Opis demonstracije

Automatizacija i orkestracija procesa na poslužiteljima

Zagreb, 30.08.2024.

**Sadržaj**

[1. CILJ POSTUPKA / DEMONSTRACIJE 2](#_Toc178149682)

[2. OPIS POSTUPKA / DEMONSTRACIJE 2](#_Toc178149683)

[Instalacija Ansible alata 2](#_Toc178149684)

[Organizacija projekta 2](#_Toc178149685)

[Ansible konfiguracija 2](#_Toc178149686)

[Konfiguracija pomoćnih alata 3](#_Toc178149687)

[Konfiguracija ciljanog poslužitelja 3](#_Toc178149688)

[Postavke ciljanog poslužitelja 3](#_Toc178149689)

[Playbook 4](#_Toc178149690)

# CILJ POSTUPKA / DEMONSTRACIJE

Upoznavanje s pripremom okoline za korištenje Ansible alata i rad s istim.

# OPIS POSTUPKA / DEMONSTRACIJE

## Instalacija Ansible alata

Naredba za instalaciju paketa:

# apt install ansible ansible-lint

## Organizacija projekta

$ tree -a .

.

├── ansible.cfg

├── .ansible-lint

├── host\_vars

│ └── bootcamp.yml

├── inventory

├── site.yml

└── .yamllint

2 directories, 6 files

## Ansible konfiguracija

Sadržaj datoteke ***ansible.cfg***:

[defaults]

inventory = inventory

interpreter\_python = auto\_silent

retry\_files\_enabled = no

no\_target\_syslog = yes

## Konfiguracija pomoćnih alata

Sadržaj datoteke ***.yamllint***:

---

rules:

line-length: disable

truthy:

allowed-values:

- "yes"

- "no"

check-keys: true

Sadržaj datoteke ***.ansible-lint***:

---

profile: production

exclude\_paths:

- .yamllint

## Konfiguracija ciljanog poslužitelja

Sadržaj datoteke ***inventory***:

bootcamp ansible\_host=<IP adresa ili hostname> ansible\_become\_method=su ansible\_become\_flags=-

## Postavke ciljanog poslužitelja

Sadržaj datoteke ***host\_vars/bootcamp.yml***:

---

ldap\_base\_dn: dc=example,dc=com

ldap\_admin\_name: <po izboru>

ldap\_admin\_username: <po izboru>

ldap\_admin\_password: <po izboru>

aosi\_allowed\_ip\_addrs:

- 192.168.122.0/24

aai\_package\_config:

- openldap-aai aai/mode select standalone

- openldap-aai aai/adminpw password {{ ldap\_admin\_password }}

- freeradius-aai aai/use-eduroam boolean false

- aosi-aai aosi/mode select standalone

- aosi-aai aosi/adminpw password {{ ldap\_admin\_password }}

- aosi-aai aosi/validusers string {{ ldap\_admin\_username }}

- certs-aai certs-aai/certificate string /etc/ssl/certs/bootcamp.pem

- certs-aai certs-aai/key string /etc/ssl/private/bootcamp.key

- certs-aai certs-aai/trusted\_certificate boolean true

- libcertify-aosi-aai libcertify-aosi-aai/enable boolean true

## Playbook

Sadržaj datoteke ***site.yml***:

---

- name: Setup server for CARNET services

hosts: bootcamp

become: yes

tasks:

- name: APT sources cleanup

ansible.builtin.lineinfile:

path: /etc/apt/sources.list

search\_string: "deb cdrom:"

state: absent

- name: Install required packages

ansible.builtin.apt:

name:

- vim

- gnupg

- python3-cryptography

- python3-ldap

- debconf-utils

state: present

update\_cache: yes

- name: Install SRCE repository signing key

ansible.builtin.apt:

deb: "https://ftp.srce.hr/srce-debian/pool/main/s/srce-keyring/srce-keyring\_2022.12.12+srce11u1\_all.deb"

- name: Configure SRCE repository

ansible.builtin.copy:

dest: /etc/apt/sources.list.d/srce.list

content: "deb http://ftp.srce.hr/srce-debian srce-bullseye main\n"

mode: "0644"

- name: Create private key

community.crypto.openssl\_privatekey:

path: /etc/ssl/private/bootcamp.key

- name: Create certificate signing request

community.crypto.openssl\_csr\_pipe:

privatekey\_path: /etc/ssl/private/bootcamp.key

common\_name: bootcamp.example.com

organization\_name: Bootcamp

subject\_alt\_name:

- DNS:bootcamp.example.com

register: bootcamp\_csr

- name: Create certificate

community.crypto.x509\_certificate:

path: /etc/ssl/certs/bootcamp.pem

csr\_content: "{{ bootcamp\_csr.csr }}"

privatekey\_path: /etc/ssl/private/bootcamp.key

provider: selfsigned

- name: Configure AAI packages

ansible.builtin.command:

cmd: debconf-set-selections

stdin: "{{ item }}"

stdin\_add\_newline: no

loop: "{{ aai\_package\_config }}"

changed\_when: yes

no\_log: yes

- name: Install AAI packages

ansible.builtin.apt:

name:

- openldap-aai

- freeradius-aai

- aosi-aai

- aosi-www-aai

update\_cache: yes

- name: Allow IP addresses for AOSI web interface # noqa: no-tabs

ansible.builtin.blockinfile:

path: /etc/aosi-www/apache.conf

insertbefore: </Directory>

prepend\_newline: yes

marker: "\t# {mark} ANSIBLE MANAGED BLOCK - additionally allowed IP addresses"

block: |

{% for ip in aosi\_allowed\_ip\_addrs -%}

{{ "Allow from %s" | format(ip) | indent(8, true) }}

{% endfor %}

notify: Reload Apache configuration

- name: Encrypt LDAP admin user password

ansible.builtin.command:

cmd: slappasswd -s {{ ldap\_admin\_password }}

register: ldap\_admin\_password\_encrypted

changed\_when: yes

- name: Create LDAP admin user

community.general.ldap\_entry:

dn: uid={{ ldap\_admin\_username }},{{ ldap\_base\_dn }}

objectClass:

- person

- organizationalPerson

- inetOrgPerson

- hrEduPerson

attributes:

uid: "{{ ldap\_admin\_username }}"

hrEduPersonHomeOrg: example.com

hrEduPersonUniqueID: "{{ ldap\_admin\_username }}@example.com"

hrEduPersonPersistentID: "{{ '%s@example.com.%s' | format(ldap\_admin\_username, ansible\_date\_time.epoch) | md5 }}"

hrEduPersonOIB: "00000000000"

hrEduPersonUniqueNumber: "OIB: 00000000000"

hrEduPersonAffiliation: djelatnik

hrEduPersonPrimaryAffiliation: djelatnik

hrEduPersonRole: administrator imenika

hrEduPersonExpireDate: NONE

userPassword: "{{ ldap\_admin\_password\_encrypted.stdout }}"

givenName: "{{ (ldap\_admin\_name | split(' '))[0] }}"

sn: "{{ (ldap\_admin\_name | split(' '))[1] }}"

cn: "{{ ldap\_admin\_name }}"

mail: "{{ ldap\_admin\_username }}@example.com"

handlers:

- name: Reload Apache configuration

ansible.builtin.systemd:

name: apache2

state: reloaded