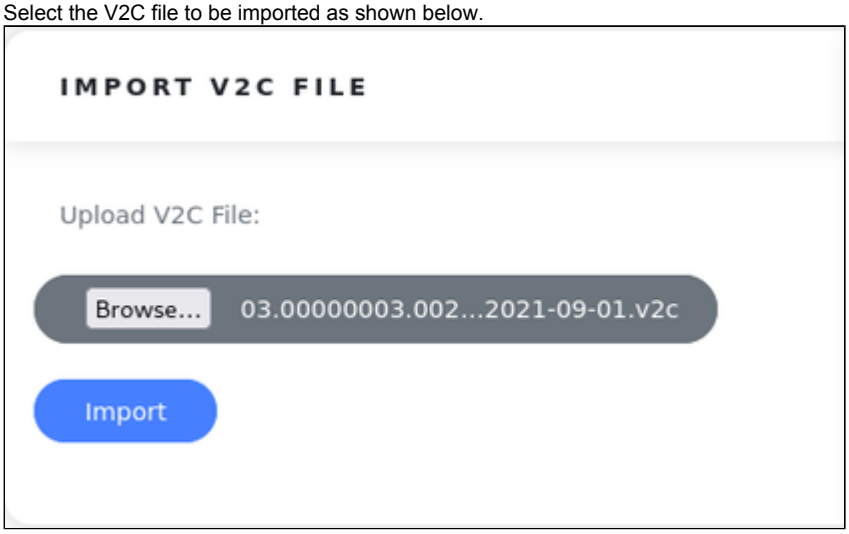
Send the C2V file to Stromasys for them to create a license.

Importing a V2C File

In response to the C2V file sent, you will receive two files from Stromasys. One text file containing the license content in human-readable form, and the V2C license file.

You can import the V2C license file using the **v2c** command-line utility, or you can use the web GUI. In the section **Import V2C File** perform the following steps:

1. Click on **Browse** to open a file browser.
2. Select the V2C file to be imported as shown below.



3. Click on **Import** to import the new/updated license. You will receive a message about the license import being complete. The license server will restart and you have to re-login to the GUI.
4. Check the new license via the **License Information** tab.

Managing Web-GUI Users

The access to the web GUI requires a username and a password. The **Users** section enable the management of such users. They are separate from the Linux system users.

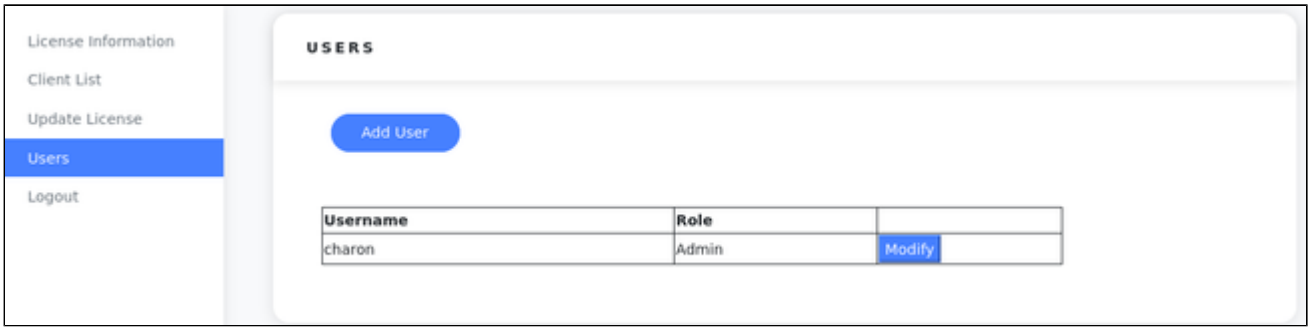
Default credentials:

- Username: **charon**
- Password: **stromasys**

Each user can have one of two roles: **Admin** or **Guest**. The role cannot be changed after a user has been created.

Admin users have access to all options. Guest users can only display information and change their password.

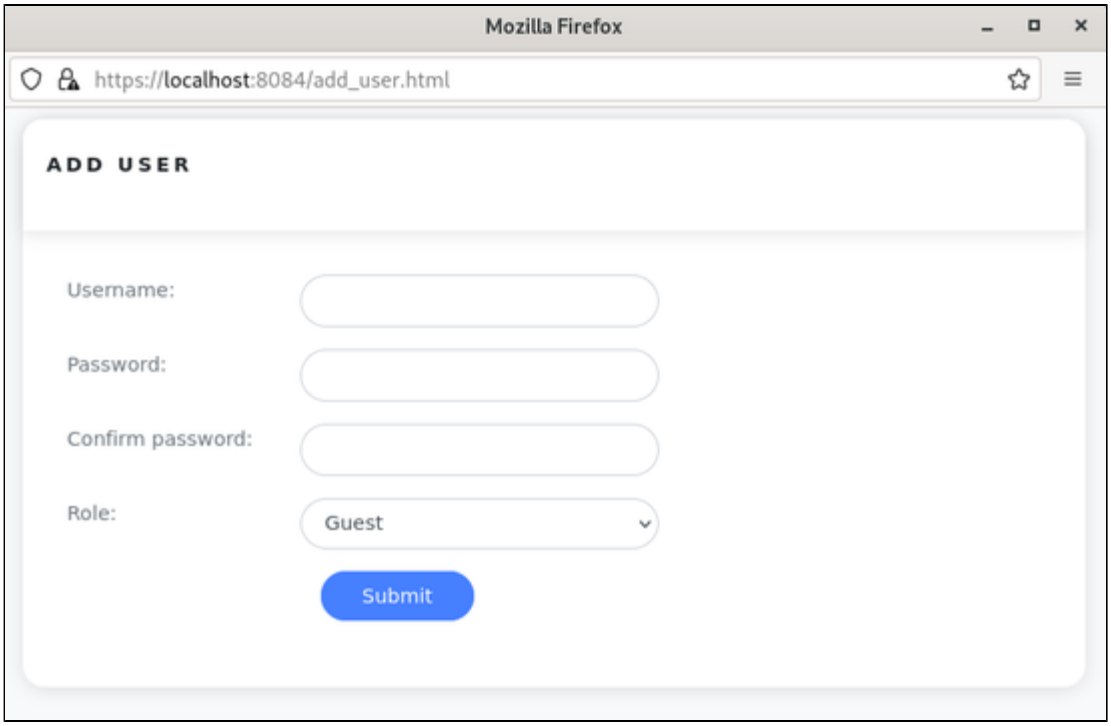
The following image shows the initial user overview:



Available options on the **Users** screen:

- **Add User**: add a new web GUI user
- **Modify**: change the password of a user
- **Remove**: available for additionally created users. Not available for the default user.

Clicking on **Add User** opens a pop-up-window similar to the following:

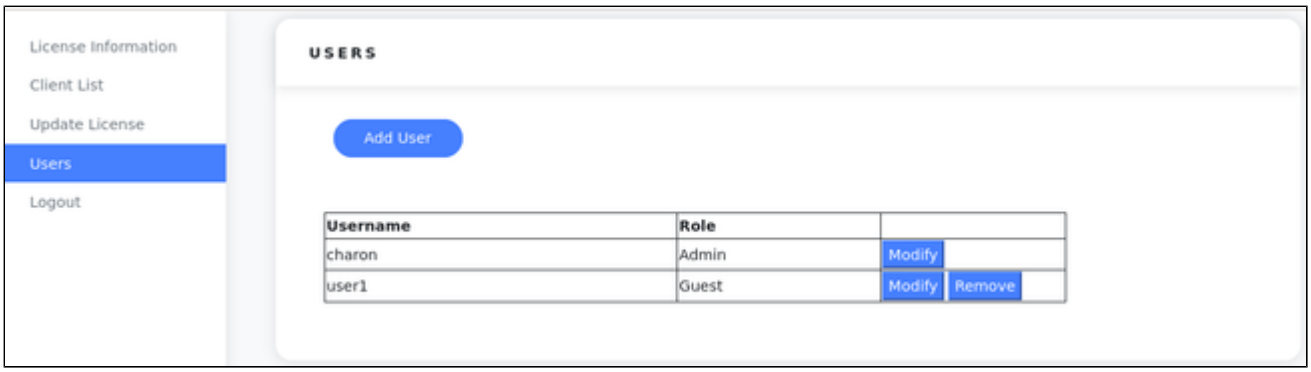


You can set the following parameters:

- Username
- Password
- Role (to change the role of a user later, the user must be deleted and recreated)

Click on **Submit** to create the user.

The following shows a list with two additional users for which the **Remove** option is also available.



Clicking on **Modify** will open a window similar to the **Add User** window - with the difference that only the password change option is enabled.

Resetting a lost Admin Password

If the password of the admin user **charon** is lost it can be reset via the command-line.

As the **root** user, use the following command:

```
# /opt/license-server/license_server -p
```

You will be prompted for the new password twice.

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 emulator products.

Contents

Sentinel/Gemalto Tools not Applicable to the VE License Server

Any Sentinel/Gemalto-specific license tools provided with the emulator installation are not applicable to the VE license server configuration.

Sentinel/Gemalto-specific tools and configuration options in Charon emulator kits:

In Charon emulator kits, the Sentinel/Gemalto-specific license tools and configuration options are available when installing the complete emulator packages. These tools and options are in particular the following:

- Charon-SSP:
  - 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*
- Charon-PAR:
  - The command-line tools in */opt/charon/bin* (including the update tool **hasp_update**, and the license viewer and C2V creation tool **hasp_srm_view**)
  - The license_id configuration parameter is not supported. To choose a specific product section, the passphrase of the section is used.

The above tools and commands cannot be used for managing VE licenses. Please ignore them if you have a VE license.

Actions that Can Invalidate a VE License

For cloud deployments: 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. **Please note that is not possible to use such a backup to revert to a previous license version**.

However, the following actions will **invalidate the license**:

1. All supported VE license server platforms:
   - 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.
   - Copying the virtual machine on which the license server runs. This includes cloning a virtual machine, or recovering a backup into a new virtual machine.
   - Changing the number of CPU cores of the license server system.
2. VMware VE license server platforms:
   - Restrictions from point 1 above.
   - If the license server is bound to the ESXi host: using vMotion on the VM in which the VE license server runs.
   - If the license is bound to a vCenter server:
     - Using vMotion to move the VM in which the license server runs to a system not controlled by the same vCenter.
     - Restoring the license server from a backup or snapshot and rebinding the restored license server to a new vCenter server (e.g., DR case).
   - Changes to the API interface of the ESXi host or vCenter Server.
   - The license can become temporarily unavailable if the user credentials or address information recorded by esxi_bind are changed. In this case, esxi_bind must be run again to define the correct user credentials and address information.
3. AutoVE license server platforms:
   - Restrictions from point 1 above.
   - Charon emulator host instance register with their license server only once at start.
     This is recorded on the license server in **/opt/license-server/instances.db**.
     If this file is lost, the license is not invalidated from the license server's point of view, but it can no longer be used from the Charon host instances as they will not register a second time. The Charon host instances would have to be recreated (fresh instance launch from a supported marketplace instance). Therefore, it is very important to backup up the instance database file. If a peer license server is used, the databases are synchronized between the two servers providing another level of data backup.
   - If the virtual hardware of the Charon emulator host is changed significantly (for example, the number of CPUs), then the registration of the Charon emulator host with the license server will be invalidated requiring that a new instance to be launched.
   - AutoVE server and Charon host instance must be in the same cloud and the Charon host instance must be launched from a supported AL marketplace image.
4. Physical VE license server platforms:
   - Restrictions from point 1 above.
   - Replacing the boot disk (i.e., the disk on which the operating system is installed).

If your license is invalidated for whatever reason and you cannot revert the action that caused the invalidation, **you must request a new license from Stromasys**. Therefore, planning your license infrastructure should include a **backup license server** to insure continuity until you received your new primary license.

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`**

The **licensed** service logs information to its log file in **/opt/license-server/log/license.log** and to **journalctl**.

Primary and Backup License Server / Peer Servers

General Information

Charon emulators for VE licenses support a backup license server to ensure service continuity should the primary license server become temporarily unavailable. The primary/backup servers in general VE license mode operate differently from the peer servers of AutoVE mode:

- For **general VE license mode**, backup licenses are typically limited to a certain number of emulator runtime hours. The backup license server is only used for failover if the primary license server fails in order not to deplete the available runtime hours unnecessarily.
- For **AutoVE mode**, the two license servers act as peers between which the client database is synchronized. The total number of instances available on both servers determines the number of Charon host cloud instances that can be licensed from the license server pair. Each instance can connect to either of the two servers. However, if one of the peers fails and there are not enough available instances on the second peer, there is no backup for an instance trying to fail over to the second peer due to failure of its primary server - and the emulators running on this instance will fail. The license on the server designated as backup server can be a countdown license (specified number of runtime hours) or a normal license.

The example below shows the output of a time-limited license:

```
# /opt/license-server/license_viewer
<<License Viewer>> Current license:
License fingerprint: 07792211fc8ce3fdc085 <truncated>
Customer name: Stromasys
License ID: 01.00000001.002.020
Key type: COUNTDOWN
Expiration date: 100 hour(s)
Platform: amazon.aws
Release date: 2021-06-17 13:08:01
Grace period: 120 minutes
License check interval: 60 minutes

Virtual Hardware: Charon-SSP/4M,Charon-SSP/4U
Product code: Charon-SSP/ALL
Expiration date: 2021-12-22 23:55:00
Major Version: 5
Minor Version: 3
Maximum CPU: 64
Maximum virtual memory: 1048576MB
Instances allowed: 3
```

The above sample is a backup license with 100 hours of emulator runtime. The remaining hours can be checked via the web interface.

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 (default for general VE license mode) or 24 hours (default for AutoVE mode), after the loss of the license has been detected, the emulator will stop. The grace period is defined on the license.

Please note: If you do not have a valid backup license and the primary license server is unavailable for more than the grace period, make sure to shut down the 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 in VE license server mode.

Log Files

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

License Server Log File

Log File Location

License server log file **/opt/license-server/log/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. The grace period implementation changed several times. In VE versions before version 4.1.21, the grace period was 24 hours. It was shortened to two hours after the introduction of the backup license server feature in 4.1.19. Since version 1.1.12, the grace period is determined by the corresponding license parameter. 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 software checks for compatible protocol versions between license server and emulator software. It logs an error if the versions are not compatible.

The following messages may logged in older versions:

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

```
2021-08-10 17:03:42 FATAL VE       License server is unavailable!
```

Newer versions have a more descriptive error message:

```
2021-08-10 17:16:41 ERROR VE       License protocol version is invalid.
```

Charon-PAR Emulator Log Files

The **default location** for the Charon-PAR emulator log files is the directory in which the emulator was started. The name and location can be influenced via the configuration file and using a start-up parameter.

By default log file name is **`charon-par.`***`<YYMMDD>-<timestamp>-<incremental number>`***`.log.`**

The link **`charon-par.log`** points to the current log file.

Log File Samples

Working license found during emulator start:

```
20211213:120216.970965:Trying to login to license server: 127.0.0.1
20211213:120219.975731:License allowed CPUs: 8.
20211213:120219.975746:License allowed memory size: 32768.
20211213:120219.979873:Connected with license server: 127.0.0.1
20211213:120219.979900:Found available license ID: 03.00000003.002.006.
20211213:120219.979908:Customer name: Stromasys
20211213:120219.979915:Grace period is 120 minutes.
20211213:120219.979928:Virtual hardware model Charon-PA9-64-L4 is licensed.
20211213:120219.979937:Maximum concurrent instances are limited to 10.
20211213:120219.979950:Maximum allowed virtual CPU(s) are 8.
20211213:120219.979959:Maximum allowed virtualized memory is 32768 MB.
20211213:120219.979967:Major allowed version number is 3.
20211213:120219.979976:Minor allowed version number is 0.
20211213:120219.979988:Expiration UTC time: 2022-06-08 23:55:00.
20211213:120219.980216:Product Name = Charon-PA9-64-L4 License key ID = 03.00000003.002.006.
```

License server not found at start:

```
20211214:193342.307175:VE primary license 192.168.2.2
20211214:193342.307701:There is no VE backup server.
20211214:193342.334171:Trying to login to license server: 192.168.2.2
20211214:193351.337196:warn:Unable to login to server because the license server failed to respond
20211214:193351.337392:err:Failed to connect with the license server.
20211214:193351.337457:err:Failed to connect with the license server.
20211214:193351.337509:err:Exit
20211214:193351.339823:err:Invalid license product name
```

Charon-AXP/VAX Emulator Log Files

The **default location** for the Charon-AXP/VAX emulator log files on Linux (Linux is required for VE licensing): if the setting of the template configuration is used, the default is the directory from which the emulator instance was started.

The name and location can be influenced via the configuration file.

By default log file name is *<model-name>***.log.**

Management GUI Web Server Log File

This log file contains errors encountered by the web server providing the management GUI of the VE license server.

Log file location: **/opt/license-server/log/webserver.log**

Sample content:

```
$ cat /opt/license-server/log/webserver.log

<attempt to start the license server a second time>
[1636549131] [error] [client ] cannot bind to 80: 98 (Address already in use)
[1636549131] [error] [client ] cannot bind to 8084s: 98 (Address already in use)
[1636549131] [error] [client ] Failed to setup server ports

<restart of the license server>
[1636551531] [error] [client 192.168.2.80] SSL syscall error 104
[1636551532] [error] [client 192.168.2.80] SSL syscall error 104
```

Updating a VE License

Please note: some parameters (e.g., the license ID and the owner of the license) cannot be changed by an update. In such cases, it is necessary to remove the existing license and then create a C2V for a new license to be created.
See also *Verifying License Installation and License Content* in Installing a License on the VE License Server, and Removing a License from a VE License Server.

An update to a license may become necessary due to

- the expiration date being reached,
- Charon emulator product upgrade,
- additional Charon emulator 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. The new license update will automatically remove the previously installed license version (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 instances before upgrading the license server.
- Please refer to the general Charon user's guide for information on how to upgrade the Charon emulator software.
- **If the old license server was uninstalled before installing the new version** (instead of performing an upgrade), the license (V2C file) must be imported again using the v2c utility.

In the description below, the placeholders used have the following meaning:

- *<mykey>* is the private key of the key-pair you associated with your cloud instance
  (for an on-premises VMware installation or an installation on a physical system where logging in with username/password is allowed, this is not needed).
- *<user>* is the user associated with your license server instance (e.g., *opc* on OCI, *centos* for a CentOS instance on AWS, or the custom user on your VMware virtual machine;
  for an instance installed from a Stromasys-provided Charon AL or VE emulator marketplace image, use user *charon* for SFTP and user *sshuser* for interactive login.
- *<linux-ip>* is the ip address of your license server system.

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

1. **Copy the license server software package to the license server host (if needed)**:
   a. For example, use **sftp** to connect to the VE license server system.
      `# sftp -i ~/.ssh/<mykey> <user>@<linux-ip>`
   b. Copy the software package to the license server system using the following SFTP command:
      `> put <local-path-to-license-server-package>`

2. **Use ssh to log in on the license server host**.
   `# ssh-i ~/.ssh/<mykey> <user>@<linux-ip>`

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>`
      If you used SFTP to copy the package to an instance installed from a prepackaged Charon marketplace image, the home directory of the *charon* user and the default location for file transfers is */charon/storage*.
   c. For VE license server 2.2.4 and above, unpack the archive and agree to the end-user license agreement:
      i. `# chmod a+x license-server-<version>.rpm.sh`
      ii. `# ./license-server-<version>.rpm.sh`
      This will display the EULA. After agreeing to it, the RPM installation package will be unpacked in the current directory.
   d. Install the package:
      i. Linux 7.x: `# yum update license-server*.rpm`
      ii. Linux 8.x and 9.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:

- Review the content of the license server log: **/opt/license-server/log/license.log**
- Use the ps command to check that the server is running:
  `# ps -ef |grep license-server`
- Starting with version 1.1.18, a new parameter to the license server is available to display the license server status:
  `# cd /opt/license-server`
  `# ./license_server -s`

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.
- Shut down any running emulator guest systems depending on this license server.
- Please refer to the general Charon user's guide for information on how to remove the Charon emulator software.
- **If you re-install the license server again after the deinstallation**, the license (V2C file) must be imported again using the v2c utility.

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

1. Use ssh to log in on the license server instance.
   `# ssh -i ~/.ssh/<mykey> <user>@<linux-ip>`
   a. <*mykey*> is the private key of the key-pair you associated with your cloud instance
      (not needed for an on-premises VMware installation that allows login with username/password).
   b. <*user*> is the user for interactive login associated with your license server instance (e.g., *opc* on OCI, *centos* for a CentOS instance on AWS, or the custom user of your VMware host;
      for an instance installed from a prepackaged, supported Charon marketplace image, use *sshuser*)
   c. <*linux-ip*> 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:

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

The 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**: to run on the IBM cloud • **nutanix**: to run on Nutanix AHV • **esxi**: to run in a VMware environment • **physical**: physical host system
`-a, --auto`	Create a C2V for an AutoVE license (mutually exclusive with general, non AutoVE licenses).
`-t, --transfer`	Export a transfer file (.tfr) to transfer the license to another system.
`-d, --debuglog`	Print a debug log.
`-h, --help`	Print the usage information. Default if no parameter is selected.

The v2c Utility

The **v2c** (Vendor-to-Customer) 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.
`-s, --silent`	Run v2c in silent mode. New in version 1.1.23. Using this option will suppress the change confirmation dialog when updating an existing license.
`-d, --debuglog`	Print a debug log.
`-h, --help`	Print the usage information. Default if no parameter is selected.

Please note:

- If the V2C file installed is an **update** to an existing license, the **v2c** command will first **show the difference** between old and new license and wait for the user confirmation before proceeding with the update. If absolutely required, this behavior can be suppressed using the **-s** option. **Carefully review the changes before accepting them**.
- To import the same license repeatedly will not cause a problem. In this case, the user will not be asked to confirm the import.
- The difference between old and new license is shown as a side-by-side list of the old and new license parameters. This list uses short parameter names to keep the old and new parameter on one line.

Example output of the comparison list:

```
<<V2C>> Going to import "/home/centos/03.00000003.002.007-2022-11-08.v2c" ...

Imported License:                                New License:

KEYSEC                                           KEYSEC

K_FINGER=5aaa364f9fc602323eaab2c8c4aa0bd07a9bf0b0d K_FINGER=5aaa364f9fc602323eaab2c8c4aa0bd07a9bf0b0d

K_LICENSE_ID=03.00000003.002.007                 K_LICENSE_ID=03.00000003.002.007

K_TYPE=NORMAL                                    K_TYPE=NORMAL

K_EXPIRED=10-MAY-2022 23:55:00                   K_EXPIRED=10-MAY-2023 23:55:00

<lines removed>
```

The license_viewer Utility

The **license_viewer** utility enables the user to displayed installed licenses.

Usage: **`license_viewer`** `[options]`

The options are described in the table below:

Option	Description
`-c, --client`	Displays the license clients connected to the server.
`-r, --register`	Displays the registered license clients.
`-o, --output` *`file.csv`*	Send command output to a CSV file. New in version 1.1.23.
`-u, --usage`	Shows license utilization. That is, it shows how many of the allowed instances for each product sections are currently used and how many instances are still available. New in version 1.1.23. After a license server restart, it could take up to one hour for the output to be correct again (time to the next connection made by the active emulators).
`-n`, **`--number`** *`count`*	Used in combination with the **`-r`** parameter, this parameter shows the last *count* hosts that registered with the AutoVE server. Useful especially for servers with many registered clients.
`-h, --help`	Print the usage information
No parameter	If run without parameters, the installed licenses will be displayed.

The esxi_bind Utility

The **esxi_bind** utility is used to establish the connection between license server and ESXi host or vCenter Server.

Usage: **esxi_bind** *[options]*

The options are described in the table below:

Option	Description
-a, --address *ip-address*	IP address of the ESXi host or vCenter Server.
-u, --username *username*	Username of a user on the ESXi host or vCenter Server. **Important notes regarding the user on the ESXi host or the vCenter Server:** 1. The **username on the vCenter Server** can take different forms: • Simple username example for web-GUI: `myusername` example for esxi_bind command: **`-u`** `myusername` • Username includes a domain name in one of the following two formats: ◦ *<domain>**<username>* example for web-GUI: `mydomain\myusername` example for esxi_bind command: **`-u`** `'mydomain\myusername'` ◦ *<username>*@*<domain>* example for web-GUI: `myusername@mydomain` example for esxi_bind command: **`-u`** `myusername@mydomain` 2. The user must have at least the following **global permissions** (i.e. the permissions cannot be limited to a specific VM): • Datastore > Allocate Space • VirtualMachine > Config > AddNewDisk • VirtualMachine > Config > RemoveDisk **Please note**: if username and/or password contain Unix shell meta-characters, these characters must be escaped (enclose the string in single quotes, or add a backslash character in front of the meta-character).
-p, --password *password*	Password of the user specified in the username option.
-d, --debuglog	Print a debug log.
-h, --help	Print the usage information. Default if no parameter is selected.

Please note: if username and/or password contain Unix shell meta-characters, these characters must be escaped (enclose the string in single quotes, or add a backslash character in front of the meta-character).

Command-Line Options of the License Server

The license server itself has some command-line options. They are described below.

Usage: **license_server** *[options]*

Option	Description
-p, --password	Change the password of the web GUI user **charon**. Available starting with version 1.1.14.
-s, --status	Display the status of the license_server. Available starting with version 1.1.18.
-l debug	Enable debug log output when starting the license server.
-h, --help	Print the usage information.
No parameter	If run without parameters, the system will attempt to start the license server.

Additional Information

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

Contents

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 (versions < 1.1.23 only)

Please note: this step is only required if running a VE license server with a **version earlier than 1.1.23**. Starting with version 1.1.23, this no longer is a requirement.

The Charon 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.

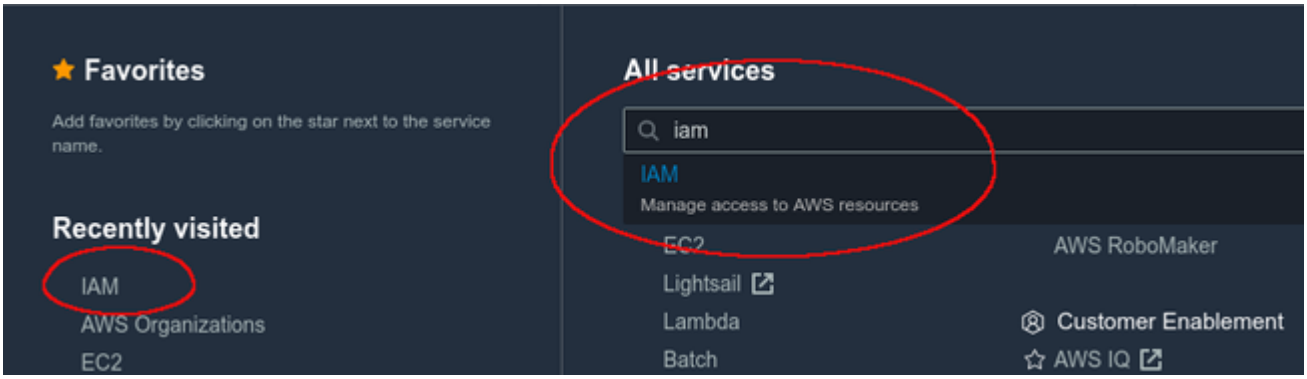
The basic steps to create and attach a new IAM role definition are the following:

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:

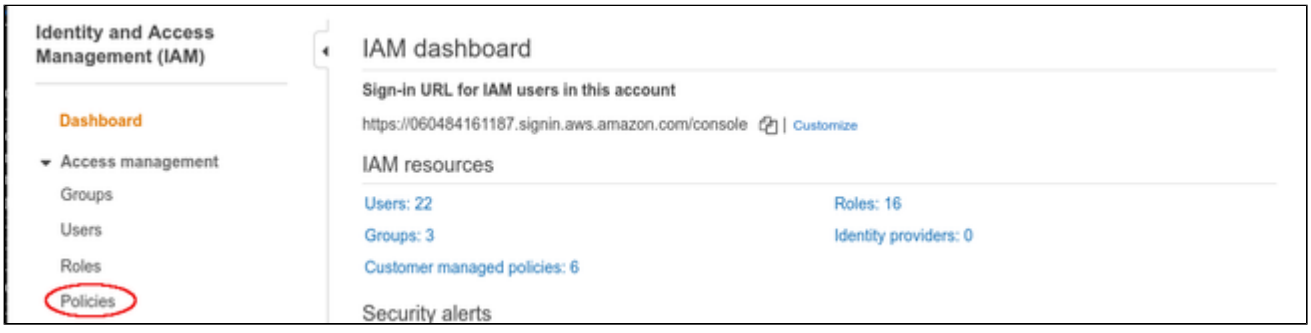
Open the services overview and search for IAM or open it from the Recently Visited list:



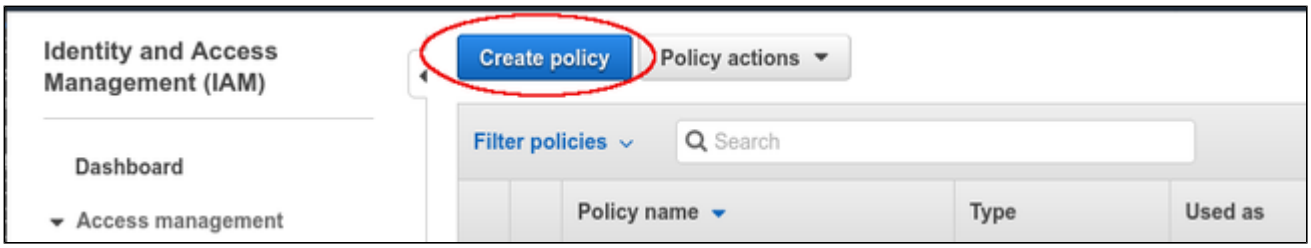
This will open the IAM dashboard.

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

Select **Policies** in the IAM dashboard:

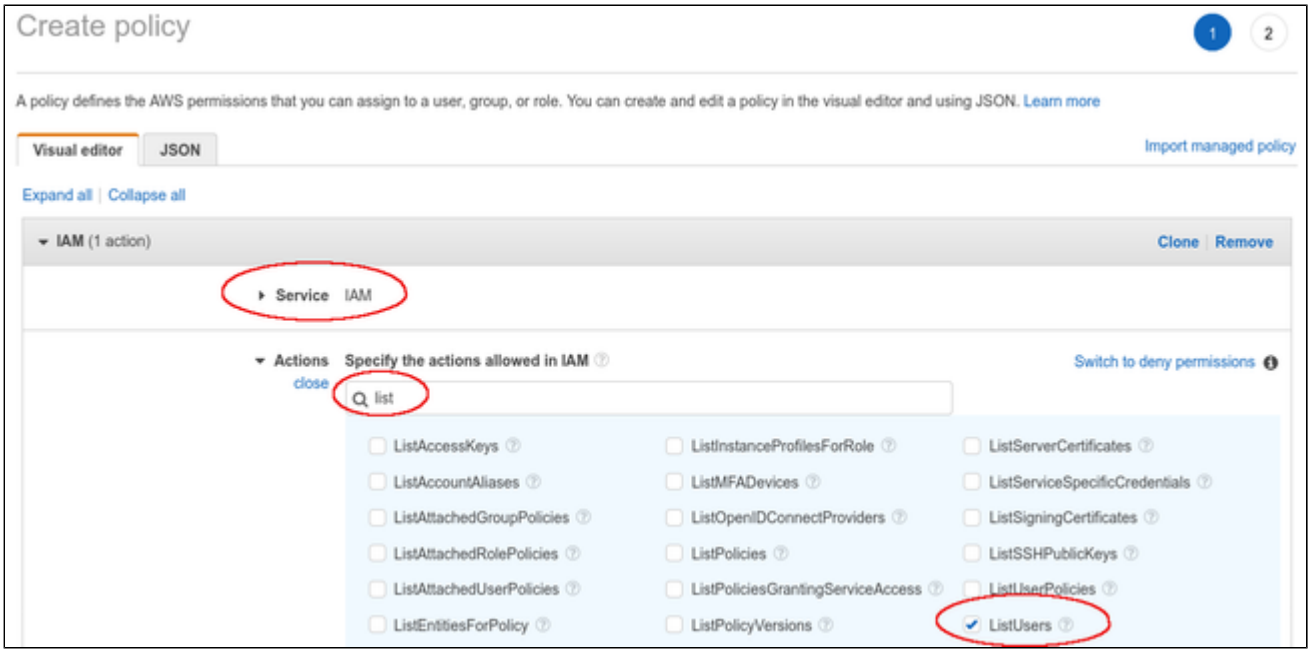


This will open a list of existing policies. If the required policy does not already exist, click on **Create policy** to create a new one as shown below:



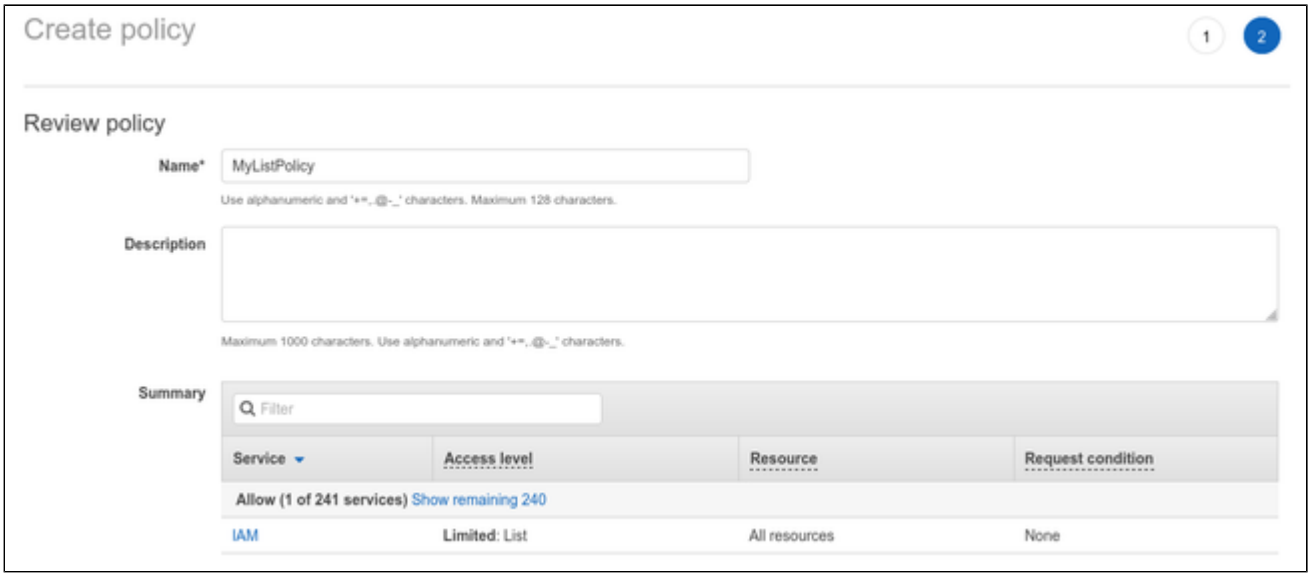
The **Create policy** window opens.

- 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**.

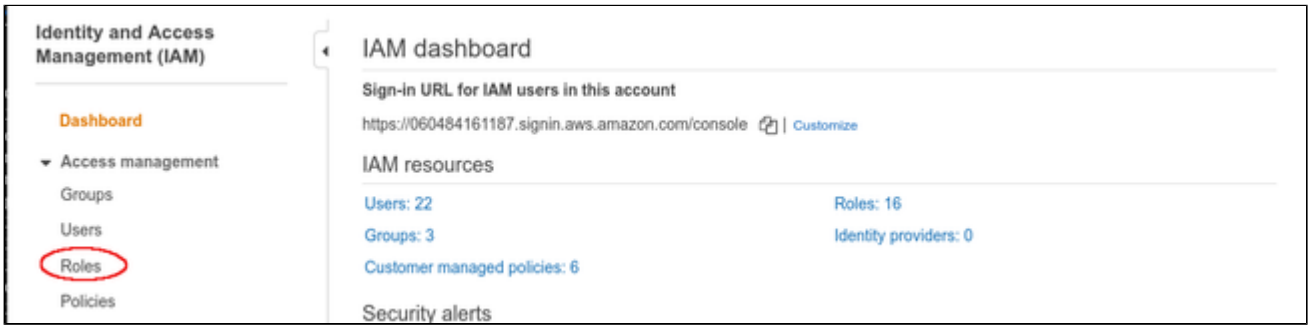
The review page opens:



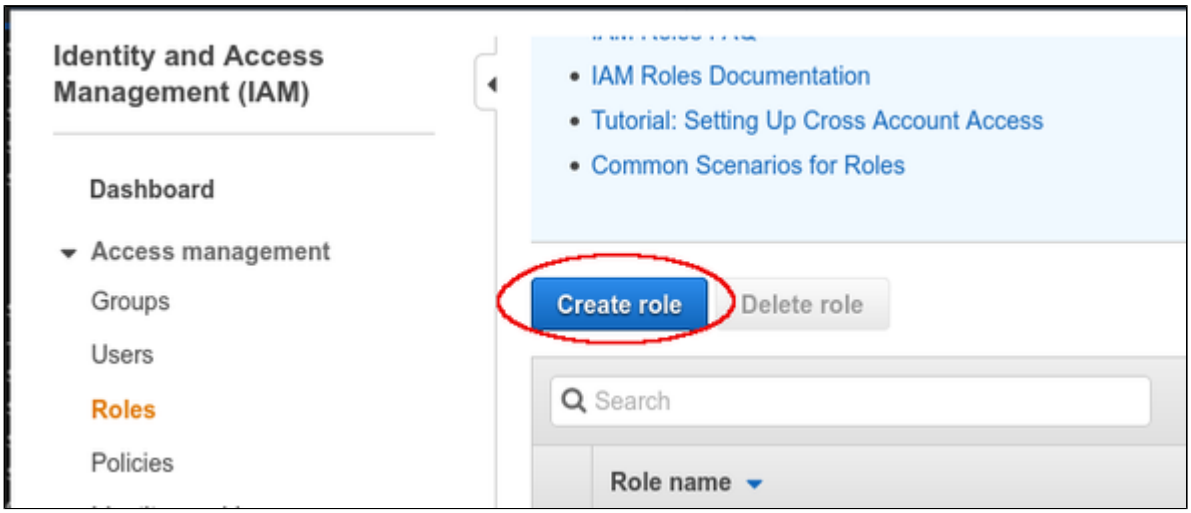
Add a name for the policy and click on **Create policy** at the bottom of the page.

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):

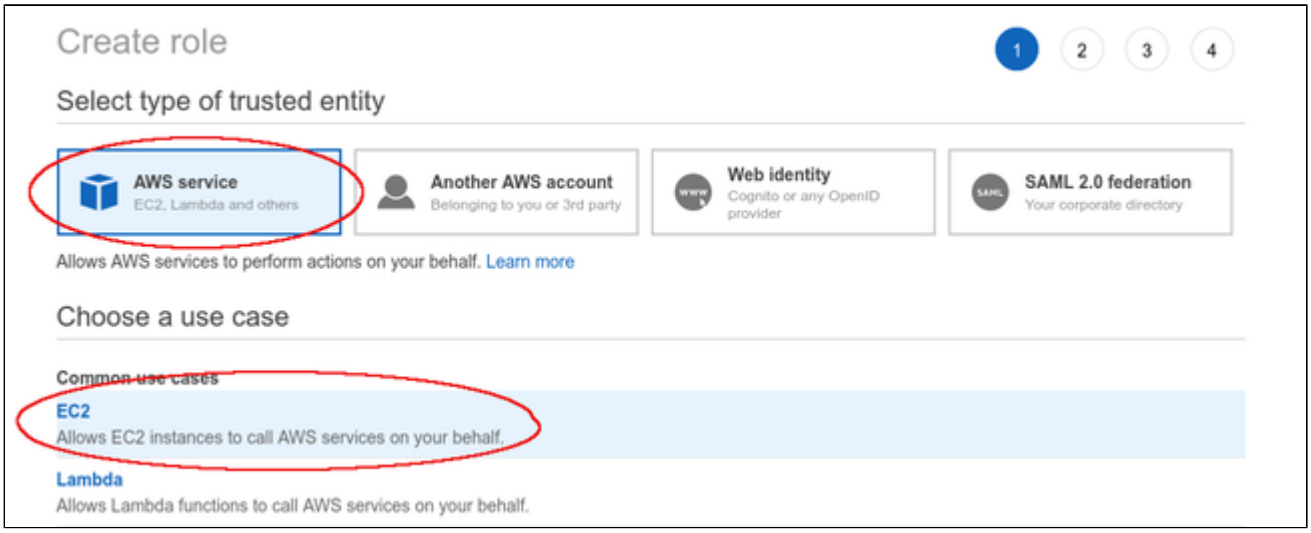


This will open a list of existing roles. To create a new role, click on **Create role**.



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.

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:

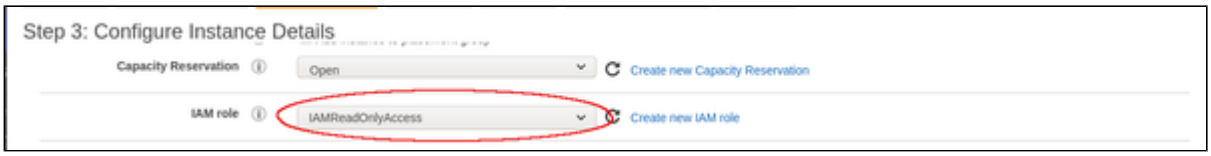
Then click on **Create role** at the bottom of the window to complete the creation of your role.

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.**

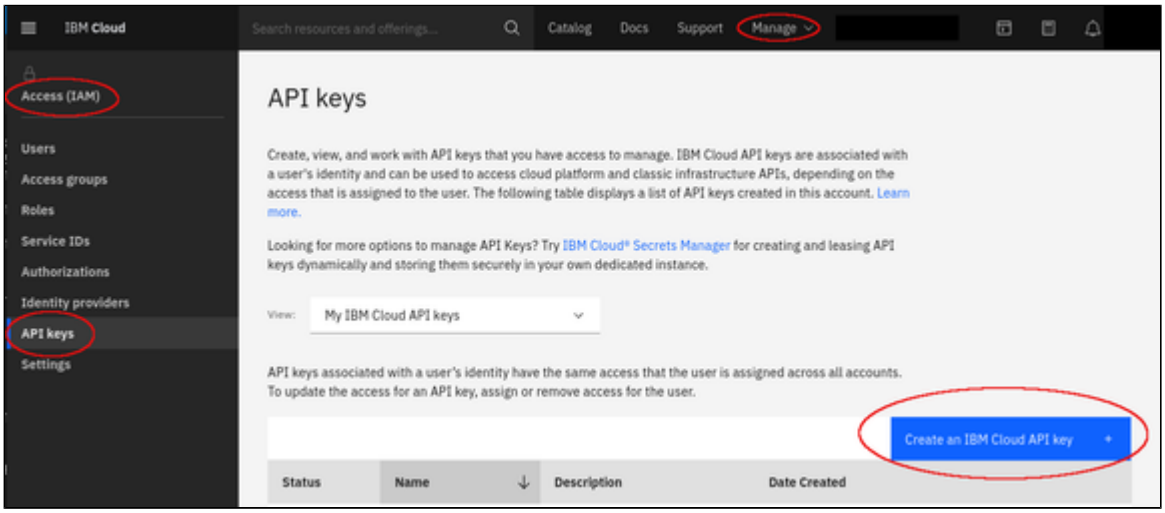
Creating and Installing an IBM API Key

The VE license server requires an API key (filename **apikey.json**) to be able to run on an instance in the IBM cloud. Perform the following steps to create and install this key:

Step 1: if you have not created an API key yet, create and download the API key.

You can use the same key for several license server systems. So this step may not be needed.

Go to **Manage > Access (IAM) > API keys** and click on **Create an IBM Cloud API key** as shown below:



This will open the **Create API key** window. In this window enter

- Name and
- Description

Then click on **Create**.

Please note: you will be offered to download the key for a short period of time after creating it. **This is the only opportunity to download it**. Therefore, download the key immediately.

Step 2: install the API key on the license server.

To install the key on the license server, do the following: copy the API key (name **apikey.json**) to the directory **/opt/license-server** on the license server instance in the cloud using your preferred method (e.g., SFTP).

Step 3: check if the license server starts normally.

If the key is missing, the license server log (*/opt/license-server/license_log/license.log;* starting with VE license server 1.1.11 the path is */opt/license-server /log/license.log*) shows the error message **Failed to find apikey.json file!** After the key has been correctly installed, this error should be gone.

Configuring AutoVE Information on the Charon AL Host

The AutoVE mode is an extension of the Automatic Licensing configuration available for selected cloud marketplaces.

Important restrictions:

- At the time of writing, AutoVE mode for Charon products is only available when using an **Automatic Licensing (AL) Charon-SSP marketplace image on AWS, GCP, OCI, or Azure (minimum version 5.3.8)** to create a Charon host instance. Please contact your Stromasys representative to get details on the availability of such marketplace images in your cloud environment.
- The AutoVE license server information must be configured before the Charon host instance is first launched. The information can be changed later, **bu t once the host system has connected to a public license server in the selected cloud, it cannot be reconfigured to use an AutoVE server (and vice-versa).**

Changed license server selection in Charon-SSP AL images starting with SSP version 5.6.8:

Starting with version 5.6.8, the license server selection in cloud-specific AL images has changed to simplify the operation of the SSP Amazon Linux AMI used in the new AWS service.

Case 1: **user provides no license server information** in the instance user data at initial instance launch:

a) If the file */opt/charon-license-server* exists and contains valid AutoVE server information, the cloud instance will use the AutoVE license servers specified in the file. This file exists by default in the SSP Amazon Linux AMI where it points to the public, Stromasys-operated AutoVE license servers specific to this AWS service. Such public AutoVE servers are only available in AWS at the time of writing.

b) If the file does not exist, the cloud instance will use the public, Stromasys-operated license servers (AL mode).

Case 2: **user provides AutoVE license server information** in the instance user data at initial instance launch.

The cloud instance will use the private, customer-operated AutoVE license servers.

The following sections will discuss the AutoVE configuration for a Charon host system:

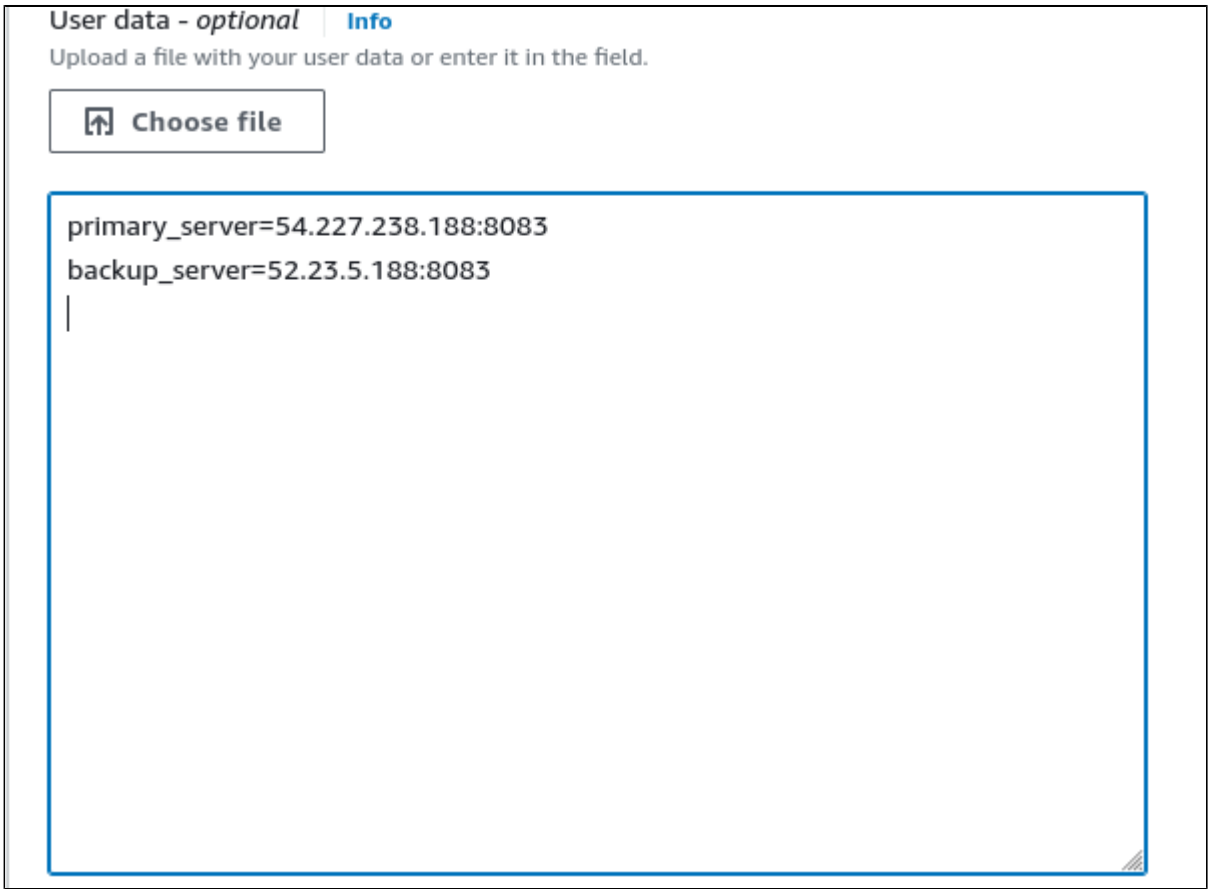
Charon AL Host Instance on AWS

Configuring the AutoVE Server Information at AWS Instance Launch

Please note:

- Should you use the SSP Amazon Linux AMI with **SSP version 5.6.8 or higher** as provided by the *AWS Mainframe Modernization - Virtualization for SPARC* service, the instance will by **default** connect to the **public, Stromasys-operated AutoVE license servers** (defined in */opt/charon-license-server*). You only need the **user data definition for older versions or to override the default** with your private AutoVE servers.
- The example below shows the appearance of the AutoVE license server information that is entered as **User Data** in the **Advanced Details** configuration section at the bottom of the **Launch an Instance** window during the initial configuration of an instance. **Scroll down** to the bottom of the configuration window to open and display the user data section in the **Advanced Details**.
- In the older GUI version, the **Advanced Details** section is part of the **Configure Instance** window - the layout is somewhat different, but the configuration options are the same.

Enter the information for the AutoVE license server as shown in the example below (it shows the public AutoVE servers):



Valid User Data configuration options:

- **`primary_server=`**`<ip-address>[:<port>]`
- **`backup_server=`**`<ip-address>[:<port>]`

where

- *<ip-address>* stands for the IP address of the primary and the backup server as applicable, and
- *<port>* stands for a non-default TCP port used to communicate with the license server (default: TCP/8083).

Please note: at least one license server must be configured at initial launch to enable AutoVE mode. This can be via the */opt/charon-license-server* file with the default public servers (SSP 5.6.8 or higher) or via the manual user data configuration. **Otherwise, the instance will bind to one of the public AL license servers operated by Stromasys.**

Changing the AutoVE Server Configuration After AWS Instance Launch

Once an instance has been launched, the AutoVE server information in the User Data can be changed. To do this, use the following steps:

- If the instance is running, it must be stopped (cleanly shut down any guest systems running in the Charon emulator before).
- Select your instance from the instance list, **right-click** on it and select **Instance settings > Edit user data.**
- Modify the AutoVE configuration in the user data as needed and click on **Save**.
- Activate the changes:
  - Restart the emulator instances and any required guest systems. It can take a minute or two until the change becomes active.
  - If changes are made to the VE license server configuration (e.g., changing the port numbers), the VE license server must also be restarted.

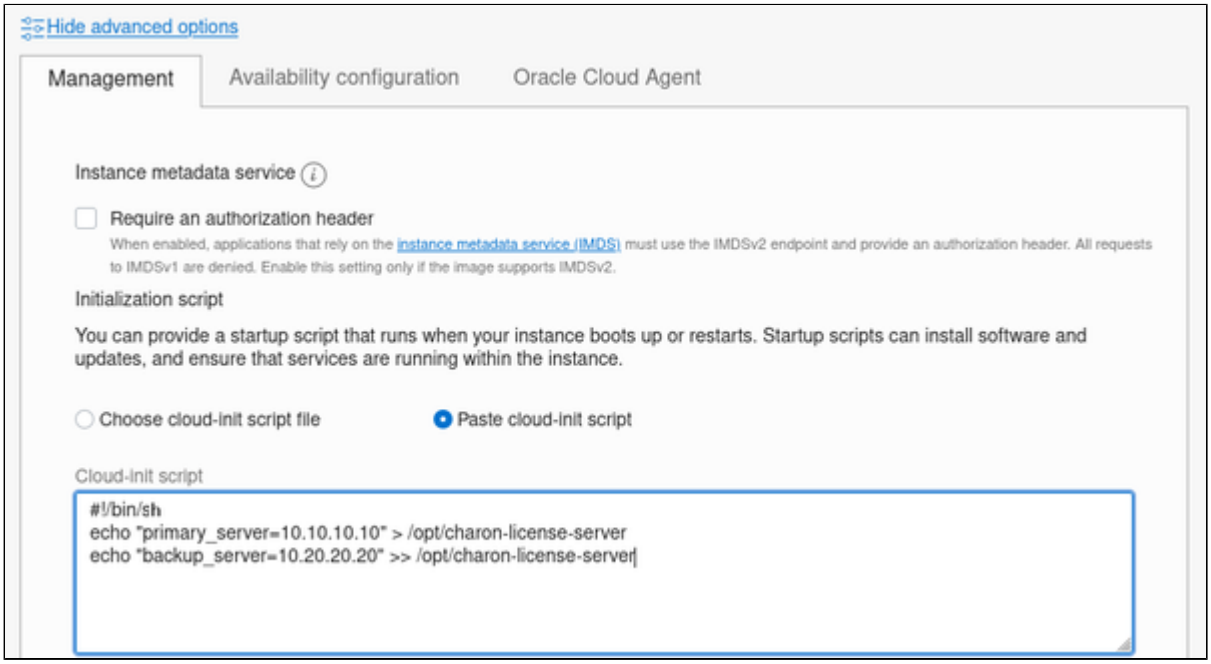
Please note: removing the AutoVE server configuration completely will **not** enable the instance to connect to the public license server

Charon AL Host Instance on OCI

Configuring the AutoVE Server Information at OCI Instance Launch

For OCI, you have to enter a cloud-init script at instance configuration in the **Advanced Options** section.

The following image shows an example:



Valid User Data configuration options:

- **`primary_server=`**`<ip-address>[:<port>]`
- **`backup_server=`**`<ip-address>[:<port>]`

where

- *<ip-address>* stands for the IP address of the primary and the backup server as applicable, and
- *<port>* stands for a non-default TCP port used to communicate with the license server (default: TCP/8083).

Please note: at least one license server must be configured at initial launch to enable AutoVE mode. **Otherwise, the instance will bind to one of the public license servers operated by Stromasys.**

Changing the AutoVE Server Configuration After OCI Instance Launch

Once an instance has been launched, the AutoVE server information in the User Data can be changed. To do this, use the following steps:

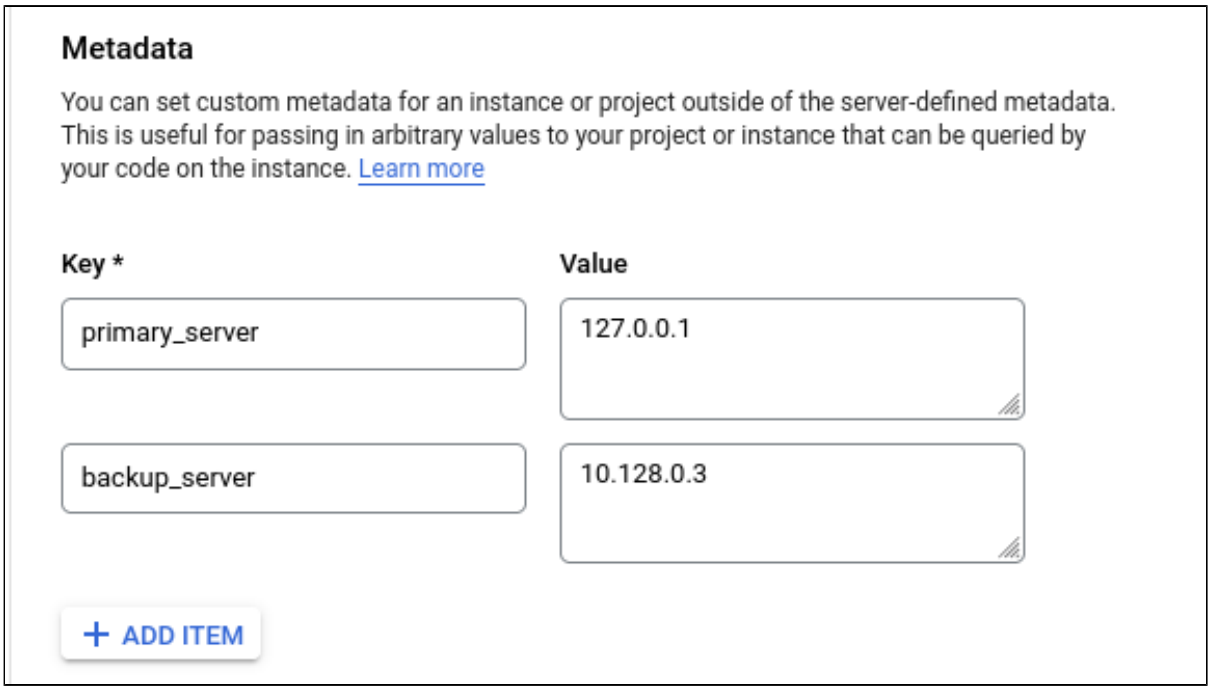
- The Charon host instance must be running.
- Log in to the Charon host instance as the **root** user.
- Open the file **/opt/charon-license-server** with a text editor.
- Modify the AutoVE configuration as needed and save the file.
- Activate the changes:
  - After cleanly shutting down any running guest operating systems, restart the emulator instances and any required guest systems. It can take a minute or two until the change becomes active.
  - If changes are made to the VE license server configuration (e.g., changing the port numbers), the VE license server must also be restarted.

Please note: removing the AutoVE server configuration completely will **not** enable the instance to connect to the public license server.

Charon AL Host Instance on GCP

Configuring the AutoVE Server Information at GCP Instance Launch

The AutoVE license server information is entered as **Custom Metadata**. In the initial instance configuration window, go to the bottom where the **NETWORKING, DISKS, SECURITY, MANAGEMENT...** configuration section is located. Open it and select the **Management** section. Add the Custom Metadata as shown in the example below:



Valid User Data configuration options:

- **`primary_server`** *<ip-address>*`[:`*<port>*`]`
- **`backup_server`** *<ip-address>*`[:`*<port>*`]`

where

- *<ip-address>* stands for the IP address of the primary and the backup server as applicable, and
- *<port>* stands for a non-default TCP port used to communicate with the license server (default: TCP/8083).

Please note: at least one license server must be configured at initial launch to enable AutoVE mode. **Otherwise, the instance will bind to one of the public license servers operated by Stromasys.**

Changing the AutoVE Server Configuration After GCP Instance Launch

Once an instance has been launched, the AutoVE server information in the Custom Metadata section can be changed. To do this, use the following steps:

- In the GCP management console, open the details window of your Charon host instance.
- Click on the **Edit** symbol at the top of the page.
- Scroll down to the Custom Metadata section.
- Modify the AutoVE configuration as needed and click on **Save** at the bottom of the page.
- Activate the changes:
  - After cleanly shutting down any running guest operating systems, restart the emulator instances and any required guest systems. It can take a minute or two until the change becomes active.
  - If changes are made to the VE license server configuration (e.g., changing the port numbers), the VE license server must also be restarted.

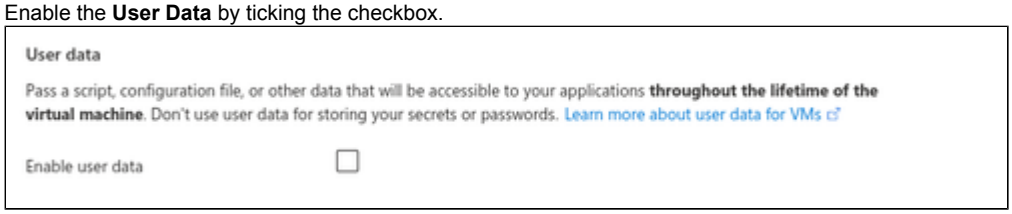
Please note: removing the AutoVE server configuration completely will **not** enable the instance to connect to the public license server.

Charon AL Host Instance on Azure

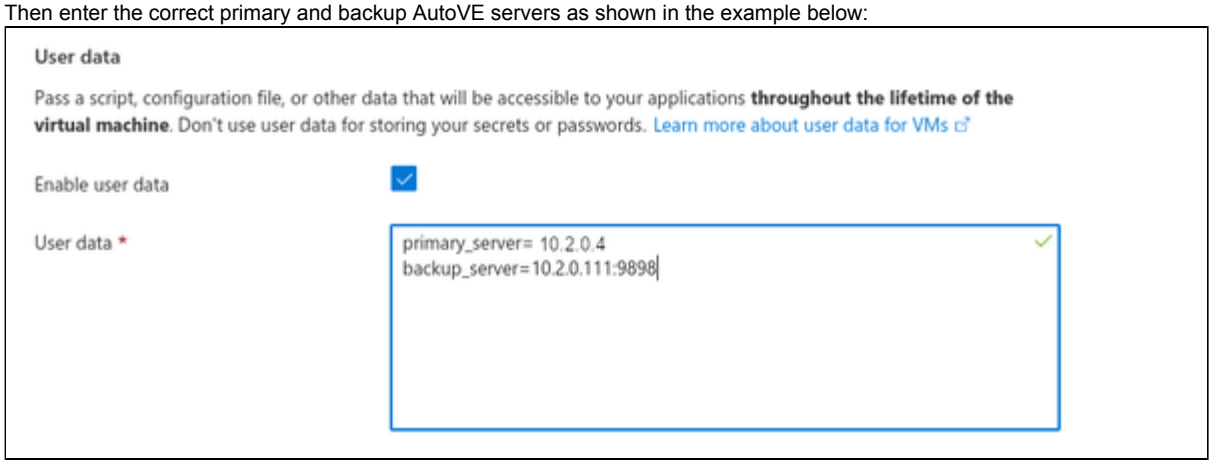
Configuring the AutoVE Server Information at Azure Instance Launch

The AutoVE license server information is entered as instance **User Data**. In the initial instance configuration window, go to the **Advanced** section.

- Open it and scroll down to the **User Data** section.
- Enable the **User Data** by ticking the checkbox.



- Then enter the correct primary and backup AutoVE servers as shown in the example below:



Valid User Data configuration options:

- **`primary_server=`**`<ip-address>[:<port>]`
- **`backup_server=`**`<ip-address>[:<port>]`

where

- *<ip-address>* stands for the IP address of the primary and the backup server as applicable, and
- *<port>* stands for a non-default TCP port used to communicate with the license server (default: TCP/8083).

Please note: at least one license server must be configured at initial launch to enable AutoVE mode. **Otherwise, the instance will bind to one of the public license servers operated by Stromasys.**

Changing the AutoVE Server Configuration After Azure Instance Launch

Once an instance has been launched, the AutoVE server information in the User Data section can be changed. To do this, use the following steps:

- In the Azure management console, open the **Overview** window of your Charon host instance.
- Find the **Configuration** option in the left-hand pane and open it.
- Scroll down to the **User Data** section and tick the checkbox that enables editing the data.
- Modify the AutoVE configuration as needed and click on **Save** at the top of the page.
- Activate the changes:
  - After cleanly shutting down any running guest operating systems, restart the emulator instances and any required guest systems. It can take a minute or two until the change becomes active.
  - If changes are made to the VE license server configuration (e.g., changing the port numbers), the VE license server must also be restarted.

Please note: removing the AutoVE server configuration completely will **not** enable the instance to connect to the public license server.

Setting up a Linux Instance in AWS (New GUI)

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.

This page reflect the AWS GUI changes in spring 2022.

Content

General 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:

- **Amazon account and Marketplace subscriptions**:
  - To set up a Linux instance in AWS, you need an Amazon AWS account with administrator access.
  - Identify the AWS region in which you plan to launch your instance. If planning to use an AWS service, use the following link to check if this service is available in the desired region:
    https://aws.amazon.com/about-aws/global-infrastructure/regional-product-services
  - Identify the VPC and subnet in which you plan to launch your instance.
  - If your instance requires Internet access, ensure that the route table associated with your VPC has an Internet Gateway. If your instance requires a VPN access to your on-premises network, ensure that a VPN gateway is available. The exact configuration of your VPC and its subnets will depend on your network design and application requirements.
  - To subscribe to a specific marketplace service select **AWS Marketplace Subscriptions** in the management console and then select **Manage Subscriptions**.
  - Search for the service you plan to use and subscribe to it (accepting the terms and conditions). After a successful subscription, you will find the subscription in the Manage Subscriptions section. From there you can directly launch a new instance.
  - The AWS service providing metered Charon-SSP emulator instance is called *AWS Mainframe Modernization - Virtualization for SPARC*.

- **The instance hardware and software prerequisites will be different depending on the planned use of the instance**:
  - Option 1: the instance is to be used as a **Charon emulator host system**:
    - Refer to the hardware and software prerequisite sections of the *User's Guide* and/or *Getting Started* guide of your Charon product to determine the exact hardware and software prerequisites that must be fulfilled by the Linux instance. The **image** you use to launch your instance and the **instance type** you chose determine the software and hardware of your cloud instance.
    - If you use Charon emulator marketplace image, the software prerequisites are already fulfilled.
    - A Charon product **license** is required to run emulated legacy systems. Refer to the licensing information in the documentation of your Charon product, or contact your Stromasys representative or Stromasys VAR for additional information. Emulator marketplace images with Automatic Licensing use public license servers and will create their license automatically at first launch of the instance.
  - Option 2: the instance is to be used as a dedicated **VE license server**:
    - Refer to the *VE License Server Guide* for detailed prerequisites.
- Certain legacy operating systems that can run in the 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.

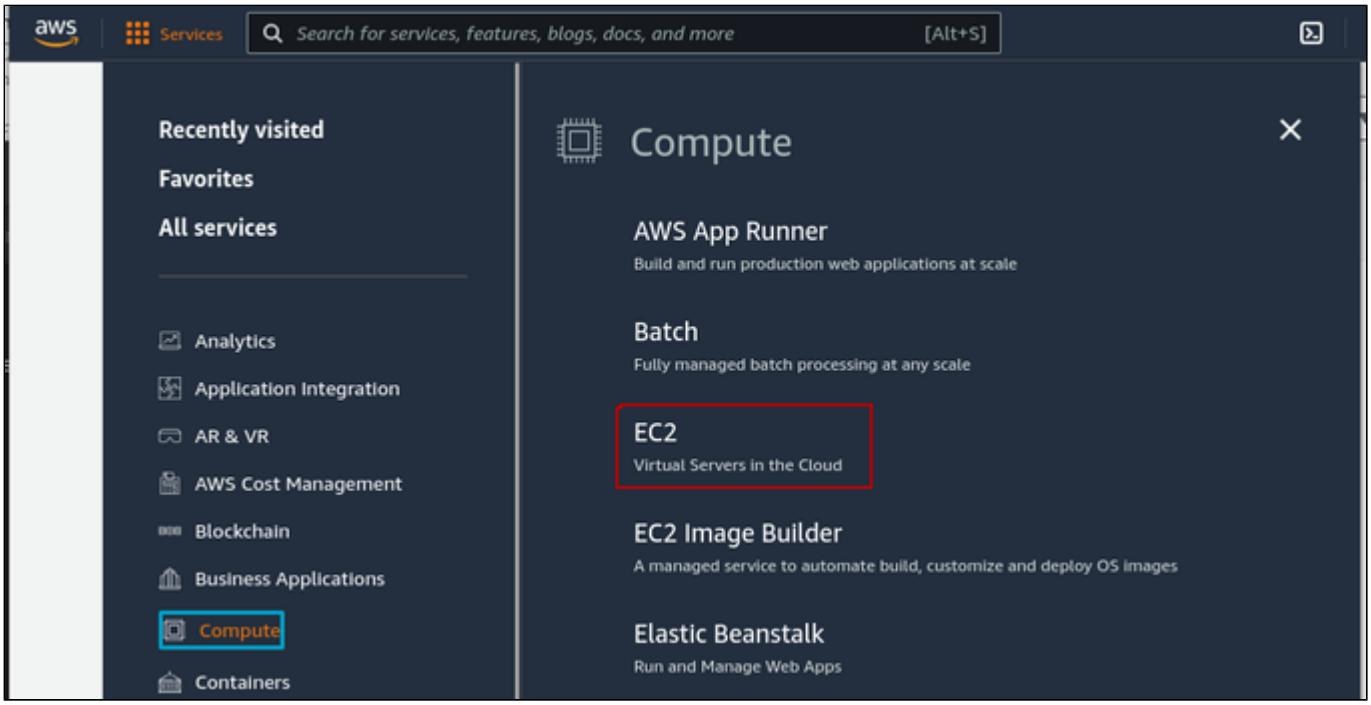
AWS Login and New Instance Launch

Please note that the AWS GUI occasionally changes. This may lead to screenshots not always reflecting the exact appearance of an configuration screen.

To start the creation of a new cloud instance, perform the following steps:

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

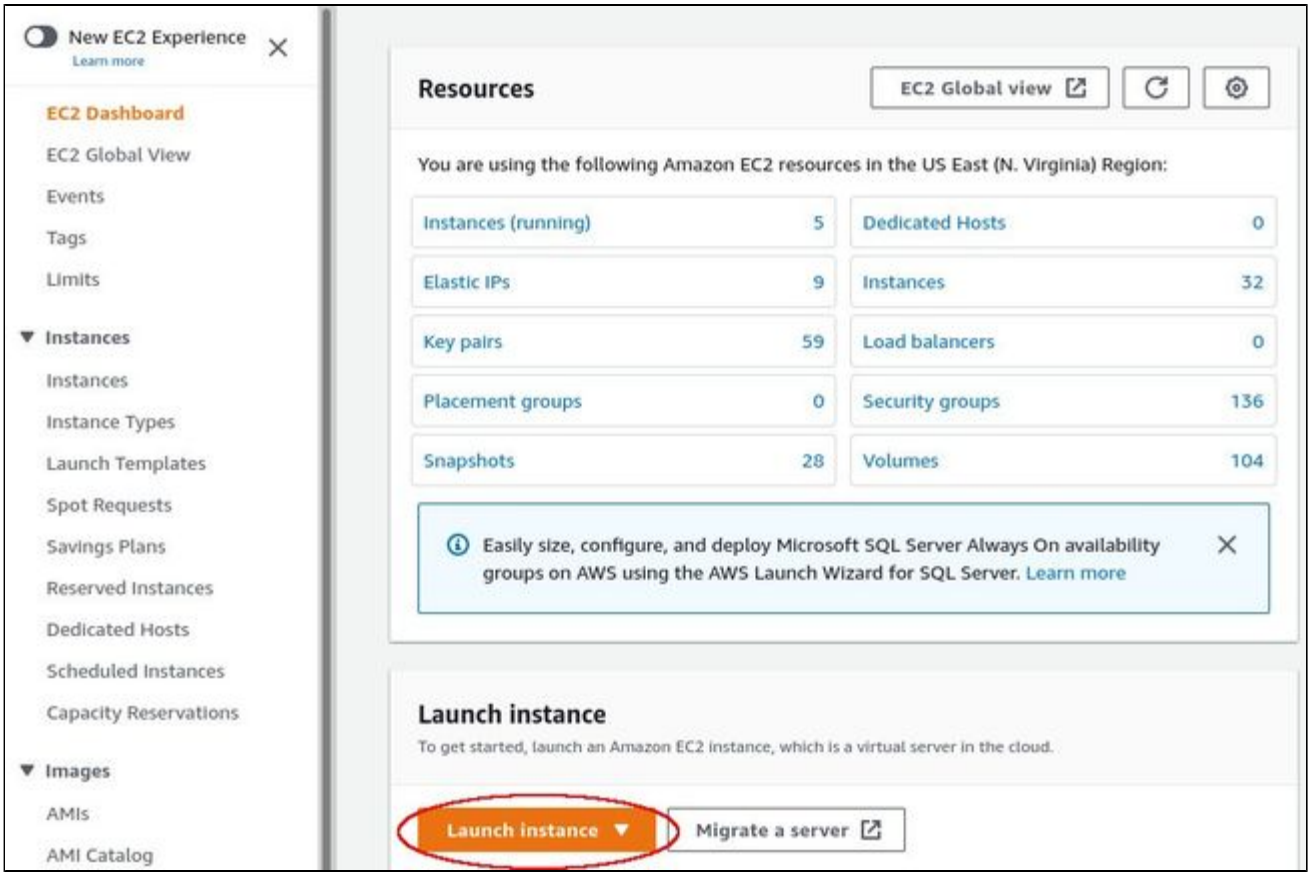
2. Find and select the **EC2 service**. You can find it in the **Recently visited section**, or use the services drop down menu (alternatively, you can also start from your **Manage Subscriptions** page and launch the instance there):



This will open the E2C dashboard.

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

3. On the EC2 dashboard click on the **Launch Instance** button.



Clicking on **Launch Instance** and selecting the launch instance option will allow you to initiate the instance creation process consisting of seven steps:

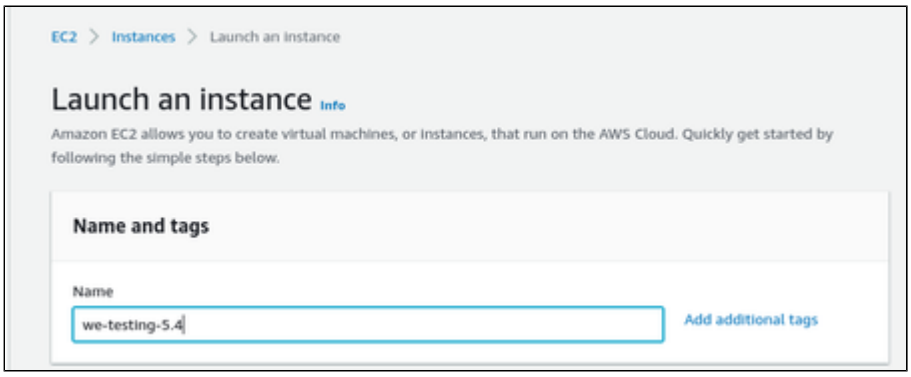
1. Enter an instance name
2. Choose AMI
3. Choose Instance Type
4. Key pair configuration
5. Network and security group configuration
6. Storage configuration
7. Advanced details
8. Launch instance

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. Enter an instance name:



If needed, you can add additional tags to the instance.

When done, **proceed** to the **Application and OS Images** section to choose an AMI (Amazon Machine Image).

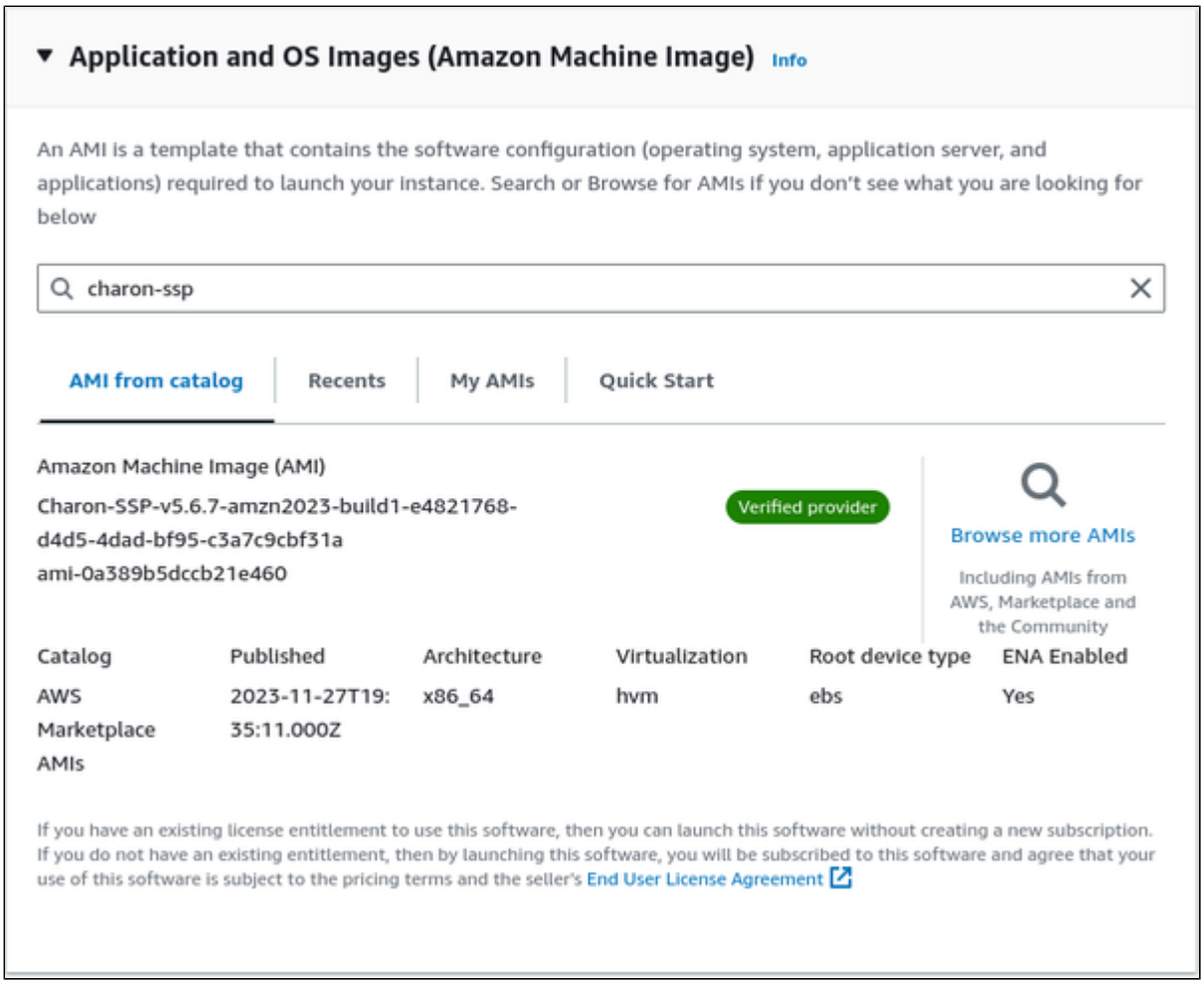
2. Choose AMI:

AMIs are prepackaged images used to launch cloud instances. They usually include the operating system and applicable application software.

Which AMI you select depends on the planned use of the instance:

- If the instance is to be used as a **Charon emulator host system** several AMI choices are possible:
  - **Installing the Charon host system from a prepackaged Charon marketplace image**: they contain the underlying operating system and the preinstalled Charon software.
    - Please check with your Stromasys representative which options are currently available in your cloud providers marketplace.
    - Depending on the cloud provider and the Stromasys product release plans, there may be two variants:
      - *Automatic licensing (AL)* for use with a public, Stromasys-operated license server. Please contact your Stromasys representative if you require a private, customer-operated AutoVE license server
      - *Virtual environment (VE)* for use with a private, customer-operated VE license server
  - **Installing the Charon host system using a conventional Charon emulator installation** with the Charon emulator installation RPM packages for Linux:
    - Choose a Linux AMI of a distribution supported by your selected Charon product and version (see the **user's guide** of your product on the Stromasys documentation site).
- If the instance is to be used as a dedicated **VE license server**:
  - Please refer to the *VE License Server Guide* in Licensing Documentation for the requirements of the Linux instance.

After deciding on which AMI is required, select a matching Linux or Charon product AMI in the Marketplace or (depending on your environment) from My AMIs.



You can use the search field or select one of the categories displayed to start your search. **Select the Linux AMI appropriate to your planned use of the instance**, that is,

- a prepackaged Charon VE marketplace image (as shown in the example above - note the string "**ve**" in the AMI name), or
- a prepackaged Charon AL marketplace image for Automatic Licensing or AutoVE, or
- a Linux version supported for an RPM product installation, or
- a Linux version supported for the VE license server.

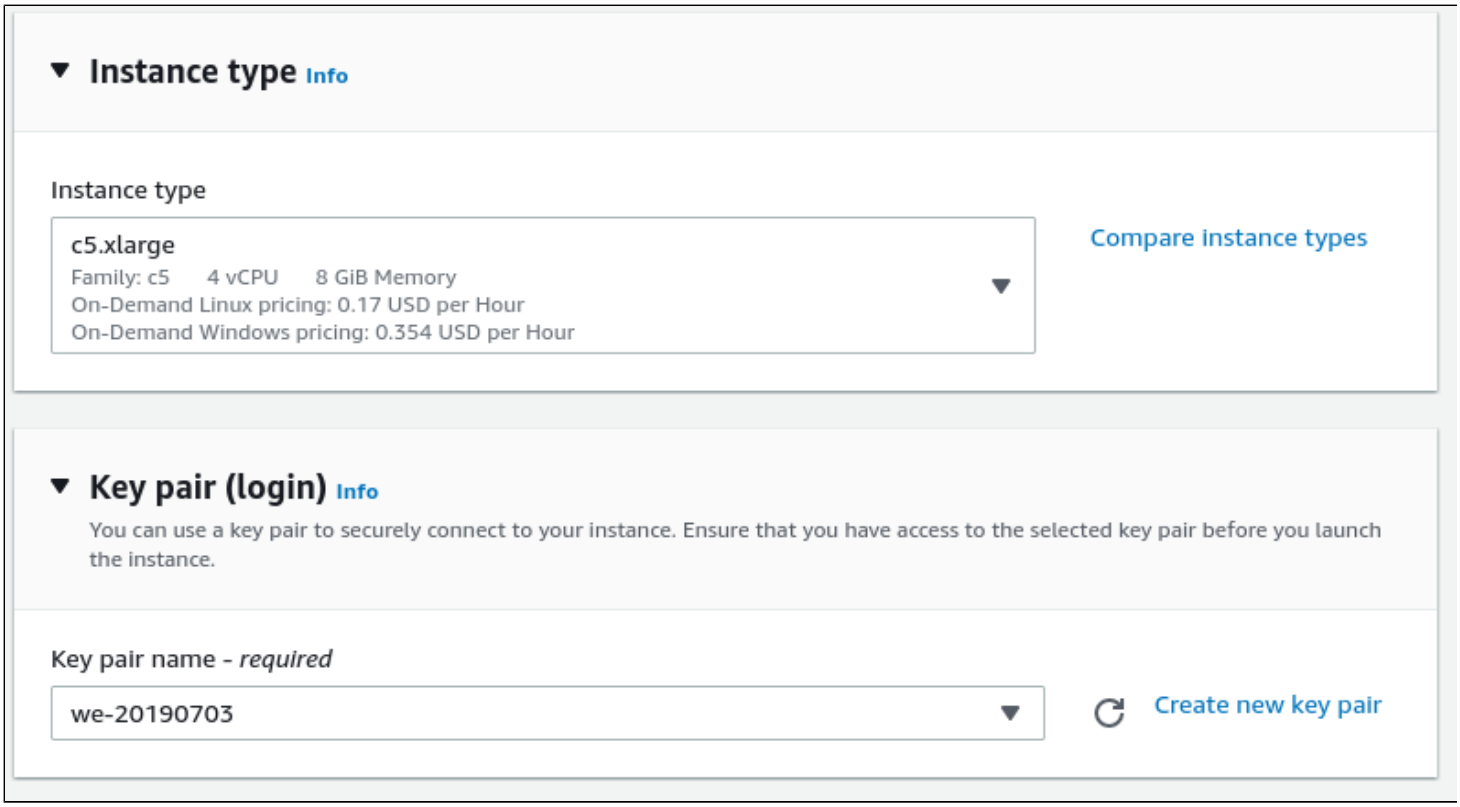
Then **proceed** to the next section, the **Instance type** selection.

3. Choose Instance Type:

Amazon EC2 offers instance types with varying combinations of CPU, memory, storage, and networking capacity.

Select an instance type that matches the requirements of the Charon product to be used. Please note that some marketplace images have a restricted selection of instance types.

When done, **proceed** to the **Key pair** configuration.



4. SSH key pair configuration:

In this section, you can

- either **create a new SSH key pair** and download the private key, or
- you can **select an existing key pair** to use for logging in to the new instance. If you select an existing key pair, make sure you have the matching private key. Otherwise, you will not be able to log in.

Please note: if your management system supports it, for RHEL 9.x, Rocky Linux 9.x, and Oracle Linux 9.x use SSH key types ECDSA or ED25519. This will allow connecting to these Charon host Linux systems using an SSH tunnel without the default crypto-policy settings on the Charon host having to be changed for less secure settings. This is, for example, important for the Charon-SSP Manager. See also: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/security_hardening/using-the-system-wide-cryptographic-policies_security-hardening.

After configuring your key pair, **proceed** to the **Network settings** section.

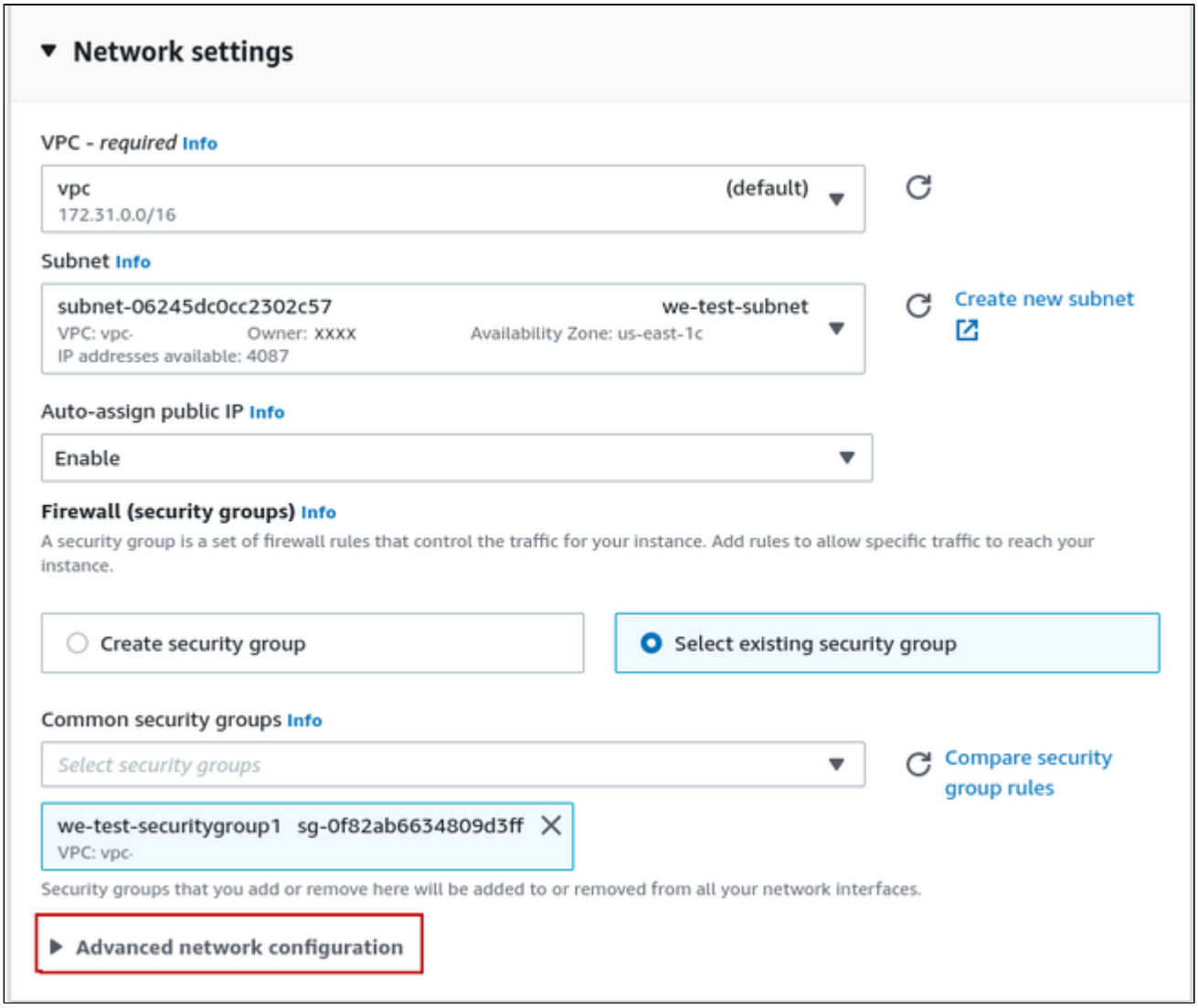
5. Network configuration:

This section offers basic default settings to connect your instance to the network. However, in most cases, you will have to adjust the settings to your environment.

To do this, click on the **Edit** button at the top of the section:

This will open the edit window and allow additional settings:

- The VPC (if a non-default VPC is to be used)
- The desired subnet (either an existing one or a newly created subnet)
- Enable or disable the automatic assignment of a public IP address to the primary interface (**automatic assignment is only possible if a single network interface is selected for the instance**)
- Assign an existing or new custom security group (cloud-provided firewall). The security group must allow at least SSH to access the instance. Any ports required by applications planned to run on the instance must also be allowed (the security group can be modified at any time after the instance has been created).



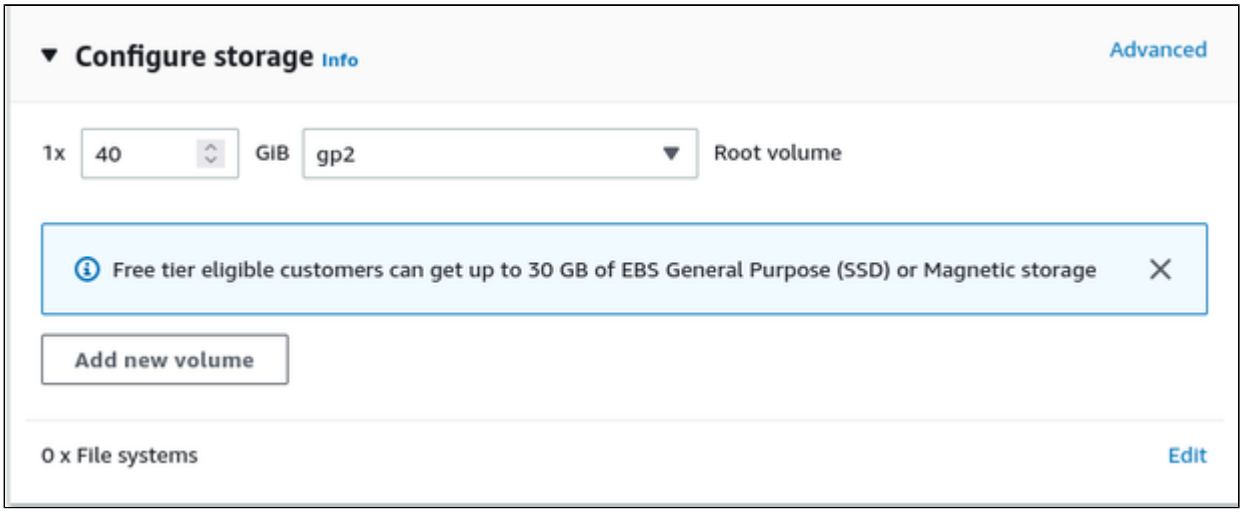
The **Advanced network configuration** option at the bottom of the section opens an additional configuration section in which you can set more advanced interface options and add additional network interfaces (automatic assignment of a public IP address only works if there is **only one network interface** attached to the instance). Additional interfaces can also be added to the instance after it has been first launched.

Once you are done with the network configuration, **proceed** to the **Configure storage** section.

6. Storage configuration:

The size of the root volume (the system disk) must be appropriate for your environment (recommended minimum system disk size for the Linux system: 30GB). You can add more storage now or later to provide space for virtual disk containers and other storage requirements, but the system disk size should cover the Linux system requirements including any applications/utilities planned to be installed on it.

Please note: It is recommended to **create separate storage volumes for Charon application data** (e.g., disk images). If required, such volumes can later easily be migrated to another instance.



If needed, open the **Advanced details** section to access additional settings.

7. Advanced details:

In this section, you can set many parameters. Three that are more likely to be useful to a Charon emulator environment are shown here as examples:

CPU characteristics (enable or disable more than one thread per CPU core, options depend on the selected instance type). **This can only be set at instance launch. It cannot be changed later**.

IAM role

Only for a VE license server system with a **version earlier than 1.1.23**, you must assign the required IAM role (allowing the ***ListUsers*** action) to the instance. For more information see the Virtual Environment (VE) License Server Documentation.

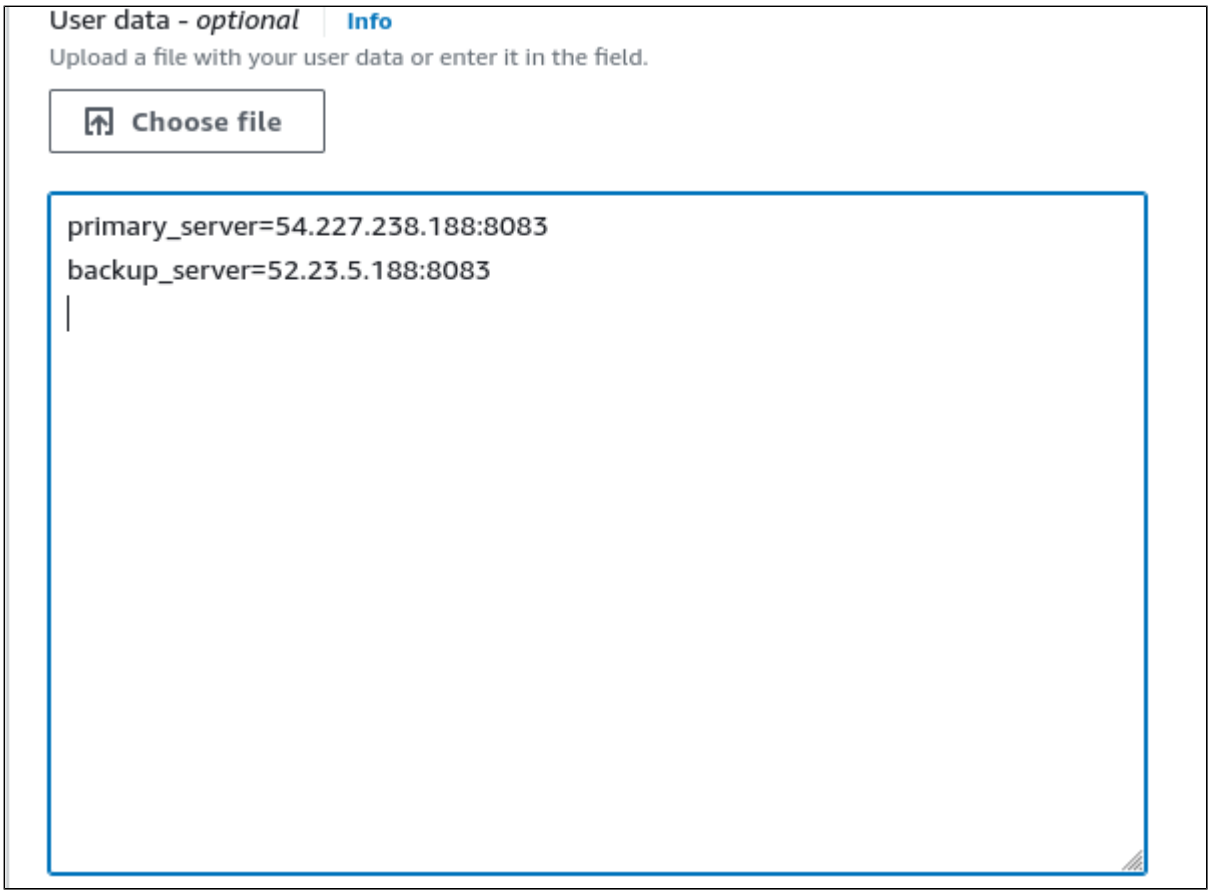
User data

If your instance is based on a **Charon AL marketplace image** and planned to be used for **AutoVE licensing** (instead of the Stromasys-operated public license servers) or based on the **Charon-SSP Amazon Linux image**, you must add the corresponding information to the instance configuration **before** the first launch of the instance.

Please note:

- Should you use the SSP Amazon Linux AMI with **SSP version 5.6.8 or higher** as provided by the *AWS Mainframe Modernization - Virtualization for SPARC* service, the instance will by **default** connect to the **public, Stromasys-operated AutoVE license servers** (defined in */opt/charon-license-server*). You only need the **user data definition for older versions or to override the default** with your private AutoVE servers.
- The example below shows the appearance of the AutoVE license server information that is entered as **User Data** in the **Advanced Details** configuration section at the bottom of the **Launch an Instance** window during the initial configuration of an instance. **Scroll down** to the bottom of the configuration window to open and display the user data section in the **Advanced Details**.
- In the older GUI version, the **Advanced Details** section is part of the **Configure Instance** window - the layout is somewhat different, but the configuration options are the same.

Enter the information for the AutoVE license server as shown in the example below (it shows the public AutoVE servers):



Valid User Data configuration options:

- **`primary_server=`**`<ip-address>[:<port>]`
- **`backup_server=`**`<ip-address>[:<port>]`

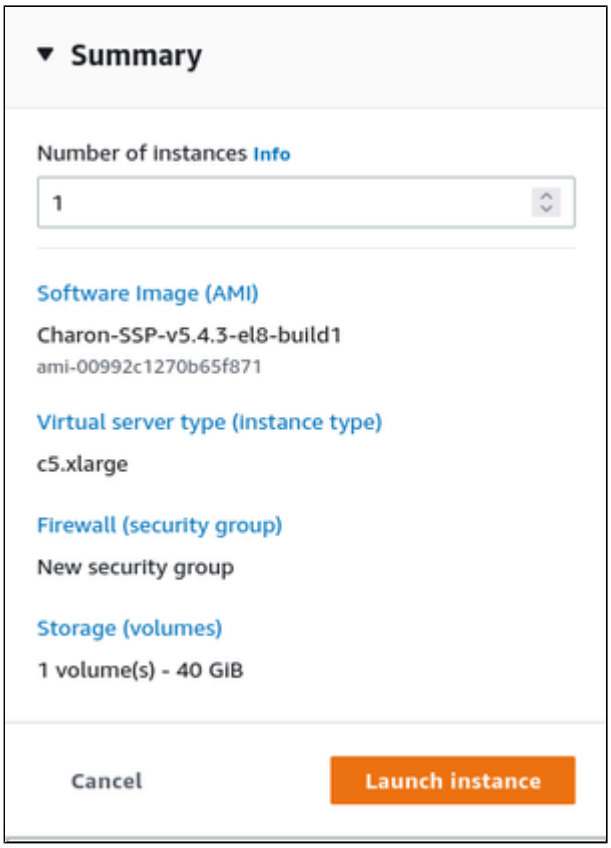
where

- <*ip-address*> stands for the IP address of the primary and the backup server as applicable, and
- <*port*> stands for a non-default TCP port used to communicate with the license server (default: TCP/8083).

Please note: at least one license server must be configured at initial launch to enable AutoVE mode. This can be via the */opt/charon-license-server* file with the default public servers (SSP 5.6.8 or higher) or via the manual user data configuration. **Otherwise, the instance will bind to one of the public AL license servers operated by Stromasys.**

8. Launch your instance:

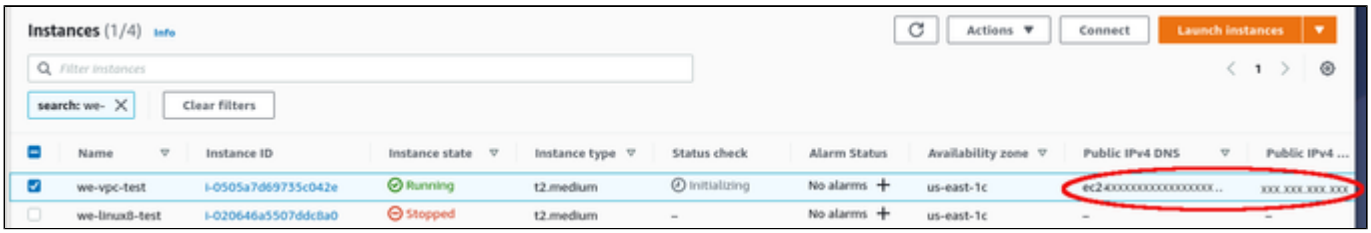
Click on Launch instance in the right-hand pane to launch your instance (if the launch button is not visible, you may have to close overlaying text panes first):



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.You will eventually see a launch success message with a link to your instance. Clicking on this link will take you to your new instance in the instance overview list.

In addition to the instance state, 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.

Please note:

- If you select your instance, the bottom of the screen will show a detailed description and status information of your instance.
- You can rename your instance after creating it by clicking on the pencil symbol that will appear next to the instance name when placing the mouse pointer over it, or by editing the name tag of the 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 **private key** used must correspond to the public key installed in the *authorized_keys* file of the cloud instance management user. This is usually done during initial cloud instance launch.
- The management user account normally allows sudo access to privileged commands (use **sudo -i**).
- If the instance was created using a Stromasys-provided AL or VE marketplace image, the management user for **interactive login** is the user **sshuser**.

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-name>@<cloudhost-IP-address>
```

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 **private key** used must correspond to the public key installed in the *authorized_keys* file of the cloud instance management user. This is usually done during initial cloud instance launch.
- If the instance was created using a Stromasys-provided AL or VE marketplace image, the management user for **file transfer** is the user **charon**.
- If the user **charon** is used to transfer files, the home directory for the file transfer will be */charon/storage*.

Setting up a Linux Instance in OCI

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

Contents

General 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.
- Secondly, **prerequisites will be different depending on the planned use of the instance**:
  - Option 1: the instance is to be used as a **Charon emulator host system**:
    - Refer to the hardware and software prerequisite sections of the User's Guide and/or Getting Started guide of your Charon product to determine the exact hardware and software prerequisites that must be fulfilled by the Linux instance. The **image** you use to launch your instance and the **instance type** you chose determine the software and hardware of your cloud instance.
    - A Charon product **license** is required to run emulated legacy systems. Contact your Stromasys representative or Stromasys VAR for details.
  - Option 2: the instance is to be used as a dedicated **VE license server**:
    - Refer to the VE License Server Guide for detailed prerequisites.
- Certain legacy operating systems that can run in the 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.

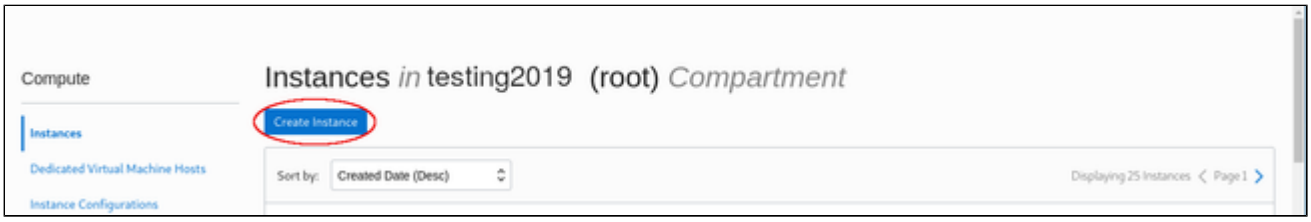
OCI New Instance Launch

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 cloud instance, perform the following steps:

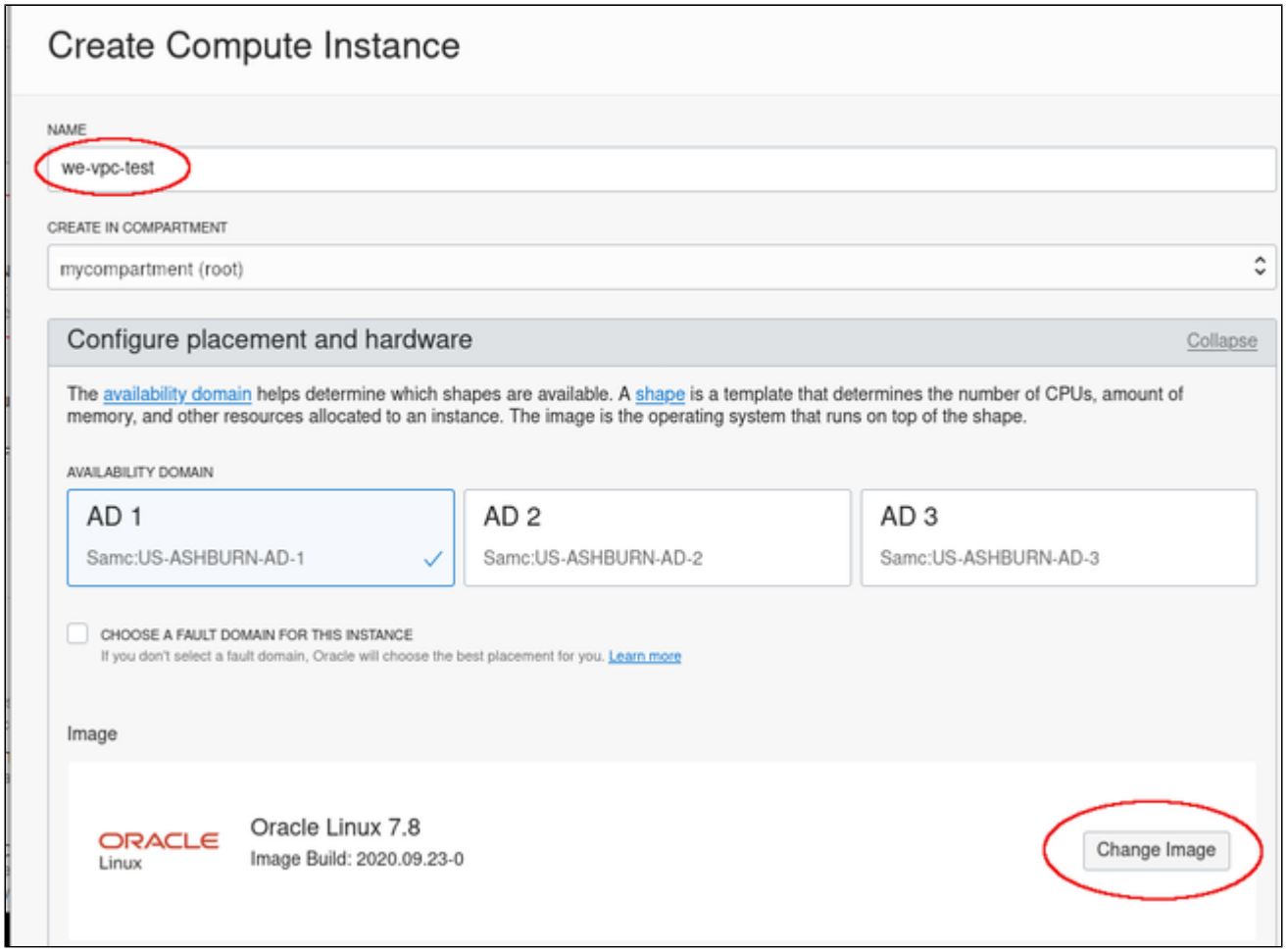
Step 1: log in to your Oracle Cloud environment.

Step 2: go to the instance list in the compute section and click on **Create Instance**.



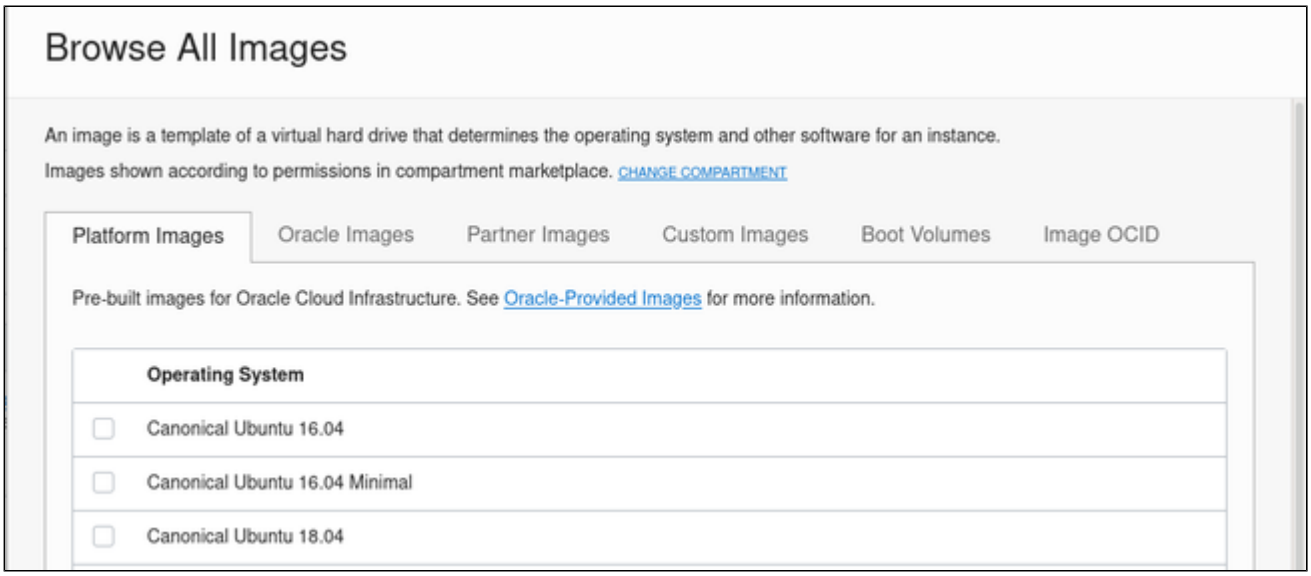
This opens the **Create Compute Instance** window.

Step 3: on the first part of **Create Compute Instance** window, name your instance and select the correct image for it. If installing a prepackaged marketplace Charon image, this image must be used. If you plan to install Charon using RPM packages, use a Linux version supported for your Charon product version.



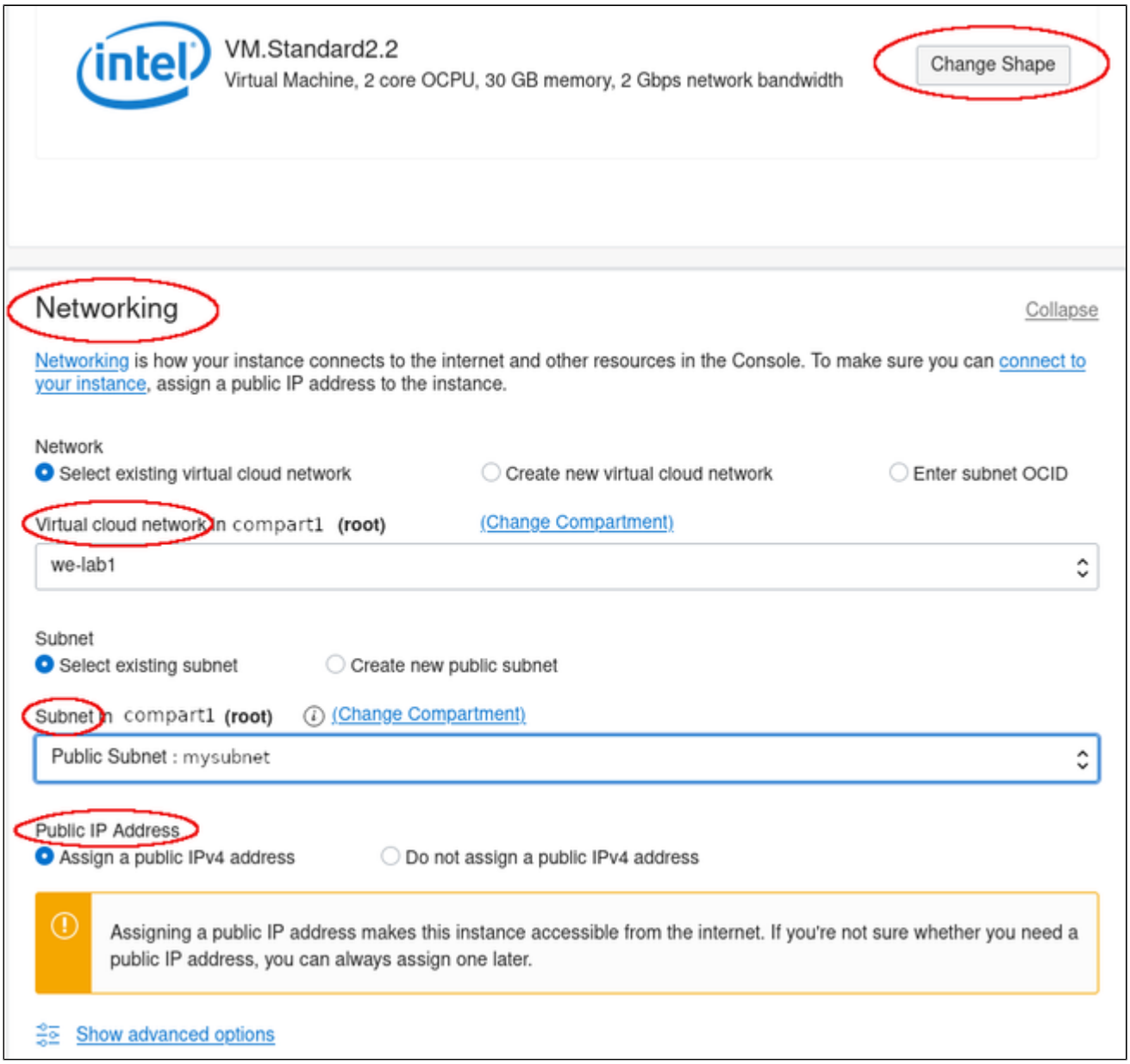
To select the correct image, select **Change Image**. This will allow you to browse the different available categories for the image from which to launch your instance.

The image below shows an example of the image selection screen:



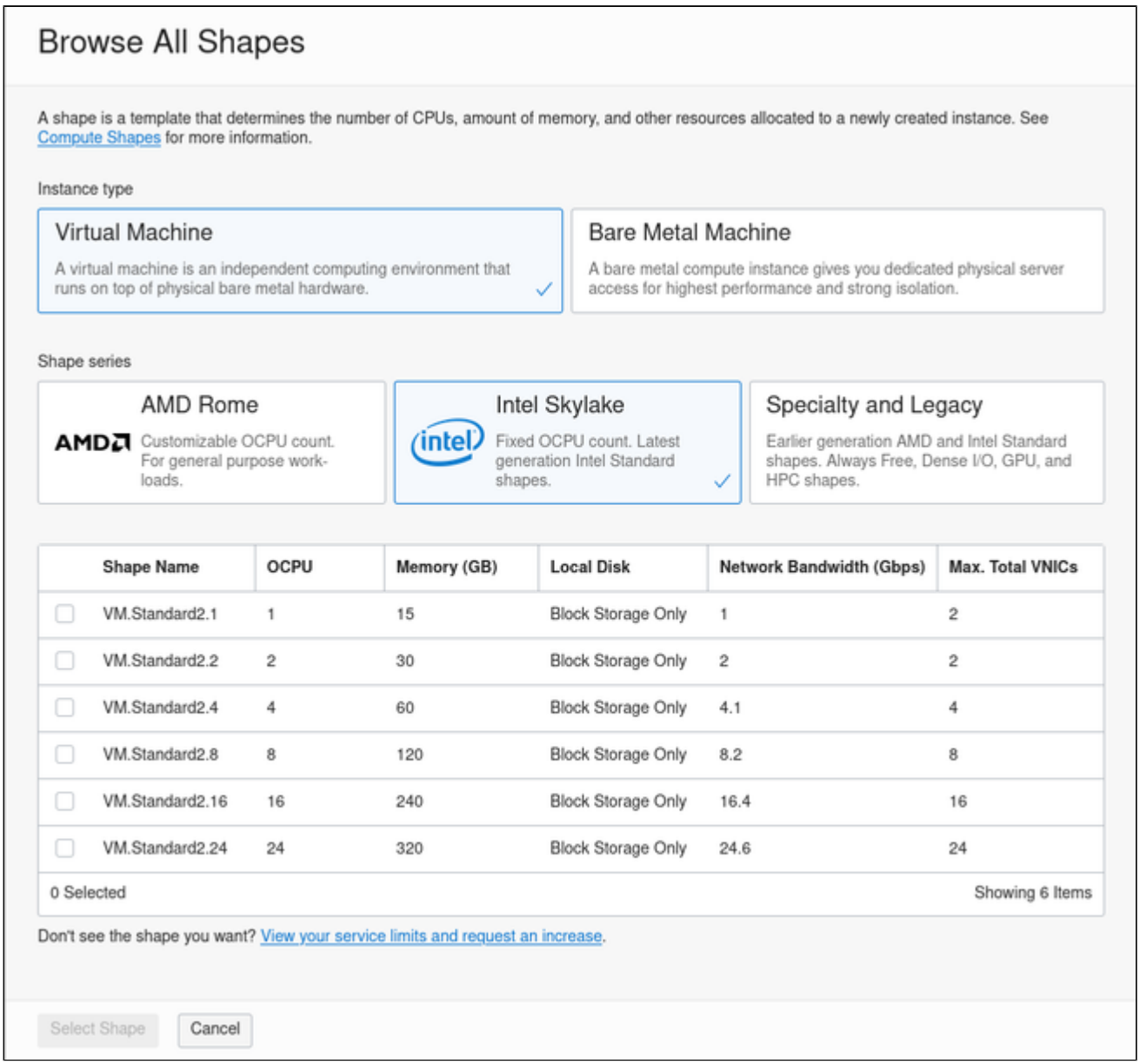
Optionally, change the compartment. Select the correct image and confirm your selection by clicking on **Select Image** at the bottom of the page. This will take you back to the **Create Compute Instance** window.

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**.

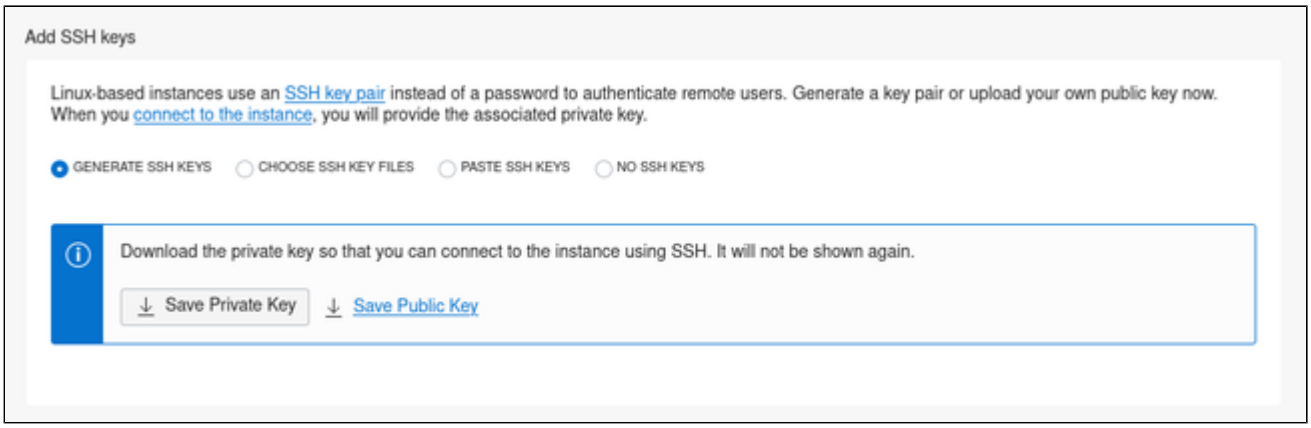
This will open a window where you can select the correct system type. For flexible shapes you will have to configure the required number of OCPUs.



Select the appropriate shape and confirm your selection by clicking on **Select Shape** at the bottom of the page. This will take you back to the **Create Compute Instance** window.

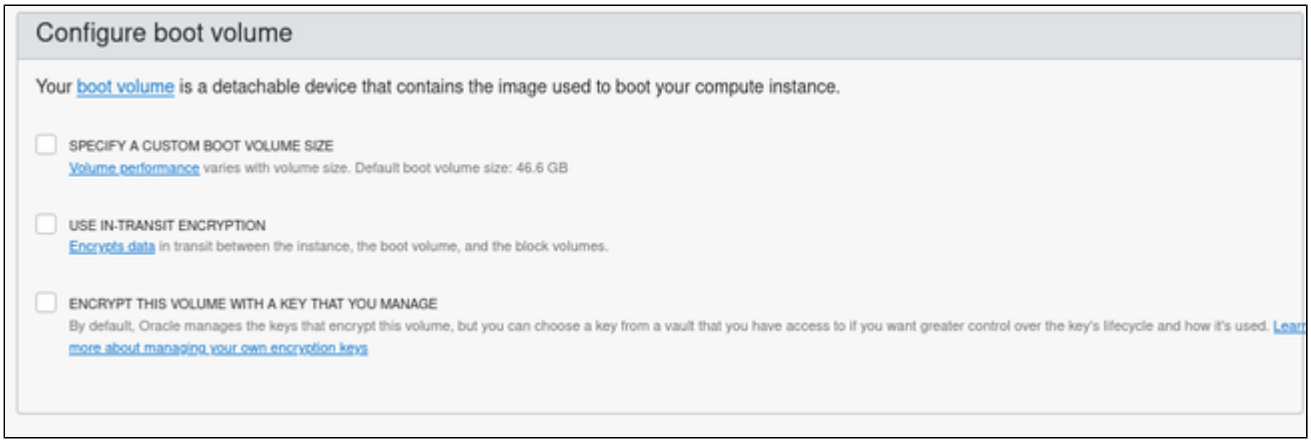
Step 5: near the bottom of the **Create Compute Instance** window create a new SSH key-pair or upload the public SSH key of an existing key-pair that you will use to access your instance. If you create a new key-pair, you must download the private key and store it in a save place for later use. Optionally,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

Please note: if your management system supports it, for RHEL 9.x, Rocky Linux 9.x, and Oracle Linux 9.x use SSH key types ECDSA or ED25519. This will allow connecting to these Charon host Linux systems using an SSH tunnel without the default crypto-policy settings on the Charon host having to be changed for less secure settings. This is, for example, important for the Charon-SSP Manager. See also: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/security_hardening/using-the-system-wide-cryptographic-policies_security-hardening.

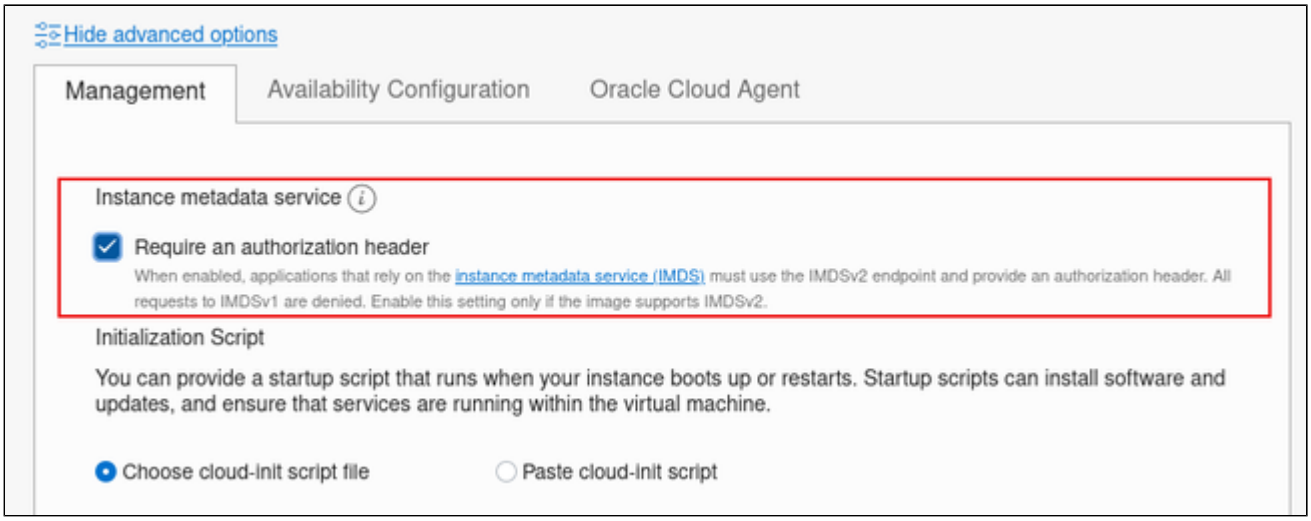


Step 6: optionally define non-default parameters (including the size) for the boot volume.

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).



Step 7: 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:



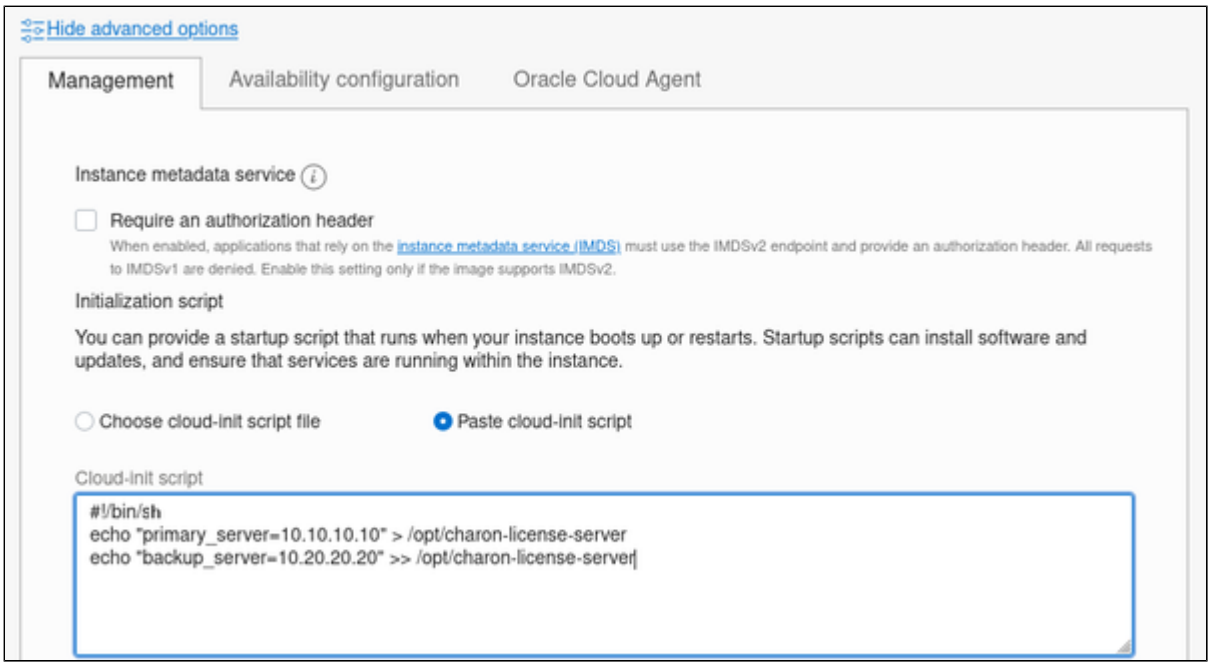
For Charon-SSP marketplace images, this is supported starting with Charon-SSP marketplace images version 4.2.2 and VE license server 1.0.33. On existing instances, this parameter can be changed, by editing the instance metadata service settings for the instance (go to **Instance Details** and click on **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 VE installation, verify the capabilities of the image used before you enable the new IMDSv2 feature.

Step 8: Additional configuration for **AutoVE** setup.

If the instance is launched from a Charon AL marketplace image and is planned to use AutoVE licensing (instead of the public license servers), you must add the corresponding information to the instance configuration **before** the first launch of the instance:

For OCI, you have to enter a cloud-init script at instance configuration in the **Advanced Options** section.

The following image shows an example:



Valid User Data configuration options:

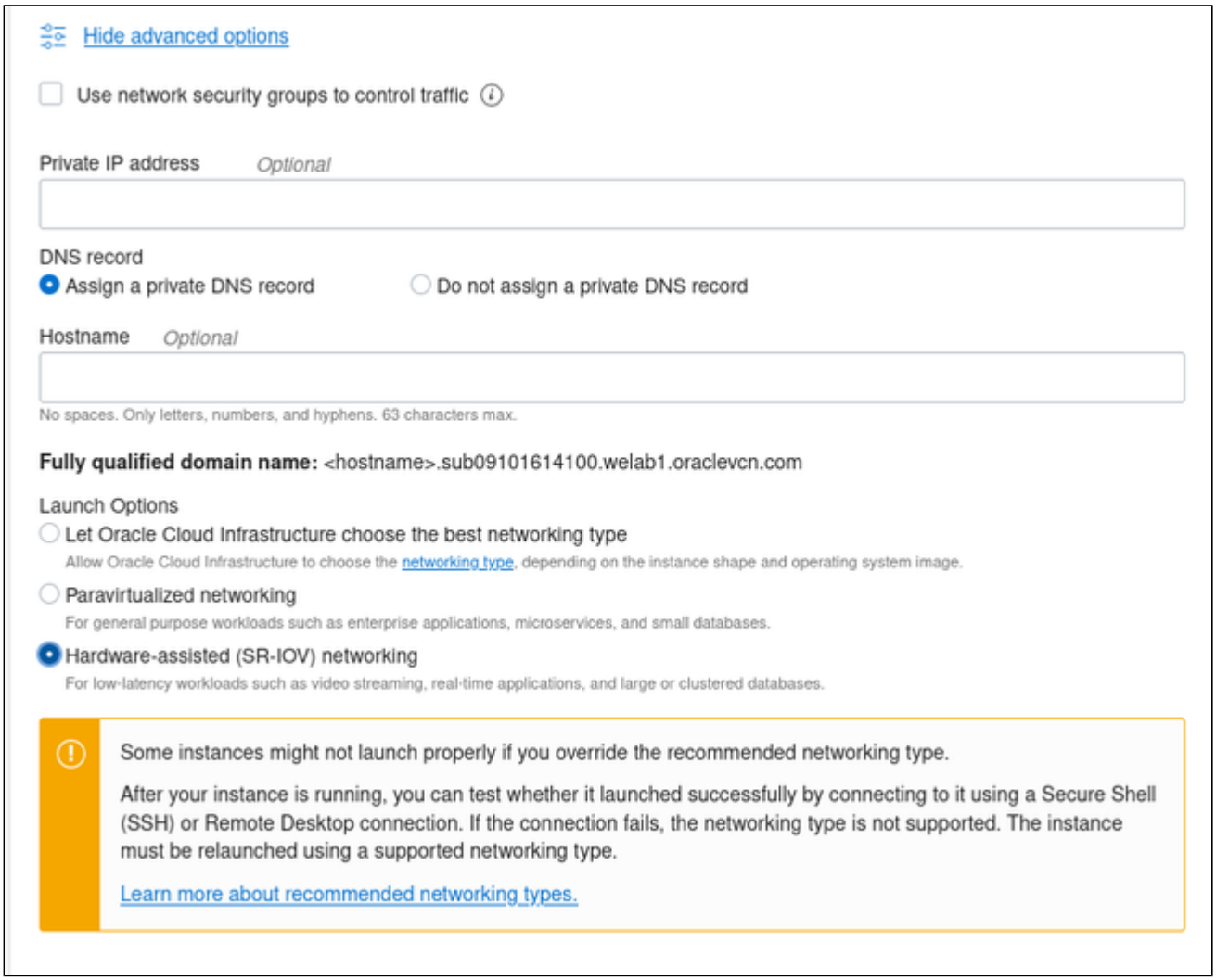
- **`primary_server=`**`<ip-address>[:<port>]`
- **`backup_server=`**`<ip-address>[:<port>]`

where

- *<ip-address>* stands for the IP address of the primary and the backup server as applicable, and
- *<port>* stands for a non-default TCP port used to communicate with the license server (default: TCP/8083).

Please note: at least one license server must be configured at initial launch to enable AutoVE mode. **Otherwise, the instance will bind to one of the public license servers operated by Stromasys.**

Step 9: The networking type selection may be required to allow offloading parameters to be disabled on an Ethernet interface dedicated to the emulator. For the Charon emulators, offloading parameters on the Ethernet interfaces it uses must be disabled. 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 other emulator products, this is required if a dedicated interface is used by the emulator and there are problems with disabling offloading parameters. For this, open the additional options section by clicking on **Show Advanced Options** at the bottom of the network configuration section 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 10: Click on **Create** at the bottom of the page to create your instance.

Step 11: verify 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 **private key** used must correspond to the public key installed in the *authorized_keys* file of the cloud instance management user. This is usually done during initial cloud instance launch.
- The management user account normally allows sudo access to privileged commands (use **sudo -i**).
- If the instance was created using a Stromasys-provided AL or VE marketplace image, the management user for **interactive login** is the user **sshuser**.

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-name>@<cloudhost-IP-address>
```

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 **private key** used must correspond to the public key installed in the *authorized_keys* file of the cloud instance management user. This is usually done during initial cloud instance launch.
- If the instance was created using a Stromasys-provided AL or VE marketplace image, the management user for **file transfer** is the user **charon**.
- If the user **charon** is used to transfer files, the home directory for the file transfer will be */charon/storage*.

Setting up a Linux Instance on Azure

Contents

General 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:

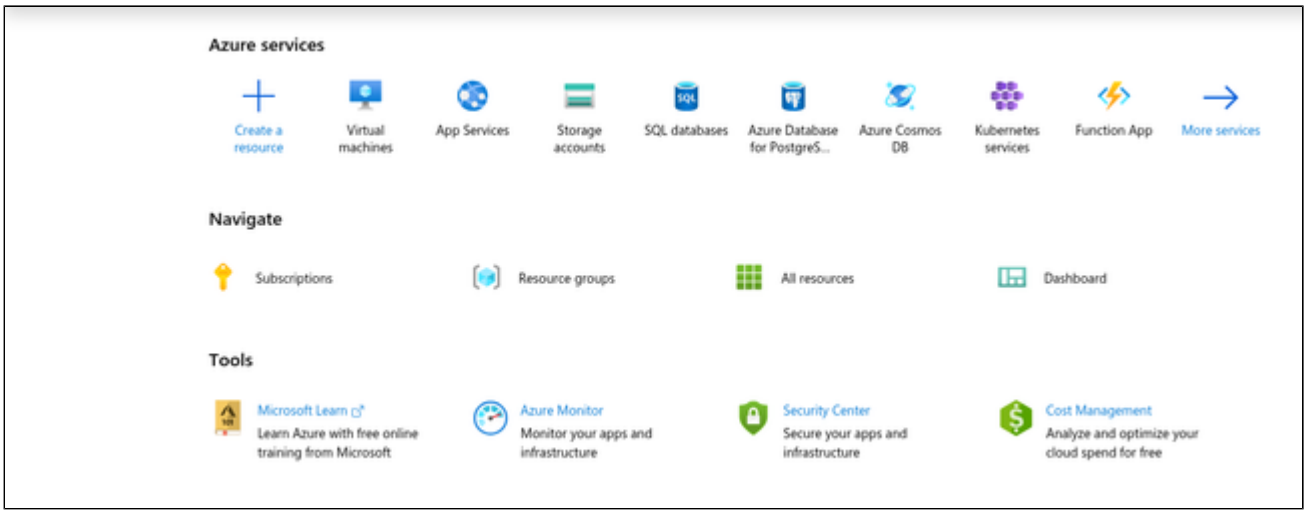
- To set up a Linux instance in Azure, you need an Azure account.
- Secondly, **prerequisites will be different depending on the planned use of the instance**:
  - Option 1: the instance is to be used as a **Charon emulator host system**:
    - Refer to the hardware and software prerequisite sections of the *User's Guide* and/or *Getting Started guide* of your Charon product to determine the exact hardware and software prerequisites that must be fulfilled by the Linux instance.
      The **image** you use to launch your instance and the **instance type** you chose determine the software and hardware of your cloud instance.
    - A Charon product **license** is required to run emulated legacy systems. Contact your Stromasys representative or Stromasys VAR for details.
  - Option 2: the instance is to be used as a dedicated **VE license server**:
    - Refer to the VE License Server Guide for detailed prerequisites.
- Certain legacy operating systems that can run in the 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

Logging in to your Azure account

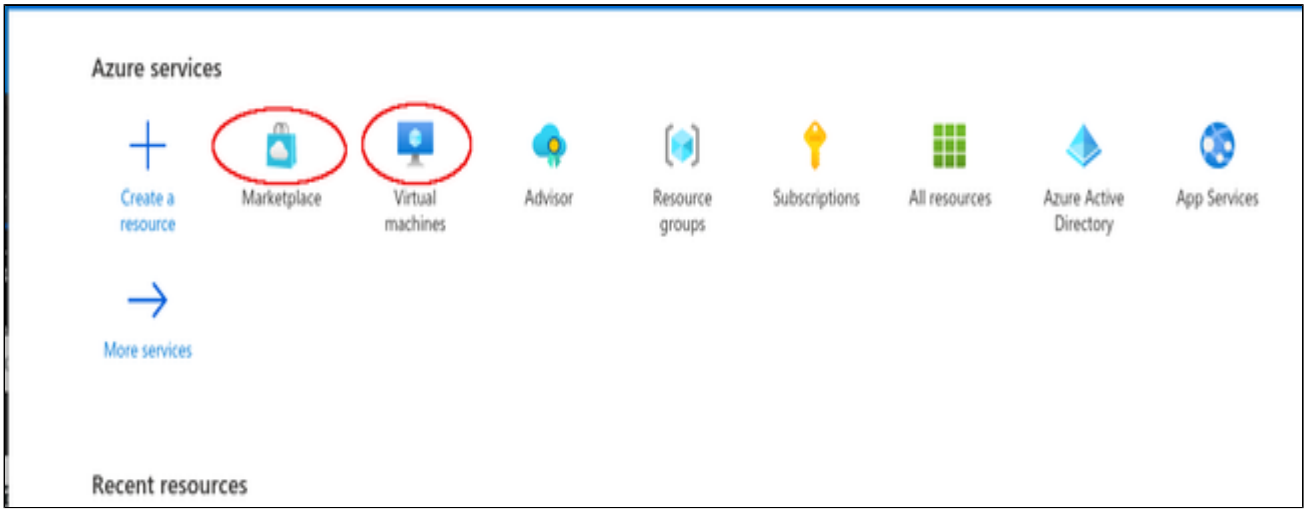
To log in perform the following steps:

- 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:



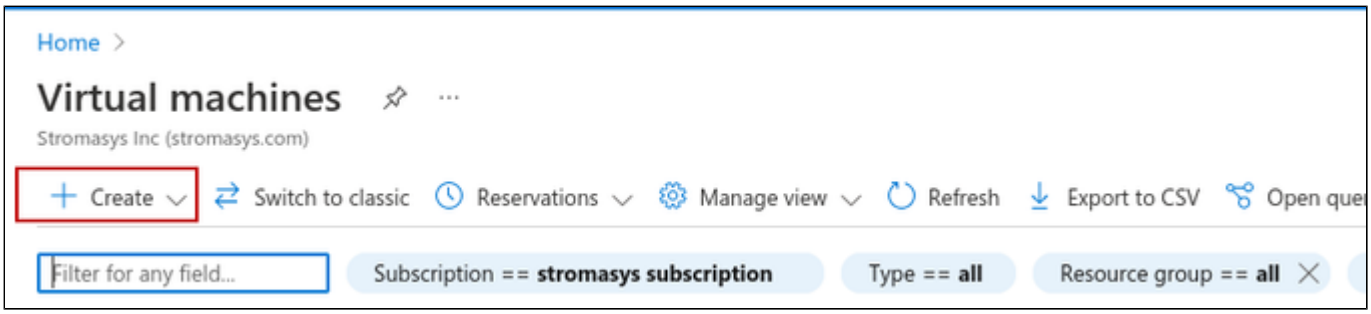
Creating a Virtual Machine

Step 1: Click on the **Virtual machines** or on the **Marketplace** icon on the home page. If you create your instance via the Marketplace icon, please select the Charon listing from the Marketplace offerings, select to create an instance, and continue with Step 3.



Clicking on **Virtual machines** opens the virtual machines overview list.

Step 2: Click on the **Create** link in the overview list.



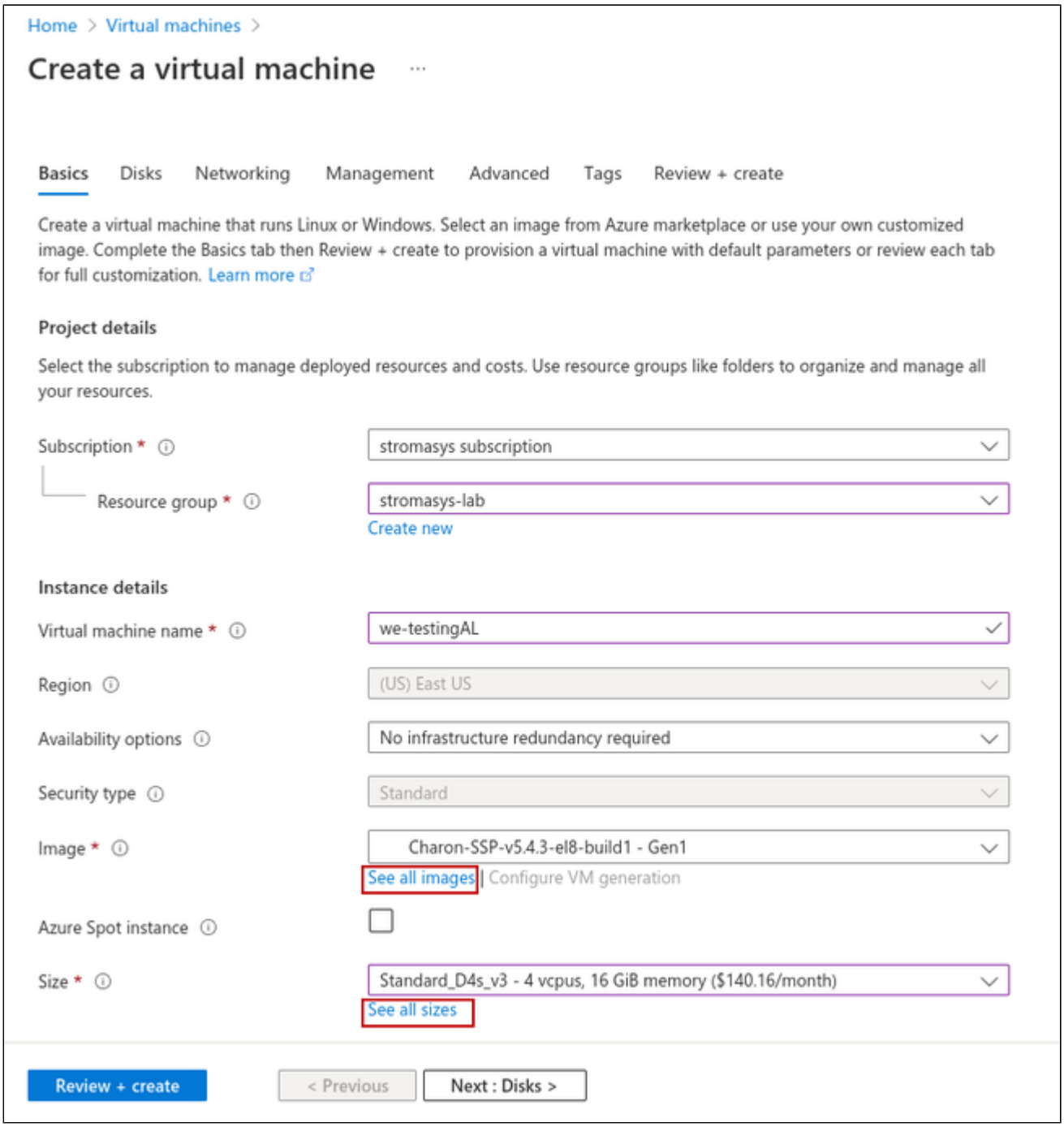
For a basic setup, select **Azure virtual machine** from the drop down list opened by the **Create** link. This opens the **Basics** tab of the **Create a Virtual Machine** window.

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 (cannot be changed after launching the instance)
- Region for the virtual machine
- The Azure image from which to launch your instance. Click on **See all images** to select the correct image. If installing a prepackaged marketplace Charon image, select the matching image. If you plan to install Charon using RPM packages, use a Linux version supported by your Charon emulator product.
- Size of your VM (click on **See all sizes** to see a list of available sizes)

Basics tab **upper part** sample:

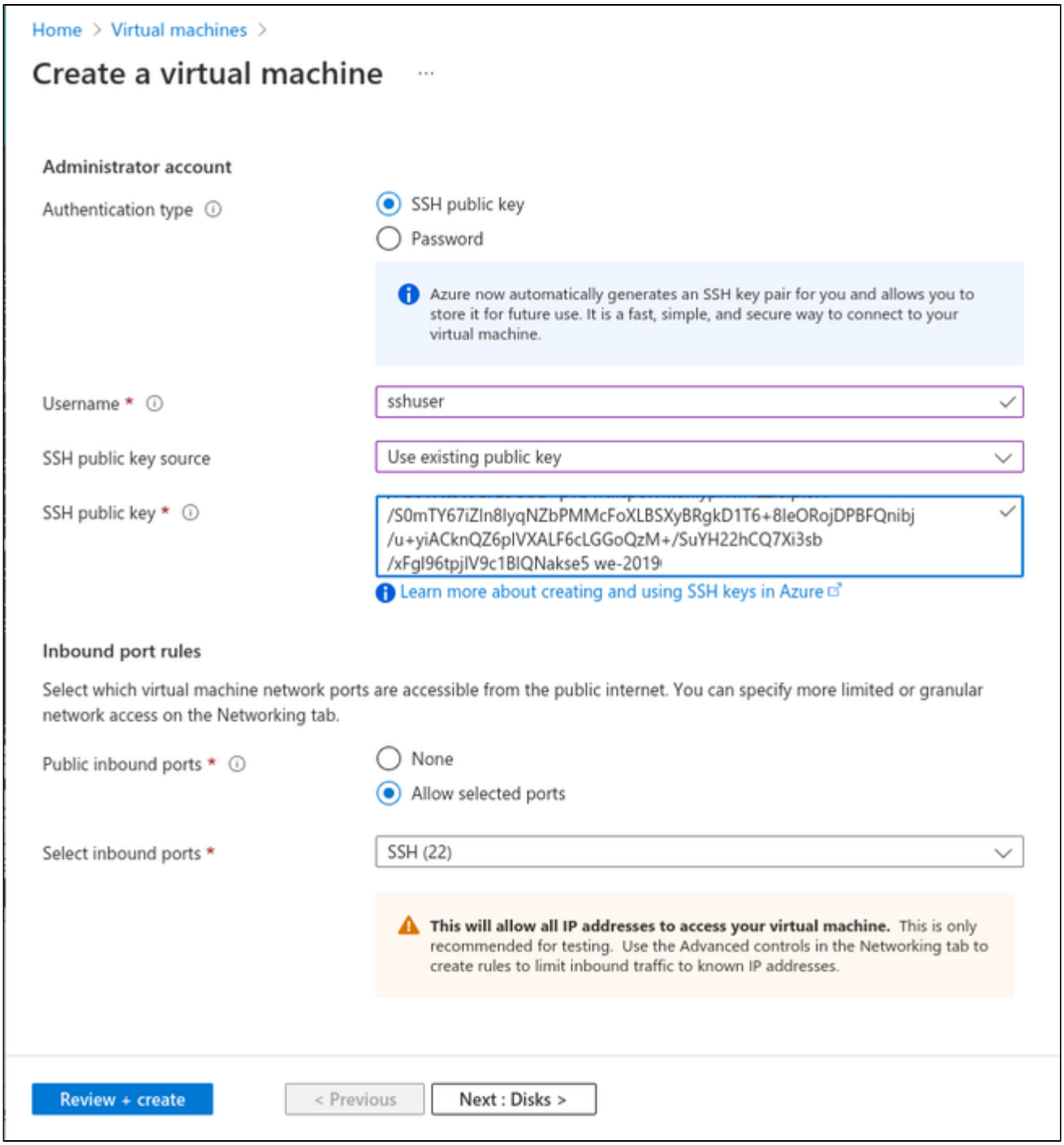
Select the image from which to launch your instance and the correct size of your instance (please review the sizing requirements above). Enter the other information in accordance to your environment.



Basics tab **lower part** sample:

- Enter the user **sshuser** as 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. Some images may also have preconfigured access rules that cannot be changed during the launch of the instance. In either case, remember to adapt the rules to your requirements after creating the instance or in the Networking tab (advanced) during the creation of the instance.

Please note: if your management system supports it, for RHEL 9.x, Rocky Linux 9.x, and Oracle Linux 9.x use SSH key types ECDSA or ED25519. This will allow connecting to these Charon host Linux systems using an SSH tunnel without the default crypto-policy settings on the Charon host having to be changed for less secure settings. This is, for example, important for the Charon-SSP Manager. See also: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/security_hardening/using-the-system-wide-cryptographic-policies_security-hardening.

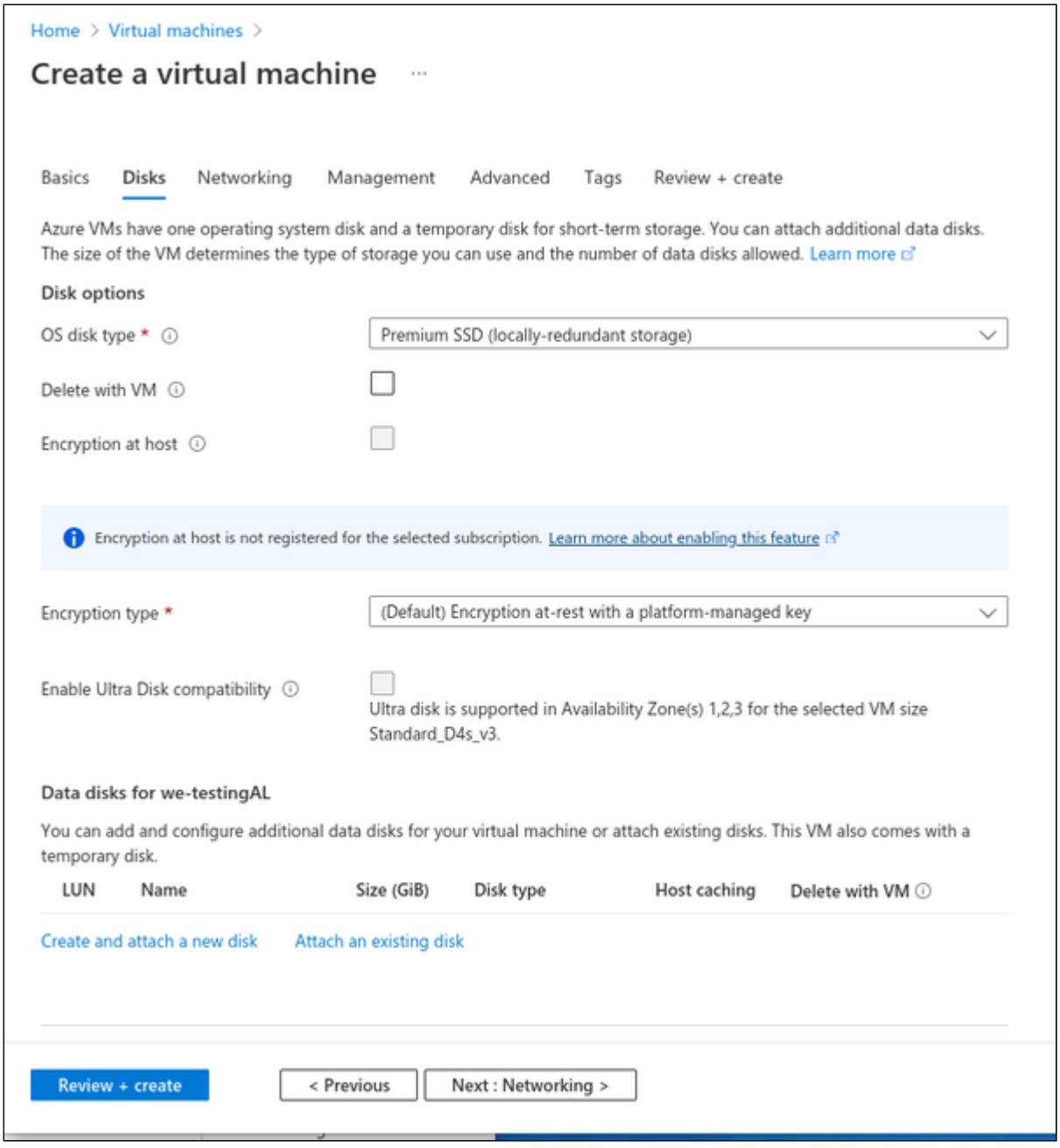


Click on **Next: Disks**. This will open the **Disks** tab of the VM creation window.

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). The recommended minimum system disk size is 30GB. You can attach existing additional data disks, or create new disks and attach them.

Disks tab sample:



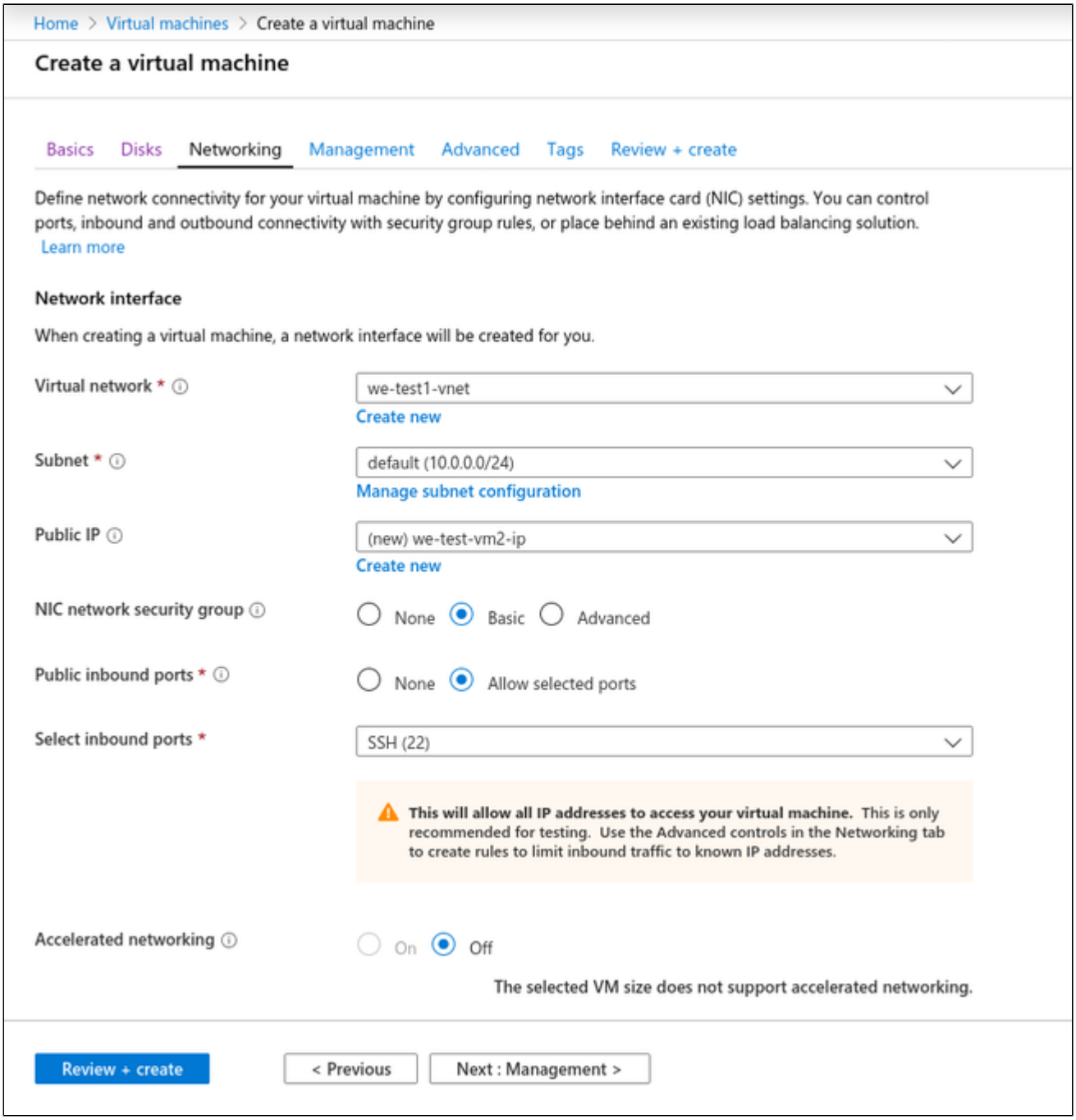
Click on **Next: Networking**. This will open the **Networking** tab of the VM creation window.

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 (note that if you use an image requiring a public, Stromasys-operated license server, this server must be accessed via a public IP address from the Azure range)
- Basic, advanced, or preconfigured security settings (which ports are open for access to the VM).

Networking tab sample:

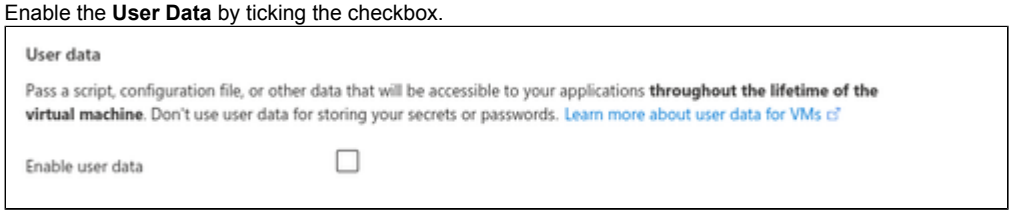


Optionally, you can proceed to the **Management**, **Advanced**, and **Tags** tabs to configure additional details of your VM. However, for a basic test, this is not required. Click on **Review + Create** to proceed to the review screen.

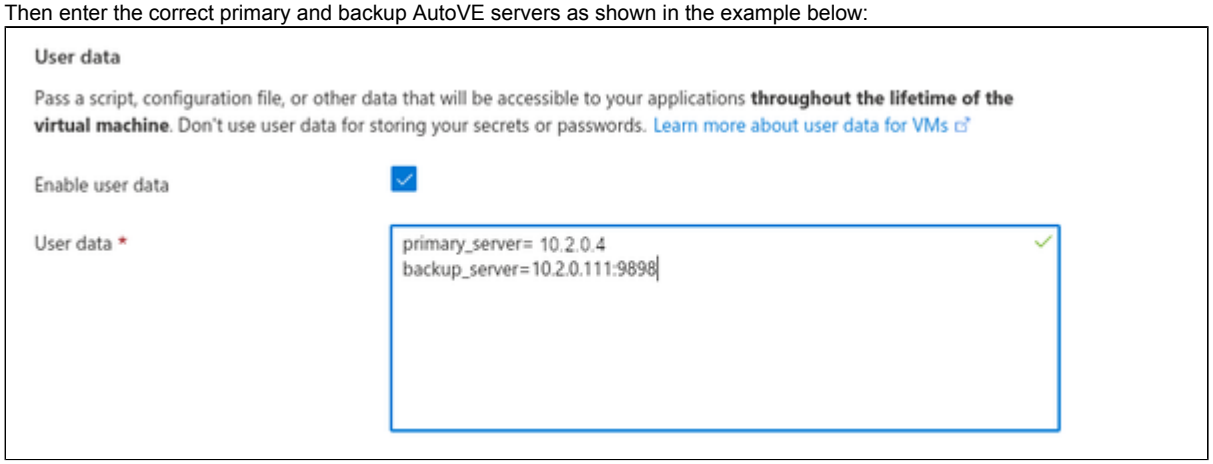
Step 6: additional configuration for **AutoVE** setup.

If the instance is launched from a Charon AL marketplace image and is planned to use AutoVE licensing (instead of the public license servers), you must add the corresponding information to the instance configuration **before** the first launch of the instance:
The AutoVE license server information is entered as instance **User Data**. In the initial instance configuration window, go to the **Advanced** section.

- Open it and scroll down to the **User Data** section.
- Enable the **User Data** by ticking the checkbox.



- Then enter the correct primary and backup AutoVE servers as shown in the example below:



Valid User Data configuration options:

- **`primary_server=`**`<ip-address>[:<port>]`
- **`backup_server=`**`<ip-address>[:<port>]`

where

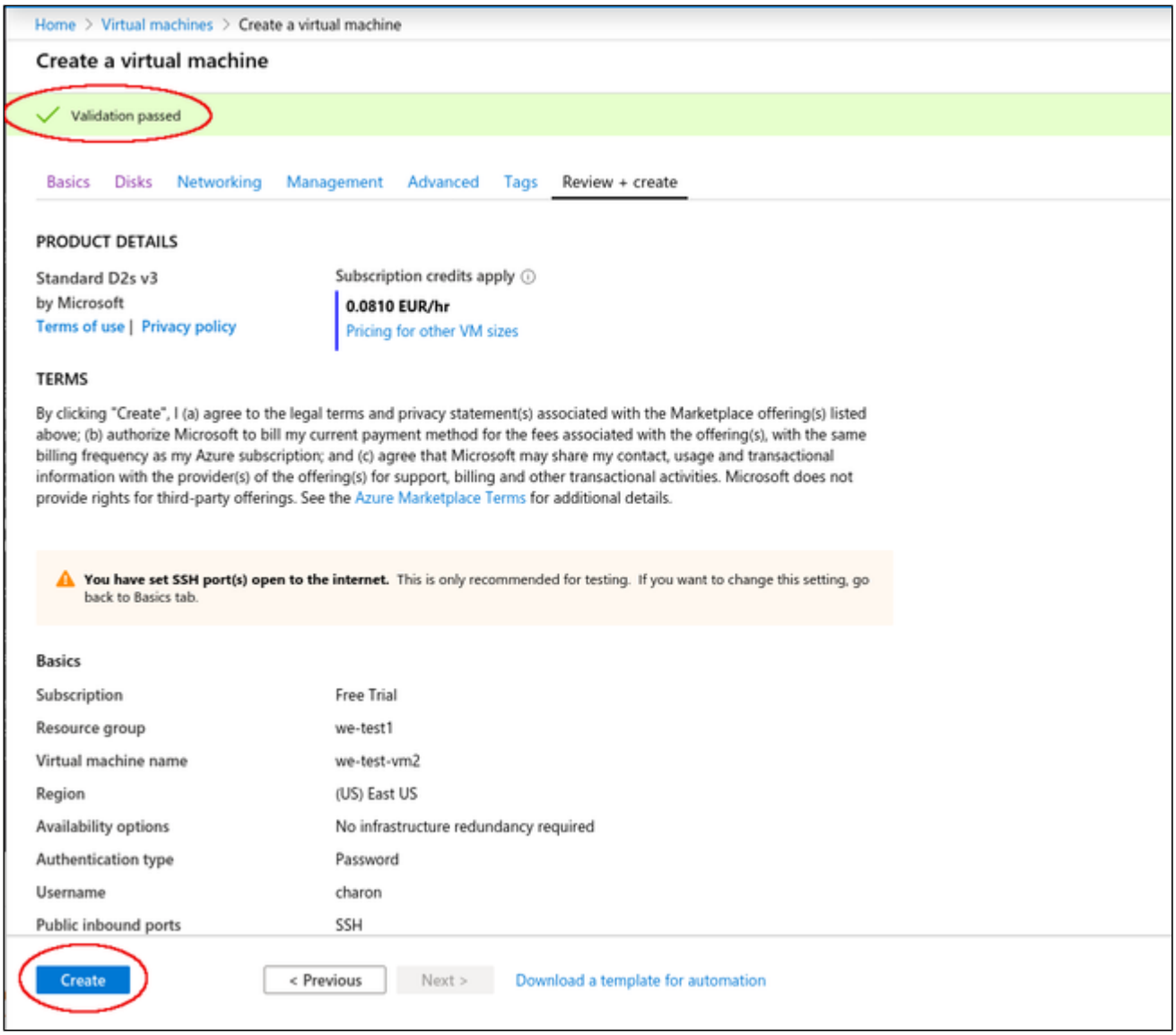
- *<ip-address>* stands for the IP address of the primary and the backup server as applicable, and
- *<port>* stands for a non-default TCP port used to communicate with the license server (default: TCP/8083).

Please note: at least one license server must be configured at initial launch to enable AutoVE mode. **Otherwise, the instance will bind to one of the public license servers operated by Stromasys.**

Step 7: Check the data on the Review + Create screen and create VM.

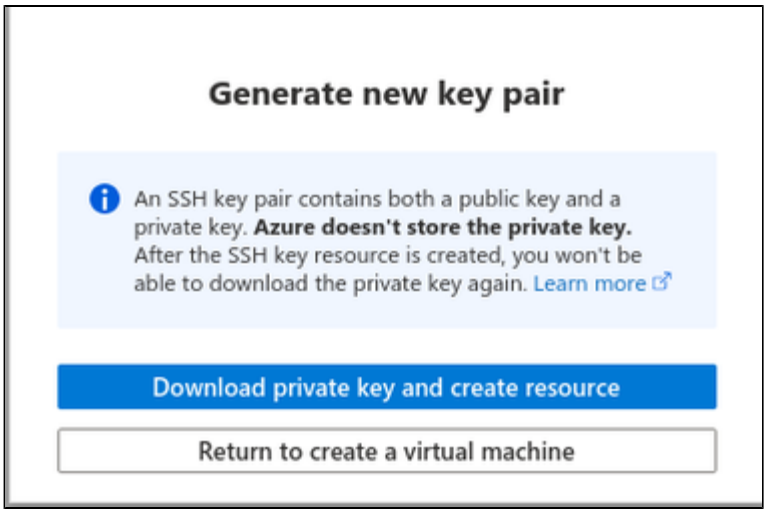
Verify that the checks passed successfully and click on **Create** to create the VM.

Sample **Review+Create** screen:


Home > Virtual machines > Create a virtual machine
Create a virtual machine
Validation passed
Basics Disks Networking Management Advanced Tags Review + create
PRODUCT DETAILS
Standard D2s v3
by Microsoft
Terms of use | Privacy policy
Subscription credits apply
0.0810 EUR/hr
Pricing for other VM sizes
TERMS
By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.
You have set SSH port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.
Basics
Subscription Free Trial
Resource group we-test1
Virtual machine name we-test-vm2
Region (US) East US
Availability options No infrastructure redundancy required
Authentication type Password
Username charon
Public inbound ports SSH
Create
< Previous
Next >
Download a template for automation

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

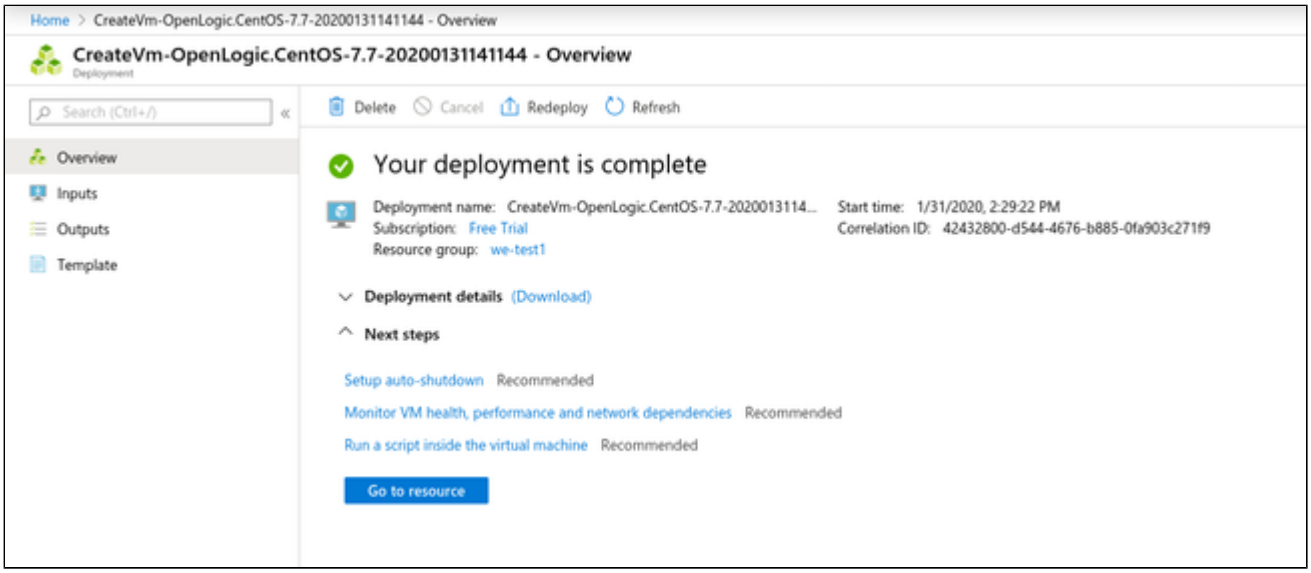
If you chose to let Azure create a new SSH key-pair, you will be asked to download the private key after clicking on the Create **button**, this step is very important as this is the only opportunity to download the private key, which is required to access your VM. The image below shows a sample of this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



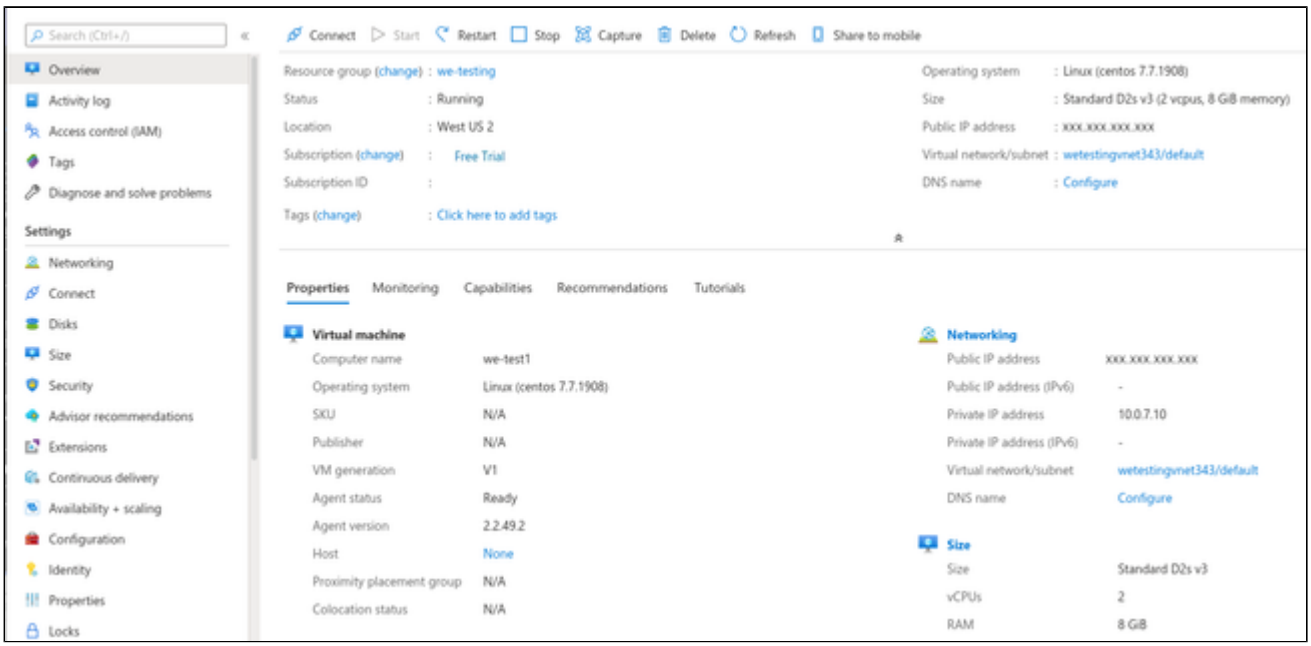
The Deployment page:

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 **private key** used must correspond to the public key installed in the *authorized_keys* file of the cloud instance management user. This is usually done during initial cloud instance launch.
- The management user account normally allows sudo access to privileged commands (use **sudo -i**).
- If the instance was created using a Stromasys-provided AL or VE marketplace image, the management user for **interactive login** is the user **sshuser**.

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-name>@<cloudhost-IP-address>
```

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 **private key** used must correspond to the public key installed in the *authorized_keys* file of the cloud instance management user. This is usually done during initial cloud instance launch.
- If the instance was created using a Stromasys-provided AL or VE marketplace image, the management user for **file transfer** is the user **charon**.
- If the user **charon** is used to transfer files, the home directory for the file transfer will be */charon/storage.*

Setting up a Linux Instance on GCP

Contents

General Prerequisites

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

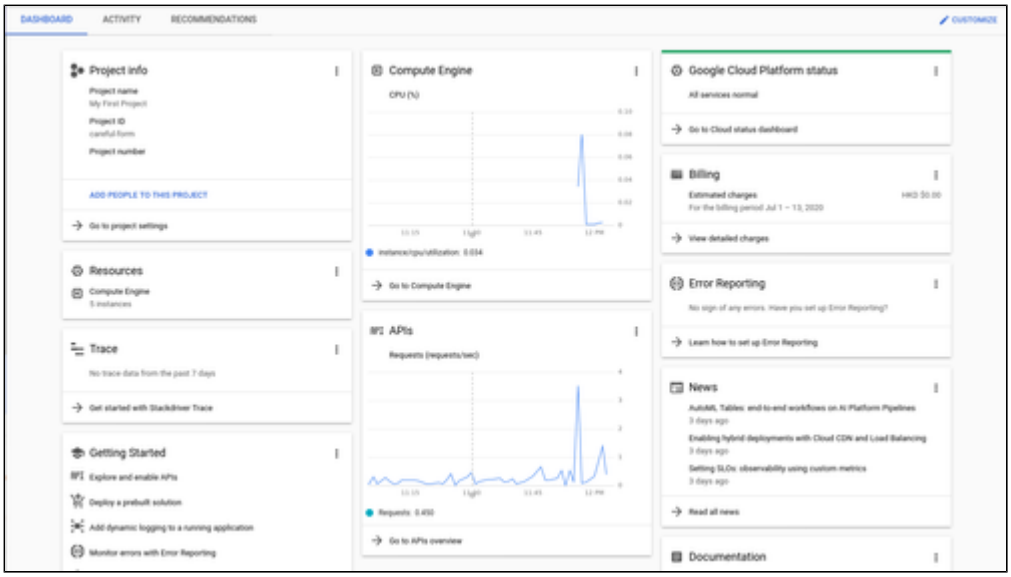
- To set up a Linux instance in the GCP cloud, you need an GCP account.
- Secondly, **prerequisites will be different depending on the planned use of the instance**:
  - Option 1: the instance is to be used as a **Charon emulator host system**:
    - Refer to the hardware and software prerequisite sections of the User's Guide and/or Getting Started guide of your Charon product to determine the exact hardware and software prerequisites that must be fulfilled by the Linux instance. The **image** you use to launch your instance and the **instance type** you chose determine the software and hardware of your cloud instance.
    - A Charon product **license** is required to run emulated legacy systems. Contact your Stromasys representative or Stromasys VAR for details.
  - Option 2: the instance is to be used as a dedicated **VE license server**:
    - Refer to the VE License Server Guide for detailed prerequisites.
- Certain legacy operating systems that can run in the 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:

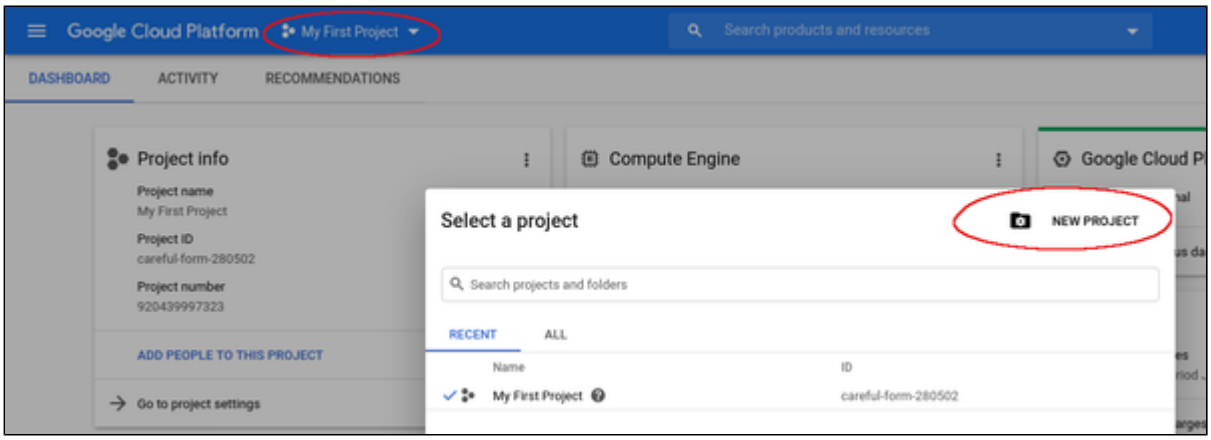


Preparation

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

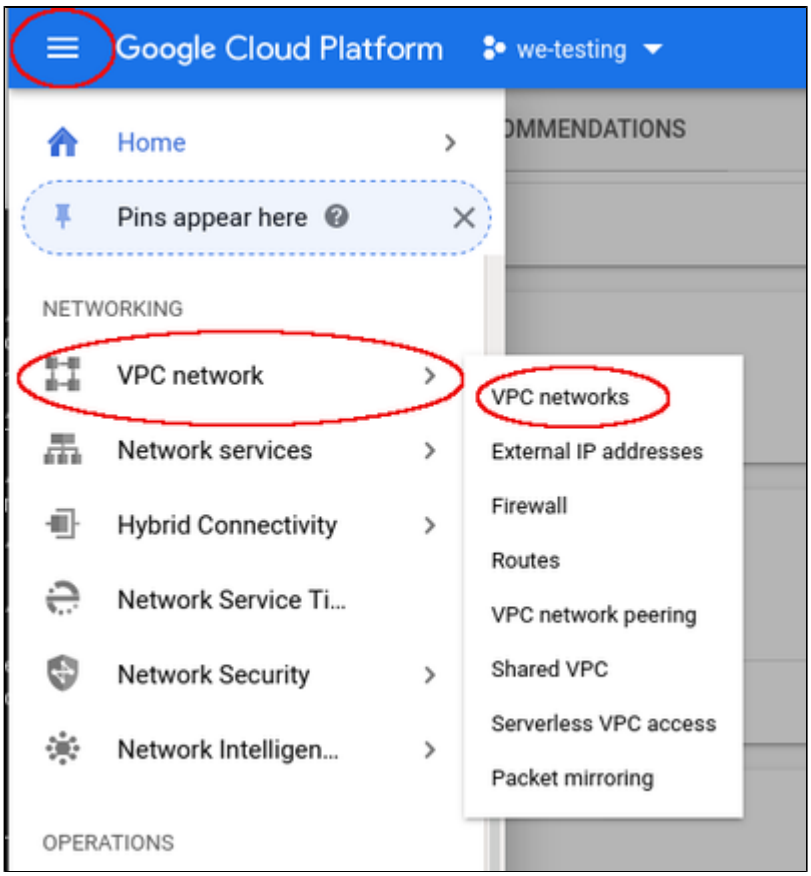
Important rules for Google cloud instances with respect to network interfaces:

- 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.
- A VPC network has a default transmission unit (MTU) of `1460` bytes for Linux images and Windows Server images. During the creation of a VPC you can set the MTU to a different value (e.g., 1500). In your instance (especially, if it does not rely on DHCP), set the MTU to the same value as configured for the VPC to avoid the increased latency and packet overhead caused by fragmentation, or even connectivity problems. For an MTU size of 1460, client applications that communicate with GCP instances over UDP must have a maximum payload of 1432 bytes to avoid fragmentation. In particular, **ensure that the MTU used on any Linux interface dedicated to the emulator is not smaller than the MTU used by the legacy guest system**. Failing to do so will cause network problems. For more information refer to the section *Interface MTU Considerations* in this guide.

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

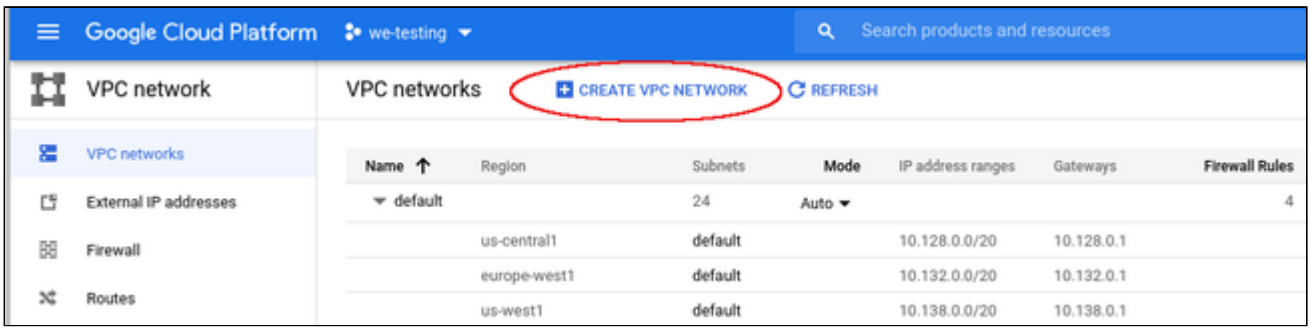
To create additional VPCs (if required), perform the following steps.

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.

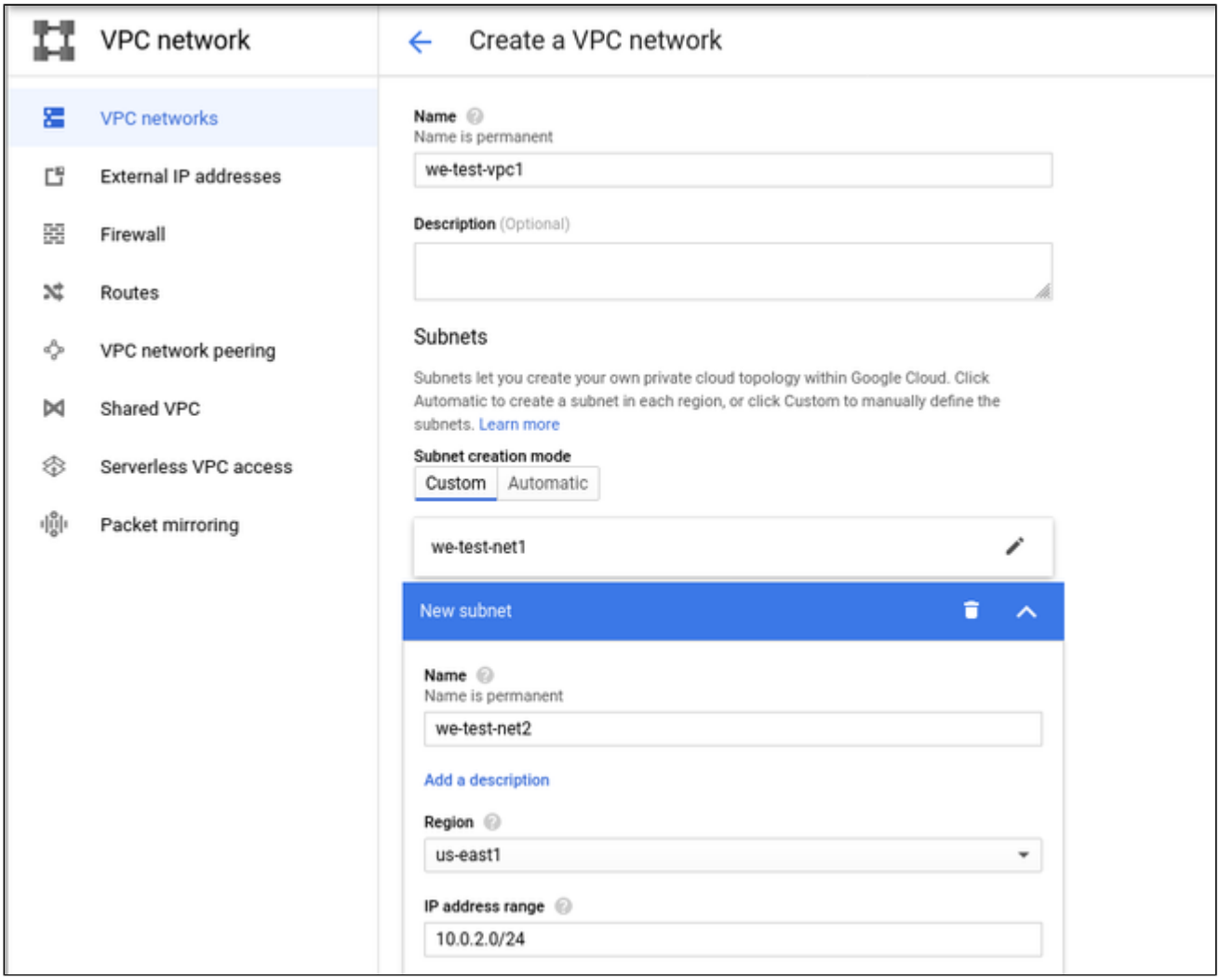


This opens the VPC configuration window.

Step 3: Create VPC and subnets.

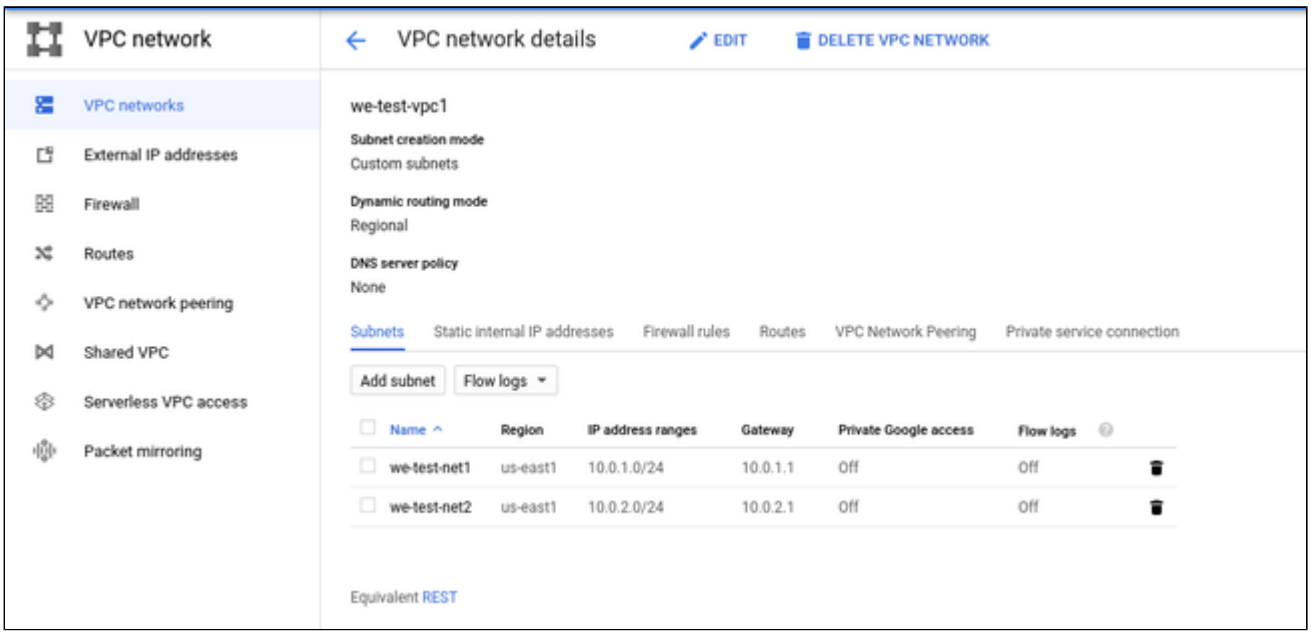
In the VPC configuration window, enter

- the VPC name,
- the subnet name, region and address, and
- optionally, an **alternative MTU size** (at the bottom of the window). The default MTU is 1460 bytes. If you want to dedicate an interface in this VPC to the emulator, this may cause problems as the default MTU size of the legacy guest systems is usually 1500 bytes. **The interface dedicated to the emulator must not have an MTU smaller than the MTU used by the legacy guest system**.



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

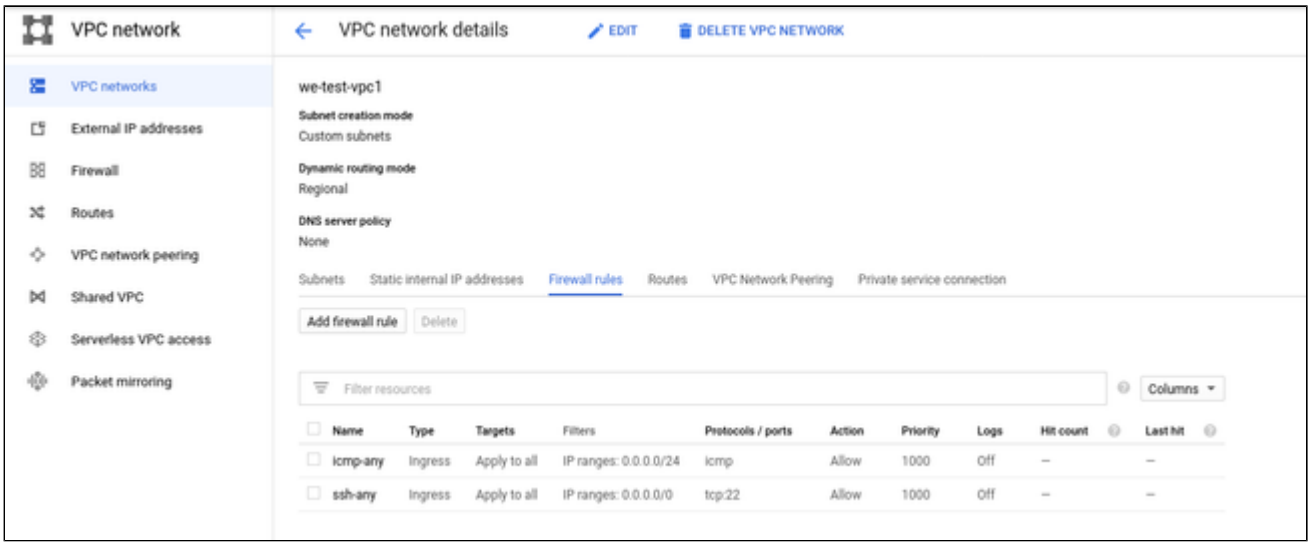
The new VPC should appear in the VPC overview list. Selecting the VPC in the overview list will open the detail information window. Example:



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.

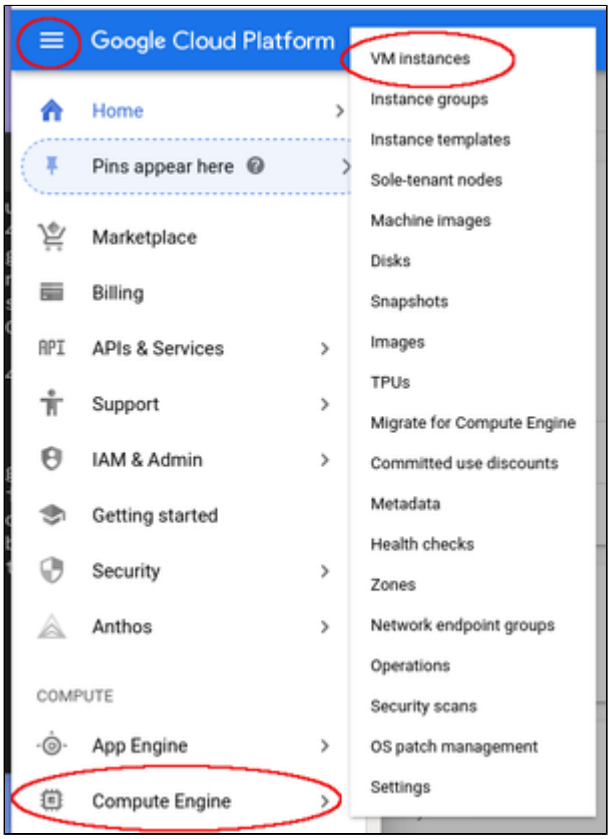
An example of a small set of firewall rules that allow incoming SSH and ICMP is shown below:



Creating a New VM Instance

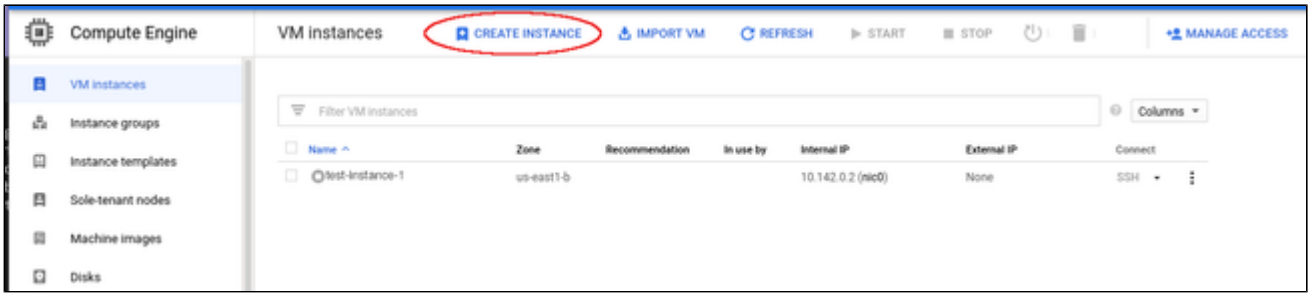
Step 1: Go to the VM instance overview page.

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.



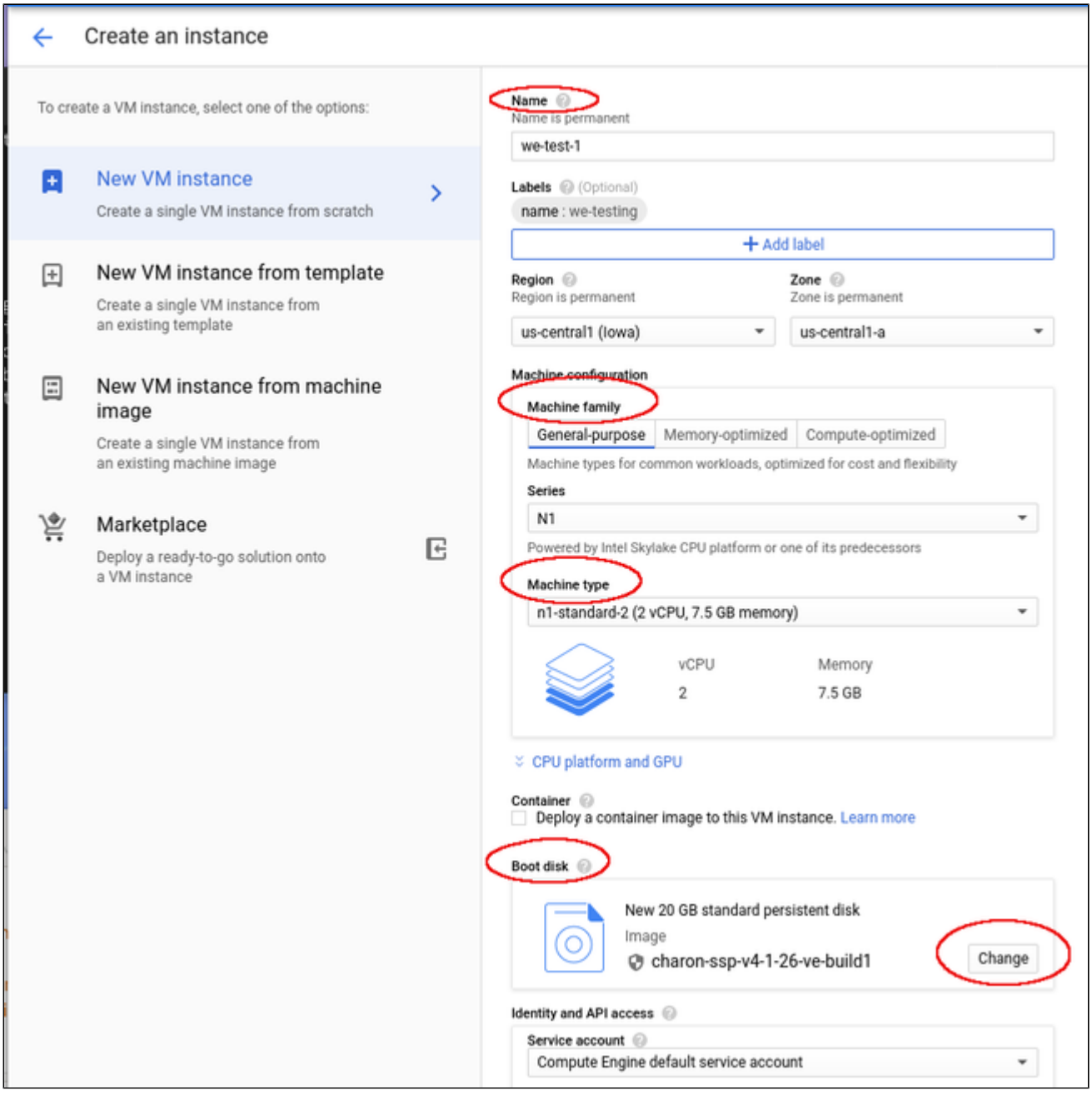
This will open the VM creation window as shown below.

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 requirements of the Charon products installed on the instance.
- **Boot disk** type and size, and the image to use as the operating system (recommended minimum system disk size: 30GB). To change the image for, press the **Change** button and select the correct image. If installing a prepackaged marketplace Charon image, select the matching image. If you plan to install your Charon product using RPM packages, use a Linux version supported for your product.

The following image illustrates the basic settings:

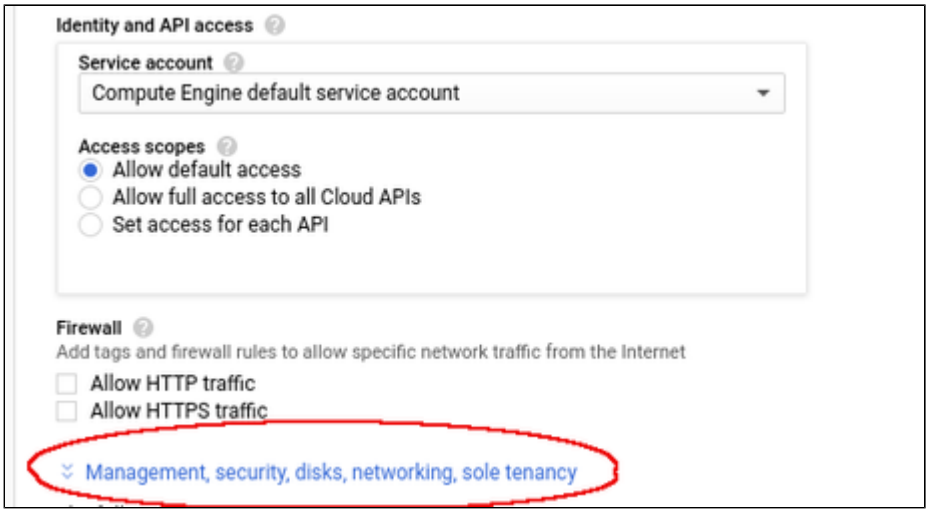


Additional points to note:

- The **CPU platform and GPU** section provides the option to define the vCPU to core ration. That is, you can modify the settings such that each CPU visible to the host operating system corresponds to one CPU core of the GCP instance.
- In the **Identity and API access** section by default a service account (**Compute Engine default service account**) and the **Default access** scope are assigned to the instance. If this instance is to be used as a VE license server, **do not modify these settings** unless you are confident that you can provide equivalent permissions in a custom configuration. The VE license server will not function correctly without these permissions.

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.

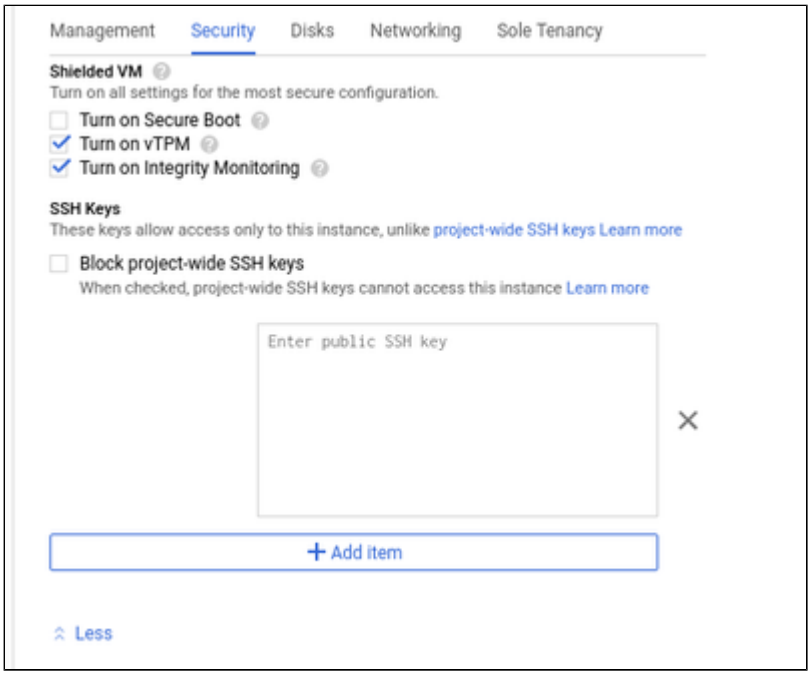


The advanced settings allow you to create and add disks and network interfaces during the creation of a VM.

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 (the username extracted from the key will be displayed).
- **Please note**: if your management system supports it, for RHEL 9.x, Rocky Linux 9.x, and Oracle Linux 9.x use SSH key types ECDSA or ED25519. This will allow connecting to these Charon host Linux systems using an SSH tunnel without the default crypto-policy settings on the Charon host having to be changed for less secure settings. This is, for example, important for the Charon-SSP Manager. See also: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/security_hardening/using-the-system-wide-cryptographic-policies_security-hardening.

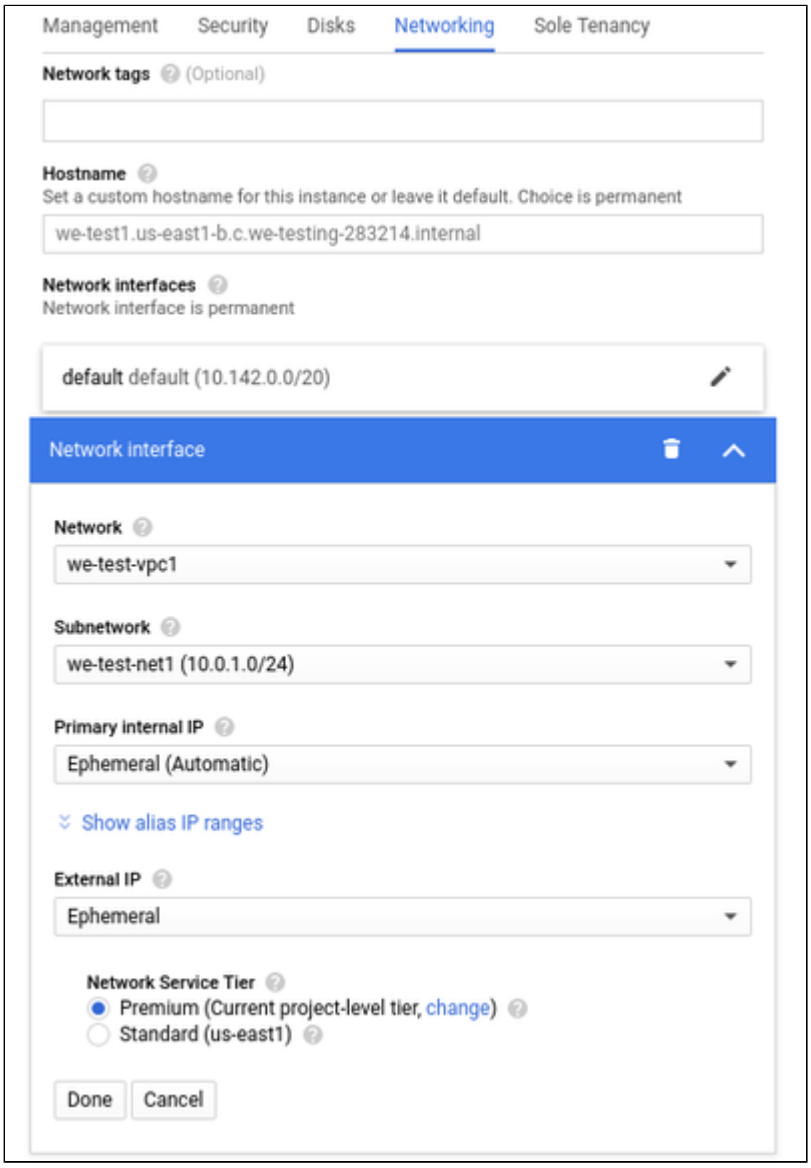


You can collapse the section again by clicking on **Less**.

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:

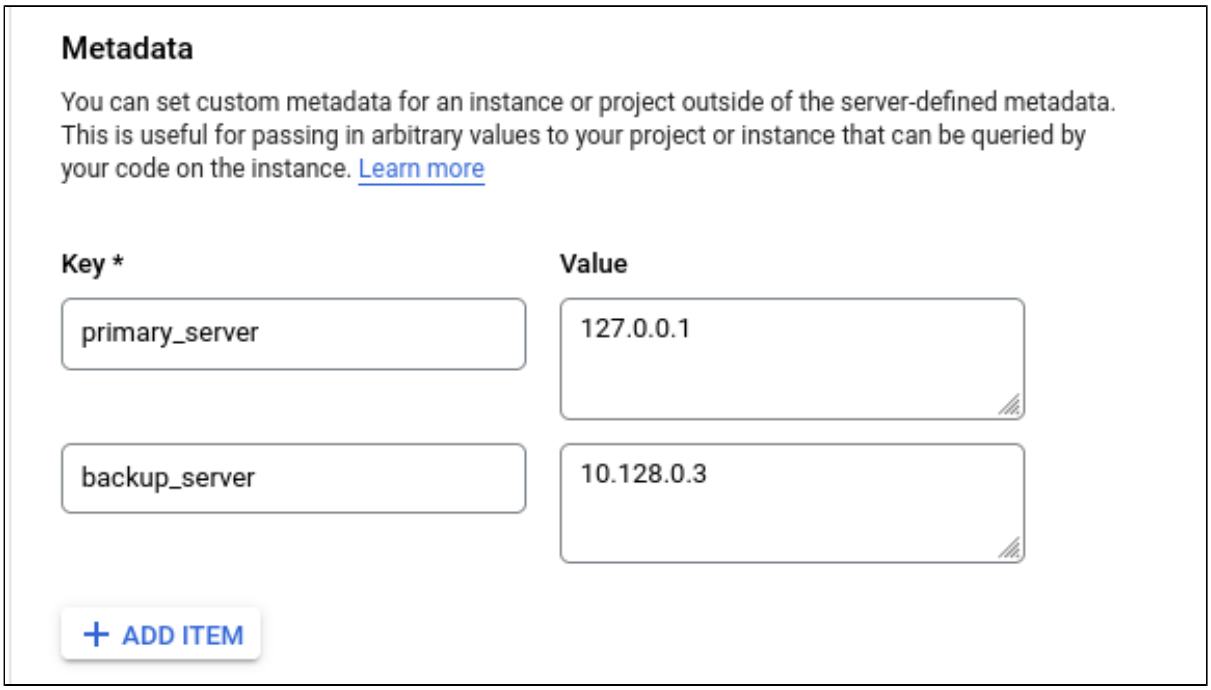
- Open the advanced settings at the bottom of the VM creation window by clicking on **Management, security, disks,...** at the bottom of the page.
- Select Networking from the advanced settings section.
- Select the edit option for the default NIC.
- Enable IP forwarding
- Click on **Done**.

Please note: you have to set up a firewall manually when you add additional network interfaces. See Network Management and the GCP documentation for more detail.

Step 6: additional configuration for **AutoVE** setup.

If the instance is launched from a Charon AL marketplace image and is planned to use AutoVE licensing (instead of the public license servers), you must add the corresponding information to the instance configuration **before** the first launch of the instance:

The AutoVE license server information is entered as **Custom Metadata**. In the initial instance configuration window, go to the bottom where the **NETWORKING, DISKS, SECURITY, MANAGEMENT...** configuration section is located. Open it and select the **Management** section. Add the Custom Metadata as shown in the example below:



Valid User Data configuration options:

- **`primary_server`** *`<ip-address>`*`[:`*`<port>`*`]`
- **`backup_server`** *`<ip-address>`*`[:`*`<port>`*`]`

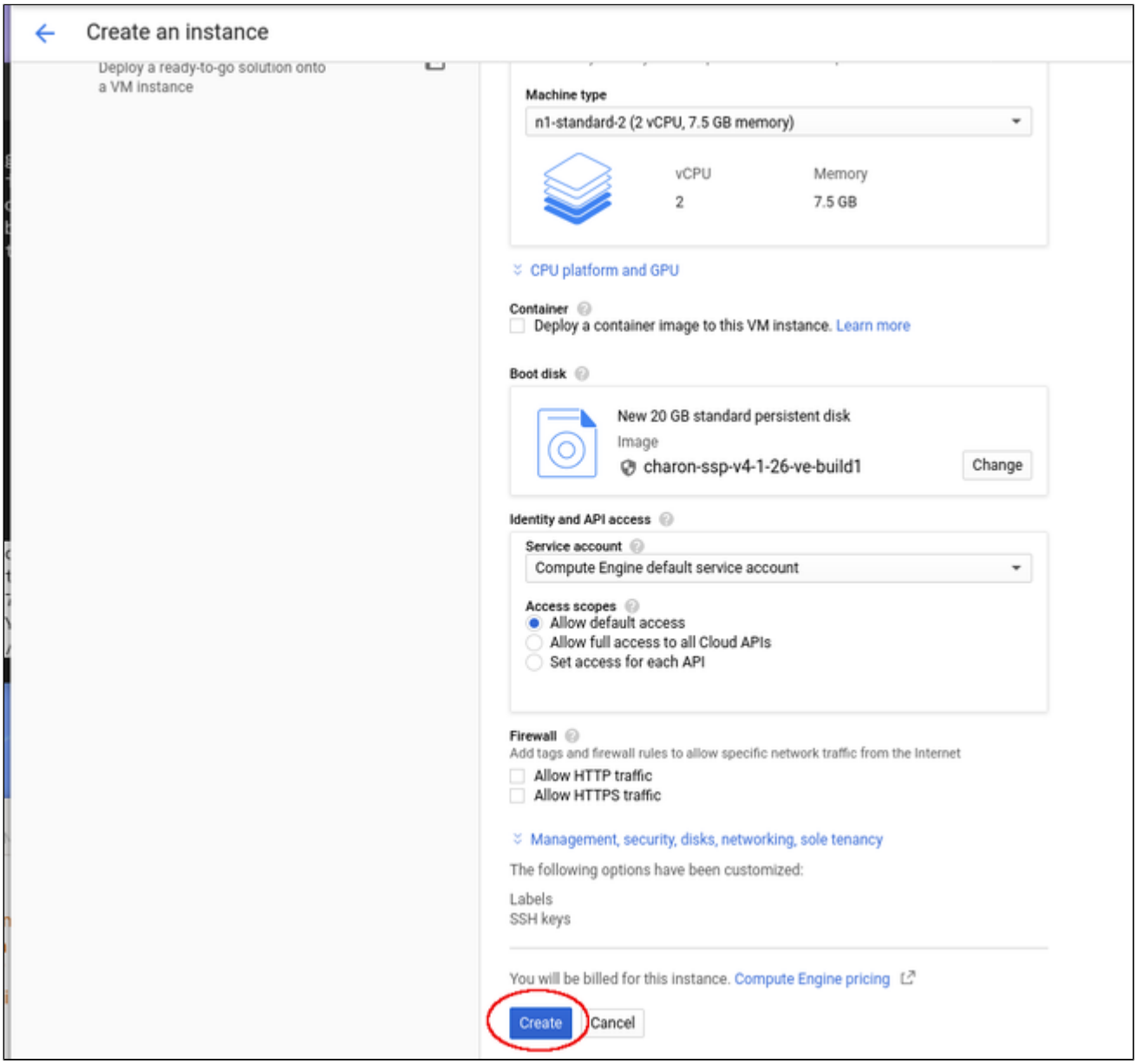
where

- *<ip-address>* stands for the IP address of the primary and the backup server as applicable, and
- *<port>* stands for a non-default TCP port used to communicate with the license server (default: TCP/8083).

Please note: at least one license server must be configured at initial launch to enable AutoVE mode. **Otherwise, the instance will bind to one of the public license servers operated by Stromasys.**

Step 7: Create the VM.

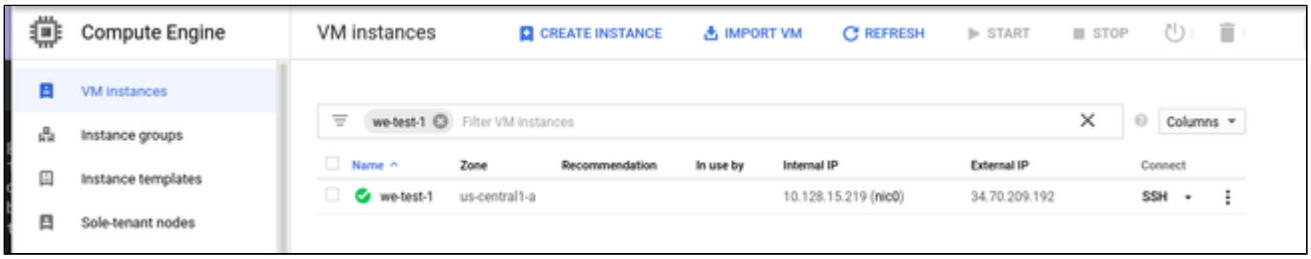
Once you filled in all the required data, create the VM by pressing the **Create** button at the bottom of the page:



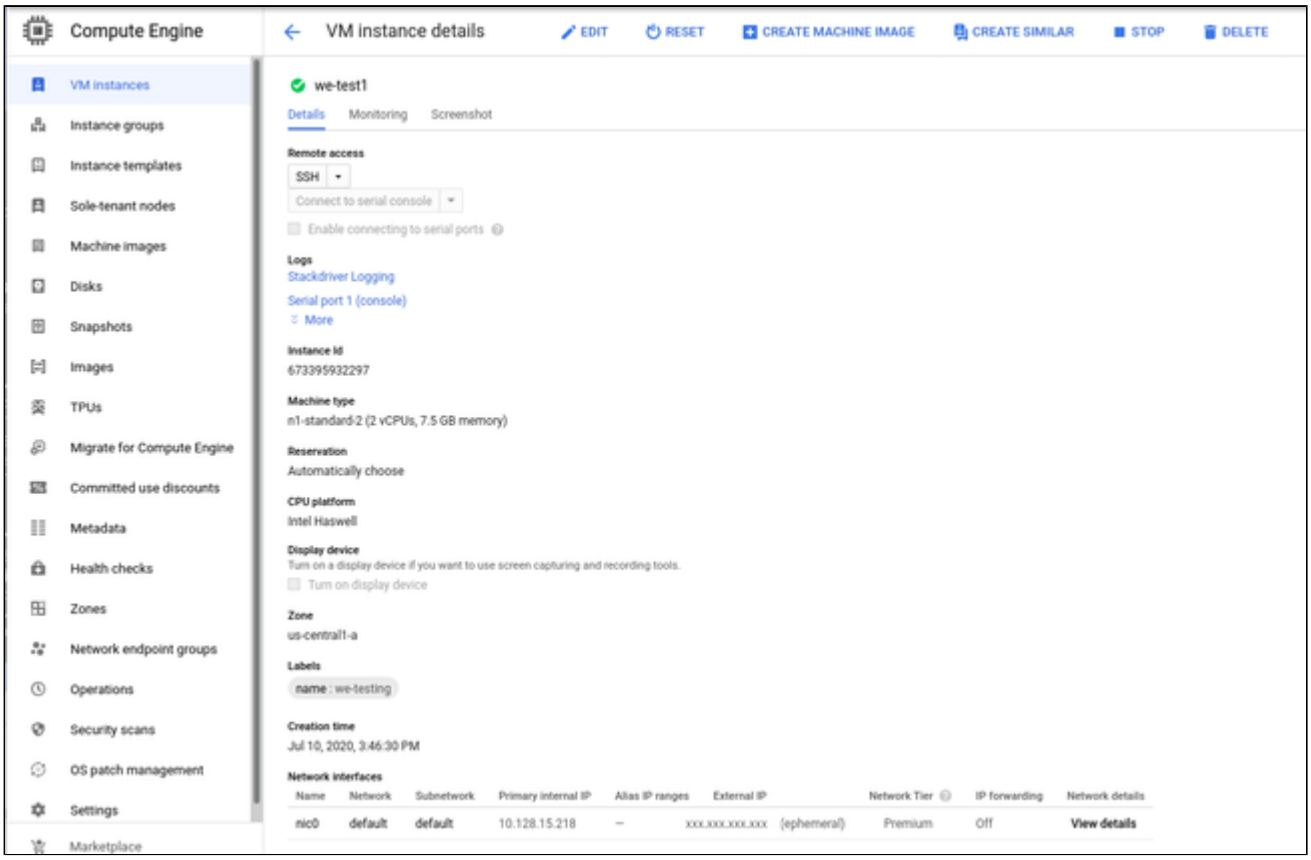
This will create the VM, start it and show it in the VM instances list.

Step 8: 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 **private key** used must correspond to the public key installed in the *authorized_keys* file of the cloud instance management user. This is usually done during initial cloud instance launch.
- The management user account normally allows sudo access to privileged commands (use **sudo -i**).
- If the instance was created using a Stromasys-provided AL or VE marketplace image, the management user for **interactive login** is the user **sshuser**.

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-name>@<cloudhost-IP-address>
```

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 **private key** used must correspond to the public key installed in the *authorized_keys* file of the cloud instance management user. This is usually done during initial cloud instance launch.
- If the instance was created using a Stromasys-provided AL or VE marketplace image, the management user for **file transfer** is the user **charon**.
- If the user **charon** is used to transfer files, the home directory for the file transfer will be */charon/storage.*

Setting up a Linux Instance in the IBM Cloud

Contents

General Prerequisites

As this description shows the basic setup of a Linux instance in the IBM cloud, 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 the IBM cloud, you need an IBM account.
- Secondly, **prerequisites will be different depending on the planned use of the instance**:
  - Option 1: the instance is to be used as a **Charon emulator host system**:
    - Refer to the hardware and software prerequisite sections of the User's Guide and/or Getting Started guide of your Charon product to determine the exact hardware and software prerequisites that must be fulfilled by the Linux instance. The **image** you use to launch your instance and the **instance type** you chose determine the software and hardware of your cloud instance.
    - A Charon product **license** is required to run emulated legacy systems. Contact your Stromasys representative or Stromasys VAR for details.
  - Option 2: the instance is to be used as a dedicated **VE license server**:
    - Refer to the VE License Server Guide for detailed prerequisites.
- Certain legacy operating systems that can run in the 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.

IBM Cloud Login and New Instance Launch

Logging in to IBM Cloud

To log in perform the following steps:

- Go to https://cloud.ibm.com. You will see the login screen.
- Enter your login credentials.
- Upon successful login, your cloud dashboard screen will be displayed.

Preparation

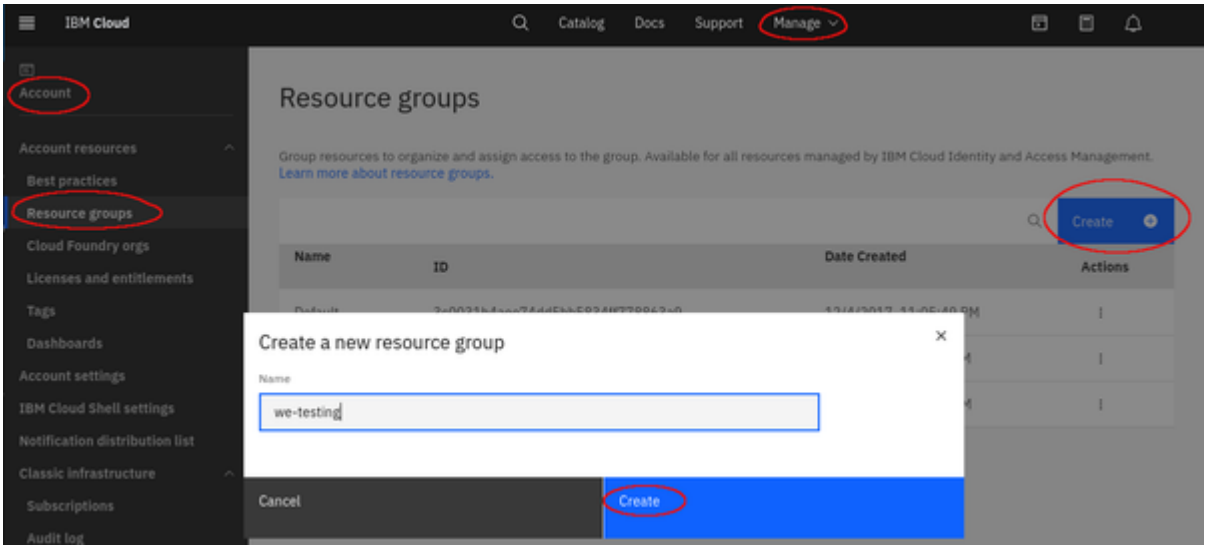
Please note: if you want to use an existing resource group and VPC, select the correct VPC from the resource list (click on the menu symbol at the top left of the cloud console screen and select Resource List).

Creating a Resource Group if Required

To organize resources in your account, you can group related resources in a resource group. If you have not already created a resource group, you can do so by selecting:

Manage > Account > Resource Groups and then clicking on the **Create** button. Add the name of the group in the pop-up window and confirm with **Creat**
.

A sample screen is shown below.

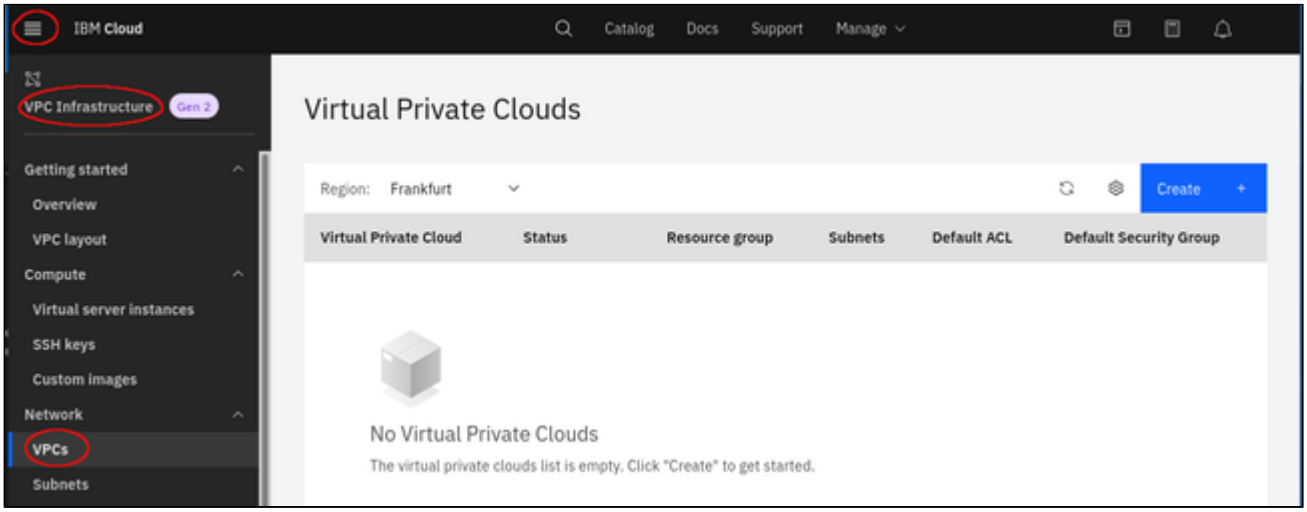


Creating VPCs and Subnets for Instance

If the necessary VPC and the associated subnets do not exist yet, create them before you create your virtual server. A virtual server can be a member of one VPC.

Step 1: go to the VPC section.

Select the ***Menu*** at the top left, and then **VPC Infrastructure > *Network* > VPCs.** This will open the list of existing VPCs or an empty list as shown in the sample below:



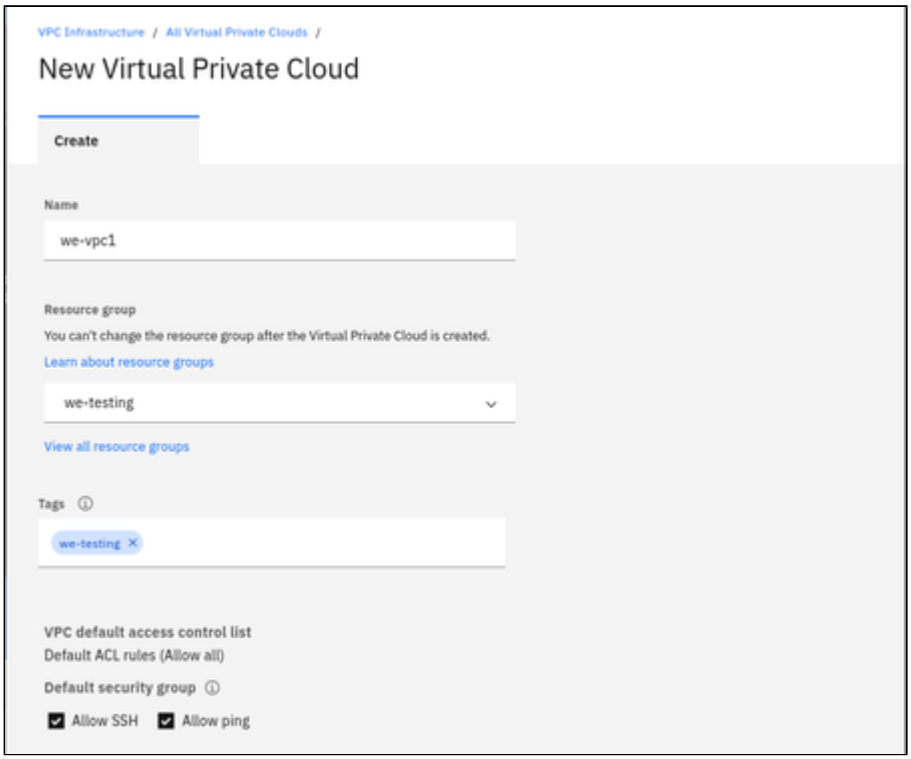
Step 2: start the VPC creation.

To open the VPC creation window, click on the **Create** button at the top right of the VPC list.

Step 3: enter the required information for the new VPC and the first subnet.

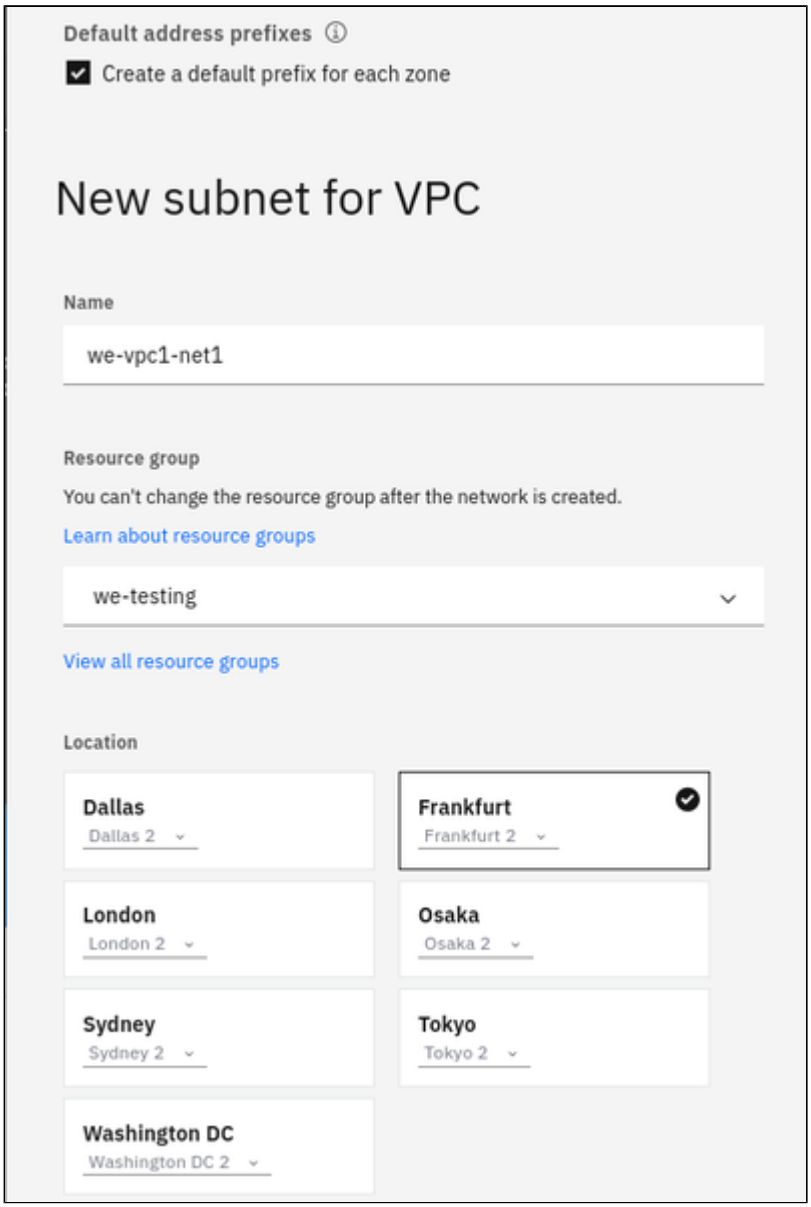
At the top of the VPC creation window, enter the following information as shown in the sample below:

- VPC Name
- Resource group to which the VPC belongs
- Tags (optional)
- Access allowed by the default security group.



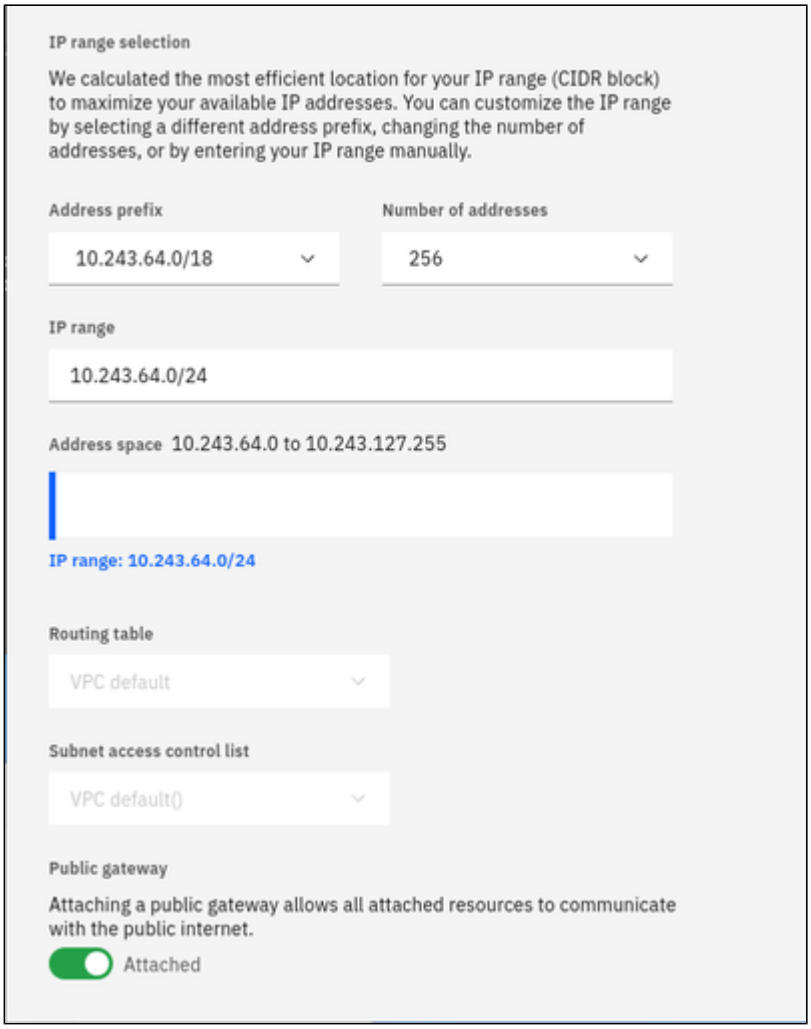
In the middle of the VPC creation window enter the following information as shown in the sample below:

- Whether a default address prefix should be created for each zone.
- Information for the first subnet in the VPC:
  - Subnet name
  - Resource group for the subnet
  - Location of the subnet



At the bottom of the VPC creation window enter at least the following information as shown in the sample below:

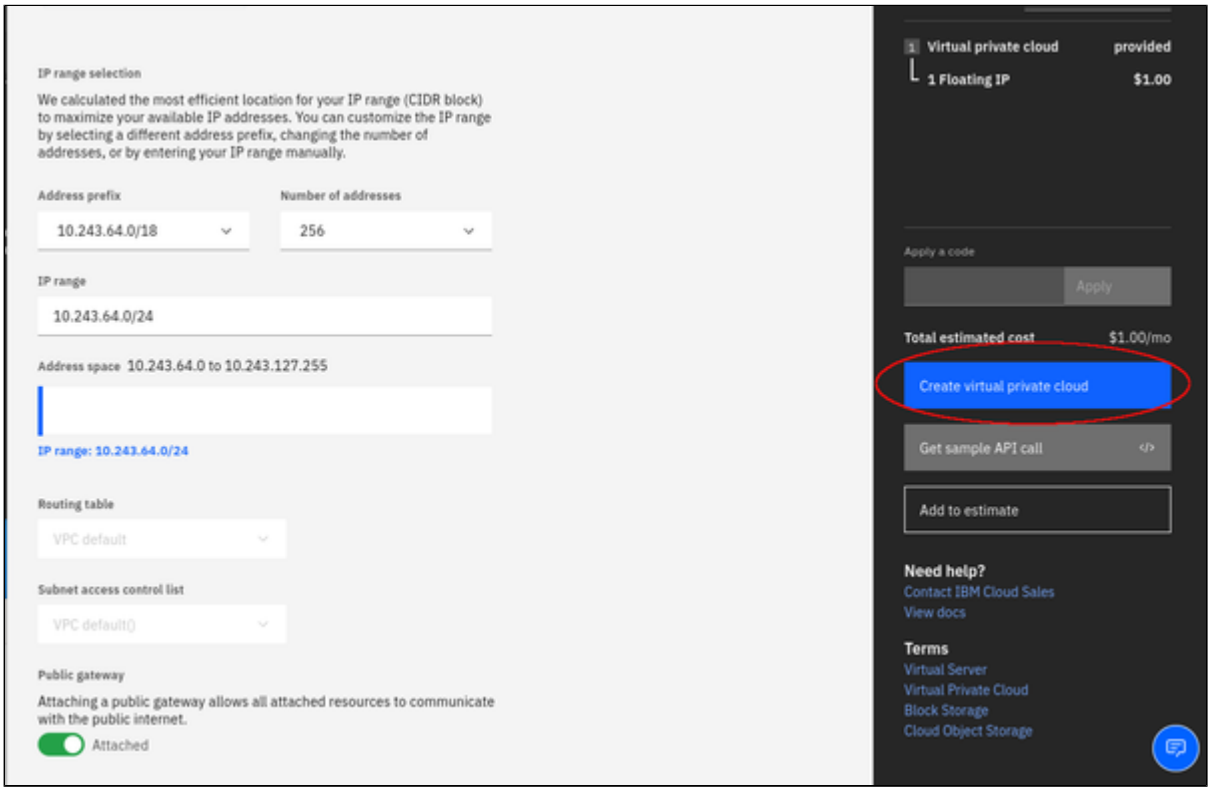
- IP range for the subnet (the size of the subnet cannot be changed later!)
- Whether a public gateway for Internet traffic should be attached to the subnet (enables outgoing Internet access for systems on this subnet)



You can add additional subnets later.

Step 4: confirm your data and create VPC and subnet.

To complete the creation of VPC and subnet, click on the blue button **Create virtual private cloud** on the right pane of the window:



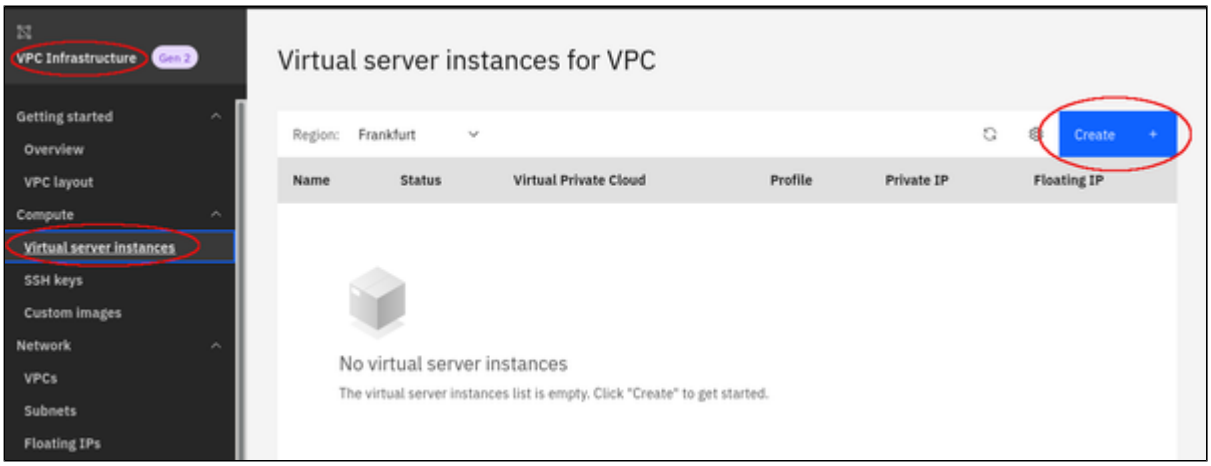
After this, your new VPC should be visible in the VPC list.

If required, you can now configure the ACL for the subnet (by default, it allows all traffic), or other parameters of the VPC. To get to these options, click on the name of the VPC in the list.

Creating a New Virtual Server Instance

Step 1: open the virtual server list and start the creation of a new server.

In the **VPC infrastructure** section under **Compute**, click on **Virtual server instances**. This opens the list of existing virtual servers. At the top right of this list click on **Create**. The image below provides an illustration of these steps:

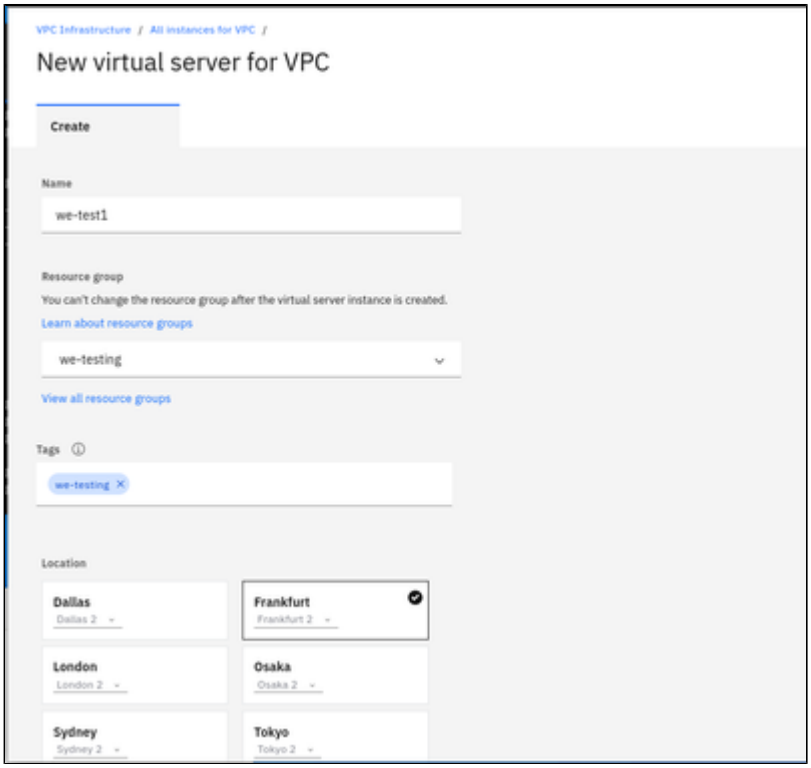


This will open the section for creating a virtual server.

Step 2: enter the required information to create a new virtual server.

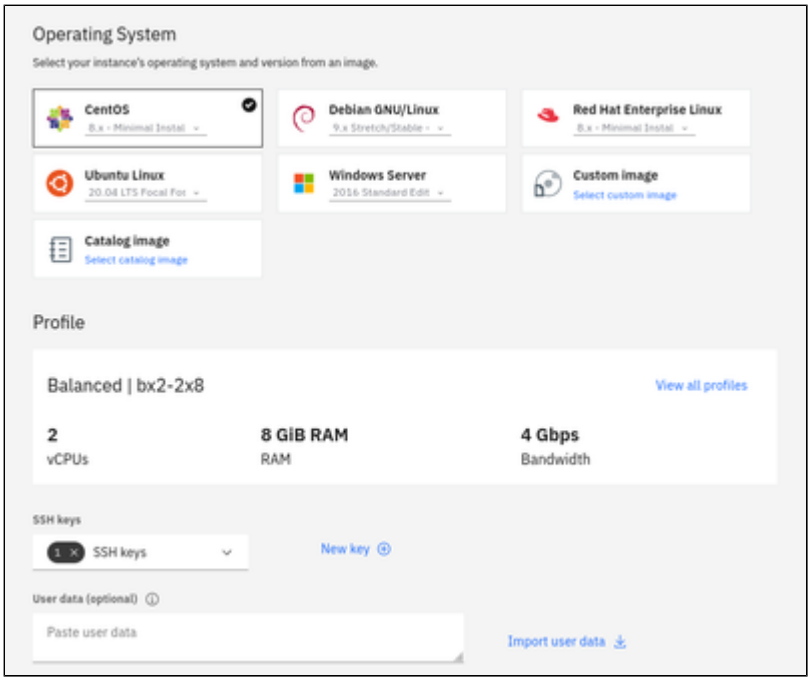
At the top of the Virtual Server creation window, enter the following information as shown in the sample below:

- Name of the virtual server
- Resource group to which the server will belong
- Tags (optional)
- Location of the virtual server



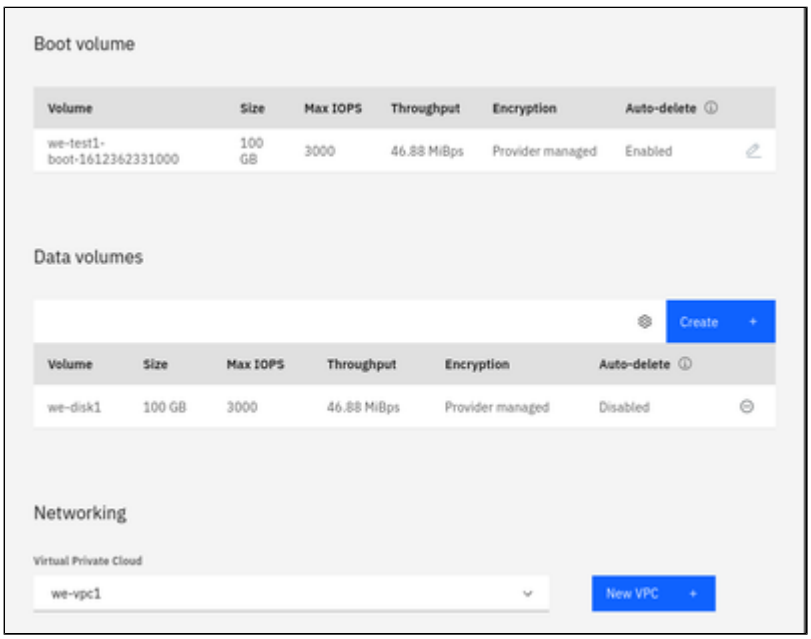
In the next section of the Virtual Server creation window, enter the following information as shown in the sample below:

- Operating system and version for your instance (refer to the general Charon product User's Guide for supported distributions and versions).
- Select the hardware profile (it must fulfill the requirements of the emulated SPARC system(s) you plan to run on the instance. To select the profile you need, click on **View all profiles**. The profile **cannot be changed** after the instance has been created.
- If necessary add a new SSH key or use an existing one.
- **Please note**: if your management system supports it, for RHEL 9.x, Rocky Linux 9.x, and Oracle Linux 9.x use SSH key types ECDSA or ED25519. This will allow connecting to these Charon host Linux systems using an SSH tunnel without the default crypto-policy settings on the Charon host having to be changed for less secure settings. This is, for example, important for the Charon-SSP Manager. See also: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/security_hardening/using-the-system-wide-cryptographic-policies_security-hardening.

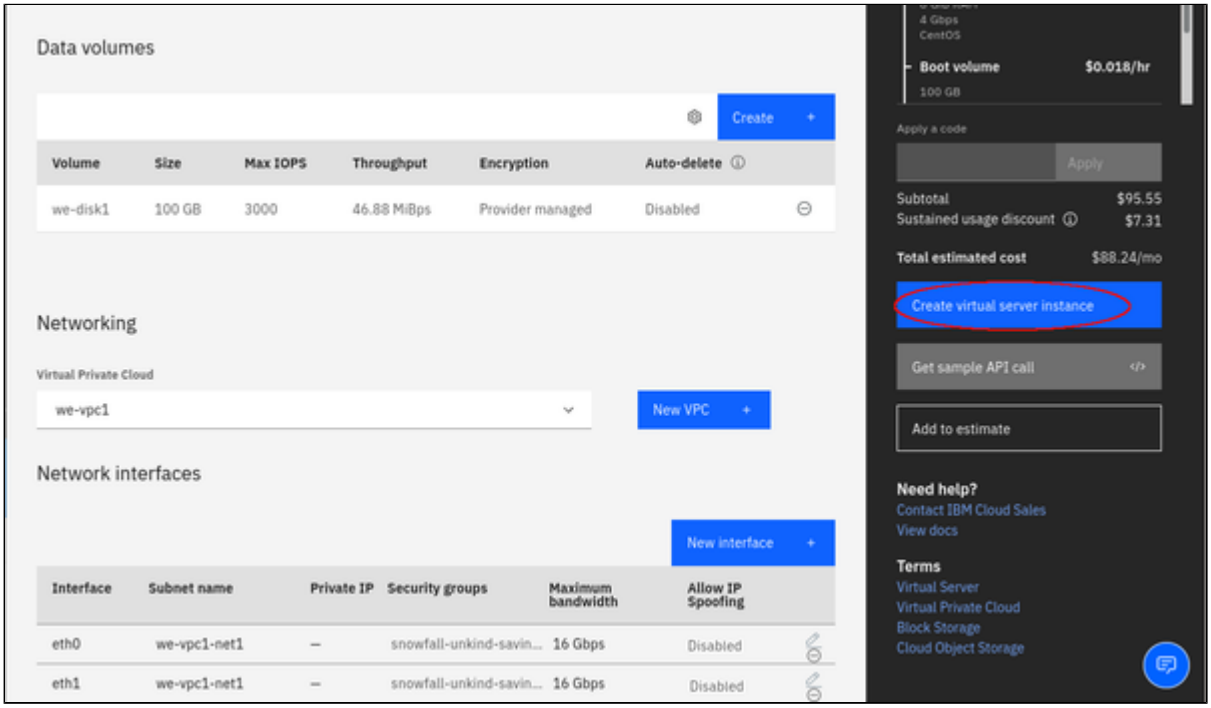


In the next section of the Virtual Server creation window, enter the following information as shown in the sample below:

- Verify the boot volume configuration.
- Add a new or existing data volume as required.
- Select the VPC for the virtual server.



At the bottom of the Virtual Server creation window, enter the the required network interfaces. Editing them allows adding IP Spoofing (necessary for routing).



Then, in the right pane, click on **Create virtual server instance** to create the server instance. The new server will be displayed in the virtual server list.

Step 3: add a public IP address if required.

Once the virtual server is available in the list of active servers, perform the following steps to add a public IP address:

- Click on the server name. This will open the virtual server details window.
- Scroll down to the network interfaces and click on the edit symbol next to the primary interface (default name: eth0).
- In the configuration window that opens, click on **Reserve a new floating IP**.
- Save the changes by clicking on **Save** at the bottom of the edit window.

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 **private key** used must correspond to the public key installed in the *authorized_keys* file of the cloud instance management user. This is usually done during initial cloud instance launch.
- The management user account normally allows sudo access to privileged commands (use **sudo -i**).
- If the instance was created using a Stromasys-provided AL or VE marketplace image, the management user for **interactive login** is the user **sshuser**.

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-name>@<cloudhost-IP-address>
```

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 **private key** used must correspond to the public key installed in the *authorized_keys* file of the cloud instance management user. This is usually done during initial cloud instance launch.
- If the instance was created using a Stromasys-provided AL or VE marketplace image, the management user for **file transfer** is the user **charon**.
- If the user **charon** is used to transfer files, the home directory for the file transfer will be */charon/storage.*

Installing the Charon-SSP 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, for the management of a remote Charon host, the Charon Manager is installed on a system on customer premises, and uses an encrypted connection to manage the Charon host in the cloud. The Charon Manager can also be installed on the Charon host itself and 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). Please note that as of 1 January 2022 CentOS 8 is EOL. For new deployments, it is recommended to use a non-EOL alternative. For existing installations, the possible negative impacts of staying with an EOL host operating system should be carefully evaluated.
  - Rocky Linux version 8.x (64-bit) or higher
  - Ubuntu 17 or higher (64-bit)
- **Microsoft Windows:** versions 7, 8, 10, and (starting with Charon-SSP 5.6.1) version 11

Restriction: the Charon-SSP Manager is not supported on Linux hosts using Wayland when they run in a VMware instance with 3D-graphics. The Manager will show erratic behavior in such cases.

Installation Packages

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

Please note: starting with SSP version 5.6.1, the RPM packages are distributed in an self-extracting archive. The archive required for the Charon-SSP Manager is **charon-gui-**<*version*>**.sh**. It also contains the Charon-SSP Agent which must be installed on the Charon host system to be managed by the Charon Manager. The archive must be unpacked on a Linux system (even if you need the kit for Microsoft Windows).

Use the following command to unpack the RPM packages:

- Go to the directory containing the self-extracting archive.
- Run the script: `# sh charon-gui-<version>.sh`
- Read the end-user agreement and accept it.
- The RPM packages will be extracted in a subdirectory (*charon-gui-*<*version*>) of your current working directory.

Names of the Charon-Manager installation packages:

- 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 cloud marketplace image:

The packages are included in the Charon-SSP cloud-specific image (in */charon/storage*). Once a new instance has been launched, you can download the Charon-SSP Manager archive 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-gui-`*`<version>`***`.sh`**

b) For installation on a Charon host where a conventional RPM installation was performed: Stromasys will provide you with a download link. The Charon Manager packages are also included in the Charon agent RPM and available in */opt/charon-agent/ssp-agent/bin/* once the agent has been installed.

Charon-Manager Installation on Linux

Prerequisites

The Charon Manager can be installed on the Charon host itself or on a remote management system. For the Charon Manager to work, the **Charon Agent must have been installed on the Charon host system**. The Charon Manager communicates with the Agent to configure and manage the emulator instances.

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** or **dnf** 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 (from one of the sources described above).	Installation on the Charon-SSP host system in the cloud (non-typical installation): • Log in and become the root user on the Charon host using the following commands: **$ ssh -i** *<path-to-private-key>* **sshuser@***<cloud-instance-ip>* **# 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	**Unpacking the shell archive**:	
	• Run the script: `# sh charon-gui-<version>.sh` • Read the end-user agreement and accept it. • The RPM packages will be extracted in a subdirectory (*charon-gui-<version>*) of your current working directory	
4	**Installing the package:**	
	Assuming you are in the subdirectory containing the RPM file, use the following commands for supported Linux systems with RPM package management: • Linux 7.x: `# yum install <filename-of-package>` • Linux 8.x and higher: `# dnf 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>`	

Installation Steps on Microsoft Windows

The Charon-SSP Manager for Windows software is shipped as a zipped archive package which is contained in the **charon-gui-**<*version*>**.sh** archive. After unpacking the archive on a Linux system, copy the ZIP file to your Microsoft Windows system and use the following instructions to complete the installation.

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).

Notes:

- Typically, **Charon-SSP Manager** is installed either on the Charon host itself (if this system has a graphical interface) on a management 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 a non-graphical Charon host in the cloud or in a VMware environment and be displayed on a remote system using X11-Forwarding via an SSH connection.
- **For accessing a Charon host instance in a cloud across the Internet using its public IP address**:
  - 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 know 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 a Charon host instance in a cloud 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 a Charon-SSP host 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 itself 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:

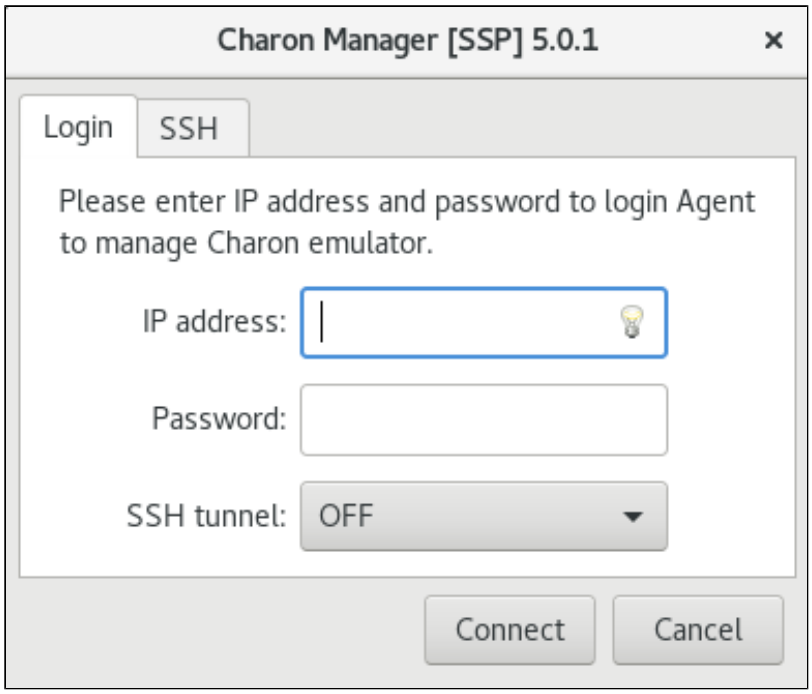
```
$ /opt/charon-manager/ssp-manager/ssp-manager
```

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



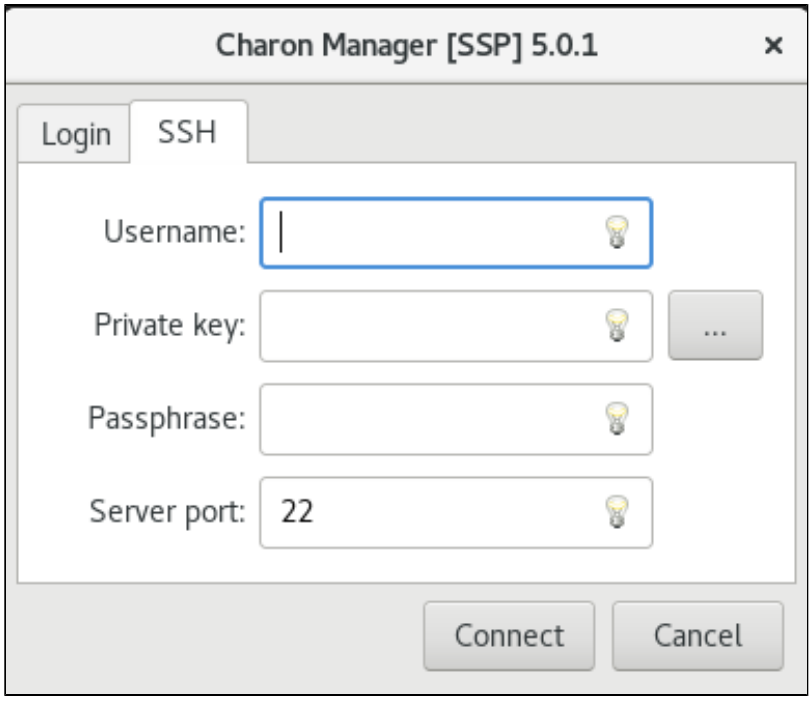
If the management password has not yet been set, perform the following steps:

- Enter the IP address of your Charon-SSP host instance in the **IP address** field.
- Leave the **Password** field empty.
- For cloud instances enable the SSH tunnel configuration (select **ON**).
  Set to **OFF** if connected to *localhost*. The SSH tunnel can generally be used if key-based SSH login is enabled on the target system.
- Change to the SSH tab to fill in the required information if the SSH tunnel has been enabled.

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

- Enter the 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 (key-based SSH login required).
- 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



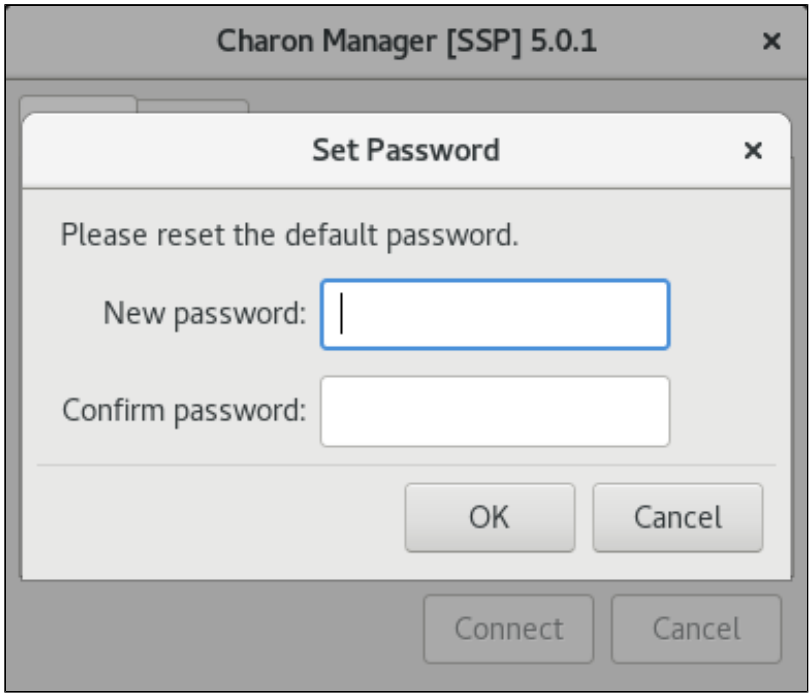
If you use the integrated SSH tunnel, perform the following steps:

- 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).

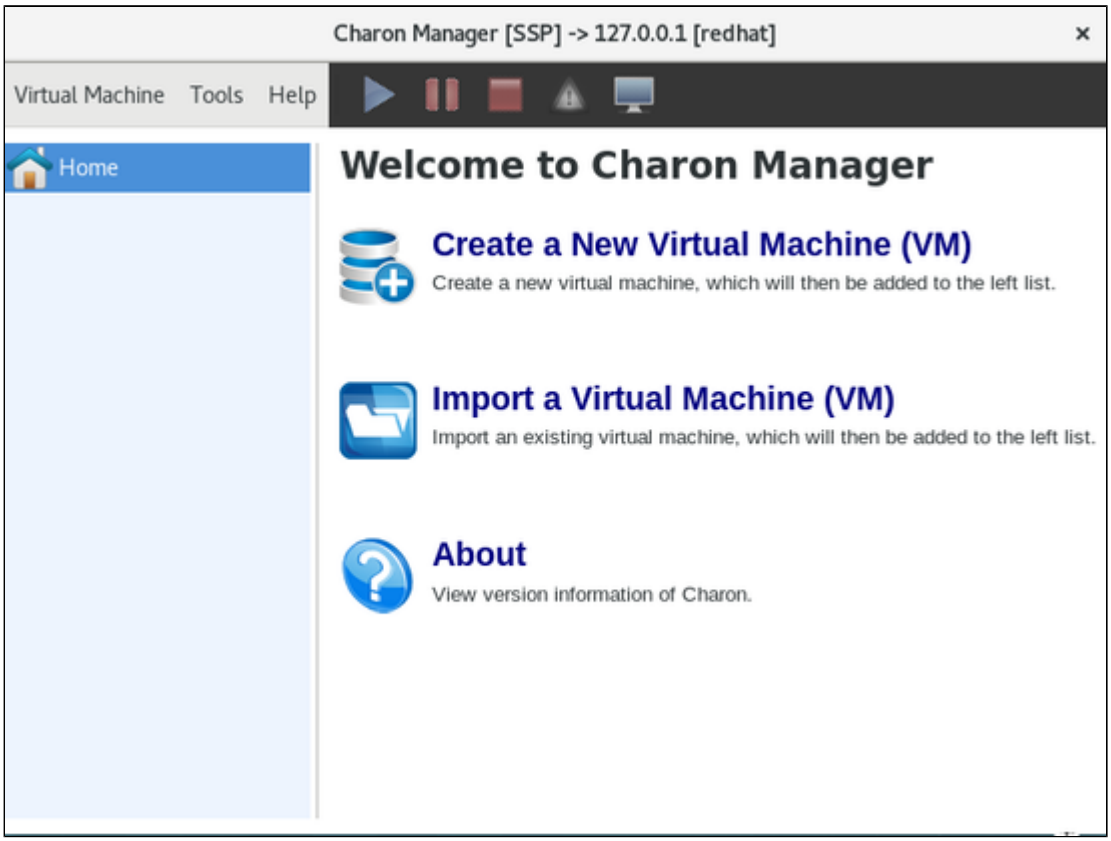
Step 3: connecting to the Charon host system

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. This management password is then valid for all subsequent logins by the same or a different user until it is changed again. It is not removed if Charon-SSP is reinstalled. Note that older versions of the product will not prompt for the password at first login but will use a default password (**stromasys**). If you need to reset a forgotten management password, please refer to the Charon-SSP user's guide.
- 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 VE License Server and Charon Emulator),
- security list of the subnet to which the instance belongs, and
- VNIC-specific Network Security Groups.

In addition to allowing SSH, the different firewall levels must be configured to permit the ports required by the VE license server.

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, the different firewall levels must be configured to permit the ports required by the VE license server.

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, the different firewall levels must be configured to permit the ports required by the VE license server.

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, the different firewall levels must be configured to permit the ports required by the VE license server.

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.

IBM Firewall Information

Access to an IBM cloud instance can be controlled by

- an external firewall,
- the operating system firewall of the instance,
- IBM-specific security groups, and
- IBM-specific subnet ACLs.

In addition to allowing SSH, the different firewall levels must be configured to permit the ports required by the VE license server.

IBM Cloud Security Groups

Security Groups are **associated with a virtual server instance**. They have the following characteristics:

- Stateful: once an inbound connection is permitted, return traffic is allowed.
- Only **allow** rules are possible.
- All rules are considered to determine if traffic should be permitted.
- An instance can have several security groups.

IBM Cloud Subnet ACLs

Subnet ACLs are **associated with subnets in a VPC**. They have the following characteristics:

- Stateless: inbound and outbound connections must be explicitly allowed.
- Allow and deny rules are possible.
- Rules are processed in sequence.
- One ACL can be assigned to several subnets.
- The default ACL allows all traffic.