|  |  |
| --- | --- |
|  |  |

COMPETENCE TASK

"Network and System Administration."

Final of the Professionals Professional Skills Championship in 2024.

2024 г.

The competition task is developed by the expert community and approved by the Competence Manager, which establishes the following rules and the necessary requirements for the possession of professional skills for participation in professional skills competitions.

**The competition task includes the following sections:**

[1. BASIC COMPETENCE REQUIREMENTS 4](#_Toc142037183)

[1.1 General information on competence requirements 4](#_Toc142037184)

[1.2 List of professional tasks of a specialist in the competence "\_\_\_\_\_\_\_\_\_" 4](#_Toc142037185)

[1.3 Requirements for the evaluation scheme 6](#_Toc142037186)

[1.4 Competence Assessment Specification 6](#_Toc142037187)

[1.5 Competition task 7](#_Toc142037188)

[1.5.1 Development/selection of the competition task 7](#_Toc142037189)

[1.5.2 Structure of modules of the competition task (invariant/variant) 8](#_Toc142037190)

[2. SPECIAL RULES OF COMPETENCE 9](#_Toc142037191)

[2.1 Contestant's personal instrument 9](#_Toc142037192)

[2.2 Materials, equipment and tools prohibited on the site 9](#_Toc142037193)

[3. APPENDICES. 9](#_Toc142037194)

**USED ABBREVIATIONS**

1. FGOS - Federal State Educational Standard
2. PS - Professional Standard
3. CP - Competitive task
4. IL - Infrastructure sheet
5. ICS - Information and Communication System
6. CS - Computer Network
7. OS - Operating System

1. BASIC COMPETENCE REQUIREMENTS

1.1. GENERAL INFORMATION ON COMPETENCE REQUIREMENTS

The requirements of the competency (TC) "Network and System Administration" define knowledge, skills, abilities, skills and labor functions , which underlie the most relevant requirements of employers in the industry.

The purpose of competence competitions is to demonstrate the best practices and high level of work performance in the relevant working specialty or profession.

The competency requirements are a guide for training competitive, highly qualified specialists/workers and their participation in professional skills competitions.

In competence-based competitions, knowledge, skills, abilities and labor functions are tested by assessing the performance of practical work.

The competency requirements are divided into clear sections with numbers and headings, with each section assigned a percentage of relative importance, the sum of which is 100.

1. 2. LIST OF PROFESSIONAL REQUIREMENTS FOR THE COMPETENCY "Network and System Administration"

*The list of professional activities, skills and knowledge and professional labor functions of a specialist (from FSES/PS/ETKS...) and is based on the requirements of the modern labor market for this specialist*

*Table No. 1*

**List of professional tasks of a specialist**

|  |  |  |
| --- | --- | --- |
| **No. n/a** | **Section** | **Importance in %** |
| 1 | Identification and remediation of incidents in information and communications technology systems | 25 |
| - The specialist must know and understand:  License requirements for setting up and operating the software to be installed  Fundamentals of architecture, device and functioning of computer systems  Principles of organization, composition and schemes of operation of operating systems  Standards of information interaction between systems  Regulations for preventive maintenance on the administered information and communication system  Instructions for installing administered network devices  Operating instructions for administered network devices  Instructions for installing the administered software  Instructions for the operation of the administered software  Occupational safety requirements when working with hardware, software and hardware and software tools of the administered information and communication system. |
| - The specialist must be able to:  Identify incidents that occur during software installation and decide whether to change the installation procedure  Assess the criticality of application software incidents  Resolve incidents as they arise  Localize failure and initiate corrective actions  Use normative and technical documentation in the field of info-communication technologies  Monitor the information and communication system being administered  Configure the operating systems of network devices  Use control and measuring instruments and equipment  Document accounting information on the utilization of network resources according to the approved schedule |
| 2 | Maintenance of information and communications technology systems hardware and software tools | 25 |
| - The specialist must know and understand  Use modern methods to monitor the performance of the information and communication system; Analyze error messages in network devices and operating systems; Locate failures and initiate corrective actions; Use hardware and software tools to diagnose network device failures and errors; Use in-house hardware and software tools to monitor the performance of the network infrastructure of the information and communication system; Use external hardware and software tools to monitor the performance of the network infrastructure of the information and communication system; Use external hardware and software tools to monitor the performance of the network infrastructure of the information and communication system. |
| - The specialist must be able to:  General principles of functioning of hardware, software and hardware-software means of the administered network; Architecture of hardware, software and hardware-software means of the administered network; Instructions for installation of administered network devices; Instructions for operation of administered network devices; Instructions for installation of administered software; Instructions for operation of administered software; Protocols of link, network, transport and application layers of the model of interaction between the network and the administered network; Protocols of link, network, transport and application layers of the model of interaction between the administered network and the administered network; Protocols of link, network, transport and application layers of the model of interaction between the administered network and the administered network. |
| 3 | Implementation of a scheme for backing up, archiving and restoring configurations of information and communications technology systems hardware and software according to approved plans | 25 |
| - The specialist must know and understand:  General principles of functioning of hardware, software and hardware-software means of the administered information and communication system; Architecture of hardware, software and hardware-software means of the administered information and communication system; Instructions for installation of the administered network devices of the information and communication system; Instructions for operation of the administered network devices of the information and communication system; Instructions for installation of the administered software; |
| - The specialist must be able to:  Use data recovery procedures; identify data recovery points; work with archiving servers and operating system management tools; Use regulatory and technical documentation in the field of info-communication technologies; Perform scheduled software archiving of user devices according to schedule; |
| 4 | Modifications to information and communications technology systems hardware and software according to the approved workplan | 25 |
| - The specialist must know and understand:  Use modern methods to monitor the performance of the information and communication system; Analyze error messages in network devices and operating systems; Locate failures and initiate corrective actions; Use hardware and software tools to diagnose network device failures and errors; Use in-house hardware and software tools to monitor the performance of the network infrastructure of the information and communication system; Use external hardware and software tools to monitor the performance of the network infrastructure of the information and communication system; Use external hardware and software tools to monitor the performance of the network infrastructure of the information and communication system. |
| - The specialist must be able to:  General principles of functioning of hardware, software and hardware-software means of the administered network; Architecture of hardware, software and hardware-software means of the administered network; Instructions for installation of administered network devices; Instructions for operation of administered network devices; Instructions for installation of administered software; Instructions for operation of administered software; Protocols of link, network, transport and application layers of the model of interaction between the network and the administered network; Protocols of link, network, transport and application layers of the model of interaction between the administered network and the administered network; Protocols of link, network, transport and application layers of the model of interaction between the administered network and the administered network. |

1.3. REQUIREMENTS FOR THE EVALUATION SCHEME

The sum of the points awarded for each aspect must fall within the range of points defined for each competency area identified in the requirements and shown in Table #2.

*Table No. 2*

**Matrix of conversion of competence requirements into assessment criteria**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Criterion/Module** | | | | **Total points for the COMPETENCY REQUIREMENTS section** |
| **Sections**  **COMPETENCE REQUIREMENTS** |  | **B** | **D** |  |
| **1** | 25 | 0 | 25 |
| **2** | 25 | 0 | 25 |
| **3** | 5 | 20 | 25 |
| **4** | 5 | 20 | 25 |
| **Total points for criterion/module** | | 60 | 40 | **100** |

1.4. COMPETENCE ASSESSMENT SPECIFICATION

The evaluation of the Competition assignment will be based on the criteria specified in Table No. 3:

*Table No. 3*

**Evaluation of the competition task**

|  |  |  |
| --- | --- | --- |
| **Criterion** | | **Methodology for testing skills in the criterion** |
| **B** | **Customization of technical and software tools of information and communication systems** | According to the OS and Network Equipment used |
| **D** | **Ensuring fault tolerance** | According to the OS and Network Equipment used |

1.5. COMPETITION TASK

Total duration of the Competition task: 15 hours.

Number of competition days: 3 days (day 1 and 2 - Module B; day 3 - Module D).

Regardless of the number of modules, the CP must include an assessment for each section of the competency requirements.

The assessment of the participant's knowledge shall be carried out through practical fulfillment of the Competition task.

1.5.1 Development/selection of the competition task

The competition task consists of 2 modules, includes a mandatory part (invariant) - 1 module, and a variable part - 1 module. The total number of points of the competition task is 100.

1.5.2 Structure of the modules of the competition task

**Module B. (*Configuration of technical and software tools of information and communication systems*) (invariant)**

*Time to complete the module 10 hours*

**Assignments**:

**Part 1 (1 day - 5 hours)**

**1) Basic setup**

a) Configure the device names according to the topology

1. use the fully qualified domain name

b) Configure the device addresses as desired.

1. The network 192.168.11.0/24 is allocated to the HQ office

2. The network 192.168.33.0/24 is allocated for the DT office

3. The network 10.10.10.0/24 is allocated for tunnels between offices

i. The tunnel must accommodate the minimum possible number of addresses

4. The network data must be divided into subnets for each vlan.

i. VLAN110 must hold no more than 64 addresses

ii. VLAN220 must accommodate a maximum of 16 addresses

iii. The VLAN330 must accommodate a maximum of 8 addresses

c) On all devices (except FW-DT) create a sshuser user with the password P@ssw0rd

1. The sshuser user must be able to run the sudo utility without additional authentication.

2. On routers, the sshuser user must have maximum privileges.

**2) Configuring the disk subsystem**

a) On the SRV1-DT, configure the RAID array

1. RAID 1 disk array level.

2. use the disk array name md0.

3. use two unmapped hard disks.

4. use 100% of the disk space

5. Use the xfs file system.

6. Configure automatic mounting of the disk array.

7. Mount point /opt/ansible.

b) On SRV1-HQ, configure LVM

1. use two unmapped hard disks.

2. Create a VG logical volume group

3. Create a DATA logical volume

4. use 100% of the disk space

5. Use the xfs file system.

6. Configure automatic volume mounting

7. Mount point /opt/data

**3) Switching settings**

a) Configure switches SW1-HQ, SW2-HQ, SW3-HQ.

1. use Open vSwitch

2. the switch name must match the short name of the device

i. Use capital letters

3. Pass all physical ports to the switch.

4. Ensure ports are enabled if necessary

5. Create management interfaces on the switches and name them MGMT.

i. Use vlan330 for management interfaces.

6. Configure the main tree protocol

i. The root of the tree shall be SW1-HQ.

b) Configure the SW-DT switch

1. Use the appropriate virtual switch as the switch.

c) For each office, the devices must be on the appropriate VLANs

1. Clients - vlan110,

2. Servers are in vlan220,

3. administrators are in vlan330.

**4) Configure the routers' connections to the ISP**

a) To connect R-DT to the ISP, you must use the last address from the network 172.16.4.0.0/28.

b) To connect the R-HQ to the ISP, the last address from the network 172.16.5.0/28 must be used.

(c) The provider uses the first address from each network

**5) Configuring dynamic address translation**

a) Configure dynamic address translation on the routers.

(b) All devices in all offices must have Internet access

**6) Configuring the Dynamic Host Configuration Protocol**

a) On R-HQ and R-DT, configure the Dynamic Host Configuration Protocol for Clients (CLI)

1. network address - according to topology

i. Exclude the default gateway address from the range of issued addresses

2. default gateway address - according to the topology

i. The gateway for the HQ network is the R-HQ router

ii. The gateway for the DT network is the FW-DT firewall

3. DNS suffix - au.team

4. Configure clients to receive dynamic addresses.

**7) An ip tunnel must be configured between DT and HQ offices**

(a) Use GRE

**8) Configure OSPF dynamic routing**

a) Between DT and HQ offices

1. Routers must be protected against route injection from any interfaces other than those on which route exchange is explicitly required.

2. secure the routing protocol with password protection

i. Use the password P@ssw0rd

b) Between R-DT and FW-DT

1. the R-DT must learn about the networks connected to the FW-DT via OSPF.

2. the FW-DT should receive the default route and other required routes from the R-DT via OSPF.

3. the R-DT must be protected against route injection from any interfaces other than those on which route exchange is explicitly required.

**9) Configuring DNS for SRV1-HQ and SRV1-DT**

a) Implement the company's primary DNS server on SRV1-HQ

1. A and PTR records must be created for all devices of both offices.

2. CNAME records must be created for all enterprise services.

3. Uploading records from SRV1-HQ must only be allowed for SRV1-DT

b) Configure the SRV1-DT as a backup DNS server.

c) Implement Response Policy Zone on the primary and backup DNSs

1. from the DT network, the name test.au.team must resolve to the SRV1-HQ address, and from the HQ network, it must resolve to the SRV1-DT address.

c) All devices must be configured to use both internal DNS servers.

1. For the HQ office, the primary DNS server is SRV1-HQ

2. For the DT office, the primary DNS server is SRV1-DT

d) Use any public DNS server as the DNS forwarding server

**10) Configure time synchronization between network devices using NTP protocol**.

a) The SRV1-HQ shall be the server

1. Use Stratum 5

2. use ntp2.vniiftri.ru as an external time synchronization server

b) All devices must synchronize their time with SRV1-HQ.

1. use chrony wherever possible.

c) Use the Moscow time zone on all devices.

**11) SAMBA AD domain infrastructure implementation**

a) Configure the primary domain controller on SRV1-HQ

1. use the BIND9\_DLZ module

2. Create 30 users user1-user30 with the password P@ssw0rd.

3. Users user1-user10 must be a member of group1.

4. Users user11-user20 must be part of group2.

5. Users user21-user30 must be part of group3.

6. Create CLI and ADMIN units

i. Place clients into units based on their role.

7. The domain clients are ADMIN-DT, CLI-DT, ADMIN-HQ, CLI-HQ.

f) Use SRV1-DT as a standby domain controller.

1. use the BIND9\_DLZ module

h) Implement a shared folder on SRV1-HQ

1. use the name SAMBA

2. use the /opt/data location

**Part 2 (Day 2 - 5 hours)**

**12) Domain Management with ADMC**

a) Domain management with ADMC shall be performed with ADMIN-HQ

b) For the CLI unit, configure the policy to change the desktop to the company picture, and disallow users from changing network settings and changing desktop graphics settings.

c) For the ADMIN unit, implement a SAMBA shared folder connection using domain policies.

**13. Configuring the firewall**

1. Servers and DT Office Administrators must have access to all devices

2. DT office clients shall only have access to servers

3. Allow ICMP requests by DT office administrators to the internal interfaces of the firewall

4. Allow DT office administrators to remotely manage the firewall via SSH and HTTP.

**14) Configure the log collection server on the SRV1-HQ.**

a) SRV1-DT, SRV2-DT, SRV3-DT act as clients

b) Use the auditd service to collect authorization logs

c) Logs shall be collected on the SRV1-HQ server in the directory /var/log/HOSTNAME.log

**15) Implementation of shared folder backup on SRV1-HQ server using systemctl**

a) The backup should archive all data in tar.gz format and store it in the /var/bac/ directory.

1. archiving should be performed thanks to a service type unit named backup.

2. The service should be activated automatically at booting.

b) The time to perform a backup is every day at 8 PM.

1. use a unit of type timer to execute.

2. If the device is switched off, archiving is performed immediately after startup.

**16) Deploying applications in Docker on SRV2-DT**

a) Create a local Docker Registry.

b) Write a Dockerfile for the web application.

1. Use nginx:alpine as the base image

2. Contents index.html

**<html>**

**<body>**

**<center><h1><b>WEB</b></h1></center>**

**</body>**

**</html>.**

3. Build a web application image and upload it to your Registry.

i. Use version number 1.0 for your application

ii. The image must be available for downloading and further running on a local machine

c) Deploy the Docker container using the image from the local Registry.

1. web container name

2. The container must be running on port 80

3. ensure that the container starts after the computer restarts

**17) Configuring the centralized monitoring system**

a) Use SRV3-DT as the server of the centralized monitoring system

b) Use Zabbix as a centralized monitoring system

1. Use PostgreSQL as the database server

i. Database name: zabbix

ii. Database user: zabbix

iii. Database user password: zabbixpwd

2. Use Apache as the web server

(c) The centralized monitoring system shall be available to internal users at http://<IP address SRV3-DT>/zabbix

1. the administrator of the monitoring system should be the Admin user with the password P@ssw0rd

2. The default time zone should be Europe/Moscow

d) Configure the centralized monitoring system node

1. Use SRV1-DT, SRV2-DT, SRV3-DT, SRV-HQ as network nodes.

2. the network node name must match the full name of the device

**18) Configure the nginx web server as a reverse proxy server on the SRV1-DT**

a) When accessing the domain name www.au.team, the client should be redirected to SRV2-DT on the web container

b) When accessing the zabbix.au.team domain name, the client should be redirected to SRV3-DT on the Zabbix service.

c) If necessary, configure the network equipment to provide the required services.

**19) Configuring the Ansible management node**

a) Configure the control node based on ADMIN-DT

1. use the standard batch version of ansible.

b) Configure the inventory

1. the inventory must be located at the path /etc/ansible/inventory.

i. Customize the default startup of this inventory

2- The inventory shall contain three groups of devices:

i. Networking (R-DT, R-HQ)

ii. Servers (SRV1-HQ, SRV1-DT, SRV2-DT, SRV3-DT)

iii. Clients (ADMIN-HQ, ADMIN-DT, CLI-HQ, CLI-DT)

3. Realize access to all devices based on SSH settings

i. Connection is made by the sshuser user

ii. Use the correct Python interpreter

iii. Disable SSH key validation on the host

c) Run the test command "ping" with ansible tools

1. Make sure all devices respond with "pong" without warning messages

2. Make sure that ansible commands are run from the user user user without using sudo

**20) On the SRV3-DT server, configure the VPN server**

a) Use wireguard as a VPN server.

b) Use the address space 10.6.6.0/24 as the VPN network

c) Clients must have full access to the DT office

1. The CLI acts as the client

e) Starting the connection is done by the wg\_connect script, stopping it is done by wg\_disconnect.

1. Scripts should be called from any directory without specifying the full path

2. Scripts must be run from the User user using sudo

**Module D. (*Fault Tolerance*) (option)**

*Time to complete the module 5 hours*

**Assignments**:

**1) Preparing the ControlVM machine**

(a) General Guidelines:

1. All job verification will be done from the ControlVM machine.

2. DO NOT delete the ControlVM instance after the job completes.

b) Create and configure a ControlVM instance:

1. Create a virtual instance named **ControlVM** and connect it to the Internet.

2. Set the following parameters for the virtual machine:

i. **Virtual machine type:** 2 vCPUs, 4 GB RAM.

ii. **Disk size:** 30 GB.

3. Select **Alt Server 10** as the operating system.

4. Configure the instance to allow external SSH connections.

5. Save the key pair for access on your local PC on your desktop with a **.pem** extension.

c) Configure an external connection to ControlVM:

1. Install the SSH **PuTTY** SSH client on the local PC.

2. Create a profile in PuTTY named **cloud**.

3. Verify that you can establish a connection to the ControlVM instance from a local PC via PuTTY without having to enter additional parameters.

4. Use the **altlinux** username and the previously saved key pair to connect.

**2) Preparing cloud infrastructure:**

a) Virtual Machine Requirements:

1. key features for ControlVM:

i. Operating system: Alt Server p10-cloud

ii. Number of vCPUs: 1.

iii. RAM capacity: 1024 MB.

iv. Disk capacity: 30 GB

1. basic characteristics for all other wm:

i. Operating system: Alt p10 StarterKit

ii. Number of vCPUs: 1.

iii. RAM capacity: 1024 MB.

iv. Disk capacity: 10 GB

b) Prepare a scenario to automate the deployment of cloud infrastructure:

1. Creating virtual machines and networks:

i. Virtual machines and networks must be created strictly according to the proposed topology (see Topology below).

ii. The names of virtual machines, networks, subnets, and routers must match the names specified in the Topology.

iii. Ensure that virtual machines are properly connected to the appropriate networks within the given topology.

2. security and access:

i. Allow ICMP traffic for all virtual machines to diagnose network connections.

ii. Assign IP addresses to all machines. Save the external IP addresses of all machines in the /home/altlinux/white.ip file on the ControlVM machine.

iii. Configure public key-based authentication for SSH.

iv. If external access to virtual machines is provided, allow it only via SSH (public key, password disabled) and only from appropriate IP addresses.

3. load balancing:

i. Create a load balancer and distribute traffic between servers Web1 and Web2 (see Topology).

ii. Limit external access to the balancer to HTTP and HTTPS protocols only. All other ports should be closed.

iii. Load balancing shall utilize the round robin algorithm.

iv. A call to the external address of the load balancer shall output a response from the application running on the internal Web1 and Web2 servers.

4. Configuring the connection:

i. Configure the WebAdm machine so that it can connect via SSH using the altlinux user and password "P@ssw0rd" to the Web1 and Web2 servers using a VPN tunnel.

ii. Verify that the ControlVM machine can connect to the WebAdm machine using the altlinux user key pair via SSH through its global IP address.

**3) Create and configure the script on the ControlVM machine:**

a) Creating an automation script:

1. On the ControlVM machine, create the cloudinit.sh script.

2. Use the path /home/altlinux/bin as the working directory.

3. The script should use the configuration file /home/altlinux/bin/cloud.conf to configure the connection to the cloud provider.

You can use the following structure as a template for the cloud.conf file:

|  |
| --- |
| export OS\_AUTH\_URL=https://edu.cyber-infrastructure.ru:5000/v3  export OS\_IDENTITY\_API\_VERSION=3  export OS\_AUTH\_TYPE=password  export OS\_PROJECT\_DOMAIN\_NAME=Competence\_SiSA  export OS\_USER\_DOMAIN\_NAME=Competence\_SiSA  export OS\_PROJECT\_NAME=Project# #Project name  export OS\_USERNAME=Project1 #Username to connect to the cloud provider  export OS\_PASSWORD="'@y\*X9?wtOuAW}w-G9fV6@T" #User password to connect to the cloud provider |

4. When checking a task, experts can change settings only in the cloud.conf file. Other files will not be edited.

It is allowed to leave comments in the cloud.conf file to explain the purpose of the parameters.

(b) Script requirements:

1. The script should be designed so that it can be executed from any directory without having to specify the full path to the executable file.

2. Use infrastructure deployment automation tools to complete the task.

3. The script must include mechanisms for checking the availability of created resources and their proper functioning, including the availability of Web servers through a load balancer.

**4) Deploying applications in Docker**

(a) General Requirements:

All activities are performed on the ControlVM machine. Perform Python script deployment to Docker, configure WordPress using Docker Compose, and deploy the underlying ELK stack to collect and display logs.

b) Deploying a Python script to Docker

1. Write a Python script in the user's home directory py.py that performs the following tasks:

i. Checks if the input.txt file exists in the root working directory.

ii. Outputs a message with the contents.

iii. If the input.txt file does not exist, displays an error message.

2. Create a Dockerfile for the Python script py.py:

i. Use the python:3.8-alpine base image.

ii. The Python script py.py must be executed inside the container.

iii. Implement copying the input.txt file into a container (this file can contain arbitrary text).

iv. The container should output the contents of the input.txt file on startup, and then terminate.

3. Assembling and launching the container:

i. Build a Docker image named file-copy-python.yml.

ii. Start the container and verify that the file contents are output by the input.txt file.

c) Deploying WordPress using Docker Compose

3.1 Creating the wordpress.yml file:

i. In the user's home directory, create a wordpress.yml file that describes the container stack for WordPress and MySQL.

3.2 Docker Compose stack configuration:

i. Define two services:

1. **wordpress**:
   * + Use the **wordpress:latest** image.
     + Link to wordpress-network.
     + Flush port 80 to access WordPress from the outside.
     + Set up the necessary environment variables (WORDPRESS\_DB\_HOST, WORDPRESS\_DB\_USER, WORDPRESS\_DB\_PASSWORD, WORDPRESS\_DB\_NAME, etc.).

**2) mysql**:

* + - Use **mysql** image**:5.7**.
    - Link to wordpress-network.
    - Create a volume to store the database data.
    - Set the necessary environment variables (MYSQL\_DATABASE,MYSQL\_USER, MYSQL\_PASSWORD, MYSQL\_ROOT\_PASSWORD, etc.).

3.3 Starting the stack:

i. Start Docker Compose with the wordpress.yml file.

ii. Verify that WordPress is available on the specified port and is ready to be configured.

**4) Deployment of the ELK base stack**

a) Creating the elk.yml file:

1. In the user's home directory, create an elk.yml file that describes the container stack for Elasticsearch, Logstash, and Kibana.

(b) Docker Compose stack configuration:

1- Identify three services:

1. **elasticsearch:**
   * + Use the **elasticsearch:7.10.1** image.
     + Route port 9200 to access the Elasticsearch API.

**2) logstash**:

* + - Use the **logstash:7.10.1** image.
    - Configure Logstash to retrieve the data and send it to Elasticsearch.

**3) kibana**:

* + - Use image **kibana:7.10.1**.
    - Route port 5601 to access the Kibana web interface.

(c) Stack Startup:

1. Start Docker Compose with the elk.yml file.

2. Make sure that all services are running and Kibana is available on port 5601.

**5) Deployment of cloud services**

a) On the ControlVM machine, create the script /home/altlinux/bin/DeployApp.sh.

1. The script should be executed from any directory without explicitly specifying the path to the executable file.

b) Prepare the App1 web application

1. Download the app1.py and Dockerfile files at:

<https://github.com/auteam-usr/champs/tree/main/final>

2. Build an application image and upload it to a local Docker repository of your choice.

c) The DeployApp.sh command should run automation tools to configure the operating systems.

1. Deploy the web application App1 from the Docker repository to virtual machines Web1 and Web2.

2. provide load balancing between Web1 and Web2.

3. provide external access to the web application using the https protocol.

4. When accessing via the http protocol, an automatic

redirects to the https protocol.

5. Providing credibility to the certificate is not required.

**6) Completion of work**

a) At the end of business hours, release the cloud provider resources used for automatically created objects.

b) Delete all automatically created virtual machines, networks, objects, and other resources.

**c) Caution:** DO NOT delete **ControlVM** and the resources required for it to function.

d) Important: If objects other than those required for **ControlVM** or created by default remain in the cloud infrastructure, the job will not be validated.

2. SPECIAL RULES OF COMPETENCE

1. Participants may use Internet resources in completing all modules, with the exception of:

-Version control systems

-Communication via forums/messengers/other means of communication -video hosting sites

2. Participants have the right to ask clarifying questions to the experts (except for the mentor expert) and have the right to receive an answer, if the question does not imply obtaining information on the implementation of a particular technology

2.1. Contestant's Personal Instrument

Zero - you can't bring anything in.

2.2 Materials, equipment and tools prohibited on the site

Mobile devices, photo-video recording devices, data carriers.

3. Appendices

Annex 1: Instructions for filling in the competition task matrix

Appendix 2. Matrix of the competition task

Annex 3: Occupational Health and Safety Instruction

Appendix 4: Drawings, flow charts, algorithms, schemes