

Инсталляция “Katello Foreman” на сервер OEL 7

3 сентября 2019 г.

Содержание

1	Firewall	2
2	Инсталляция пакетов	2
2.1	Установка необходимых репозиториев.	3
3	Инсталляция “Katello”	3
3.1	Смена пароля	4
3.2	Добавление доменов	4
3.3	Добавление подсетей	4
3.4	Добавление продуктов	4
3.4.1	Создание нового продукта	4
3.4.2	Добавление GPG-ключей	5
3.4.3	Добавление EPEL 7-репозитория	5
3.4.4	Синхронизация репозиториев	6
3.5	Livecycle	6
3.6	Content View	7
3.6.1	Публикование “Content View”	7
3.7	Создание ключей активации	7
4	Регистрация клиента на “Katello”-сервере	8
5	Модули для “Puppetserver”	9
5.1	Модуль “ntp”	9
5.2	Удаление модуля	11
6	Установка плагина “Remote Execution”	11
6.1	Настройка ключей SSH	12

Создание сервера

- Операционная система - OEL 7¹.
- Необходимое требование к монтированию каталога “/tmp” - **не должно быть опции “noexec”**.

1 Firewall

Необходимо, чтобы были открыты следующие порты:

Порт	Протокол	Назначение
80	TCP	HTTP, used for provisioning purposes
443	TCP	HTTPS, used for web access and api communication
5647	TCP	qdrouterd - used for client and Smart Proxy actions
8140	TCP	Puppet agent to Puppet master connections
9090	TCP	HTTPS - used for communication with the Smart Proxy

Таблица 1: Открытые порты для “Katello”

Открытие портов:

```
# firewall-cmd --get-active-zones
public
# firewall-cmd \
--zone=public \
--add-port="53/udp" --add-port="53/tcp" \
--add-port="67/udp" --add-port="69/udp" \
--add-port="80/tcp" --add-port="443/tcp" \
--add-port="5000/tcp" --add-port="5647/tcp" \
--add-port="8000/tcp" --add-port="8140/tcp" \
--add-port="8443/tcp" --add-port="9090/tcp" \
--permanent
# firewall-cmd --reload
```

2 Инсталляция пакетов

В состав дистрибутива “OEL 7” не входит пакет “subscription-manager”, который надо устанавливать отдельно:

```
# wget https://copr.fedoraproject.org/coprs/dgoodwin/
subscription-manager/repo/epel-7/dgoodwin-
subscription-manager-epel-7.repo -O /etc/yum.repos.
d/dgoodwin-subscription-manager-epel-7.repo
```

¹Для пробы системы “Katello” использовалась виртуализация VirtualBox. Под систему было выделено 12ГБ ОЗУ и 2 виртуальных процессора.

Кроме того, если установлены следующие пакеты:

- rhn-check
- rhn-client-tools
- rhn-setup
- rhn-setup-gnome
- rhnlib
- rhnsd
- yum-rhn-plugin

то их надо удалить.

2.1 Установка необходимых репозиториев.

```
# yum -y localinstall https://fedorapeople.org/groups/
katello/releases/yum/3.12/katello/el7/x86_64/
katello-repos-latest.rpm
# yum -y localinstall https://yum.theforeman.org/
releases/1.22/el7/x86_64/foreman-release.rpm
# yum -y localinstall https://yum.puppet.com/puppet6-
release-el-7.noarch.rpm
# yum -y localinstall https://dl.fedoraproject.org/pub
/epel/epel-release-latest-7.noarch.rpm
```

3 Инсталляция “Katello”

Внимание: перед установкой необходимо обратить внимание на возможность установки с дополнительными флагами.

```
# yum -y install foreman-release-scl
# yum -y install katello
# foreman-installer --scenario katello \
--foreman-initial-organization="Example" \
--foreman-initial-location="Latvia" \
--foreman-initial-admin-username=admin \
--foreman-initial-admin-password="Passw0rd"
Installing                               Done

[100%]
Success!
* Katello is running at https://foreman.bank.
  baltikums.com
* To install an additional Foreman proxy on separate
  machine continue by running:
```

```
foreman-proxy-certs-generate --foreman-proxy-  
  fqdn "$FOREMAN_PROXY" --certs-tar "/root/  
  $FOREMAN_PROXY-certs.tar"  
The full log is at /var/log/foreman-installer/  
  katello.log  
yum install -y -q rh-mongodb34-syspaths finished  
successfully!
```

3.1 Смена пароля

При необходимости можно сменить административный пароль:

```
# foreman-rake permissions:reset  
/usr/share/foreman/lib/foreman.rb:8: warning: already  
  initialized constant Foreman::UUID_REGEXP  
/usr/share/foreman/lib/foreman.rb:8: warning: previous  
  definition of UUID_REGEXP was here  
Reset to user: admin, password: HfWLyceWA5bdRon3
```

Если была произведена смена пароля, то в файле
“/root/.hammer/cli.modules.d/foreman.yml” также необходимо изменить па-
роль.

3.2 Добавление доменов

```
# hammer domain create --name habital.lv
```

3.3 Добавление подсетей

```
# hammer domain list  
---|-----  
ID | NAME  
---|-----  
1  | habital.lv  
---|-----  
# hammer subnet create \  
  --organizations "Example" \  
  --locations "Latvia" \  
  --name "VirtualBox Net" \  
  --network "10.0.3.0" \  
  --mask "255.255.255.0" \  
  --network-type "IPv4" \  
  --domain-ids "1"
```

3.4 Добавление продуктов

3.4.1 Создание нового продукта

```
# hammer organization list
# hammer product create \
  --name='Extra Packages for Enterprise Linux' \
  --organization-id 1 \
  --description 'Extra Packages for Enterprise Linux'
```

3.4.2 Добавление GPG-ключей

```
# hammer organization list
# wget -q https://dl.fedoraproject.org/pub/epel/RPM-
  GPG-KEY-EPEL-7 -O ~/RPM-GPG-KEY-EPEL-7
# hammer gpg create \
  --key ~/RPM-GPG-KEY-EPEL-7 \
  --name 'GPG EPEL 7' \
  --organization-id 1
```

Name	Organization	Type	Product Count	Repository Count
GPG-EPEL-7	Example	GPG Key	1	1
GPG-KEY-OEL-7	Example	GPG Key	1	4
GPG-KEY-PUPPET	Example	GPG Key	1	1

Рис. 1: Content Credentials

3.4.3 Добавление EPEL 7-репозитория

```
# hammer organization list
# hammer gpg list --organization-id 1
# hammer repository create \
  --name='EPEL 7 - x86_64' \
  --organization-id 1 \
  --product='Extra Packages for Enterprise Linux' \
  --content-type='yum' \
  --download-policy "on_demand" \
  --publish-via-http=true \
  --url=https://dl.fedoraproject.org/pub/epel/7/x86_64
  / \
  --gpg-key="GPG EPEL 7"
```

Кроме этого надо добавить ключи, репозитории для продуктов “Oracle Enterprise Linux 7”, “Puppet Client for RHEL/CentOS 7”.

Name	Description	Sync Status	Sync Plan	Repositories
<input type="checkbox"/> EPEL 7 - x86_64	Extra Packages for Enterprise Linux	Last synced 3 hours ago.	Daily Sync (daily)	1
<input type="checkbox"/> Oracle Enterprise Linux 7	Oracle Enterprise Linux 7	Last synced 3 hours ago.	Daily Sync (daily)	4
<input type="checkbox"/> Puppet Client for RHEL/CentOS 7	Puppet client repository to use with RHEL/CentOS 7	Last synced 2 hours ago.	Daily Sync (daily)	1

Рис. 2: Продукты Katello

3.4.4 Синхронизация репозиториев

После создания нескольких репозиториев их необходимо синхронизировать:

```
# hammer repository list
...
1 | EPEL 7 - x86_64      | EPEL 7 - x86_64
6 | OL7_Addons          | Oracle Enterprise Linux 7
3 | OL7_Latest          | Oracle Enterprise Linux 7
5 | OL7_Optional_Latest | Oracle Enterprise Linux 7
4 | OL7_UEKR5           | Oracle Enterprise Linux 7
2 | puppet_pc1_x86_64   | Puppet Client for RHEL/
  CentOS 7
...

# hammer product list --organization-id 1
...
1 | EPEL 7 - x86_64 | Extra Packages for Enterprise
  Linux
4 | Oracle Enterprise Linux 7 | Oracle Enterprise
  Linux 7
2 | Puppet Client for RHEL/CentOS 7 | Puppet client
  repository to use with RHEL ?CentOS 7
...

# for i in $(seq 3 6); do \
hammer repository synchronize \
--product "Oracle Enterprise Linux 7" \
--id "$i"; \
done
```

Синхронизацию можно осуществить также и через WEB-UI.

3.5 Lifecycle

Создание:

```
# hammer lifecycle-environment create \
--name "Production" \
```

```
--description "Production" \  
--prior "Library"  
--organization-id 1
```

3.6 Content View

```
# hammer content-view create \  
  --name "OEL7_content" \  
  --description "Content view for OEL7" \  
  --organization-id 1
```

3.6.1 Публикование “Content View”

```
# hammer content-view publish \  
  --name "OEL7_content" \  
  --description "Publishing repositories"
```

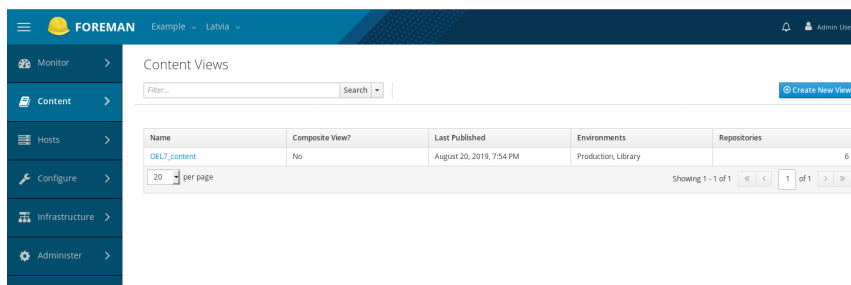


Рис. 3: Content View

3.7 Создание ключей активации

```
# hammer activation-key list --organization-id 1  
---|-----|-----|-----|  
ID | NAME | HOST LIMIT | LIFECYCLE ENVIRONMENT |  
  CONTENT VIEW  
---|-----|-----|-----|  
# hammer lifecycle-environment list  
---|-----|-----  
ID | NAME          | PRIOR  
---|-----|-----  
1  | Library      |  
2  | Production   | Library  
---|-----|-----  
# hammer content-view version list  
...  
2  | OEL7_content 1.0          | 1.0    | Library  
  ,Production
```

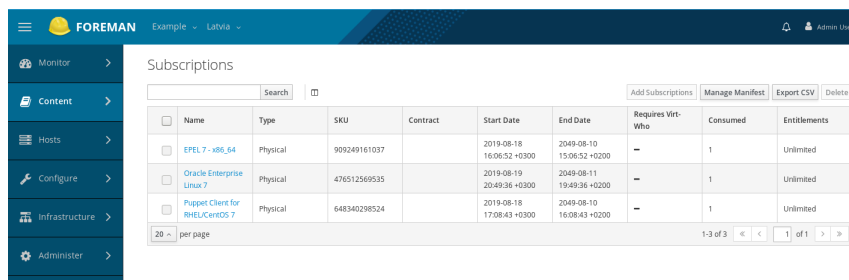
4 РЕГИСТРАЦИЯ КЛИЕНТА НА “KATELLO”-СЕРВЕРЕ

```
1 | Default Organization View 1.0 | 1.0 | Library
...
```

Создадим ключ активации для “Content View - OEL7_content”:

```
# hammer activation-key create \
--name "OEL7-key" \
--description "Key to use with OEL7" \
--lifecycle-environment "Library" \
--content-view "OEL7_content" \
--unlimited-hosts \
--organization-id 1
Activation key created.
```

Все подписки можно увидеть через WEB-UI:



Name	Type	SKU	Contract	Start Date	End Date	Requires Virt-Who	Consumed	Entitlements
EPFL 7 - x86_64	Physical	909249161037		2019-08-18 16:06:52 +0300	2049-08-10 15:06:52 +0200	-	1	Unlimited
Oracle Enterprise Linux 7	Physical	476512569535		2019-08-19 20:49:36 +0300	2049-08-11 19:49:36 +0200	-	1	Unlimited
Puppet Client for RHEL/CentOS 7	Physical	648340298524		2019-08-18 17:08:43 +0300	2049-08-10 16:08:43 +0200	-	1	Unlimited

Рис. 4: Subscriptions

4 Регистрация клиента на “Katello”-сервере

На стороне клиента надо проверить, что установлен “subscription-manager”:

```
# yum install subscription-manager
```

А также:

```
# yum install -y https://yum.theforeman.org/client
/1.22/el7/x86_64/foreman-client-release.rpm
# curl --insecure --output katello-ca-consumer-latest.
noarch.rpm https://foreman.habital.lv/pub/katello-
ca-consumer-latest.noarch.rpm
# yum localinstall katello-ca-consumer-latest.noarch.
rpm
# yum install katello-agent
```

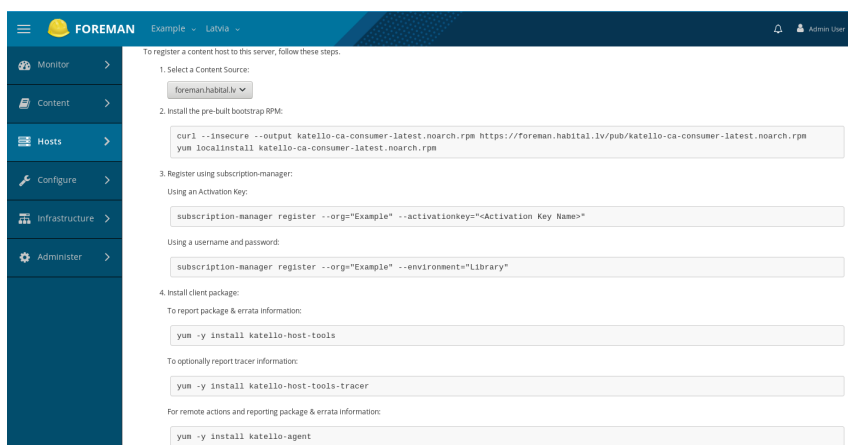



Рис. 5: Katello Content Host Registration

Если используется виртуализация на основе “VmWare”, “Hyper-V”, “Xen”, “VDSM” или “RHEVM”, то надо установить на гостевые узлы пакет “virt-who” и его настроить (см. <https://access.redhat.com/labsinfo/virtwhoconfig>). В связи с тем, что система “Katello” устанавливалась на VirtualBox, настройка пакета “virt-who” не проводилась.

После успешной регистрации “Katello”-сервера и гостевых узлов эти узлы можно сразу увидеть в “Content Hosts”:

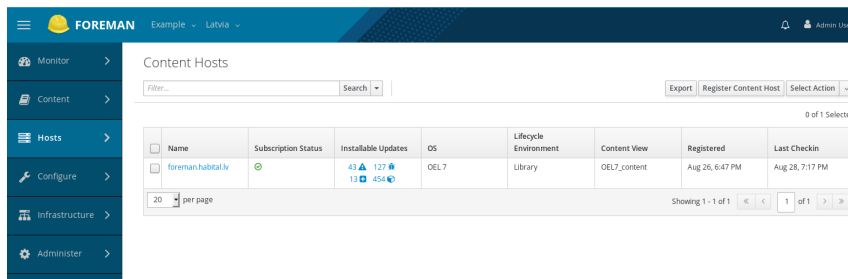


Рис. 6: Content Hosts

5 Модули для “Puppetserver”

На сайте <https://forge.puppet.com/> можно найти готовые модули для puppetserver.

5.1 Модуль “ntp”

Для проверки работы модулей можно с вышеуказанного сайта выбрать модуль ‘ntp’ и установить его:

```
# puppet module install puppetlabs-ntp --version 8.0.0
```

```
Notice: Preparing to install into /etc/puppetlabs/code
  /environments/production/modules ...
Notice: Downloading from https://forgeapi.puppet.com
...
Notice: Installing -- do not interrupt ...
/etc/puppetlabs/code/environments/production/modules
|-- puppetlabs-ntp (v8.0.0)
   |-- puppetlabs-stdlib (v6.0.0)
```

Изменим содержимое файла “site.pp” на следующее:

```
class { 'ntp':
  servers => [ '0.pool.ntp.org', '1.pool.ntp.org' ],
  restrict => [
    'default ignore',
    '-6 default ignore',
    '127.0.0.1',
    '-6 ::1',
  ],
}

include ntp
```

и на хосте с “puppet-агентом” принудительно пересчитаем “pp-файл”:

```
# puppet agent -t
```

После добавления модуля следует пересчитать содержимое (рис.7, 8):

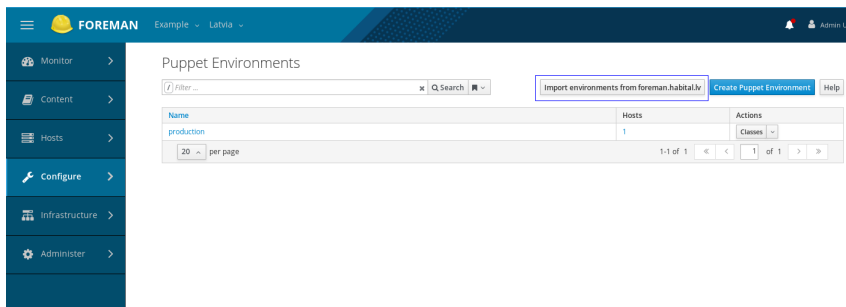


Рис. 7: Puppet environments

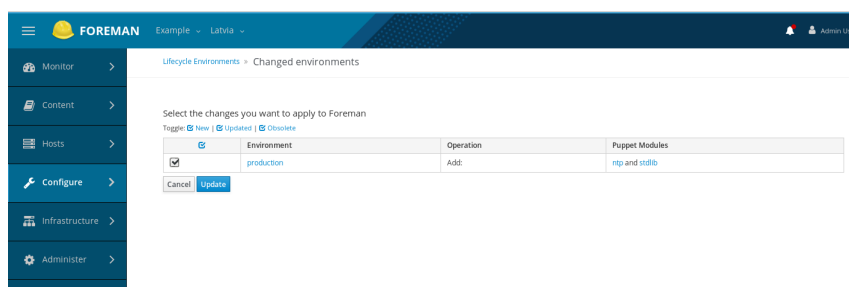


Рис. 8: Puppet change

5.2 Удаление модуля

Для начала надо проверить список установленных модулей:

```
# puppet module list /etc/puppetlabs/code/environments
  /production/modules
|--- puppetlabs-apache (v5.0.0)
|--- puppetlabs-concat (v6.1.0)
|--- puppetlabs-ntp (v8.0.0)
|--- puppetlabs-stdlib (v6.0.0)
|--- puppetlabs-translate (v2.0.0)
/etc/puppetlabs/code/environments/common (no modules
  installed)
/etc/puppetlabs/code/modules (no modules installed)
/opt/puppetlabs/puppet/modules (no modules installed)
/usr/share/puppet/modules (no modules installed)
# puppet module uninstall puppetlabs-ntp
Notice: Preparing to uninstall 'puppetlabs-ntp' ...
Removed 'puppetlabs-ntp' (v8.0.0) from /etc/puppetlabs
  /code/environments/production/modules
```

6 Установка плагина “Remote Execution”

Для возможности удалённого выполнения команд надо добавить плагин “Remote Execution”. Он может устанавливаться как при исходной установке, так и после.

```
# foreman-installer \
--enable-foreman-plugin-remote-execution \
--enable-foreman-proxy-plugin-remote-execution-ssh
Preparing installation Done

Success! * Katello is running at https://foreman.
habital.lv * To install an additional Foreman
proxy on separate machine continue by running:
foreman-proxy-certs-generate --foreman-proxy-
fqdn "$FOREMAN_PROXY" --certs-tar "/root/
```

```
$FOREMAN_PROXY-certs.tar" The full log is
at /var/log/foreman-installer/katello.log
```

6.1 Настройка ключей SSH

На сервере надо создать пару ключей “SSH”:

```
# cd /usr/share/foreman-proxy/.ssh
# sudo -u foreman-proxy ssh-keygen \
-f ~foreman-proxy/.ssh/id_rsa_foreman_proxy -N ''
```

При наличии уже имеющихся ключей их надо будет обновить. В случае, если включен “SELinux”, надо выполнить команду:

```
# restorecon -RvF ~foreman-proxy/.ssh
```

После чего выполнить рестарт “httpd”, “foreman-tasks” и “foreman-proxy”, а также скопировать публичный ключ на удалённые хосты:

```
# ssh-copy-id -i ~foreman-proxy/.ssh/
id_rsa_foreman_proxy.pub \ root@remotehost.habital.
lv
```

Затем следует проверить на “Katello”-сервере в WEB-UI, что добавлены “Dynflow” и “SSH”:

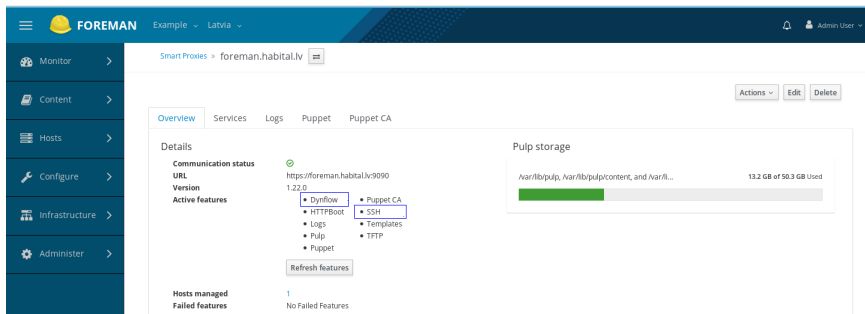


Рис. 9: SmartProxies