Foreman-Puppet, Foreman-Ansible

-
-
- Puppet
  -
    -
    - (locales)
    - Puppet Server
- Puppet Agent
  -
  -
  - ssh
  -
- Ansible Foreman
  - /etc/ansible/hosts
  - Foreman
-
  - Foreman + Puppet
  - Foreman + Ansible
- ansible foreman
- SSH
-
-

:

- Astra Linux Special Edition .10015-01 (1.7), .10015-10
- Astra Linux Special Edition .10015-17
- Astra Linux Special Edition .10015-37 (7.7)
- Astra Linux Special Edition .10152-02 (4.7)
- Astra Linux Common Edition 2.12.30

Astra Linux Special Edition .10015-01 x.7 (. Astra Linux Special Edition x.7: ,).

Foreman , , web- apache2.
, FreeIPA (. FreeIPA Astra Linux).

, : *foreman*, *puppet*, *ansible*.

- **Foreman** - , , (Ansible, Puppet .) . Foreman web-, API CLI, , . .
- **Puppet** - , , . ;
- **Ansible** - , . , , . ;

: 10.0.2.120 master.astra.lan

: 10.0.2.121 agent1.astra.lan

, . , , SSH.

DNS-, IP- /etc/hosts .

3 .

Puppet

Puppet Server Puppet Agent , . :

- DNS;
- */etc/hosts* ( ).

master.astra.lan. ( ):

```
sudo hostnamectl set-hostname master.astra.lan
```

/et/hosts. IP- (10.0.2.120) (master.astra.lan, master puppet). /etc/hosts :

```
127.0.0.1 localhost
10.0.2.120 master.astra.lan master puppet
10.0.2.121 agent1.astra.lan agent1
# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

, IP- 10.0.2.120, - 10.0.2.121.

(locales)

en_US.utf8 :

```
locale -a | grep en_US.utf8
```

en_US.utf8 , ,

```
echo "en_US.UTF-8 UTF-8" | sudo tee -a /etc/locale.gen
sudo locale-gen
```

, en_US.UTF-8 UTF-8 , , :

```
sudo apt update
sudo dpkg-reconfigure locales
```

Puppet Server

> Astra Linux Special Edition x.7.0 x.7.1 , 2022-0819SE17 (1.7.2) astra-ce (. Astra Linux Special Edition x.7: ,).

:

```
sudo apt update
sudo apt install openjdk-11-jre-headless puppetserver
```

openjdk-11-jre-headless , .

Puppet Server IP- 8140. , . ufw:

```
sudo ufw allow 8140
```

Puppet Server :

```
sudo systemctl enable puppetserver
sudo systemctl start puppetserver
```

:

```
systemctl status puppetserver
```

Puppet Agent

IP- (- 10.0.2.121)

:

```
sudo hostnamectl set-hostname agent1.astra.lan
```

/etc/hosts. /etc/hosts :

```
127.0.0.1 localhost
10.0.2.121 agent1.astra.lan agent1
10.0.2.120 master.astra.lan master puppet

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

/etc/hosts .

- (SSH):

```
sudo apt update
sudo apt install puppet-agent ssh
```

/etc/puppetlabs/puppet/puppet.conf, :

```
server = master.astra.lan
show_diff = true
```

, Puppet Server, IP- 8140. , . ufw:

```
sudo ufw allow 8140
```

Puppet Agent :

```
sudo systemctl enable puppet
sudo systemctl start puppet
```

ssh

ssh:

1. :

   ```
   sudo useradd -m <_>
   ```

   -m . (/etc/ansible/hosts);

2. :

   ```
   sudo passwd <_>
   ```

3. sudo. /etc/sudoers.d/<_> ALL=NOPASSWD: ALL:

   ```
   echo "<_>   ALL=NOPASSWD:   ALL" | sudo tee -a /etc/sudoers.d/<_>
   ```

root . root root ssh. root ssh /etc/ssh/sshd_config PermitRootLogin, yes SSH ( ):

```
sudo passwd root
sudo sed -i 's/#PermitRootLogin prohibit-password/PermitRootLogin yes
/' /etc/ssh/sshd_config
sudo systemctl restart sshd
```

Puppet Agent Puppet Server . :

```
sudo /opt/puppetlabs/bin/puppetserver ca list
```

```
Requested Certificates: agent1.astra.lan (SHA256) F7:D5:E5:AB:AA:86:7F:EF:
19:3D:D9:B9:E3:E9:63:DC:AE:31:17:57:67:3D:2B:D7:A5:1C:71:E3:46:E0:A7:1E
```

, agent1.astra.lan.

:

```
sudo /opt/puppetlabs/bin/puppetserver ca sign --certname agent1.astra.lan
```

```
Successfully signed certificate request for agent1.astra.lan
```

:

1.

```
sudo systemctl stop puppet
```

2. , :

```
sudo /opt/puppetlabs/bin/puppet agent --test
```

```
Info: csr_attributes file loading from /etc/puppetlabs/puppet
/csr_attributes.yaml
Info: Creating a new SSL certificate request for agent1.astra.lan
Info: Certificate Request fingerprint (SHA256): F7:D5:E5:AB:AA:86:7F:EF:
19:3D:D9:B9:E3:E9:63:DC:AE:31:17:57:67:3D:2B:D7:A5:1C:71:E3:46:E0:A7:1E
Info: Downloaded certificate for agent1.astra.lan from puppet
Info: Using configured environment 'production'
Info: Retrieving pluginfacts Info: Retrieving plugin
Info: Retrieving locales
Info: Caching catalog for agent1.astra.lan
Info: Applying configuration version '1568370748'
Info: Creating state file /opt/puppetlabs/puppet/cache/state/state.yaml
Notice: Applied catalog in 0.02 seconds
```

3. :

```
sudo systemctl start puppet
```

Ansible Foreman

Ansible Foreman, :

ansible :

```
sudo apt install ansible
```

/etc/ansible/hosts

/etc/ansible/hosts, [agents] (.. , agents). agent1.astra.lan IP- 10.0.2.121:

```
echo -e "agents:\n hosts:\n  agent1.astra.lan:\n   ansible_user: <_>" |
sudo tee -a /etc/ansible/hosts
```

ansible_user <_> , .
/etc/ansible/hosts (- username):

```
agents:
 hosts:
  agent1.astra.lan:
   ansible_user: username
```

YAML- . ( ) . .

Ansible ssh , :

```
ssh-keygen -f ~/.ssh/id_rsa -N ''
```

, ansible. ansible sudo, sudo ( ).

, , :

```
ssh-copy-id -i ~/.ssh/id_rsa <_>@agent1.astra.lan
```

Ansible, agents:

```
ansible -m ping agents
```

```
agent1.astra.lan | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
```

Foreman

:

, , shared-mime-info, :

```
sudo apt install shared-mime-info
```

foreman-installer:

```
sudo apt install foreman-installer
```

, /etc/debian_version 9.0, , , 9.0.

:

"Initial credentials are admin / ...." admin web-, web-. :

```
sudo foreman-rake permissions:reset username=admin password=<_>
```

```
sudo foreman-installer
```

```
Preparing installation Done *
Foreman is running at https://master.astra.lan
Initial credentials are admin / NRLJth9ufmAkTsF5 *
Foreman Proxy is running at https://master.astra.lan:8443 *
Puppetmaster is running at port 8140 The full log is at /var/log/foreman-
installer/foreman.log
```

"Initial credentials are admin / ...." admin web-, web-.

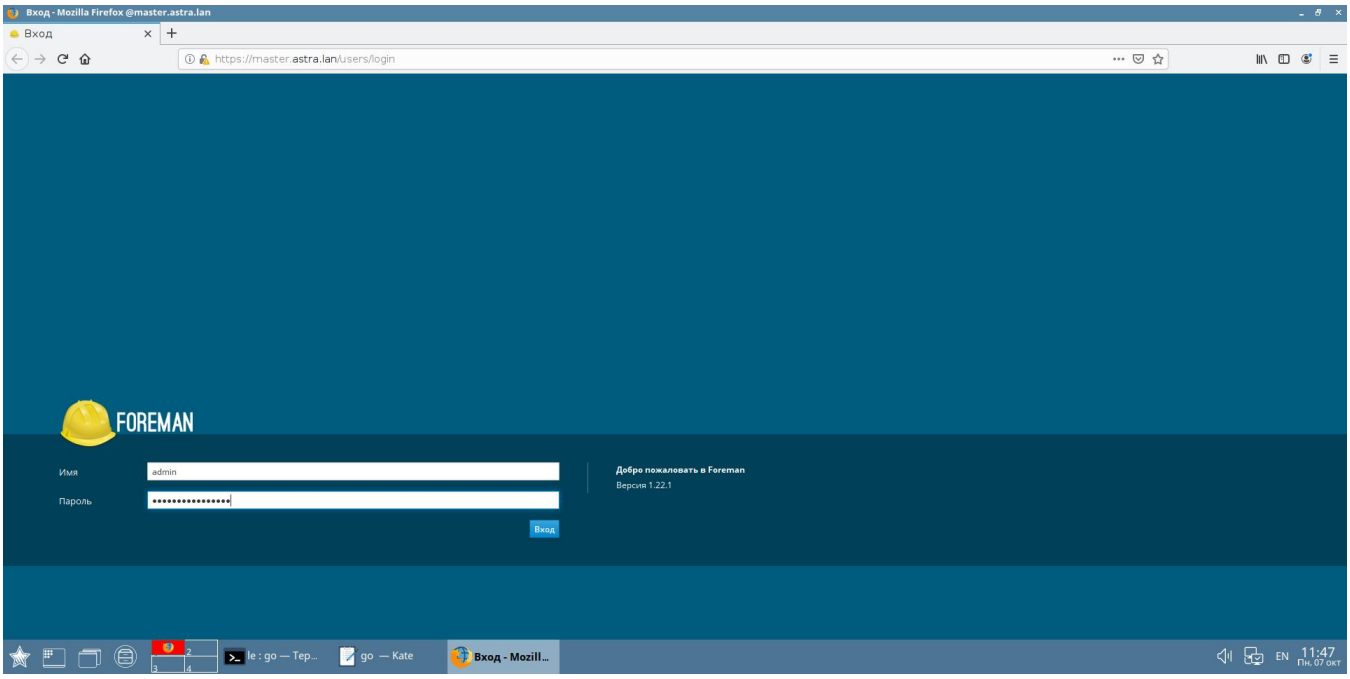
foreman-proxy:

```
sudo curl -k -X GET -H Accept:application/json https://master.astra.lan:8443
/features --tlsv1
```

```
["httpboot","logs","puppet","puppetca","tftp"]
```

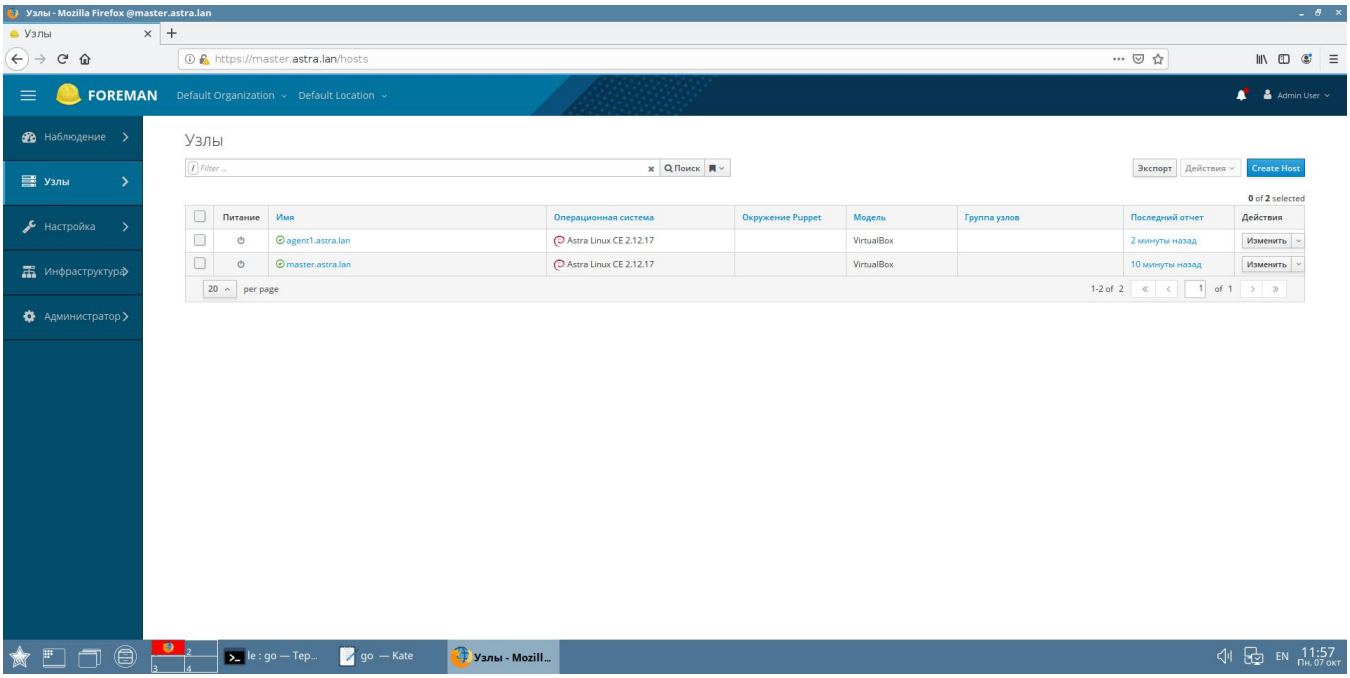
Foreman + Puppet

https://master.astra.lan ( )



admin , .

"" - "All hosts" ("Hosts" -> "All Hosts"), :



, , , () :

```
sudo systemctl restart puppet
```

web-.

, "" - "" ("Infrastructure" -> "Smart Proxies") proxy. proxy , :

- "" - "" ("Administer" - "Locations");
  - Default location;
  - " " ("Fix mismatches");
  - "" ("Submit");

- "" - "" ("Administer" - "Organizations");
    - Default organization;
    - " " ("Fix mismatches");
- "" ("Submit");

"" - "" ("Infrastructure" -> "Smart Proxies") proxy.

Foreman + Ansible

:

- Ansible: *foreman-plugin-ansible*, *foreman-proxy-plugin-ansible*;
- Ansible playbooks : *foreman-plugin-remote-execution*, *foreman-proxy-plugin-remote-execution-ssh*

```
sudo foreman-installer --enable-foreman-plugin-ansible \
--enable-foreman-proxy-plugin-ansible \
--enable-foreman-plugin-remote-execution \
--enable-foreman-proxy-plugin-remote-execution-ssh
```

(foreman-proxy,):

```
sudo -u foreman-proxy ssh-keygen -f ~foreman-proxy/.ssh
/id_rsa_foreman_proxy -N ''
sudo -u foreman-proxy ssh-copy-id -i ~foreman-proxy/.ssh
/id_rsa_foreman_proxy <_>@agent1.astra.lan
```

Ansible playbook. Ansible playbook ( ):

1. ():
    a. "" ("" -> "All Hosts");
    b. ;
    c. "" -> "Scheduled Remote Job";
2. :
    a. "" ("" -> "All Hosts");
    b. "Scheduled Remote Job" -> "Run Ansible roles";
3. :
    a. " "
    b. ""

ansible -. :

1. "Ansible roles" ("" -> "")
2. .

ansible foreman

ansible foreman:

1. Astra Linux Common Edition 2.12 (python2) ansible (/etc/ansible/hosts) :

```
ansible_python_interpreter: /usr/bin/python3

agents:
 hosts:
  client.astra.lan:
   ansible_user: vagrant
  client2.astra.lan: # ALSE 1.7
   ansible_user: vagrant
  alce.astra.lan: # ALCE 2.12.44
   ansible_user: vagrant
   ansible_python_interpreter: /usr/bin/python3
```

ansible (.) :

```
"module_stderr": "Shared connection to alce.astra.lan closed.\r\n",
    "module_stdout": "/bin/sh: /usr/bin/python:     \r\n",
    "msg": "MODULE FAILURE\nSee stdout/stderr for the exact error",
```

2. /etc/ansible/ansible.cfg:
   a. [defaults] :

```
bin_ansible_callbacks = True
callback_whitelist = foreman
```

:

```
sudo sed -i "/\[defaults\]/a bin_ansible_callbacks =
True\ncallback_whitelist = foreman" /etc/ansible/ansible.cfg
```

   b. [callback_foreman] :

```
[callback_foreman]
url = https://`hostname`
ssl_cert = /etc/puppetlabs/puppet/ssl/certs/master.astra.lan.pem
ssl_key = /etc/puppetlabs/puppet/ssl/private_keys/master.astra.lan.pem
verify_certs = /etc/puppetlabs/puppet/ssl/certs/ca.pem
```

:

```
echo "[callback_foreman]
url = https://`hostname`
ssl_cert = /etc/puppetlabs/puppet/ssl/certs/master.astra.lan.pem
ssl_key = /etc/puppetlabs/puppet/ssl/private_keys/master.astra.lan.
pem
verify_certs = /etc/puppetlabs/puppet/ssl/certs/ca.pem" | sudo tee
-a  /etc/ansible/ansible.cfg
```

/etc/foreman-proxy/ansible.cfg;

3. foreman , : "" - "" - " " - "Trusted hosts":List of hostnames, IPv4, IPv6 addresses or subnets to be trusted in addition to Smart Proxies for access to fact/report importers and ENC output. (python). (Classless Inter-Domain Routing, CIDR), 10.2.0.0/24;

4. :

```
sudo ansible -m setup localhost
```

foreman (- localhost). , :

```
sudo ansible -m setup client.example.com
```

(- client.example.com)

SSH

, . , .

ssh ssh-copy-id sshpass (sshpass). :

```
sudo apt install sshpass
```

:

1. :

```
touch <_>
```

2. , :

```
chmod 600 <_>
```

3. , ;
4. , , :

```
sshpass -f <_> ssh-copy-id -i ~/.ssh/id_rsa <_>@agent1.`hostname -d` -o
StrictHostKeyChecking=no
```

```
sudo -u foreman-proxy sshpass -f <_> ssh-copy-id -i ~foreman-proxy/.ssh
/id_rsa_foreman_proxy <_>@agent1.astra.lan -o StrictHostKeyChecking=no
```

:

-f <_> ;
-o StrictHostKeyChecking=no ;

sshpass . :

```
man sshpass
```

. Ansible Puppet.

:

foreman :

> /usr/share/foreman/vendor/ruby/2.3.0/gems/pg-1.1.4/lib/pg.rb:56:in `initialize': could not connect to server: No such file or directory (PG::ConnectionBad)

:

/etc/postgresql//main/postgresql.conf*, **listen_addresses '*'**.

:

```
sudo systemctl restart postgresql foreman
```

:

puppetserver.service. /var/log/syslog :

```
puppetserver[10217]: Execution error (Error) at puppetlabs.services.master.master-core/validate-memory-
requirements! (master_core.clj:1279).
puppetserver[10217]: Not enough available RAM (1 860MB) to safely accommodate the configured JVM heap size
of 1 963MB. Puppet Server requires at least 2 159MB of available RAM given this heap size, computed as 1.1 *
max heap (-Xmx). Either increase available memory or decrease the configured heap size by reducing the -Xms
and -Xmx values in JAVA_ARGS in /etc/sysconfig/puppetserver on EL systems or /etc/default/puppetserver on
Debian systems.
```

:

3 ( ).