PRA TEST PROJECT
MODUL C - Infrastructure Programmability & Automation

IT NETWORK SYSTEMS ADMINISTRATION

KELOMPOK INFORMATION AND COMMUNICATION TECHNOLOGY

Dokumen ini merupakan Pra-Test Project yang menjadi subject perubahan maksimal 30% untuk Actual Test Project. Pelaksanaan kompetisi LKS Nasional nanti akan menggunakan Actual Test Project yang akan dipublikasi pada saat kompetisi. Perubahan itu meliputi Topology, Functionality, Aplikasi dan Task yang diminta.

Introduction

This Test Project consists of the following documentation/files:

- ITNSA_MC_PRA_en.docx
- hosts (on HOST VM: /etc/ansible)
- users.csv (on HOST VM: /etc/ansible)
- .vault_pass (on HOST VM: /etc/ansible)
- customers.json (on HOST VM: /etc/ansible)

Accurate and up-to-date documentation has always been a challenge in IT. With multiple engineers working on the same systems, it is hard to keep track of who changed what. Applix Corporation decided to fix this problem and hired you to modernize, harden and extend their infrastructure.

Documentations

The following documentations installed to DEV VMs. You can use it with Zeal Docs.

- Ansible (version 2.10.8)
- Python 3 (version 3.9.2)
- Jinja (version 2.11.3)

Description of Project and Tasks

You will be migrating VMs to Infrastructure as Code (IaC) and simplify the process of creating new services. You have access to development VMs (DEV-LIN). These VMs can be used for developing and testing your work.

Login for all VMs and Devices:

Linux

Username	: root/debian
Password	: P@ssw0rd

Windows

Username	: administrator/user
Password	: P@ssw0rd

All VMs and devices are connected to the management network (10.22.0.0/24) and have a statically configured IP address. All IP addresses in network table will not change for marking. The management network will be used for configuring the different hosts. You can login using username and password over SSH or WinRM.

You may install any additionally required packages and features on the VMs.

Instructions to the Competitor

Part 1. Linux

Use Ansible to configure the Linux hosts LIN[1-4] from HOST VM. there is preconfigured hosts file located under /etc/ansible/hosts. Do not change this file. Before assessment all LIN[1-4] VMs will be reset to original state and the LIN[1-4] VMs will be randomly removed and added to different groups in the hosts file. For marking, all playbooks will be run in order using the command “ansible-playbook playbookname.yml” in the /data/ansible/linux directory.

Variables like “hostname”, “webport” and “webcolor” in /etc/ansible/hosts are subject to change for marking.

General

- Create a directory /data/ansible/linux
  - Place all playbooks directly inside this directory.
  - Feel free to create any additional folders or files you might need within this directory for executing the playbooks again.
  - When you run the playbooks for the second time, every task should either be in the “ok” state or be “skipped.”
  - For security, use the /etc/ansible/.vault_pass file to encrypt the ansible username and password, ensuring they are automatically decrypted when the playbooks are executed.

Hostname

- Create a playbook called 1-hostname.yml for configuring the hostname
  - Every host should be assigned a hostname, derived from the “hostname” variable found in the /etc/ansible/hosts file.

nftables

- Create a playbook called 2-nftables.yml for filtering incoming traffic on all LIN hosts.
  - By default, incoming packets should be dropped.
  - Allow minimal traffic for the services to work
  - Configure a list named “trusted” which contains HOST VM and DEV VMs and use it in the firewall rules
  - For members of the “trusted” list, permit SSH and ICMP traffic to the LIN hosts.
  - Ensure that nftables configurations remain intact even after system reboots.

DNS

- Create a playbook called 3-dns-server.yml for configuring at least two DNS servers
  - Install a DNS service on all hosts in the group “dns”
  - The first host in “dns” group should be master for the domain “applix.com”
  - All other hosts in this group should be slave DNS servers for domain “applix.com”
  - Ensure every host listed in /etc/ansible/hosts has an A record for <hostname>.applix.com.
  - The domain intranet.applix.com must point to 10.22.0.51.
- Create a playbook called 4-dns-client.yml
  - Make sure, that all LIN Servers and HOST use first DNS host as primary DNS server and all slave DNS servers as secondary nameserver
  - Set the DNS suffix to “applix.com”.

Web

- Create a playbook called 5-web-server.yml for configuring two or more web servers
- Install a web service on all hosts in the group “web”
  - The local website should listen on port “webport” variable in /etc/ansible/hosts
  - Display the following content with textcolor based on the “webcolor” variable in /etc/ansible/hosts file

```
“Hello from <hostname> !”
```

- Create a virtual host listening on port 8081 called “intranet.applix.com” displaying the following content

```
“Welcome to the intranet of Applix”
“This site was served by <hostname>”
```

High availability intranet

- Create a playbook called 6-ha-intranet.yml for configuring two or more HA servers
- Install keepalived and HAProxy on all hosts in the group “ha”
  - Configure 10.22.0.51 as floating IP and use the last host in “ha” group as VRRP master
  - If the master fails, the second last server in the ha group should take over and so on (priority in reverse order)
  - Use password authentication
  - Configure HAProxy to load balance “http://intranet.applix.com” between all available web servers using round robin
    - Add Header “x-haproxy-host” with the hostname of current HAProxy host

Users

- Create a playbook called 7-users.yml for importing users on all LIN hosts
  - Import the users from /etc/ansible/users.csv on all LIN hosts
  - Make sure, that password is not changed if there is already an existing user with same username and UID

Part 2. Windows

Use Ansible for configuring the Windows hosts, labeled as WIN, from the HOST VM. A pre-configured hosts file is already available at /etc/ansible/hosts. This file should remain unchanged. For evaluation purposes, all playbooks will be executed in sequence using the command “ansible-playbook playbookname.yml” within the /data/ansible/windows directory.

General

- Create a directory /data/ansible/windows
  - All playbooks should be located at the root of this directory
  - You are free to create folders/files in this directory for running the playbooks
  - Make sure ansible username, password and certificate secrets are encrypted and automatically decrypted when running the playbooks

Hostname

- Create a playbook called 1-hostname.yml for configuring the hostname
  - All hosts should receive the hostname based on the “hostname” variable in /etc/ansible/hosts file

Security and logging

- Create a playbook called 2-sec-log.yml for configuring security settings
  - Stop and disable the Remote Desktop Service on all Windows hosts

Customer Deployments

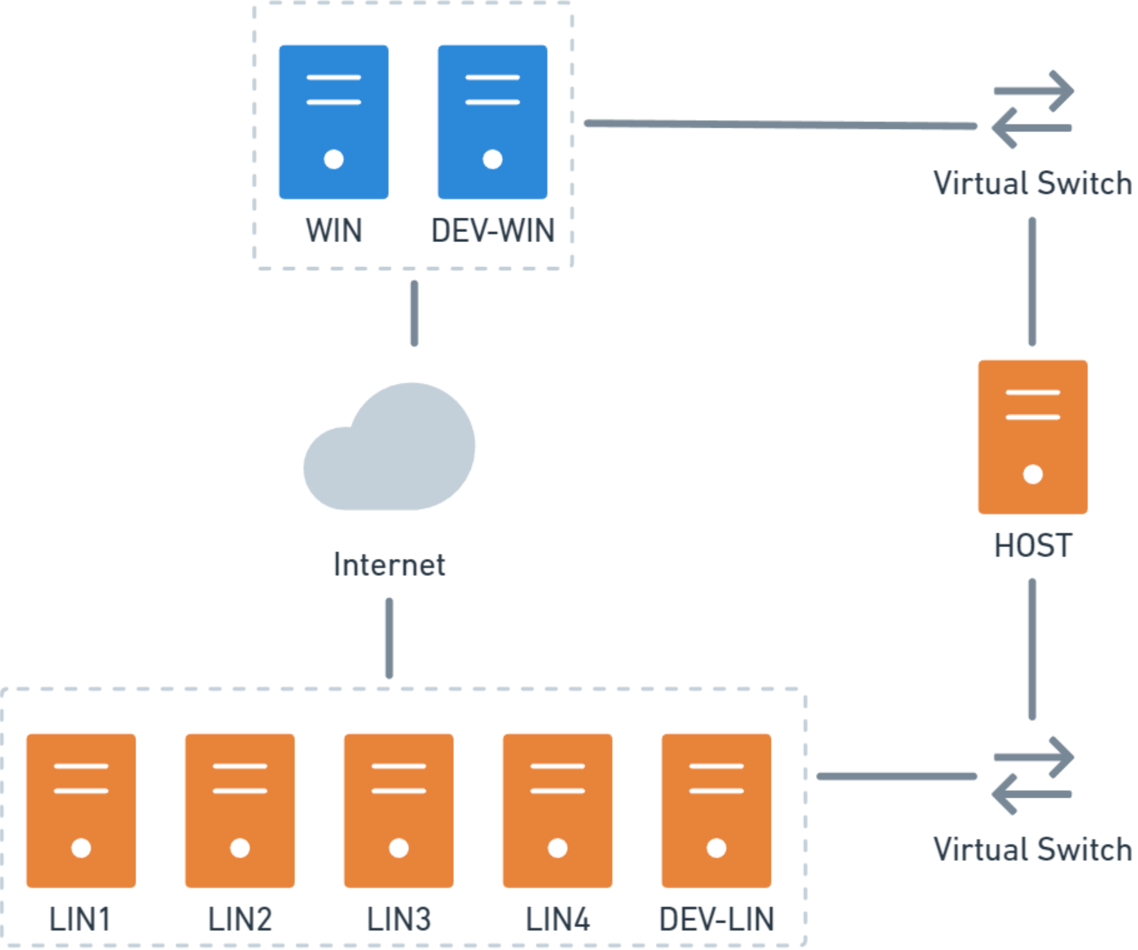
- Create a playbook called 3-environment.yml for installing the customer environment
  - Configure all servers in group “dc” as DNS servers on all WIN hosts
  - Configure all servers in group “dc” as domain controller
    - Use customers.com as domain name
    - Use “P@ssw0rd” as safe password
  - Install IIS feature in group “iis”
- Create a playbook called 4-customers.yml for deploying customer web environments
  - For each customer in /etc/ansible/customers.json file
    - Create an OU based on “name” attribute
    - Create an AD user based on “username” and “password” attribute in this OU
    - Create a DNS entry for domain_prefix.customers.com pointing to a random IIS server and use domain_prefix as randomization seed
    - Create a virtual host listening on port 80 on the selected IIS server which displays the “message” attribute

Equipment, machinery, installations, and materials required

Network table

ID	IP	OS	DESCRIPTION
DEV-LIN	10.22.0.251	Debian 11.7 (GNOME)	Development VM with the following software installed: - Python3
DEV-WIN	10.22.0.252	Windows 10 Enterprise LTSC	Development VM with the following software installed: - Python3
HOST	10.22.0.50	Debian 11.7	Host Server
LIN1	10.22.0.1	Debian 11.7	Dynamic Config
LIN2	10.22.0.2	Debian 11.7	Dynamic Config
LIN3	10.22.0.3	Debian 11.7	Dynamic Config
LIN4	10.22.0.4	Debian 11.7	Dynamic Config
LIN5	10.22.0.5	Debian 11.7	Dynamic Config
WIN	10.22.0.101	Windows Server 2019	Dynamic Config

Topology


WIN
DEV-WIN
Virtual Switch
Internet
HOST
LIN1
LIN2
LIN3
LIN4
DEV-LIN
Virtual Switch