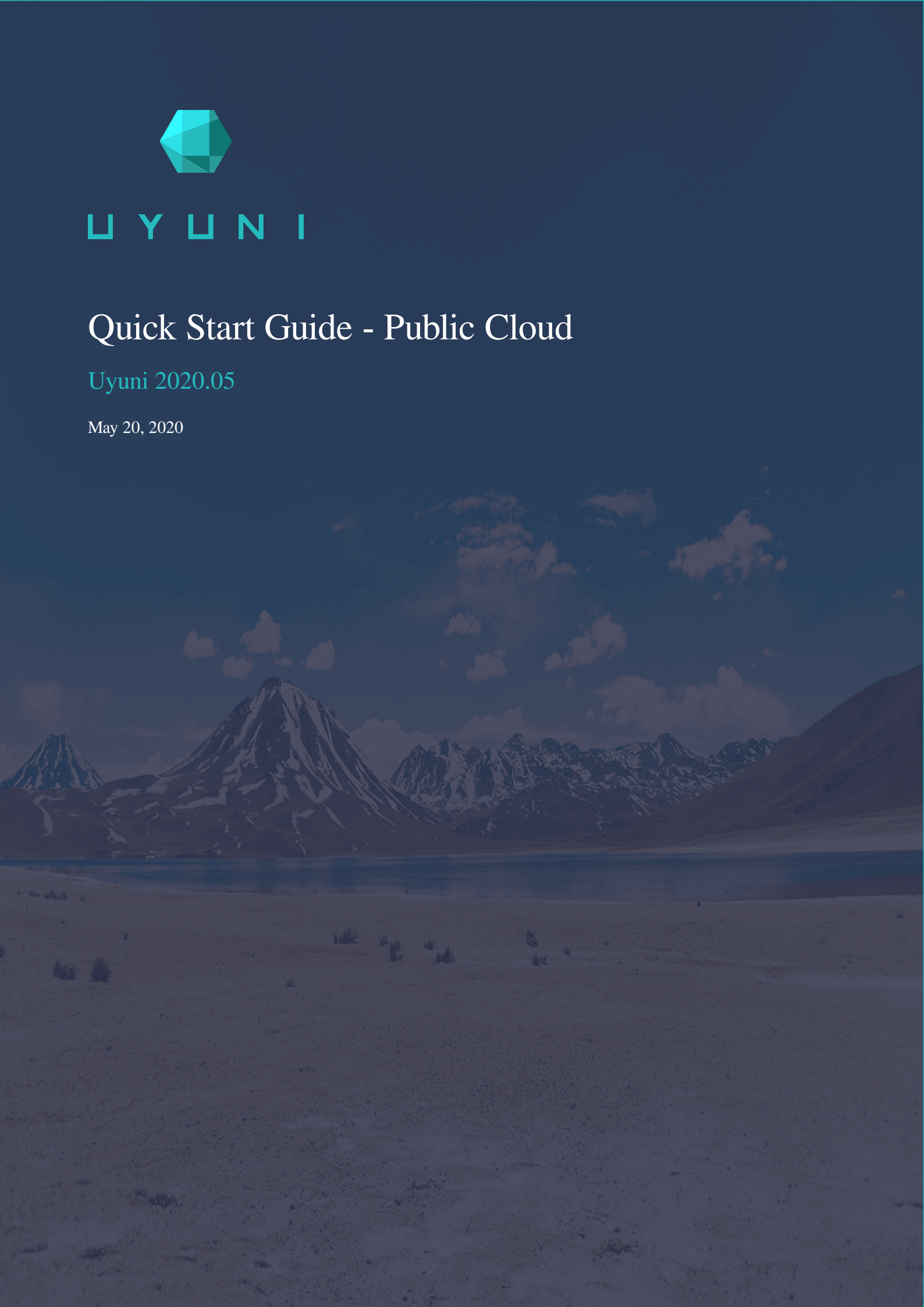

Quick Start Guide - Public Cloud

Uyuni 2020.05

May 20, 2020

Table of Contents

Introduction

Publication Date: 2020-05-20

This guide shows you the fastest way to get Uyuni up and running in a public cloud using on-demand or BYOS services. Additionally, it assumes that you are installing the Uyuni Server on a single cloud instance. It has been tested on Amazon Web Services, Microsoft Azure, and Google Cloud Engine.

For more information on using Uyuni, see the official Uyuni documentation at https://documentation.suse.com/suma.

Setting Up

We have tested these instructions on Amazon EC2, Google Compute Engine, and Microsoft Azure, but they should work on other providers as well, with some variation.

You need to start by logging in to your chosen public cloud provider, and launching a Uyuni instance.

Depending on the public cloud you are using, you can usually locate the Uyuni Server images by searching for `suse manager`. In EC2, you will need to search within the Community AMIs. In GCE and Azure, search the marketplace.

As you prepare your new instance, pay attention to these settings:

For hardware, select an instance with at least:

- 32 GB RAM
- 8 cores

For more information about hardware requirements, see **[Installation › Hardware-requirements ›]**.

For network security and access settings, you will need to enable HTTPS access. This allows you to access the Uyuni Web UI.

In EC2 and Azure, create a new security group, and add inbound and outbound rules for HTTPS. In GCE, check the `Allow HTTPS traffic` box under the `Firewall` section.

When running Uyuni on public clouds, make sure you apply security measures to limit access to the right people. A world-accessible Uyuni would give access to your infrastructure to anyone, and could breach your SUSE support agreement.

For storage settings, ensure the root volume of the Uyuni Server is 100 GB or larger. Add an additional storage disk of 500 GB or more, and choose SSD storage if you can. The cloud images for Uyuni Server use a script to assign this separate volume when your instance is launched. The name of the device node will vary depending on your provider, and the instance type you selected.

When you launch your instance, you can log in to the Uyuni Server and use this command to find all available storage devices:

```
hwinfo --disk | grep -E "Device File:"
```

If you are not sure which device to choose, use the `lsblk` command to see the name and size of each device. Choose the name that matches with the size of the virtual disk you are looking for.

You can set up the external disk with the `suma-storage` command. This creates an XFS partition mounted at `/manager_storage` and uses it as the location for the database and repositories:

```
/usr/bin/suma-storage <devicename>
```

For more information about setting up a public cloud instance, see **[Installation › Pubcloud-requirements ›]**.

Installation

Public clouds provide Uyuni under a Bring Your Own Subscription (BYOS) model. That means that they pre-install Uyuni, so you do not need to perform any installation steps. However, Uyuni Server needs to be registered with SUSE Customer Center to receive updates before you can sign in.

Follow the cloud providers instructions to SSH into the instance.

Run this command to start set up:

```
yast2 susemanager_setup
```

Follow the prompts, and wait for the setup to finish.

For detailed instructions on setting up Uyuni with YaST, see **[Installation › Server-setup ›]**.

Register your instance with SUSE Customer Center, using this command as root, specifying the registration number and the email address associated with it:

```
SUSEConnect -r <Registration_Number> -e <registered_email_address>
```

You can get your registration number by logging in to SUSE Customer Center from your browser.

For more information about registering Uyuni with SUSE Customer Center, see **[Installation › General-requirements ›]**.

When you have registered, all SUSE Linux Enterprise modules will be activated. You will also need to activate the Public Cloud module. Do this from the command prompt on your instance:

```
SUSEConnect -p sle-module-public-cloud/15.2/x86_64
```

For more information on activating public clouds, see **[Installation › Pubcloud-setup ›]**.

Open the Uyuni Web UI with a web browser, using an address like this:

```
https://<public_IP>
```

Sign in to the Uyuni Web UI with the administrator account. The username and password varies depending on your provider.

Table 1. Default Administrator Account Details

Provider	Default Username	Default Password
Amazon EC2	`admin`	`<instance-ID>`

Provider	Default Username	Default Password
Google Compute Engine	`admin`	`<instance-ID>`
Microsoft Azure	`admin`	`<instance-name>-suma`

When you sign in to the administrator account for the first time, you will have an automatically generated organization name. Change this by navigating to **Admin › Organizations**, and editing the organization name.

When you have signed in to the administrator account for the first time, change the default password to protect your account.

For more information about setting up your Uyuni Server, see **[Installation › Server-setup ›]**.

Use the Uyuni Web UI to add the required software products, and schedule a repository synchronization. The best way to do this is to navigate to **Admin › Setup Wizard** and follow the prompts.

For more information about the setup wizard, see **[Installation › Setup-wizard ›]**.

If you are intending to register Ubuntu or Red Hat Enterprise Linux clients, you will need to set up custom repositories and channels. For more information, see **[Client-configuration › Non-suse-clients ›]**.

To synchronize your channels, navigate to **Software › Manage › Channels**. Click each channel you created, navigate to the **Repositories › Sync** tab, and click **`[Sync Now]`**. You can also schedule synchronization from this screen.

Before bootstrapping a client, make sure all the selected channels for that product are synchronized.

Synchronization can sometimes take several hours, in particular for openSUSE, SLES ES and RHEL channels.

Content Lifecycle Management

Content lifecycle management allows you to customize repositories and test packages before updating production clients. This is especially useful if you need to apply updates during a limited maintenance window.

This is achieved through a series of environments that your software channels can move through on their lifecycle. Most environment lifecycles include at least test and production environments, but you can have as many environments as you require.

When you have created your project, defined environments, and attached sources and filters, you can build the project for the first time. For more information about content lifecycle management, see **[Administration › Content-lifecycle ›]**.

When your project is built successfully, you will need to add the new channel to an activation key. For more information about custom channels, see **[Administration › Custom-channels ›]**.

Procedure: Creating a Content Lifecycle Project

Go to **Content Lifecycle › Projects**, create a project and assign it a label and a name. Then use **`[Attach/Detach Sources]`** to attach a base channel and child channels, and finally save.

You can now **`[Attach/Detach Filters]`** to fine tune what packages will be included in the resulting channel. A number of filters are available: name, date, synopsis, reboot required or not, etc.

At this point you can define your environments by clicking **`[Add Environment]`** in the `Environment Lifecycle` dialog. Test and Production are usually the bare minimum most customers will have but you may need more. Continue creating environments until you have all the environments for your lifecycle completed.

The final step is building the project, which will take a little while.

For more information about content lifecycle management, including worked examples , see **[Administration › Content-lifecycle ›]**.

Register Clients

When you have your Uyuni Server set up, you are ready to start registering clients.

You can use Uyuni to manage clients using either the Salt stack or the traditional stack (inherited from Spacewalk). Most new features and enhancements are only available for Salt-managed clients, which makes this stack the preferred one. For more details, see **[Client-configuration › Supported-features ›]**

In the Uyuni Web UI, navigate to **Systems › Bootstrapping**, then fill in the `Host`, `SSH Port`, `User` and `Password` fields. Make sure you use stable FQDNs for the `Host` field, or Uyuni will not be able to find your host when your Public Cloud gives you a different short-lived FQDNS.

Public cloud images usually do not allow SSH login with username and password, but only SSH with a certificate. If you want to use bootstrap from the Web UI, you will need to enable SSH login with username and password. You can do this by navigating to **Systems › Bootstrapping** and changing the authentication method.

When the bootstrap process has completed successfully, your client will be listed at **Systems › System List**.

- If you want more control over the process, have to register many clients, or are registering traditional clients, we recommend that you create a bootstrap script. For more information, see **[Client-configuration › Registration-bootstrap ›]**.
- For Salt clients and even more control over the process, executing single commands on the command line can be useful. For more information, see **[Client-configuration › Registration-cli ›]**.

Activation Keys

Activation keys are used with traditional and Salt clients to ensure that your clients have the correct software entitlements, are connecting to the appropriate channels, and are subscribed to the relevant groups. Each activation key is bound to an organization, which you can set when you create the key.

Procedure: Creating an Activation Key

1. In the Uyuni Web UI, as an administrator, navigate to **Systems › Activation Keys**.
2. Click the **`[Create Key]`** button.
3. On the `Activation Key Details` page, in the `Description` field, enter a name for the activation key.
4. In the `Key` field, enter the distribution and service pack associated with the key. For example, `SLES12-SP4` for SUSE Linux Enterprise Server 12 SP4.

Do not use commas in the `Key` field for any SUSE products. However, you **must** use commas for Red Hat Products. For more information, see **[Reference › Systems ›]**.

5. In the `Base Channels` drop-down box, select the appropriate base software channel, and allow the relevant child channels to populate. For more information, see reference:admin/setup-wizard.pdf and **[Administration › Custom-channels ›]**.
6. Select the child channels you need (for example, the mandatory SUSE Manager tools and updates channels).
7. We recommend you leave the `Contact Method` set to `Default`.
8. We recommend you leave the `Universal Default` setting unchecked.
9. Click **`[Create Activation Key]`** to create the activation key.
10. Check the `Configuration File Deployment` check box to enable configuration management for this key, and click **`[Update Activation Key]`** to save this change.

The `Configuration File Deployment` check box does not appear until after you have created the activation key. Ensure you go back and check the box if you need to enable configuration management.

For more on activation keys, see **[Client-configuration › Clients-and-activation-keys ›]**.

System Set Manager

System Set Manager (SSM) is used to administrate groups of systems, rather than performing actions on one system at a time. It works for both Salt and traditional clients.

For a complete list of the tasks that you can perform with the SSM, see **[Reference › Systems ›]**.

You need to select which systems or system group you want to work with before you can use SSM to perform operations.

You can access SSM in three different ways:

- Navigate to **Systems › System List**, select systems you want to work with, and navigate to **Systems › System Set Manager**.
- Navigate to **Systems › System Groups**, and click **`[Use in SSM]`** for the system group you want to work with.
- Navigate to **Systems › System Groups**, select the group you want to work with, and click **`[Work with Group]`**.

For more on SSM, see **[Client-configuration › Using-ssm ›]**.