Foreman installation

Table of Contents

ACME Ltd.
IT

Mr. Chad Badguy
Main St 1
02120 Boston MA

Author:	Simone Giertz <s.giertz@shittyrobots.loc>
Publisher:	Doge Consulting Ltd Leetstreet 1337 65205 Leetbaden
Date:	09.07.2023
Version:	1.0

Legend

🔥 **This might be important to know**

❗ **Important hint**

ℹ️ **An information hint**

💡 **A tip to make things easier**

⚠️ **Please pay attention**

Scenario

[Scenario] | *scenario.jpg*

This scenario consists of a Foreman **main instance** in the **XYZ** datacenter. It will be used to manage approximately **20 servers**.

VM configuration

The VM was created with the following parameters:

Table 1. VM configuration main instance

Setting	Value
vCPU	8
Memory	32 GB
OS HDD/controller	100 GB (*SCSI-ID 0:0*)
Data HDD/controller	500 GB (*SCSI-ID 1:0*)
Storage provisioning	Thin Provision
SCSI controller	VMware Paravirtual
Network adapter #1	Lab network

Operating system installation

CentOS Stream 8 x86_64 was installed using the [ISO image](#).

Partitioning

Table 2. Main instance partitioning

Disc	Volume group	Mount point	Size	Description
`/dev/sda`	`vg_system`	`/`	10 GB	Root filesystem
		`/var`	10 GB	Variable data
		`/opt`	1 GB	Third-party software
		`swap`	9 GB	Swap partition
		`/tmp`	4 GB	Temporary files
		`/home`	10 GB	User home directories
`/dev/sdb`	`vg_foreman`	`/var/lib/pgsql`	20 GB	Foreman database (*PostgreSQL*)
		`/var/lib/pulp`	300 GB	Package storage
		`/var/lib/qpidd`	1 GB	Cache

> 🛈 The recommended **xfs** was used as file system.

Customization

The following parameters were defined during installation:

Table 3. Installation parameter

Language	Englisch / Englisch (United States)
Keyboard layout	German (no dead keys)
Region / City	Europe / Berlin
Base Environment	Minimal Install

Table 4. Netzwerk parameter

Network interface	`ens192`
Hostname / FQDN	`linmgmt001` / `linmgmt01.shittyrobots.loc`
IP address	`10.10.22.42`
Network mask	`255.255.255.0`
Gateway	`10.10.22.1`
DNS server	`10.10.22.1`, `10.10.22.2`
Search domains	`shittyrobots.loc`
Require IPv4 addressing for this connection to complete	**yes**

NTP server	10.10.22.1

Table 5. User

Full name	Administrator
User name	administrator
Require a password to use this account	**yes**

DNS validation

```
# hostnamectl set-hostname linmgmt001
# nslookup 10.10.22.42
# nslookup linmgmt01.shittyrobots.loc
```

Administrator

Installation

Installation took place on **06.03.2023** when **Foreman 3.7** and **Katello 4.9** were the most recent versions.

Preparation

> ℹ️ The installation was execution in accordance with the project documentation.

Updating the system

```
# dnf update
# reboot
```

Ansible

As Ansible was used for the installation, Ansible needed to be installed:

Installing Ansible

```
# dnf install ansible-core
```

For the installation an **Inventory** and additional **variables** were created:

lab-inventory.ini

```
[foreman]
foreman.shittyrobots.loc ansible_host=192.168.1.10 ansible_user=max ansible_become_pass=chad
```

group_vars/foreman/foreman.yml

```
---
foreman_org: Shitty Robots

foreman_content_credentials:
  - name: RPM-GPG-KEY-CentOS-Official
    url: https://centos.org/keys/RPM-GPG-KEY-CentOS-Official
  - name: RPM-GPG-KEY-foreman
    url: http://yum.theforeman.org/RPM-GPG-KEY-foreman

foreman_syncplans:
  - name: daily-sync
    interval: daily
    sync_date: "2023-01-01 04:00:00 UTC"

foreman_products:
  - name: CentOS Stream 9 x86_64
    sync_plan: daily-sync
    gpg_key: RPM-GPG-KEY-CentOS-Official
  - name: Foreman Client EL9 x86_64
    sync_plan: daily-sync
    gpg_key: RPM-GPG-KEY-foreman

foreman_repositories:
  - name: BaseOS_x86_64
    product: CentOS Stream 9 x86_64
    url: https://mirror.stream.centos.org/9-stream/BaseOS/x86_64/os/
  - name: AppStream_x86_64
    product: CentOS Stream 9 x86_64
    url: https://mirror.stream.centos.org/9-stream/AppStream/x86_64/os/
  - name: ForemanClient_EL9_x86_64
    product: Foreman Client EL9 x86_64
    url: http://yum.theforeman.org/client/latest/el9/x86_64/
```

```yaml
foreman_content_views:
  - name: CentOS Stream 9 x86_64
    repositories:
      - name: BaseOS_x86_64
        product: CentOS Stream 9 x86_64
      - name: AppStream_x86_64
        product: CentOS Stream 9 x86_64
  - name: Foreman Client EL9 x86_64
    repositories:
      - name: ForemanClient_EL9_x86_64
        product: Foreman Client EL9 x86_64
  - name: CentOS Stream 9 x86_64 + Tools
    composite: true
    auto_publish: true
    components:
      - content_view: CentOS Stream 9 x86_64
        latest: true
      - content_view: Foreman Client EL9 x86_64
        latest: true

foreman_lifecycle_environments:
  - name: Development
    label: dev
    description: Development systems
  - name: QA
    label: qa
    prior: Development
    description: QA systems
  - name: Production
    label: prod
    prior: QA
    description: Production systems

foreman_content_view_versions:
  - name: CentOS Stream 9 x86_64
    version: '1.0'
    lifecycle_environments:
      - Development
  - name: Foreman Client EL9 x86_64
    version: '1.0'
    lifecycle_environments:
      - Development

foreman_activation_keys:
  - name: ak-centos9s
    lifecycle_environment: Development
    content_view: 'CentOS Stream 9 x86_64'

foreman_hostgroups:
  - name: centos-9s
```

group_vars/foreman/firewall.yml

```yaml
---
# firewall settings
foreman_firewall_services:
  - service: ssh
    state: enabled
  - service: http
    state: enabled
  - service: https
    state: enabled
  - service: RH-Satellite-6
    state: enabled
```

group_vars/foreman/storage.yml

```yaml
---
# storage settings
foreman_vg: vg_data
foreman_pv: /dev/vdb
foreman_filesystems:
  - name: lv_pgsql
    type: xfs
    mountpoint: /var/lib/pgsql
    size: 20480
  - name: lv_pulp
    type: xfs
    mountpoint: /var/lib/pulp
    size: 20480 # should be 300G
  - name: lv_qpidd
    mountpoint: /var/lib/qpidd
    type: xfs
    size: 1024 # ~2MB per content host
```

The complete source code is added to the **appendix** of this document.

> ❗ Credentials are not part of the appendix as they need to created in the `host_vars/linmgmt01.shittyrobots.loc/credentials.yml` file.

Customization

Backup

ℹ️ This section is still missing (TODO)

Settings

The following configuration parameters were set:

Setting	Value	Description
`default_download_policy`	`on_demand`	Default download policy; `on_demand` saves disk space and network bandwidth by only downloading metadata in full. The actual packages are downloaded only when they are first used.

Organizations and locations

The following organizations and locations were created:

Table 6. Organizations and locations

Organization	Location	Description
Shitty Robots	Default Location	Main organization unit

Third-party products

The following third-party products were configured:

- CentOS Stream 9 x86_64

ℹ️ Product-related definitions are part of the **appendix**.

Content Views

The following CVs were configured:

Table 7. CV overview

Name	Repositories
`CentOS 9 x86_64`	`Base_x86_64`, `AppStream_x86_64`, `ForemanClient_EL9_x86_64`
`Foreman Client EL9 x86_64`	`ForemanClient_EL9_x86_64`

ℹ️ CV-related definitions are part of the **appendix**.

Lifecycle Environments

A **Lifecycle Environment Path** with the following environments was created:

- Development
- QA
- Production

ℹ️ No application-specific Lifecycle Environment Paths were defined.

Activation Keys

The following activation keys were created:

Table 8. Activation Key overview

Name	Content View	Lifecycle Environment
ak-centos9s	CentOS 9 Stream x86_64	Development

ℹ️ **Auto-Attach** and **Simple Content Access** are used.

Sync Plans

The following Sync Plans were created:

Table 9. Sync Plan overview

Name	Products	Time
daily	CentOS 9, Foreman Client EL9 x86_64	daily, 04:00 UTC

Hostgroups

The following hostgroups were created:

Table 10. Hostgroup overview

Name	Nested
centos-9s	no

Appendix

Registering CentOS clients

To register CentOS clients, it is sufficient to execute the following commands:

Registering a CentOS client

```
# yum localinstall https://linmgmt01.shittyrobots.loc/pub/katello-ca-consumer-latest.noarch.rpm
# subscription-manager register --activationkey=ak-centos9s --org Shitty Robots
```

Ansible source code

This section contains the Ansible code to bootstrap the environment.

ansible/foreman.yml

```yaml
---
- name: Prepare systems
  hosts: all
  become: true
  tasks:
    - name: Set /etc/hosts
      ansible.builtin.template:
        src: templates/hosts.j2
        dest: /etc/hosts
        mode: '0644'
        owner: root
        group: root

- name: Install Foreman/Katello
  hosts: foreman
  become: true
  pre_tasks:
    - name: Import storage tasks
      ansible.builtin.import_tasks: storage.yml
      tags: storage

    - name: Import software tasks
      ansible.builtin.import_tasks: software.yml
      tags: software

  roles:
    - role: fedora.linux_system_roles.firewall
      firewall: "{{ foreman_firewall_services }}"

    - role: theforeman.operations.foreman_repositories
      foreman_repositories_version: "3.7"
      foreman_repositories_katello_version: "4.9"

    - role: theforeman.operations.puppet_repositories
      foreman_puppet_repositories_version: 7

    - role: theforeman.operations.installer
      foreman_installer_package: foreman-installer-katello
      foreman_installer_scenario: katello
      foreman_installer_timeout: 6000
      foreman_installer_options:
        - '--foreman-initial-organization "{{ foreman_org }}"'
        - '--foreman-initial-admin-username "{{ foreman_admin_username }}"'
        - '--foreman-initial-admin-password "{{ foreman_admin_password }}"'

  post_tasks:
    - name: Import content tasks
      ansible.builtin.import_tasks: content.yml
      tags: content
```

ansible/templates/hosts.j2

```
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6

127.0.0.1 localhost.localdomain

127.0.1.1 localhost.localdomain {{ ansible_hostname }}

192.168.23.100  00-foreman.sva.de 00-foreman foreman
192.168.23.101  00-client.sva.de 00-client client
```

ansible/storage.yml

```yaml
---
- name: Create a volume group for Foreman
  community.general.lvg:
    vg: "{{ foreman_vg }}"
    pvs: "{{ foreman_pv }}"
  become: true

- name: Create logical volumes, file systems and mount points
  become: true
  block:
    - name: Create logical volumes
      community.general.lvol:
        vg: "{{ foreman_vg }}"
        lv: "{{ item.name }}"
        size: "{{ item.size }}"
      loop: "{{ foreman_filesystems }}"
    - name: Create file systems
      community.general.filesystem:
        fstype: "{{ item.type }}"
        dev: "/dev/mapper/{{ foreman_vg }}-{{ item.name }}"
      loop: "{{ foreman_filesystems }}"
    - name: Create mount points
      ansible.posix.mount:
        path: "{{ item.mountpoint }}"
        src: "/dev/mapper/{{ foreman_vg }}-{{ item.name }}"
        fstype: "{{ item.type }}"
        opts: auto
        state: mounted
      loop: "{{ foreman_filesystems }}"
```

ansible/software.yml

```yaml
---
- name: Disable EPEL repository
  ansible.builtin.yum_repository:
    name: epel
    state: absent

- name: Install requirements
  ansible.builtin.dnf:
    name:
      - chrony

- name: Configure services
  ansible.builtin.service:
    name: "{{ item }}"
    state: started
    enabled: true
  loop:
    - chronyd.service
```

ansible/content.yml

```yaml
---
- name: Install requirements
  ansible.builtin.dnf:
```

```yaml
      name:
        - python3-requests

- name: Create content credentials
  theforeman.foreman.content_credential:
    username: "{{ foreman_admin_username }}"
    password: "{{ foreman_admin_password }}"
    server_url: "https://{{ ansible_fqdn }}"
    name: "{{ item.name }}"
    content_type: gpg_key
    organization: "{{ foreman_org }}"
    content: "{{ lookup('url', item.url, split_lines=false) }}"
  become: false
  loop: "{{ foreman_content_credentials }}"

- name: Create sync plans
  theforeman.foreman.sync_plan:
    server_url: "https://{{ ansible_fqdn }}"
    username: "{{ foreman_admin_username }}"
    password: "{{ foreman_admin_password }}"
    name: "{{ item.name }}"
    enabled: true
    interval: "{{ item.interval }}"
    sync_date: "{{ item.sync_date }}"
    organization: "{{ foreman_org }}"
  become: false
  loop: "{{ foreman_syncplans }}"

- name: Create products
  theforeman.foreman.product:
    username: "{{ foreman_admin_username }}"
    password: "{{ foreman_admin_password }}"
    server_url: "https://{{ ansible_fqdn }}"
    name: "{{ item.name }}"
    organization: "{{ foreman_org }}"
    sync_plan: "{{ item.sync_plan }}"
    gpg_key: "{{ item.gpg_key | default(omit) }}"
  become: false
  loop: "{{ foreman_products }}"

- name: Create repositories
  theforeman.foreman.repository:
    username: "{{ foreman_admin_username }}"
    password: "{{ foreman_admin_password }}"
    server_url: "https://{{ ansible_fqdn }}"
    name: "{{ item.name }}"
    state: present
    content_type: "{{ item.content_type | default('yum') }}"
    product: "{{ item.product }}"
    organization: "{{ foreman_org }}"
    url: "{{ item.url }}"
    download_policy: "{{ item.download_policy | default('on_demand') }}"
  become: false
  loop: "{{ foreman_repositories }}"

- name: Sync products
  theforeman.foreman.repository_sync:
    server_url: "https://{{ ansible_fqdn }}"
    username: "{{ foreman_admin_username }}"
    password: "{{ foreman_admin_password }}"
    product: "{{ item.name }}"
    organization: "{{ foreman_org }}"
  loop: "{{ foreman_products }}"
  become: false
  tags: sync

- name: Create content views
  theforeman.foreman.content_view:
    username: "{{ foreman_admin_username }}"
    password: "{{ foreman_admin_password }}"
    server_url: "https://{{ ansible_fqdn }}"
    name: "{{ item.name }}"
    organization: "{{ foreman_org }}"
    repositories: "{{ item.repositories | default(omit) }}"
```

```yaml
      composite: "{{ item.composite | default(omit) }}"
      auto_publish: "{{ item.auto_publish | default(omit) }}"
      components: "{{ item.components | default(omit) }}"
    become: false
    loop: "{{ foreman_content_views }}"

  - name: Create lifecycle environments
    theforeman.foreman.lifecycle_environment:
      server_url: "https://{{ ansible_fqdn }}"
      username: "{{ foreman_admin_username }}"
      password: "{{ foreman_admin_password }}"
      name: "{{ item.name }}"
      label: "{{ item.label }}"
      organization: "{{ foreman_org }}"
      prior: "{{ item.prior | default('Library') }}"
      description: "{{ item.description }}"
    become: false
    loop: "{{ foreman_lifecycle_environments }}"

  - name: Publish content view versions
    theforeman.foreman.content_view_version:
      server_url: "https://{{ ansible_fqdn }}"
      username: "{{ foreman_admin_username }}"
      password: "{{ foreman_admin_password }}"
      content_view: "{{ item.name }}"
      organization: "{{ foreman_org }}"
      version: "{{ item.version }}"
      lifecycle_environments: "{{ item.lifecycle_environments | list }}"
    become: false
    loop: "{{ foreman_content_view_versions }}"

  - name: Create hostgroups
    theforeman.foreman.hostgroup:
      server_url: "https://{{ ansible_fqdn }}"
      username: "{{ foreman_admin_username }}"
      password: "{{ foreman_admin_password }}"
      name: "{{ item.name }}"
      organization: "{{ foreman_org }}"
      lifecycle_environment: "{{ item.lifecycle_environment | default(omit) }}"
      content_view: "{{ item.content_view | default(omit) }}"
      parameters: "{{ item.parameters | default(omit) }}"
    become: false
    loop: "{{ foreman_hostgroups }}"

  - name: Create activation keys
    theforeman.foreman.activation_key:
      server_url: "https://{{ ansible_fqdn }}"
      username: "{{ foreman_admin_username }}"
      password: "{{ foreman_admin_password }}"
      name: "{{ item.name }}"
      organization: "{{ foreman_org }}"
      lifecycle_environment: "{{ item.lifecycle_environment }}"
      content_view: "{{ item.content_view }}"
      auto_attach: true
    become: false
    loop: "{{ foreman_activation_keys }}"
```