

# SUSE Studio Onsite

1.3

[www.suse.com](http://www.suse.com)

January 12, 2016

Deployment and Administration Guide



# Deployment and Administration Guide

Copyright © 2006–2016 SUSE LLC and contributors. All rights reserved.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or (at your option) version 1.3; with the Invariant Section being this copyright notice and license. A copy of the license version 1.2 is included in the section entitled “GNU Free Documentation License”.

For SUSE or Novell trademarks, see the Novell Trademark and Service Mark list <http://www.novell.com/company/legal/trademarks/tmlist.html>. All other third party trademarks are the property of their respective owners. A trademark symbol (®, ™ etc.) denotes a SUSE or Novell trademark; an asterisk (\*) denotes a third party trademark.

All information found in this book has been compiled with utmost attention to detail. However, this does not guarantee complete accuracy. Neither SUSE LLC, SUSE LINUX Products GmbH, the authors, nor the translators shall be held liable for possible errors or the consequences thereof.

The GPL requires that SUSE makes available certain source code that corresponds to the GPL-licensed material. The source code is available for download at <http://www.suse.com/download-linux/source-code.html>. Also, for up to three years from SUSE's distribution of the SUSE product, upon request SUSE will mail a copy of the source code. Requests should be sent by e-mail to [sle\\_source\\_request@suse.com](mailto:sle_source_request@suse.com) or as otherwise instructed at <http://www.suse.com/download-linux/source-code.html>. SUSE may charge a fee to recover its reasonable costs of distribution.

# Contents

<b>About this Guide</b>	<b>v</b>
1 Feedback .....	v
2 Documentation Conventions .....	vi
3 For More Information .....	vi
<b>1 Deploying and Installing</b>	<b>1</b>
1.1 System Requirements .....	2
1.2 Deploying SUSE Studio Onsite .....	3
1.3 Deploying z Runner on IBM System z .....	7
1.4 Setting up IBM System z Runner for SUSE Studio .....	8
1.5 Supporting Special Hardware .....	9
1.6 Configuring SUSE Studio Onsite .....	11
1.7 Customizing SUSE Studio Onsite .....	14
1.8 Using Templates After Maintenance Update .....	17
1.9 Keeping SUSE Studio Onsite Up-to-Date .....	18
1.10 Upgrading from SUSE Studio Onsite 1.1 to Version 1.2 .....	18
1.11 Upgrading from SUSE Studio Onsite 1.2 to Version 1.3 .....	19
<b>2 Administering SUSE Studio Servers</b>	<b>23</b>
2.1 Logging in to SUSE Studio Onsite .....	23
2.2 Inviting New Users .....	24
2.3 Managing Your Repositories .....	25
2.4 Building Images Using SMT Staging .....	26

2.5 Changing Repository Order .....	27
2.6 Managing Builds and Appliances .....	28
2.7 Adding New Cron Jobs .....	29
2.8 Setting Administrator E-Mail for Nagios .....	31
2.9 Setting the Read-Only Mode .....	32
2.10 Allowing Outgoing TCP Connections in Testdrive .....	32
2.11 Extending Disk Storage .....	32
2.12 Enabling OVF Format .....	33
2.13 Changing Maximum Number of Slots .....	33
2.14 Setting Up a Secure Web Server with SSL .....	34
<b>3 Monitoring SUSE Studio Onsite Servers</b>	<b>41</b>
3.1 Viewing Build Statistics .....	41
3.2 Getting Diary Information .....	42
3.3 Monitor SUSE Studio Onsite with Nagios and Munin .....	43
<b>A SUSE Studio Onsite Services</b>	<b>45</b>
<b>B Administration Panel—Menu Structure</b>	<b>47</b>
B.1 Dashboard .....	47
B.2 Diary .....	47
B.3 Advanced .....	47
<b>C Troubleshooting</b>	<b>51</b>

# About this Guide

SUSE Studio™ Onsite is a Web application for building and testing appliances in a Web browser. It supports the creation of virtual appliances and live systems based on SUSE Linux operating systems. The publicly hosted version is available at <http://susestudio.com>.

This manual introduces the administrative part of SUSE Studio. It shows you how to deploy, configure, monitor and administer your SUSE Studio Onsite server. Most of the options mentioned in this manual are accessible after clicking on your login name (or the *Admin User* link if you have administrator's privileges) in the main navigation.

For an overview of the documentation available for your product and the latest documentation updates, refer to [http://www.suse.com/documentation/suse\\_studio/](http://www.suse.com/documentation/suse_studio/).

## 1 Feedback

Several feedback channels are available:

### Bugs and Enhancement Requests

For services and support options available for your product, refer to <http://www.suse.com/support/>.

To report bugs for a product component, log into the Novell Customer Center from <http://www.suse.com/support/> and select *My Support > Service Request*.

### User Comments

We want to hear your comments about and suggestions for this manual and the other documentation included with this product. Use the User Comments feature at the bottom of each page in the online documentation or go to <http://www.suse.com/documentation/feedback.html> and enter your comments there.

## Mail

For feedback on the documentation of this product, you can also send a mail to `doc-team@suse.de`. Make sure to include the document title, the product version and the publication date of the documentation. To report errors or suggest enhancements, provide a concise description of the problem and refer to the respective section number and page (or URL).

# 2 Documentation Conventions

The following typographical conventions are used in this manual:

- `/etc/passwd`: directory names and filenames
- *placeholder*: replace *placeholder* with the actual value
- `PATH`: the environment variable `PATH`
- `ls, --help`: commands, options, and parameters
- `user`: users or groups
- `Alt, Alt + F1`: a key to press or a key combination; keys are shown in uppercase as on a keyboard
- *File, File > Save As*: menu items, buttons
- **#amd64 em64t**: This paragraph is only relevant for the specified architectures. The arrows mark the beginning and the end of the text block. ◀
- *Dancing Penguins* (Chapter *Penguins*, ↑Another Manual): This is a reference to a chapter in another manual.

# 3 For More Information

Additional information about SUSE Studio can be found here:

<https://www.suse.com/partners/integrated-systems/>

Information about appliances and the SUSE Appliance Program.

[http://en.opensuse.org/Portal:SUSE\\_Studio](http://en.opensuse.org/Portal:SUSE_Studio)

The portal site about SUSE Studio with a tour, HowTos, and information for developers.





# Deploying and Installing

To deploy SUSE Studio Onsite, install it on your server and proceed with the installation in a Web browser. This chapter provides a step-by-step instruction to successfully complete deployment and installation of SUSE Studio Onsite on your designated server.

SUSE Studio Onsite is delivered in two variants, a compressed raw image and a CD. The raw image is a bitwise copy of a complete hard disk and contains a full Linux operating system including a boot sector and partition information. The CD is bootable and deploys the SUSE Studio Onsite image.

---

## **WARNING: Erasing Your Disk**

Installing SUSE Studio Onsite will erase your disk *completely*. If you have any important data on this disk, make a backup before you proceed.

---

## **WARNING: Unencrypted Ports Are Open**

Deploy SUSE Studio Onsite only on an isolated network (DMZ). Do not connect it to any other internal network. If you want to deploy SUSE Studio Onsite in an internal network, make sure it is not accessible *from* the Internet. Access from SUSE Studio Onsite *to* the Internet should be allowed.

---

# 1.1 System Requirements

Before you install SUSE Studio Onsite on your server, boot a Live CD and check if your machine fulfills the following system requirements:

## CPU: 64-Bit and Virtualization Support

The CPU must support 64-bit and full virtualization. Check if your CPU supports 64-bit by executing the following command:

```
grep lm /proc/cpuinfo
```

The `grep` command will only provide output if the processor supports long mode, indicated by the `lm` flag. If the `grep` command returns no output, your selected system only supports 32-bit addressing and does not meet the SUSE Studio Onsite requirements.

Virtualization support is needed for building appliances and using the test drive. Test the capabilities of your CPU by executing the following command in the text console or shell (the `vmx` flag is used by Intel, `svm` by AMD):

```
egrep '(vmx|svm)' /proc/cpuinfo
```

If there is no output from the `egrep` command, your processor does not support full virtualization or the feature has been disabled in the BIOS. Enable the setting in your BIOS and try again. Depending on your BIOS the entry can be named differently: *Virtualization Technology*, *VT* or something similar. Consult your main-board manual.

## RAM

A minimum of 8 GB of RAM should be installed on the server machine. RAM in addition to the 8 GB minimum is recommended. SUSE Studio Onsite requires 2 GB of RAM for the user interface, 4 GB of RAM for each logged in appliance creator and KIWI slot, and 2 GB of RAM for the test drive slot.

## Free Disk Space

The available disk space on the server should at least be 100 GB. Additional disk space is recommended. The following table provides an overview of the size requirements for ISO based repositories for the various distributions (only binary, no source or updates):

**Table 1.1:** *Minimal Amount of Disk Space for Different Products (Approximate Values)*

Product	Size
SLES 10	~6 GB
SLED 10	~11 GB
SDK 10	~8 GB
SLES 11	~7 GB
SLED 11	~10 GB
SDK 11	~8 GB
openSUSE 12.1 DVD	~4.2 GB
openSUSE 12.2 DVD	~4.2 GB

## 1.2 Deploying SUSE Studio Onsite

The following sections describe two methods for the installation of SUSE Studio Onsite: using the installation from the installation CD and the raw disk image. Using the raw image requires network access and a second machine on your network to store the raw image.

---

### **TIP: Additional Information**

Additional information for the administration is contained in the file `/srv/studio/README.onsite_user` after the installation is completed. The Release Notes contain important information regarding SUSE Studio Onsite as well as updates not reflected in this manual.

---

---

**NOTE: Always Complete Setup Before Installing Maintenance Updates**

Complete the setup first before you install any maintenance updates of SUSE Studio. If you do it the other way around and run into problems, our support asks you to install and set up your SUSE Studio server again before we look into the details of your problem.

---

## 1.2.1 Installing from CD

To start the installation process, proceed as follows:

**Procedure 1.1:** *Deploying a Raw Image from CD*

- 1 Boot your future SUSE Studio Onsite server with the installation CD. Select *Install/Restore SUSE Studio Onsite*.
- 2 Answer the question *This will destroy ALL data on /dev/sda, continue?* with *Yes* to proceed. The deployment process is taking over.
- 3 Remove the CD and reboot your server. The boot loader GRUB is started and the firstboot system takes over.

This completes the installation of SUSE Studio Onsite using the install CD. Proceed with Section 1.6, “Configuring SUSE Studio Onsite” (page 11).

## 1.2.2 Installing Over a Network

This method is useful if your server does not have a CD/DVD drive or you prefer installation over a network. You need two machines which are connected to your network: the first machine contains the raw image, the second machine is your future SUSE Studio Onsite server.

---

**NOTE: Only eth0 Connects to Your Network**

If you have a server with two network cards (`eth0` and `eth1`), only `eth0` is able to connect to your network. Currently, this is a limitation in version 1.3. Make sure your cable is always connected to the `eth0` port.

---

Installing over a network usually takes these steps:

- 1 Procedure 1.2, “Preparing Your Future SUSE Studio Onsite Server” (page 5).
- 2 Procedure 1.3, “Decompressing the Image on the Client” (page 5)
- 3 Procedure 1.4, “Deploying the Raw Image” (page 6)

**Procedure 1.2:** *Preparing Your Future SUSE Studio Onsite Server*

- 1 Boot your future SUSE Studio Onsite server with a rescue system. Such systems are available on all SUSE installation CDs or DVDs. Alternatively boot from a Live CD.
- 2 Log in as `root`. A password is not needed.
- 3 If the network in the rescue image has not been configured automatically via DHCP, it must be configured. Check for an IP address with the following command:

```
ifconfig
```

If you only get one item with an 127.0.0.1 address, you must configure your network. To configure a DHCP-based network setup use:

```
ifup-dhcp eth0
```

Remember the IP address of your system, it is needed later.

- 4 Set up a listener on an unused port (in our example, 1234) and dump the incoming data to the system disk. Generally, this is the first hard drive, in our example /dev/sda. This will destroy any data on this disk! To use the example parameters enter the following command:

```
netcat -l -v -p1234 | dd of=/dev/sda
```

- 5 Make sure you do not clean the screen as you need the output of the last step to compare it with the output of another command later.

**Procedure 1.3:** *Decompressing the Image on the Client*

- 1 Check the file type of your image with `file IMAGENAME:`
  - If you get the following output (as one line), skip this procedure and proceed with Procedure 1.4, “Deploying the Raw Image” (page 6):

```
...raw: x86 boot sector; GRand Unified Bootloader,  
stage1 version 0x3, stage2 address 0x2000, stage2 segment 0x200,
```

```
GRUB version 0.97; partition 1: ID=0x83, active, starthead 1,
startsector 63, 4192902 sectors
```

- If you get one of the following outputs, your raw image is compressed:

```
gzip compressed data, extra field, from Unix, last modified: ...
```

or

```
bzip2 compressed data, block size = 900k
```

## 2 Decompress the raw image with one of the following commands, depending on the file extension of the image:

- For an image compressed with `gzip` (file extension `.gz`), use:

```
gunzip IMAGENAME
```

- For an image compressed with `bzip2` (file extension `.bz2`), use:

```
bunzip2 IMAGENAME
```

- For an image compressed with `tar` and `gzip` (file extension `.tar.gz`), use:

```
tar xzvf IMAGENAME
```

At the end of decompression you will have a raw image with the `.raw` extension.

### **Procedure 1.4:** *Deploying the Raw Image*

- 1 Send the raw image to the machine designated as the SUSE Studio Onsite server using the following command. Replace the `RAW_IMAGE` with the path to your image and `IP_of_Client` with the IP address from Step 3 (page 5) of Procedure 1.2:

```
dd if=RAW_IMAGE | netcat IP_of_Client 1234
```

- 2 Compare the output from the last step with the output from Step 5 (page 5) of Procedure 1.2. The following shows an example of the output:

```
2625536+0 records in
2625536+0 records out
1344274432 bytes (1.3 GB) copied, 113.989 s, 11.8 MB/s
```

The time (113.989 s), the throughput (11.8 MB/s), the number of records (2625536+0), and the total size (1.3 GB) may be different in your case. However, the `records in` and `records out` as well as the size must match between the two machines. If you see any discrepancies, repeat the previous steps.

- 3 Reboot the server and remove the rescue medium from your CD or DVD drive. The boot loader GRUB is started and the firstboot system takes over.

This completes the deployment of SUSE Studio Onsite using the raw disk image. Proceed with Section 1.6, “Configuring SUSE Studio Onsite” (page 11).

## 1.3 Deploying z Runner on IBM System z

From version 1.2, SUSE Studio supports deploying z Runner on IBM System z. Make sure you fulfill all the following prerequisites:

- SUSE Linux Enterprise Server11 SP1 for System z
- Your IBM System z server is registered and contains the update repository URL in YaST (needed to get the latest Kernel update, for example.)
- A rebooted system after the installation
- Minimum of 3 GB RAM
- Minimum of 6 GB disk space
- The downloaded runner add-on for System z on a System z instance
- It is recommended to use the LPAR mode for performance reasons as hardware resources are divided into “logical partitions”.

To install the SUSE Studio add-on product on IBM System z, proceed as follows:

- 1 Prepare your IBM System z machine:
  - 1a Reboot the runner
  - 1b After the reboot, run `yast2 add-on`
  - 1c Select *Add* and go to *Local ISO image....*
  - 1d Select the add-on image for System z and accept the End User License Agreement (EULA). The software selection dialog appears.

- 1e** Register your System z add-on.
- 2** Select the filter *SUSE Studio Upgrade for System z* for the add-on repository.
- 3** Select all packages in that repository.
- 4** Choose *Install* and accept the suggestion.
- 5** Finish with *Ok* to close the YaST module.

Your System z runner is successfully installed.

## 1.4 Setting up IBM System z Runner for SUSE Studio

This section describes how to install a z Runner dedicated for building appliances for IBM's System z. It is assumed you have successfully set up your system as described in Section 1.3, “Deploying z Runner on IBM System z” (page 7).

To create an IBM System z runner, proceed as follows:

- 1** Log in to your SUSE Studio Onsite server.
- 2** Click the *Admin User* and *Advanced* links.
- 3** Click the *Extension for System z* link.
- 4** Enter the hostname or IP address of your previously configured System z runner. SUSE Studio requests all relevant information from the System z runner and creates a `/studio/filestore` directory. This directory will be made available to the System z runner host.
- 5** Wait until all the System z repositories and templates are added. This step is run automatically after the runner setup and takes some time.
- 6** Use an NFS share from SUSE Studio server on your IBM System z runner. This step is done automatically.

Your IBM System z is now correctly configured.



If you want to disable the System z template, proceed as follows:

- 1 Log in to your SUSE Studio Onsite server.
- 2 Click the *Admin User* and *Advanced* links.
- 3 Choose *Repositories > Software*.
- 4 Click the *Hide* button on the SLES11\_SP1 System z template.

If a users want to create a new appliance, it will not be shown in the list of available templates. To enable the template again, click the *Show* button.

## 1.5 Supporting Special Hardware

In almost all cases, the installation as described in Section 1.2, “Deploying SUSE Studio Onsite” (page 3) is sufficient and you can skip this section. However, special hardware may not be supported directly by SUSE Studio, for example, the driver cannot be included for legal reasons. In such case you need to integrate a third-party driver into your appliance using KIWI.

In order to repair the faulty driver you need to understand KIWI's build process. More details of KIWI's build process can be found in the PDF file under `/usr/share/doc/packages/kiwi/kiwi.pdf`, package `kiwi-doc`. The following procedure gives you a general overview on how to do this:

- 1 Install the image description for KIWI where you locate the faulty driver. For example, `kiwi-desc-oemboot` if you want to build an OEM images with a special driver.
- 2 Get to know the path of the image description and the product name, and locate the config file. In our example, KIWI's OEM image description is installed under `/usr/share/kiwi/image/oemboot/`. If you want to change that for SUSE Linux Enterprise Server 11, add `suse-SLES11` to the previous path. The full path yields `/usr/share/kiwi/image/oemboot/suse-SLES11`.
- 3 Insert the missing driver in the configuration file. Depending on the driver, you have several options:
  - If your driver is part of the standard Kernel, extend the `drivers` section as described in Step 4 (page 10).

- If your driver is *not* part of the standard Kernel, build a KMP package of your driver as described in [http://developer.novell.com/wiki/index.php/Creating\\_a\\_Kernel\\_Module\\_Package\\_%28KMP%29](http://developer.novell.com/wiki/index.php/Creating_a_Kernel_Module_Package_%28KMP%29). Insert the following highlighted line in the `packages` section:

```
<packages type="image">
  <package name="..."/>
  <package name="YOUR_KMP_PACKAGE"/>
</packages>
```

Additionally create a repository for your driver RPM. Usually this is an ordinary directory for KIWI. Edit the file `/usr/share/kiwi/image/oemboot/suse-SLE11/config.xml` and insert:

```
<repository type="rpm-dir">
  <source path="/path/to/your/repo"/></>
</repository>
```

- If your driver is *not* part of the standard Kernel and you do not want to create a KMP package, the only option is to copy your binary driver into the overlay tree of the boot image description. The overlay tree is the directory in the image description, in our case `/usr/share/kiwi/image/oemboot/suse-SLES11/root/`. The overlay tree contains all the overlay files which you have changed or added. Note that binary drivers in the overlay tree are hard to maintain as the module has to match with the Kernel version. Use this method only as your last option.

- 4 Extend the `drivers` section as indicated with the highlighted line. Replace the dots with the corresponding driver name (extension `.ko`):

```
<drivers type="drivers">
  <file name="..."/>
  <file name="drivers/..."/>
</drivers>
```

One additional note for KIWI users: KIWI tries to make the `initrd` as small as possible. As such, it removes everything which is not specified in the `drivers` section.

- 5 Create a new boot image with the following commands and replace `URL` with the repository URL:

```
kiwi -p /usr/share/kiwi/image/oemboot/suse-SLES11 \
  --root /tmp/fixed-oemboot --set-repo URL

kiwi --create /tmp/fixed-oemboot -d /tmp/myfixed-oemboot
```

**6** Copy the `initrd` and the Kernel file on a USB stick (usually mounted as `/media/disk`). Name them `initrd.kexec` and `linux.kexec`:

```
cp /tmp/myfixed-oemboot/kernel /media/disk/linux.kexec
cp /tmp/myfixed-oemboot/initrd /media/disk/initrd.kexec
```

The stick can only contain these two files.

**7** Boot the media with the Kernel option `hotfix=1`.

If there is a reboot during deployment, pass `hotfix=1` again. Usually this is not necessary for normal installation.

## 1.6 Configuring SUSE Studio Onsite

It is assumed you successfully completed one of the two installation methods in Section 1.2, “Deploying SUSE Studio Onsite” (page 3).

---

### **NOTE: Setting Secure SUSE Studio Administrator Password**

The SUSE Studio administrator password will become the `root` password automatically during system setup. For this reason, do *not* change the `root` password in a shell by yourself! The `root` password will be changed and synced during the configuration of SUSE Studio. If you have already changed the password, change it back to `linux`.

Up to this point your system root account is protected by the default password only. Therefore your system might get compromised over the network using SSH. As such, always install and configure your SUSE Studio Onsite server during one step.

For more information how to set up a secure Web server, refer to Section 2.14, “Setting Up a Secure Web Server with SSL” (page 34).

---

### **NOTE: Network Setup Without DHCP Server**

If you do not have a DHCP server on your network, you need to change the network setup after the image has been written to the disk. Proceed as described in Step 3 (page 12) of Procedure 1.5 (page 12).

---

Proceed as follows to configure SUSE Studio Onsite:

**Procedure 1.5:** *Configuring SUSE Studio Onsite*

- 1 During the boot process, press the Esc key to enter verbose boot mode.
- 2 Follow the boot messages and assure that one of the following messages is displayed:

```
Loading KVM for intel
```

or:

```
Loading KVM for amd
```

If you receive an error message check Section 1.1, “System Requirements” (page 2).

- 3 If you need to change your network parameters, log in as `root` (with password `linux`). The password is changed later in Step 5 of Procedure 1.6. Run `yast network` and select *Network Card*. There configure your network according to your needs. Find more information in the section *Configuring a Network Connection with YaST* under [http://www.suse.com/documentation/sles11/book\\_sle\\_admin/data/sec\\_basicnet\\_yast.html](http://www.suse.com/documentation/sles11/book_sle_admin/data/sec_basicnet_yast.html).

If you want to customize more than the network, use YaST to configure additional settings of your SUSE Studio Onsite server.

Proceed with the configuration of SUSE Studio Onsite using a Web browser as described in Procedure 1.6.

**Procedure 1.6:** *Configuring Your SUSE Studio Onsite Server*

- 1 Start a browser on a *different* machine and point the browser to your SUSE Studio Onsite instance. In our example it is `https://192.168.1.1`.
- 2 Accept the license agreement.
- 3 Register your SUSE Studio server with SMT or with the Novell Customer Center. The registration process is needed to get the necessary repositories in order to update SUSE Studio Onsite and to provide packages for all the images in the build step. Either way, without a successful registration you cannot proceed and SUSE

Studio Onsite will not work. Choose the registration with SMT or Novell Customer Center:

---

**NOTE: Licenses and Expiring**

If an evaluation license expires, SUSE Studio will no longer work. If a full license expires, each user will see a red message on every page telling that the license has expired. In such case, SUSE Studio will still be functional. The administrator will see a message on his home screen two months before the license eventually expires.

---

- If you have an SMT server (Subscription Management Tool), click *Use SMT* and enter the server hostname (without the protocol) to continue. The SMT server has to be configured according to this article: <https://www.novell.com/support/kb/doc.php?id=7006024>. Optionally enter the IP Address of the server as Subject Alternative Name. This ensures that clients can connect to the server via an IP address.
  - If you do not have an SMT server, register your product in the Novell Customer Center. Enter the following data to complete the registration procedure:
    - your e-mail address that you have used for registration in the Novell Customer Center,
    - your SUSE Studio registration code.
- 4** If you have used the Novell Customer Center for registration, enter username and password for your mirror credentials from the Novell Customer Center. Get your credentials from the link aside.
- 5** Create the administrator account and enter the login name, password and e-mail address. Finish with *Continue*.

Your password will now be synchronized with your SUSE Studio Onsite server's `root` password.

- 6** If you want to enable *Lightweight Directory Access Protocol* (LDAP) do the following:
- 6a** Edit the file `/srv/studio/ui-server/config/initializers/omniauth.rb` and set the variables to your LDAP server settings.

**6b** Set `ldap_authentication` to `true` in `/srv/studio/options.yml` (see Section 1.7.1, “The SUSE Studio Onsite Configuration File” (page 14).)

**6c** Restart the Apache Web server:

```
rcapache2 restart
```

**6d** Specify LDAP user credentials. The credentials will provide this user with administrator permissions for SUSE Studio.

The previous procedure completes the setup of SUSE Studio Onsite. Prior to building your first appliance you will need to wait a few minutes to let the server initialize all the repositories and complete automated setup tasks.

## 1.7 Customizing SUSE Studio Onsite

This section introduces the SUSE Studio Onsite configuration file and two system and network monitoring tools that are part of the standard installation.

### 1.7.1 The SUSE Studio Onsite Configuration File

The file `/srv/studio/options.yml` serves as the SUSE Studio Onsite configuration file. Certain aspects of the SUSE Studio Onsite application behavior can be controlled with the settings in this file, for example, restricting access to users or setting feedback options, repository notifications, or announcements.

Remove or disable any options you do not need. After modifying your configuration, restart the Apache Web server to apply your changes with the `rcapache2 restart` command.

---

## NOTE: Avoiding Syntax Errors

When modifying your configuration file, do not change the indentation and leave one or more spaces after the colon contained in each option. Find more information about the syntax at <http://www.yaml.org>.

---

### Example 1.1: Central Configuration File `/srv/studio/options.yml`

```
default:
  ### Invitation mode settings
  #invitation_required: true      # default: true ❶
  #invitation_expires: false     # default: false ❷
  #invitation_from: "studio@example.com" ❸

  ### Email Settings ❹
  #feedback_to:
  #feedback_to_name: 'The SUSE Studio Team'
  #feedback_from: '"SUSE Studio Feedback" <feedback@example.com>'

  ### Notification Settings ❺
  #repo_added_default_and_fallback_from: 'studio-status@example.com'
  #repo_added_to:
  #repo_added_host: 'studio.example.com'

  ### Announcement Settings ❻
  #announcement_enabled: false
  #announcement_message:

  ### Authentication method
  #ldap_authentication: false ❼
```

- ❶ As SUSE Studio Onsite administrator you can either choose to let users apply for accounts on the SUSE Studio Onsite login screen or you can restrict the access to certain users. For more information, refer to Section 2.2, “Inviting New Users” (page 24).

If this option is set to `true`, only the administrator can invite users. However, users can request an account by entering their e-mail address on the SUSE Studio Onsite login screen. After the administrator has approved the request, users will receive an e-mail invitation to activate the requested account.

Setting this option to `false` everybody can create an account by themselves.

- ❷ Setting this option to `true` causes invitations to expire one week after the invitation has been mailed to the user. If the user does not accept the invitation within one week, a new invitation must be issued.
- ❸ Specifies the e-mail address that is used as return address for invitation e-mails.
- ❹ Configure the feedback feature of SUSE Studio Onsite with `feedback_to`, `feedback_to_name`, and `feedback_from`. If all keywords are enabled, users will see a *Send Feedback* link on the left pane when creating appliances. Clicking the link will display a text field in the interface, allowing the user to enter feedback comments. Once a user clicks *Send feedback*, an e-mail will be sent to the address specified in the `feedback_to` option. As the return address of the e-mail the value of the `feedback_from` option will be used.
- ❺ Use the `Notification Settings` to enable a notification e-mail when SUSE Studio gets a repository for the first time. Set `repo_added_host` to the hostname of your SUSE Studio Onsite server. This will ensure that all generated URLs in the notification e-mails are correct. Set the recipient of the notification e-mail with the `repos_added_to` option.
- ❻ Setting these options allows you to display messages on the SUSE Studio Onsite login screen.
- ❼ Enables or disables the LDAP authentication method for SUSE Studio Onsite. For more information, see Step 6 (page 13) in Procedure 1.6, “Configuring Your SUSE Studio Onsite Server” (page 12).

## 1.7.2 Setting Administrator Passwords for Nagios and Munin

Nagios and Munin are network monitoring tools (see Section 3.3, “Monitor SUSE Studio Onsite with Nagios and Munin” (page 43) for more details). It is recommended to set administrator passwords for both Nagios and Munin in case you need to configure these tools later. Both services can be accessed through a Web interface with the passwords set in the following procedure:

### **Procedure 1.7:** *Setting Login Name and Passwords for Nagios and Munin*

- 1 Set the Nagios password with:

```
htpasswd2 -c /etc/nagios/htpasswd.users nagiosadmin
```

- 2 Set the Munin password with:

```
htpasswd2 -c /etc/munin/htpasswd.users admin
```



**3** Authenticate with the above usernames and passwords as follows (replace 192.168.1.1 with the IP address of your server):

**3a** Start a Web browser and login into Nagios with the URL  
`http://192.168.1.1/nagios/index.html`.

By default, Nagios starts and monitors some services automatically. Refer to Appendix A, *SUSE Studio Onsite Services* (page 45) to get an overview of these services.

**3b** Open another window in your Web browser and log in to Munin here  
`http://192.168.1.1/munin/index.html`.

In general it is sufficient to use the default configuration of Nagios and Munin to monitor the SUSE Studio Onsite server. For custom configuration of the services refer to the Nagios and Munin documentation.

## 1.7.3 Setting Up Email Server

By default, SUSE Studio Onsite uses a local Postfix server for sending mail. If you need a different mail server, open the file `/srv/studio/ui-server/config/environments/production.rb` and insert a `config.action_mailer.smtp_settings` configuration as described in [http://guides.rubyonrails.org/action\\_mailer\\_basics.html#action-mailer-configuration](http://guides.rubyonrails.org/action_mailer_basics.html#action-mailer-configuration). For example, the following code uses the domain `www.example.com`:

```
config.action_mailer.smtp_settings = {
  :address => 'smtp.yourmailserver.com',
  :domain  => 'www.example.com',
  :port    => 80,
  :user_name => 'johndoe@example.com',
  :password => 'yourpassword',
  :authentication => :plain
}
```

## 1.8 Using Templates After Maintenance Update

Templates are an important part of SUSE Studio Onsite: a template determines which operating system your appliance is based upon. After a maintenance update, new

repositories with additional templates may be available. Go to *Advance > Repositories > Templates* and click *Import* to make them available.

If you use SMT, the repositories need to be located on the SMT server. SUSE Studio Onsite shows corresponding error messages on activating the template in case the repositories are not at the expected location.

## 1.9 Keeping SUSE Studio Onsite Up-to-Date

If you previously registered SUSE Studio Onsite with the Novell Customer Center as described in Section 1.6, “Configuring SUSE Studio Onsite” (page 11), this registration enables the system to check for updates relating to bug fixes, improvements, and security fixes. Apply available updates with `zypper` by executing:

```
zypper patch
```

Find more information about `zypper` at [http://www.suse.com/documentation/sles11/book\\_sle\\_admin/?page=/documentation/sles11/book\\_sle\\_admin/data/sec\\_zypper.html](http://www.suse.com/documentation/sles11/book_sle_admin/?page=/documentation/sles11/book_sle_admin/data/sec_zypper.html).

## 1.10 Upgrading from SUSE Studio Onsite 1.1 to Version 1.2

---

### **NOTE: Upgrading from SUSE Studio 1.0**

The direct upgrade from version 1.0 to version 1.2 is not possible. Upgrade to version 1.1 first.

---

To upgrade your SUSE Studio Onsite server from version 1.1 to version 1.2, the upgrade process has to be done in the following order:

- 1 Log in to your SUSE Studio Onsite server 1.1 as `root`.
- 2 Do a maintenance update.

- 3 Check if you have enough disk space. It is recommended that at least 50% of the disk space is available.
- 4 Run the `export_from_onsite11.sh` script. This script is part of the maintenance update. Replace the `PATH` placeholder where you want to store the resulting tar archives:

```
/srv/studio/scripts/export_from_onsite11.sh PATH
```

The script stops the services (RMDS, Thoth, Apache), packs the `/studio` directory, and creates a database dump. After running this script, you will get the file `studio_export-1.1.tar.gz`.

- 5 Save the archive from Step 4 (page 19) on an external storage device.
- 6 Deploy version 1.2 on a different server as described in Section 1.2, “Deploying SUSE Studio Onsite” (page 3). **Do NOT run the setup wizard yet!**
- 7 Log in to your SUSE Studio Onsite server 1.2 as `root`.
- 8 Run the `import_to_onsite12.sh` script and insert the directory where the tar archive from Step 5 (page 19) are stored, for example:

```
/srv/studio/scripts/import_to_onsite12.sh /media/studio-backup
```

The script migrates database dumps and populates the database with the old values.

## 1.11 Upgrading from SUSE Studio Onsite 1.2 to Version 1.3

Before you upgrade your SUSE Studio Onsite server from version 1.2 to version 1.3, check first the available disk space. Make sure you have at least double the size of your data.

---

### **IMPORTANT: Change Root Password After Upgrade**

After the upgrade process is finished, the root password contains the default password. However, before you let others access your server, make sure it is changed to something more secure to avoid any security problems. After you

have successfully logged in into your SUSE Studio server, change it to a secure password by using the `passwd` command.

---

Proceed with the upgrade process in the following order:

- 1 Log in to your SUSE Studio Onsite server 1.2 as `root`.
- 2 Do a maintenance update.
- 3 Check if you have enough disk space. It is recommended that at least 50% of the disk space is available.
- 4 Run the `export_from_onsite12` script. This script is part of the maintenance update. Replace the `TAR_ARCHIVE` placeholder where the resulting tar archives will be stored:

```
/srv/studio/scripts/export_from_onsite12 TAR_ARCHIVE
```

The script stops the services, packs the `/studio` directory, and creates a database dump. After running this script, the result will be stored in `TAR_ARCHIVE`.

- 5 Save the archive from Step 4 (page 20) on an external storage device.
- 6 Deploy version 1.3 on a different server as described in Section 1.2, “Deploying SUSE Studio Onsite” (page 3). **Do NOT run the setup wizard yet!**
- 7 Log in to your SUSE Studio Onsite server 1.3 as `root`.
- 8 Run the following commands to import the tar archive from Step 5 (page 20):

```
cd /srv/studio/scripts  
bundle19 exec ./import_to_onsite13 TAR_ARCHIVE
```

Furthermore, check if the following repositories are available. These are needed to show the *Upgrade* notification on the start page. Note, these repositories are only applicable for 32 bit machines. If you have 64 bit machines, replace the `i386` part with `x86_64`.

### ***SLES Appliances***

- SLES 11 SP1 i386
- SLES 11 SP1 Updates i386

- SLE 11 SP1 SDK i386
- SLE 11 SP1 SDK Updates i386
- SLES 11 SP2 i386
- SLES 11 SP2 Updates i386
- SLE 11 SP2 SDK i386
- SLE 11 SP2 SDK Updates i386

### ***SLED Appliances***

- SLED 11 SP1 i386
- SLED 11 SP1 Updates i386
- SLE 11 SP1 SDK i386
- SLE 11 SP1 SDK Updates i386
- SLED 11 SP2 i386
- SLED 11 SP2 Updates i386
- SLE 11 SP2 SDK i386
- SLE 11 SP2 SDK Updates i386

In case you have cloned and “frozen” your image, you need to migrate your frozen repositories too. Use the `migrate_frozen_repositories.sh` as follows:

```
cd /srv/studio/sid/sid_utils/parallel_migrator/  
./migrate_frozen_repositories.sh
```



# Administering SUSE Studio Servers

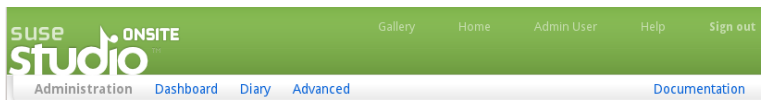
In this chapter, learn how to log in to SUSE Studio Onsite and how to execute basic administration tasks, like viewing statistics or checking events on your server, how to manage repositories, builds and appliances, and how to add cron jobs.

## 2.1 Logging in to SUSE Studio Onsite

To log in to the SUSE Studio Onsite Web interface, enter the URL of your SUSE Studio Onsite server in your browser and click *Create account/Sign in* (in the upper right hand corner).

After you have successfully logged in, your home page of SUSE Studio Onsite gives you an overview of all your appliances. To switch to the administration settings, click on your login name to show the administration panel, see Figure 2.1, “The Administration Panel” (page 23).

**Figure 2.1:** *The Administration Panel*

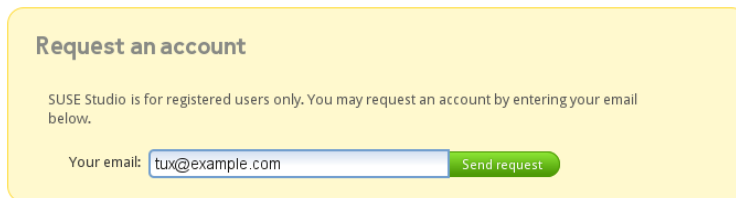


## 2.2 Inviting New Users

Accessing SUSE Studio Onsite is permission-based. Access can be granted by the administrator based on a user access request or via administrator invitation:

1. **User Issues an Account Request:** The user requests an account from the SUSE Studio Onsite home page by entering an appropriate e-mail address as shown in Figure 2.2, “Requesting an Account” (page 24) and clicking the *Send request* button. A request is generated and sent to the SUSE Studio Onsite administrator for approval.

**Figure 2.2:** *Requesting an Account*



The screenshot shows a yellow rounded rectangle containing the text "Request an account" in bold. Below this, it says "SUSE Studio is for registered users only. You may request an account by entering your email below." There is a text input field with the value "tux@example.com" and a green "Send request" button to its right.

2. **Administrator Initiates Account:** The administrator issues an invitation to a user (without a prior user request).

For both approval and invitation of a user, use the administration panel. To approve a request you have received, select *Advanced > Users > Signups* and click the *Invite* link.

If you want to initiate an account, select *Advanced > Users > Invitations* and enter the e-mail address of the user you want to invite.

After administrator approval or by direct invitation, a user account will be created and an invitation e-mail is sent to the specified e-mail address. The user must activate the account by following the instructions in the invitation e-mail. Activation requires the user to log into SUSE Studio Onsite with a username and a password.

It is possible to disable user requests by modifying the SUSE Studio Onsite configuration file. See Example 1.1, “Central Configuration File `/srv/studio/options.yml`” (page 15) for additional details.



## 2.3 Managing Your Repositories

Information about the repositories available for your appliance builds can be accessed in the administration panel by clicking *Advanced > Repositories*. Use one of the following options to add repositories:

- **From a URL** Insert the name and URL into the corresponding text fields and press the *Add* button.
- **From Media (CD/DVD)** Insert the media and press the *Scan* button to search for packages. This feature is able to copy packages from SUSE Linux Enterprise repositories of the installation media, but only those that have metadata already downloaded from SMT or Novell Customer Center.

Next to the label *Used by* a link indicates the number of appliances built using this repository. Click the link to modify or replace the references to this repository. With the action buttons at the bottom of the page you enable or disable automatic updates to the repository or delete the repository from your system. You can also disallow the URL for future addition to the repository list by clicking *Ban this URL & delete repository*.

---

### IMPORTANT: SUSE Linux Enterprise 12 Repositories

SUSE Linux Enterprise 12 repositories can only be fetched from SUSE Customer Center. This requires to set up an SMT server that is connected to SUSE Customer Center or to migrate your existing SMT server to SUSE Customer Center. Refer to the latest *Subscription Management Tool for SUSE Linux Enterprise 12* documentation on <https://www.suse.com/documentation/> for setup instructions.

To import the SUSE Linux Enterprise 12 templates from an SMT server connected to the SUSE Customer Center, proceed as follows:

1. Open the SUSE Studio Onsite Web interface and login as a user with administrator permissions.
2. Go to *Advanced > Repositories > Templates*.
3. Add the *SMT server hostname* and the port number (for example `smt.example.com:4223`) of the SMT server connected to the SUSE Customer Center.

4. Click *Import*.

5. (Optional) In order to update all existing repositories against the SMT server you just added, go to *Advanced > Repositories > Repositories* and click *Update SMT*. Note that this will only affect repositories that are served from the new SMT server.

The following repositories are required for SUSE Linux Enterprise Server 12:

```
SLES 12 x86_64
SLES 12 Updates x86_64SLED 12 x86_64
SLED 12 Updates x86_64
SLE 12 SDK x86_64
SLE 12 SDK Updates x86_64
SLE 12 Module Legacy
SLE 12 Module Legacy Updates
SLE 12 Module Public Cloud
SLE 12 Module Public Cloud Updates
SLE 12 Module Advanced Systems Management
SLE 12 Module Advanced Systems Management Updates
SLE 12 Module Web Scripting
SLE 12 Module Web Scripting Updates
```

---

## 2.4 Building Images Using SMT Staging

SMT, the Subscription Management Tool, is a package proxy system that is integrated with the Novell Customer Center and provides key capabilities locally at the customer site. It provides a repository and registration target that is synchronized with the Novell Customer Center, thus maintaining all the capabilities of the Novell Customer Center while allowing a more secure centralized deployment.

In SMT, staging is a process where you create either testing or production repositories based on the mirrored ones (see [https://www.suse.com/documentation/smt11/book\\_yep/data/smt\\_yast\\_staging\\_stage.html](https://www.suse.com/documentation/smt11/book_yep/data/smt_yast_staging_stage.html) for more information.) If you enable the staging flag of a repository for the first time, it will be moved in the SUSE Studio server from `repo/$RCE/` to `repo/full/$RCE/`. SMT offers for this repository three possible stages:

1. **Full:** contains all original SUSE patches.

2. **Testing:** with `yast-smt` you can select patches and move them from full to testing. With this tool you can assign these patches to your computer system for testing.
3. **Production:** contains all the approved patches from the testing stage.

In SUSE Studio, an image that is used in production will typically be created and updated using an SMT production stage because it contains packages and patches which have been verified to not break the application running on the appliance. The following list describes how testing stage and production stage is handled:

1. The SMT administrator will on a periodic basis stage a repository based on organizational policies like a monthly, quarterly or semi-annual update schedule. The packages in the full stage are copied into the testing stage at the time of the staging.
2. The image developer will verify that the packages in the testing stage do not break an appliance. In SUSE Studio, the image developer will create a clone of the production image and point the repositories of the clone to the testing stage. The newly built clone will contain the latest packages from the testing stage. At this point, the image developer can verify that the application running on the image clone works as expected. The image developer will notify the SMT administrator of the success or failure of testing the new packages and patches against the clone.
3. If unsuccessful, the image developer will troubleshoot why the updates in the testing stage caused a problem. Once resolved, the SMT administrator may need to restage the full to testing so the image developer can retest the packages in a clone of an image.
4. If successful, the SMT administrator will stage the testing stage to the production stage. In SUSE Studio, the image developer can update an image with the latest packages. Once the newly built production image is tested, the image can be deploying as the new production image and used by SLMS (SUSE Lifecycle Management Server) to update older versions of the production image that have already been deployed.

## 2.5 Changing Repository Order

If you have two different repositories, but with different versions of the same package, you need to change the priority of one repository. This avoids the problem of having an old version installed in your appliance.

Change the priority of the repository with the following steps:

**1** Open a file `/srv/studio/options.yml` and add the following content:

```
default:
# Note: Run "rcmemcached restart" as root after making changes here!
  repos_with_lower_priority:
    'SLES11_SP2': &repo_priority_sles11_sp2
      - 'SLE 11 SP2 SDK i386'
      - 'SLE 11 SP2 SDK x86_64'
      - 'SLE 11 SP2 SDK s390x'
      - 'SLE 11 SP2 SDK Updates i386'
      - 'SLE 11 SP2 SDK Updates x86_64'
      - 'SLE 11 SP2 SDK Updates s390x'
      - 'SLE 11 SP1 SDK i386'
      - 'SLE 11 SP1 SDK x86_64'
      - 'SLE 11 SP1 SDK s390x'
      - 'SLE 11 SP1 SDK Updates i386'
      - 'SLE 11 SP1 SDK Updates x86_64'
      - 'SLE 11 SP1 SDK Updates s390x'
      - '11.2u1-SLE11-SDK-SP1-Updates'
      - '11.2u1-SLE11-SDK-SP2-Updates'
      - '11.2u1-SLE11-SDK-SP1-Pool'
      - '11.2u1-SLE11-SDK-SP2-Core'

    'SLED11_SP2':
      *repo_priority_sles11_sp2

    'SLES11_SP2_VMware':
      *repo_priority_sles11_sp2
```

**2** Restart memcached and apache by running the following commands:

```
rcmemcached restart
rcapache2 restart
```

## 2.6 Managing Builds and Appliances

To get an overview of all your appliances, go to *Builds > Appliances*. The page shows a tabular view of all appliances that have already been built, see Figure 2.3, “Overview of Built Appliances” (page 29).

**Figure 2.3:** Overview of Built Appliances

### Appliances

Search:

Appliance name  Base system  Skip deleted appliances

Id	Name	Description	Author	Version	Is template	Base system	Number of total packages	Deleted	Actions
1	SLES 10 SP4, Server		SUSE Studio System User	0.0.1	yes	SLES10_SP4	248	no	Show Diary Delete
3	SLED 10 SP4, KDE 3 desktop		SUSE Studio System User	0.0.1	yes	SLED10_SP4	606	no	Show Diary Delete
4	SLED 10 SP4, GNOME desktop		SUSE Studio System User	0.0.1	yes	SLED10_SP4	520	no	Show Diary Delete
5	SLED 11 SP1, KDE 4 desktop		SUSE Studio System User	0.0.1	yes	SLED11_SP1	582	no	Show Diary Delete
6	SLED 11 SP1, GNOME desktop		SUSE Studio System User	0.0.1	yes	SLED11_SP1	661	no	Show Diary Delete
7	SLES 11 SP1, Just enough OS (jeOS)		SUSE Studio System User	0.0.1	yes	SLES11_SP1	172	no	Show Diary Delete
8	SLES 11 SP1, Server		SUSE Studio System User	0.0.1	yes	SLES11_SP1	303	no	Show Diary Delete
9	SLES 11 SP1, Minimal X		SUSE Studio System User	0.0.1	yes	SLES11_SP1	389	no	Show Diary Delete
10	Admin's SLES 11 SP1, SLES for VMware		Admin User	0.0.2	no	SLES11_SP1_VMWare	267	no	Show Diary Delete
2	SLES 11 SP1, SLES for VMware		SUSE Studio System User	0.0.1	yes	SLES11_SP1_VMWare	267	no	Show Diary Delete

In the right most column of the table the following action links are available:

#### Show

Displays information about this appliance, like its ID or name.

#### Diary

Displays the events diary for this appliance.

#### Edit

Allows you to grant other users read and write permissions.

#### Delete

Allows you to delete this appliance and its configuration from the server after confirming the respective pop-up message.

## 2.7 Adding New Cron Jobs

SUSE Studio allows you to easily set up preconfigured periodic task. These are also known as *cron jobs*. The following table provides a list of the available preconfigured jobs:

**Table 2.1:** *Description of Cron Jobs*

<b>Task</b>	<b>Description</b>
<code>cleanup_testdrives</code>	This job removes expired test drives and makes sure that test drive sessions ended by users are removed.
<code>delete_expired_images</code>	This job removes all appliance images that are older than one week. The configuration of the appliances is not affected by this job—the appliance configuration is retained and will continue to be displayed in the Web interface for the given user. Activating this job can help you reduce the disk space requirements for SUSE Studio.
<code>process_queues</code>	Internal job to process the build queues.
<code>sync_all_runners</code>	Internal job to keep the state of the different services synchronized.

To create a new cron job, proceed as follows:

- 1** From your administration panel select *Advanced > Cron*.
- 2** Click *New Cron Job*.
- 3** Choose a task from the pop-up menu, see the description in Table 2.1, “Description of Cron Jobs” (page 30).

## New Cron Job

check\_read\_only\_mode

Frequency (in minutes)

5

First run in UTC (server time now: Thu Oct 22 13:40:48 +0000 2009)

2009 | October | 22 | — | 13 | : | 40 |

Create

- 4 Modify the *Frequency (in minutes)* value to change the cron job execution frequency.
- 5 Optionally, change the initial start date and time by modifying the date and time entries.
- 6 Click *Create*. The configured cron job will be executed at the configured intervals.

## 2.8 Setting Administrator E-Mail for Nagios

Currently, all mails from Nagios go to the default address `nagios@localhost`. If you want to change this default address, do the following:

- 1 Open the file `/etc/nagios/objects/contacts.cfg`.
- 2 Search for the line starting with `define contact`.

- 3 Enter your new e-mail address in the `email` line.
- 4 Restart Nagios with `rcnagios reload`.

## 2.9 Setting the Read-Only Mode

Whenever you administer your SUSE Studio server it is recommended to set the site status to “read-only” prior to any changes. No new jobs can be started in this mode. Any user who is logged in is notified about the read-only state.

Go to *Advanced > Scheduler* and press the *Put the site in read-only mode* button. The site is in read-only mode now. To switch back, press the *Reenable site* button.

## 2.10 Allowing Outgoing TCP Connections in Testdrive

Outgoing TCP connections are disabled by default for security reasons. However, when you want to register your appliances in SUSE Lifecycle Management Server, you need to allow such connections.

This can be done by changing an option in the configuration file `/srv/studio/runner/config/options.yml`. Search for the option `allow_outgoing`, set it to `true`, and restart Apache with `rcapache2 restart`.

## 2.11 Extending Disk Storage

The disk storage requirements for SUSE Studio Onsite may be very high depending on your usage patterns. Therefore you may wish to mount the `/studio/filestore` directory or its subdirectories to different storage devices, particularly if you are running low on disk space.

Before moving the files in this directory, stop all SUSE Studio Onsite's services by running the following commands:

```
/etc/init.d/studio_crontick stop
/etc/init.d/studio_delayed_job stop
/usr/sbin/rcapache2 stop
```



After the disk operations are complete, start the services again:

```
/etc/init.d/studio_crontick start
/etc/init.d/studio_delayed_job start
/usr/sbin/rcapache2 start
```

After the services are started, SUSE Studio Onsite should be using the new storage device to store its data.

## 2.12 Enabling OVF Format

As already mentioned in Section “Appliance Formats” (Chapter 2, *Creating Appliances*, ↑User Guide), OVF format is disabled by default as we cannot distribute the VMware ovftool officially. As such, users need to manually download and install the ovftool from VMWare's website before enabling the format in SUSE Studio Onsite. To enable OVF format, proceed as follows:

- 1 Download and install the VMware ovftool from <http://communities.vmware.com/community/vmtn/vsphere/automationtools/ovf>. You need to register to download the file.

- 2 Install the downloaded file with the following command, for example:

```
sudo sh
  VMware-ovftool-VERSION-lin.x86_64.bundle
```

Replace *VERSION* with the correct version.

- 3 Enable the OVF format in SUSE Studio Onsite after installing with the following command (one line):

```
cd /srv/studio/ui-server; RAILS_ENV=production bundle19 \
exec rails runner 'ImageType.find_by_key("ovf").update_attributes!
(:enabled => true)'
```

The OVF build format will now appear in the build tab of the appliance editor.

## 2.13 Changing Maximum Number of Slots

The scheduler controls runners. Runners are used to build the image or control the test drive. Each runner contains a maximum slot value, which describes how many builds

or test drives a runner can handle concurrently. In most cases, the default value is sufficient and you can skip this section. It is recommended to leave this value as it is and only change it, if you know what you do.

If you need to change the maximum number of slots for a runner, go to *Advanced > Scheduler* in the administration panel. Click *Show* on the corresponding runner type to get an overview of the load average, the used and maximum slots, and other information. Go to *Edit* and change the value in the text field. Finish with *Save*.

## 2.14 Setting Up a Secure Web Server with SSL

Whenever sensitive data is transferred between Web server and client, it is desirable to have a secure, encrypted connection with authentication. `mod_ssl` provides strong encryption using the secure sockets layer (SSL) and transport layer security (TLS) protocols for HTTP communication between a client and the Web server. Using SSL/TLS, a private connection between Web server and client is established. Data integrity is ensured and client and server are able to authenticate each other.

For this purpose, the server sends an SSL certificate that holds information proving the server's valid identity before any request to a URL is answered. In turn, this guarantees that the server is the uniquely correct end point for the communication. Additionally, the certificate generates an encrypted connection between client and server that can transport information without the risk of exposing sensitive, plain-text content.

`mod_ssl` does not implement the SSL/TSL protocols itself, but acts as an interface between Apache and an SSL library. In SUSE Studio Onsite, the OpenSSL library is used. OpenSSL is automatically installed with Apache.

The most visible effect of using `mod_ssl` with Apache is that URLs are prefixed with `https://` instead of `http://`.

---

### **TIP: Example Certificate**

An example certificate for a hypothetical company “Snake Oil” is available when installing the package `apache2-example-certificates`.

---

## 2.14.1 Creating an SSL Certificate

In order to use SSL/TSL with the Web server, you need to create an SSL certificate. This certificate is needed for the authorization between Web server and client, so that each party can clearly identify the other party. To ensure the integrity of the certificate, it must be signed by a party every user trusts.

There are three types of certificates you can create: a “dummy” certificate for testing purposes only, a self-signed certificate for a defined circle of users that trust you, and a certificate signed by an independent, publicly-known certificate authority (CA).

Creating a certificate is basically a two step process. First, a private key for the certificate authority is generated then the server certificate is signed with this key.

---

### TIP: For More Information

To learn more about concepts and definitions of SSL/TSL, refer to [http://httpd.apache.org/docs/2.2/ssl/ssl\\_intro.html](http://httpd.apache.org/docs/2.2/ssl/ssl_intro.html).

---

### 2.14.1.1 Creating a “Dummy” Certificate

Generating a dummy certificate is simple. Just call the script `/usr/bin/gensslcert`. It creates or overwrites the files listed below. Make use of `gensslcert`'s optional switches to fine-tune the certificate. Call `/usr/bin/gensslcert -h` for more information.

- `/etc/apache2/ssl.crt/ca.crt`
- `/etc/apache2/ssl.crt/server.crt`
- `/etc/apache2/ssl.key/server.key`
- `/etc/apache2/ssl.csr/server.csr`
- `/root/.mkcert.cfg`

A copy of `ca.crt` is also placed at `/srv/www/htdocs/CA.crt` for download.

---

### IMPORTANT: For Testing Purposes Only

A dummy certificate should never be used on a production system. Only use it for testing purposes.

---

## 2.14.1.2 Creating a Self-Signed Certificate

If you are setting up a secure Web server for an Intranet or for a defined circle of users, it might be sufficient if you sign a certificate with your own certificate authority (CA).

Creating a self-signed certificate is an interactive nine-step process. Change into the directory `/usr/share/doc/packages/apache2` and run the following command: `./mkcert.sh make --no-print-directory /usr/bin/openssl /usr/sbin/ custom`. Do not attempt to run this command from outside this directory. The program provides a series of prompts, some of which require user input.

### **Procedure 2.1:** *Creating a Self-Signed Certificate with `mkcert.sh`*

**1** `Decide the signature algorithm used for certificates`

Choose RSA (R, the default), because some older browsers have problems with DSA.

**2** `Generating RSA private key for CA (1024 bit)`

No interaction needed.

**3** `Generating X.509 certificate signing request for CA`

Create the CA's distinguished name here. This requires you to answer a few questions, such as country name or organization name. Enter valid data, because everything you enter here later shows up in the certificate. You do not need to answer every question. If one does not apply to you or you want to leave it blank, use “.”. Common name is the name of the CA itself—choose a significant name, such as *My company* CA.

---

#### **IMPORTANT: Common Name of the CA**

The common name of the CA must be different from the server's common name, so do not choose the fully qualified hostname in this step.

---

**4** `Generating X.509 certificate for CA signed by itself`

Choose certificate version 3 (the default).

## 5 Generating RSA private key for SERVER (1024 bit)

No interaction needed.

## 6 Generating X.509 certificate signing request for SERVER

Create the distinguished name for the server key here. Questions are almost identical to the ones already answered for the CA's distinguished name. The data entered here applies to the Web server and does not necessarily need to be identical to the CA's data (for example, if the server is located elsewhere).

---

### **IMPORTANT: Selecting a Common Name**

The common name you enter here must be the fully qualified hostname of your secure server (for example, `www.example.com`). Otherwise the browser issues a warning that the certificate does not match the server when accessing the Web server.

---

## 7 Generating X.509 certificate signed by own CA

Choose certificate version 3 (the default).

## 8 Encrypting RSA private key of CA with a passphrase for security

It is strongly recommended to encrypt the private key of the CA with a password, so choose `Y` and enter a password.

## 9 Encrypting RSA private key of SERVER with a passphrase for security

Encrypting the server key with a password requires you to enter this password every time you start the Web server. This makes it difficult to automatically start the server on boot or to restart the Web server. Therefore, it is common sense to say `N` to this question. Keep in mind that your key is unprotected when not encrypted with a password and make sure that only authorized persons have access to the key.

---

### **IMPORTANT: Encrypting the Server Key**

If you choose to encrypt the server key with a password, increase the value for `APACHE_TIMEOUT` in `/etc/sysconfig/apache2`. Otherwise

you do not have enough time to enter the passphrase before the attempt to start the server is stopped unsuccessfully.

---

The script's result page presents a list of certificates and keys it has generated. Contrary to what the script outputs, the files have not been generated in the local directory `conf`, but to the correct locations under `/etc/apache2/`.

The last step is to copy the CA certificate file from `/etc/apache2/ssl.crt/ca.crt` to a location where your users can access it in order to incorporate it into the list of known and trusted CAs in their Web browsers. Otherwise a browser complains that the certificate was issued by an unknown authority. The certificate is valid for one year.

---

### **IMPORTANT: Self-Signed Certificates**

Only use a self-signed certificate on a Web server that is accessed by people who know and trust you as a certificate authority. It is not recommended to use such a certificate for a public shop, for example.

---

### **IMPORTANT: Changed Hostnames and SSL Certificate**

The *Certificate Common Name* must match your hostname. Thus, if you ever change the hostname after having created the certificate, you must create a new certificate by running the `/srv/studio/scripts/setup_sslcert.sh` script.

---

## **2.14.1.3 Getting Officially Signed Certificates**

There are a number of official certificate authorities that sign your certificates. The certificate is signed by a trustworthy third party, so can be fully trusted. Publicly operating secure Web servers usually have got an officially signed certificate.

The best-known official CAs are Thawte (<http://www.thawte.com/>) or Verisign (<http://www.verisign.com>). These and other CAs are already compiled into all browsers, so certificates signed by these certificate authorities are automatically accepted by the browser.

When requesting an officially signed certificate, you do not send a certificate to the CA. Instead, issue a Certificate Signing Request (CSR). To create a CSR, call the script `/usr/share/ssl/misc/CA.sh -newreq`.

First the script asks for a password with which the CSR should be encrypted. Then you are asked to enter a distinguished name. This requires you to answer a few questions, such as country name or organization name. Enter valid data—everything you enter here later shows up in the certificate and is checked. You do not need to answer every question. If one does not apply to you or you want to leave it blank, use “.”. Common name is the name of the CA itself—choose a significant name, such as *My company CA*. Last, a challenge password and an alternative company name must be entered.

Find the CSR in the directory from which you called the script. The file is named `newreq.pem`.

## 2.14.2 Configuring Apache with SSL

The default port for SSL and TLS requests on the Web server side is 443. There is no conflict between a “regular” Apache listening on port 80 and an SSL/TLS-enabled Apache listening on port 443. In fact, HTTP and HTTPS can be run with the same Apache instance. Usually separate virtual hosts are used to dispatch requests to port 80 and port 443 to separate virtual servers.

To enable SSL and secure HTTP transfers, use the file `/etc/apache2/vhosts.d/ui-server.conf`, remove the hash signs as it looks like Example 2.1, “Configuration of HTTPS for SUSE Studio” (page 39), and restart the Apache Web server with `rcapache2 restart`:

### **Example 2.1:** *Configuration of HTTPS for SUSE Studio*

```
<VirtualHost *:80>
  ServerName localhost
  Include /etc/apache2/vhosts.d/ui-server-common
  RewriteEngine On
  RewriteCond %{HTTPS} off
  RewriteCond %{REMOTE_HOST} !^(127.0.0.1|::1)
  RewriteCond %{REMOTE_HOST} %{REQUEST_URI} !^/backend.*$
  RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
</VirtualHost>
```





# Monitoring SUSE Studio Onsite Servers

SUSE Studio Onsite offers utilities to monitor the state of your server such as build statistics, diary information, and others.

## 3.1 Viewing Build Statistics

SUSE Studio collects data about appliance builds in various categories and appliance test drives. This data can be visualized by using the *Dashboard* menu. Each category lists the image, its version, its format, the architecture, and other useful information. Click the *Log* link on each line to get detailed information. The categories are:

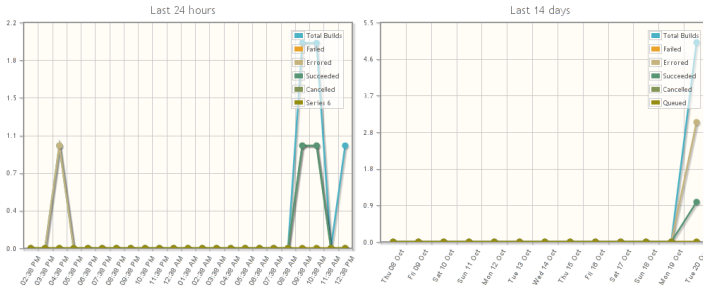
### *Build statistics*

Gives a general overview, see Figure 3.1, “SUSE Studio Onsite Dashboard” (page 42). By drawing a rectangle with your mouse on the graph you can zoom in on a particular area of interest. Double-click to return to the original view.

**Figure 3.1:** SUSE Studio Onsite Dashboard

SUSE Studio Dashboard (updated at Wed 21 Oct 2009, 01:52 PM (UTC))

Build statistics



*Active builds*

Lists appliances that are currently being built.

*Errored builds*

Indicates internal errors of your SUSE Studio Onsite server.

*Failed builds*

Lists appliances which could not be built because of errors. Usually these errors are file conflicts or problems with RPM packages.

*Completed builds*

Lists all appliances which succeeded. Narrow down the list with the pop-up menu or click *View all*. Each appliance contains a detailed graph of the build times.

*Test drives*

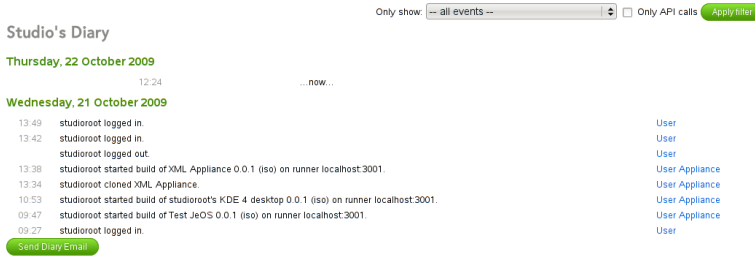
Lists all appliances started through the test drive environment.

## 3.2 Getting Diary Information

The administration panel contains a link named *Diary*. Use this link to further investigate events in SUSE Studio. Events are listed on the left. The link on the right allows you to access more detailed information about the event. The *Only show* drop-down

list allows you to filter the list based on the event type. Activate the filter with *Apply Filter*.

**Figure 3.2:** *SUSE Studio Onsite's Diary*



## 3.3 Monitor SUSE Studio Onsite with Nagios and Munin

The SUSE Studio Onsite installation contains Nagios and Munin, both system and network monitoring tools:

### Nagios

Nagios is a scalable and extensible enterprise-class network and system monitoring tool which allows administrators to monitor network and host resources such as HTTP, SMTP, POP3, disk usage and processor load. Find more information at <http://www.nagios.org/>.

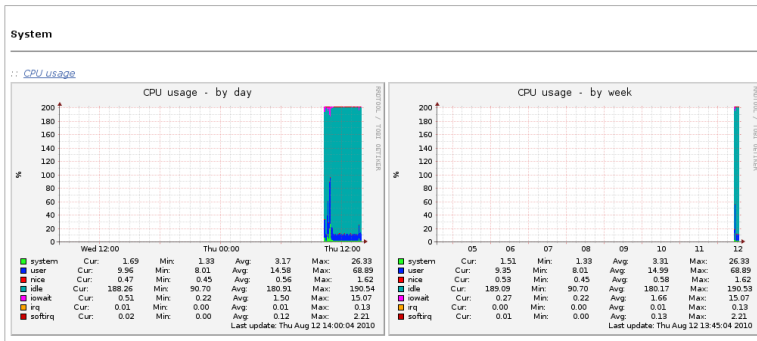
### Munin

Munin is a network and system monitoring tool. It can easily monitor the network and performance of your computers, show bottlenecks, and peak loads and memory leaks. A summary of monitoring results can be accessed through the Munin Web interface. Find more information at <http://munin-monitoring.org/>.

If you have set the administrator password as described in Section 1.7.2, “Setting Administrator Passwords for Nagios and Munin” (page 16), log in with your credentials.

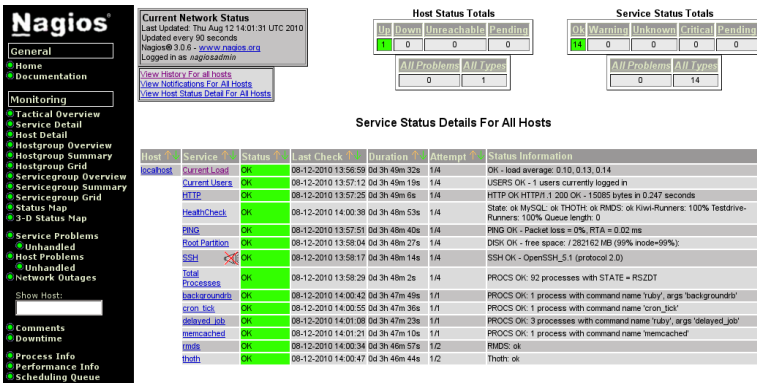
After you have logged in to Munin, the Web site displays details about network, processes, disks, and others in a graphical grid (see Figure 3.3 (page 44)).

**Figure 3.3:** Munin Web Site Displaying CPU Usage



Munin is only able to show the results in a grid whereas Nagios can be influenced by the administrator.

**Figure 3.4:** Nagios Web Site Displaying Status Information



# SUSE Studio Onsite Services



The table below lists the preconfigured SUSE Studio Onsite services running on the server. These services are started at boot time and are controlled by Nagios. It generally neither is necessary nor recommended to apply any changes to these services.

**Table A.1:** *SUSE Studio Onsite Services*

Service	Description
<code>/etc/init.d/flashpolicyd</code>	Adobe Flash daemon required for the Flash VNC applet to work correctly. Needed for the test drive and the embedded VNC session.
<code>/etc/init.d/memcached</code>	A cache store service to increase performance (used in the user interface server).
<code>/etc/init.d/ studio_crontick</code>	SUSE Studio Onsite's internal cron job system. Runs administrative tasks repeatedly and is used in the user interface server.
<code>/etc/init.d/studio_boot</code>	First boot script. It only run in first boot and sets up initial system and studio configuration.

<b>Service</b>	<b>Description</b>
<pre data-bbox="266 228 568 289">/etc/init.d/ studio_delayed_job</pre>	<p data-bbox="744 228 1139 289">Service for running tasks asynchronously in the background.</p>
<pre data-bbox="266 331 619 391">/etc/init.d/ studio_sid_downloader</pre>	<p data-bbox="744 331 1166 492">SID (Software Information Database) service that downloads the RPMs that will be used in order to build appliances. The Software Information Database performs different tasks:</p> <ul data-bbox="744 526 1161 802" style="list-style-type: none"> <li data-bbox="744 526 1076 553">• mirrors remote repositories</li> <li data-bbox="744 586 1116 613">• resolves package dependencies</li> <li data-bbox="744 646 1130 706">• keeps the local mirrors synchronized</li> <li data-bbox="744 738 1161 799">• respond to software searches made by UI server</li> </ul>
<pre data-bbox="266 842 585 902">/etc/init.d/ studio_sid_crontick</pre>	<p data-bbox="744 842 1170 971">SUSE Studio Onsite's internal cron job system for SID server used for running administrative tasks repeatedly.</p>
<pre data-bbox="266 1008 585 1068">/etc/init.d/ studio_sunspot_solr</pre>	<p data-bbox="744 1008 1134 1068">Service for running Solr search engine in the background.</p>

# Administration Panel— Menu Structure

# B

The following list is a reference of the administration panel's menu structure.

## B.1 Dashboard

The *Dashboard* gives you an overview of your build statistics and your builds. See Section 3.1, “Viewing Build Statistics” (page 41) for more information.

## B.2 Diary

The *Diary* shows events on your server. See Section 3.2, “Getting Diary Information” (page 42) for more information.

## B.3 Advanced

The availability of some menu items depends on the settings in the central SUSE Studio Onsite configuration file as mentioned below. For more information about the configuration file, see Example 1.1, “Central Configuration File `/srv/studio/options.yml`” (page 15).

## ***Servers & Services***

### *Scheduler*

Shows the processes, also referred to as runners, for appliance builds and for the test drive feature. The back-end of the appliance build process is KIWI.

### *Queue*

Lists system relevant build processes, excluding the processes triggered by the administrator.

### *Cron*

Shows the defined cron jobs and additionally lists information about the first, last, and next scheduled execution.

## ***Repositories***

### *Templates*

Lists your available templates and predefined repositories.

### *Repositories*

Lets you add repositories to the SUSE Studio Onsite configuration.

## ***Builds***

### *Appliances*

Shows the list of all built appliances.

### *Downloads*

Shows a list of the downloaded appliances.

## ***Users***

### *Users*

Provides a list of SUSE Studio Onsite users. If the option `invitation_required` in the configuration file `/srv/stu`



`dio/options.yml` is set to `false`, the user cannot request accounts. In this case, users can only be added to the system via administrator invitation.

### *Signups*

Allows you to manage the SUSE Studio Onsite users. This entry is only displayed if the option `invitation_required` in `/srv/studio/options.yml` is set to `true` (or if the option is turned into a comment or removed from the file).

### *Invitations*

Lets you create e-mail invitations. This entry is only displayed if the option `invitation_required` in `/srv/studio/options.yml` is set to `true` (or if the option is turned into a comment or removed from the file).

### *E-Mail Templates*

Set text containing replaceables. This text is sent by e-mail if some specific action is triggered, for example, an invitation failed build, etc.



# Troubleshooting

## *Installation and Setup*

SUSE Studio can not be installed on my system

If you do not have the minimum amount of RAM, SUSE Studio cannot be installed. See Section 1.1, “System Requirements” (page 2) for more details.

Can SUSE Studio run on a virtual machine?

No, this is not possible. SUSE Studio needs the hardware virtualization of your CPU. See Section 1.1, “System Requirements” (page 2).

Message “You found an error. (Sorry about that!)”

There are two possible causes for that message:

- **No Connection to Novell Customer Center** Registration of SUSE Studio Onsite can either be done with Subscription Management Tool or with Novell Customer Center. If you decided to register your product at Novell Customer Center, you need an Internet connection from your SUSE Studio Onsite server. To achieve this, you may need to set up a proxy.
- **root Password Has Been Changed** If you changed the `root` password at the command line, the setup will not work correctly. The `root` password is automatically changed and synchronized during the initial configuration. If you already changed the password manually, set it back to `linux`.

I cannot access my NFS share on my IBM System z

If you have trouble to access NFS, proceed as follows:

1. Log in as `root` on your IBM System z runner.

2. Open the file `/etc/fstab` and add the following line:

```
UI_SERVER:/studio:filestore /studio/filestore nfs rw,nolock,auto 0 0
```

Replace `UI_SERVER` with the name or IP address of your SUSE Studio On-site server.

3. Mount the share:

```
mount /studio/filestore
```

4. Open the file `/srv/studio/runner/config/options.yml` and locate the section `production:`. Change it to the following line (observe the two spaces before `scheduler`):

```
production:
  scheduler: UI_SERVER:80
```

Replace `UI_SERVER` with the name or IP address of your SUSE Studio On-site server.

5. Restart the Apache Web server:

```
rcapache2 restart
```

## ***Registering***

I cannot see any repositories (channels)

You need to register your product (SUSE Linux Enterprise) in the Novell Customer Center.

## ***Debugging***

Where can I find the SUSE Studio log file?

- UI server log file: `/srv/studio/ui-server/log/production.log`
- RMDS and Thoth: `/var/log/messages`

- Build and test drive logs: `/srv/studio/runner/log/production.log`

Some tools clutter the terminal for System z

For example, vim is affected by this issue. A known workaround is to use SSH and enable it in the networking tab.

