Configuration instructions for   
**Module C**  
infrastructure

Updated: 30.08.2023.

# Table of contents

[Radius node configuration (Ubuntu node in CML) 3](#_o1ivuqpph0gq)

[CASrv node configuration (Ubuntu node in CML) 5](#_qp8wyw967hga)

[Monitor node configuration (Ubuntu node in CML) 8](#_jvm4a58ls1x5)

[PUBWEBDNS node configuration   
(Ubuntu node in CML) 11](#_syuwyjbl27du)

[INTRAWEB node configuration   
(Ubuntu node in CML) 15](#_mtodr7lyir0h)

[RDWARRIOR CME-X03 configuration   
(Windows 10 client) 17](#_sp9evgialpeg)

[CME201 and CME101 configuration   
(Windows 10 Client) 17](#_t0q5bnd5p3xm)

[CME102 and CME301 configuration   
(Debian client) 17](#_jr8h6482uedg)

[ISP configuration 17](#_v3ohyqr36z6n)

# Radius node configuration (Ubuntu node in CML)

1. Connect VM to External Conncetor in NAT mode.
2. Change root password (if needed) according to TP:

sudo su

passwd root

***Enter password -*** *Passw0rd!*

1. Install freeradius service

apt update

apt install freeradius

1. Remove VM from External Conncetor and connect the VM back to the usw0.
2. Configure IP address:

nano /etc/netplan/50-cloud-init.yaml

***Change configuration to (changes are marked with yellow):***

network:

ethernets:

ens2:

dhcp4: **false**

**addresses: [172.16.40.101/24]**

**routes:**

**- to: default**

**via: 172.16.40.254**

**nameservers:**

**addresses:**

**- 87.250.250.1**

match:

macaddress: 52:54:00:00:8b:3a

set-name: ens2

version: 2

***Save and close (Ctrl+X Y Enter)***

netplan generate

netplan apply

1. Verify IP configuration changes:

ip a

***Should show configured IP address on ens2***

ip route

***Should show:***

default via 172.16.40.254 dev ens2 proto static

1. Configure freeradius service users:

***NB! Possibly up to competitor to configure as TP states:***

*"For LODZ1 and LODZ2 user super should automatically land in privileged mode. User regular lands in user exec mode. Both users should be created in the ~~TFTP~~ Radius server. Use local authentication in case remote authentication server is not available."*

nano /etc/freeradius/3.0/users

***Add users at the top of the file:***

regular Cleartext-Password := "Passw0rd!"

Service-Type = NAS-Prompt-User,

Cisco-AVPair = "shell:priv-lvl=1"

super Cleartext-Password := "Passw0rd!"

Service-Type = NAS-Prompt-User,

Cisco-AVPair = "shell:priv-lvl=15"

**Save and close (Ctrl+X Y Enter)**

1. Configure freeradius authorized device list (clients):

nano /etc/freeradius/3.0/clients.conf

***Add devices to clients list at the end of the file:***

client 172.16.40.1{

secret = Passw0rd!

nastype = cisco

shortname = LODZ1

}

client 172.16.40.2{

secret = Passw0rd!

nastype = cisco

shortname = LODZ2

}

**Save and close (Ctrl+X Y Enter)**

1. Restart freeradius service:

service freeradius restart

# CASrv node configuration (Ubuntu node in CML)

1. Change root password (if needed) according to TP:

sudo su

passwd root

***Enter password -*** *Passw0rd!*

1. Configure IP address:

nano /etc/netplan/50-cloud-init.yaml

***Change configuration to (changes are marked with yellow):***

network:

ethernets:

ens2:

dhcp4: **false**

**addresses: [172.16.40.102/24]**

**routes:**

**- to: default**

**via: 172.16.40.254**

**nameservers:**

**addresses:**

**- 87.250.250.1**

match:

macaddress: 52:54:00:00:8b:3a

set-name: ens2

version: 2

***Save and close (Ctrl+X Y Enter)***

netplan generate

netplan apply

1. Verify IP configuration changes:

ip a

***Should show configured IP address on ens2***

ip route

***Should show:***

default via 172.16.40.254 dev ens2 proto static

1. Create CA dir /ca

mkdir /ca

1. Create subdirectories within /ca folder:

cd /ca

mkdir newcerts certs private requests

1. Create index and serial files and insert first serial number:

touch /ca/index.txt

touch /ca/serial

echo 01 > /ca/serial

1. Copy default OpenSSL configuration file to /ca directory:

cp /etc/ssl/openssl.cnf /ca/

1. Edit configuration:

nano /ca/openssl.cnf

***Go to the configuration block [ CA\_default ] and change directory of CA   
(changes are marked with yellow):***

dir = **/ca** # Where everything is kept

**Save and close (Ctrl+X Y Enter)**

1. Generate the private key for CA:

openssl genrsa -out /ca/private/cakey.pem 4096

1. Create CA certificate:

openssl req -new -x509 -config /ca/openssl.cnf -key /ca/private/cakey.pem -out /ca/cacert.pem

1. Fill in the form with data:

Country Name (2 letter code) [AU]: PL

State or Province Name (full name) [Some-State]: Poland

Locality Name (eg, city) []: Lodz

Organization Name (eg, company) [Internet Widgits Pty Ltd]: EuroSkills

Organizational Unit Name (eg, section) []: Lodz

Common Name (e.g. server FQDN or YOUR name) []: EuroSkills Root CA

Email Address []: ca@lodz.pl

***For easier filling of the form, you can just paste these rows of text (it’s the same input as above):***

PL

Poland

Lodz

EuroSkills

Lodz

EuroSkills Root CA

ca@lodz.pl

1. Verify Root CA certificate

openssl x509 -in /ca/cacert.pem -noout -text | less

***Should contain provided data, flagged as CA:TRUE and be valid for 10 years.***

# Monitor node configuration (Ubuntu node in CML)

This instruction is valid for Debian VMs too, but instead of netplan we need to use **/etc/network/interfaces**

Configuration for interfaces file:

auto lo

iface lo inet loopback

allow-hotplug ens2

auto ens2

iface ens2 inet static

address 172.16.40.103

netmask 255.255.255.0

gateway 172.16.40.254

dns-nameservers 87.250.250.1

and

“sudo su” should be replaced with “su -” unless sudoers is installed and configured. “sudo” then can be omitted, just elevate to root and do tasks.

1. Connect VM to External Conncetor in NAT mode.
2. Change root password (if needed) according to TP:

sudo su

passwd root

***Enter password -*** *Passw0rd!*

1. Download Observium installer

apt update

wget <http://www.observium.org/observium_installscript.sh>

1. Make installer script executable

chmod +x observium\_installscript.sh

1. Install Observium

./observium\_installscript.sh

1. Select **“1. Observium Community Edition”**
2. Enter MySQL password - **Passw0rd!**
3. Press **“Enter”** to start MySQL install
4. Press **“Enter”** to add necessary repositories for installation
5. Accept installation by entering **“Y”** and pressing **“Enter”**
6. Press **“Tab”** and **“Enter”** to allow restart of services
7. Provide first user data - **root** / **Passw0rd!**
8. Press “n” and “Enter” - we don’t need to monitor Observium itself
9. Press “n” and “Enter” - we don’t need UNIX agent on this machine
10. Install TFTP server for Cisco configuration backups:

apt install tftpd-hpa

1. Modify configuration to fit TP needs:

nano /etc/default/tftpd-hpa

***Modify configuration (marked with yellow):***

# /etc/default/tftpd-hpa

TFTP\_USERNAME="tftp"

TFTP\_DIRECTORY="/tftp"

TFTP\_ADDRESS="0.0.0.0:69"

TFTP\_OPTIONS="--secure --create -v"

***Save and close (Ctrl+X Y Enter)***

1. Create TFTP root directory:

mkdir /tftp

1. Grant all permissions for root directory:

chmod -R 777 /tftp

1. Restart the TFTP service:

service tftpd-hpa restart

1. Remove VM from External Conncetor and connect the VM back to the usw0.
2. Configure IP address (For Ubuntu Nodes):

nano /etc/netplan/50-cloud-init.yaml

***Change configuration to (changes are marked with yellow):***

network:

ethernets:

ens2:

dhcp4: **false**

**addresses: [172.16.40.103/24]**

**routes:**

**- to: default**

**via: 172.16.40.254**

**nameservers:**

**addresses:**

**- 87.250.250.1**

match:

macaddress: 52:54:00:00:8b:3a

set-name: ens2

version: 2

***Save and close (Ctrl+X Y Enter)***

netplan generate

netplan apply

1. Verify IP configuration changes:

ip a

***Should show configured IP address on ens2***

ip route

***Should show:***

default via 172.16.40.254 dev ens2 proto static

1. Add **monitor.lodz.pl** ServerName to server configuration:

nano /etc/apache2/sites-available/000-default.conf

***Add line after ServerAdmin line:***

ServerName monitor.lodz.pl

***Save and close (Ctrl+X Y Enter)***

1. Add another website- **lodz.pl**:

nano /etc/apache2/sites-available/lodz.pl.conf

***Add lines:***

<VirtualHost \*:80>

DocumentRoot "/var/www/html"

ServerName lodz.pl

</VirtualHost>

1. Enable Apache2 site **lodz.pl**:

a2ensite lodz.pl.conf

1. Customize WEB page lodz.pl with simple <h1> tag:

rm /var/www/html/index.html

nano /var/www/html/index.html

***Add line:***

<h1> This is lodz.pl website! </h1>

***Save and close (Ctrl+X Y Enter)***

1. Restart apache2 service

service apache2 restart

# PUBWEBDNS node configuration (Ubuntu node in CML)

***NB! This node is very likely to be at least partially (DNS part) left for competitors to configure due to requirements in test project:***

***“  
Road Warrior***

*Connects to the network via Cisco AnyConnect VPN client. You decide the single, or multi, entry point and configure the DNS server in PUBWEBDNS with the appropriate entries to resolve vpn.ict.pl. The possible entry points are Warsaw, Krakow, or Gdansk and depending on which option is chosen the CMS extension will be 103, 203 or 303.****”***

1. Connect VM to External Conncetor in NAT mode.
2. Change root password (if needed) according to TP:

sudo su

passwd root

***Enter password -*** *Passw0rd!*

1. Install BIND9 DNS service:

apt update

apt install bind9

1. Install Apache2 WEB server:

apt install apache2

1. Remove VM from External Conncetor and connect the VM back to the ISP (Interface GigabitEthernet 0/7).
2. Configure IP address (For Ubuntu Nodes):

nano /etc/netplan/50-cloud-init.yaml

***Change configuration to (changes are marked with yellow):***

network:

ethernets:

ens2:

dhcp4: **false**

**addresses: [87.250.250.1/24]**

**routes:**

**- to: default**

**via: 87.250.250.254**

**nameservers:**

**addresses:**

**- 127.0.0.1**

**- 87.250.250.1**

match:

macaddress: 52:54:00:00:8b:3a

set-name: ens2

version: 2

***Save and close (Ctrl+X Y Enter)***

netplan generate

netplan apply

1. Verify IP configuration changes:

ip a

***Should show configured IP address on ens2***

ip route

***Should show:***

default via 87.250.250.254 dev ens2 proto static

1. Configure 000-default.conf site to work with euroskills.pl name:

nano /etc/apache2/sites-available/000-default.conf

***Edit ServerName to this:***

ServerName euroskills.pl

***Save and close (Ctrl+X Y Enter)***

1. Customize WEB page with simple <h1> tag:

rm /var/www/html/index.html

nano /var/www/html/index.html

***Add line:***

<h1> This is EuroSkills.pl website! </h1>

***Save and close (Ctrl+X Y Enter)***

1. Restart apache2 service

service apache2 restart

1. Configure DNS
2. Add zones to service:

nano /etc/bind/named.conf.local

***Add lines:***

zone "euroskills.pl" {

type primary;

file "/etc/bind/db.euroskills";

};

zone "lodz.pl" {

type primary;

file "/etc/bind/db.lodz";

};

zone "ict.pl" {

type primary;

file "/etc/bind/db.ict";

};

***Save and close (Ctrl+X Y Enter)***

1. Create files for zones:

cd /etc/bind

touch db.euroskills db.lodz db.ict

1. Edit zones

nano /etc/bind/db.euroskills

***Paste:***

$TTL 86400

@ IN SOA euroskills.pl. root.euroskills.pl. (

1 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

86400 ) ; Negative Cache TTL

;

@ IN NS euroskills.pl.

@ IN A 87.250.250.1

***Save and close (Ctrl+X Y Enter)***

nano /etc/bind/db.lodz

***Paste:***

$TTL 86400

@ IN SOA lodz.pl. root.lodz.pl. (

1 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

86400 ) ; Negative Cache TTL

;

@ IN NS lodz.pl.

@ IN A 18.31.192.3

monitor IN A 18.31.192.3

***Save and close (Ctrl+X Y Enter)***

nano /etc/bind/db.ict

***Paste:***

$TTL 86400

@ IN SOA ict.pl. root.ict.pl. (

1 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

86400 ) ; Negative Cache TTL

;

@ IN NS ict.pl.

@ IN A 172.16.30.1

***Save and close (Ctrl+X Y Enter)***

1. Edit options file to allow query from everywhere without validation:

nano /etc/bind/named.conf.options

***Change dnssec-validation:***

dnssec-validation no;

***Add allow-query:***

allow-query { any; };

***Save and close (Ctrl+X Y Enter)***

# INTRAWEB node configuration (Ubuntu node in CML)

1. Connect VM to External Conncetor in NAT mode.
2. Change root password (if needed) according to TP:

sudo su

passwd root

***Enter password -*** *Passw0rd!*

1. Install Apache2 service:

apt update

apt install apache2

1. Remove VM from External Conncetor and connect the VM back to the INTRAFW (Interface GigabitEthernet 0/1).
2. Configure IP address (For Ubuntu Nodes):

nano /etc/netplan/50-cloud-init.yaml

***Change configuration to (changes are marked with yellow):***

network:

ethernets:

ens2:

dhcp4: **false**

**addresses: [172.16.30.1/24]**

**routes:**

**- to: default**

**via: 172.16.30.254**

**nameservers:**

**addresses:**

**- 87.250.250.1**

match:

macaddress: 52:54:00:00:8b:3a

set-name: ens2

version: 2

***Save and close (Ctrl+X Y Enter)***

netplan generate

netplan apply

1. Verify IP configuration changes:

ip a

***Should show configured IP address on ens2***

ip route

***Should show:***

default via 87.250.250.254 dev ens2 proto static

1. Configure 000-default.conf site to work with ict.pl name:

nano /etc/apache2/sites-available/000-default.conf

***Edit ServerName to this:***

ServerName ict.pl

***Save and close (Ctrl+X Y Enter)***

1. Customize WEB page with simple <h1> tag:

rm /var/www/html/index.html

nano /var/www/html/index.html

***Add line:***

<h1> This is ICT.pl website! </h1>

***Save and close (Ctrl+X Y Enter)***

1. Restart apache2 service

service apache2 restart

# 

# RDWARRIOR CME-X03 configuration (Windows 10 client)

Install following software:

1. CIPC
2. AnyConncet client
3. Java
4. Virtual Audio cable

# CME201 and CME101 configuration (Windows 10 Client)

Install following software:

1. CIPC
2. Java
3. Virtual Audio cable

# CME102 and CME301 configuration (Debian client)

Install following software:

1. Zoiper

# ISP configuration

1. Select the ISP node and, if needed, stop and wipe it.
2. Paste configuration in EDIT CONFIG section in CML UI:

hostname ISP

!

interface Loopback1666

ip address 1.6.6.6 255.255.255.255

!

interface Loopback8844

ip address 8.8.4.4 255.255.255.255

!

interface Loopback8888

ip address 8.8.8.8 255.255.255.255

!

interface GigabitEthernet0/0

ip address 100.10.9.6 255.255.255.252

ip tcp adjust-mss 1200

duplex auto

speed auto

media-type rj45

no mop enabled

no mop sysid

!

interface GigabitEthernet0/1

ip address 132.87.2.254 255.255.255.0

ip tcp adjust-mss 1200

duplex auto

speed auto

media-type rj45

no mop enabled

no mop sysid

!

interface GigabitEthernet0/2

ip address 94.121.72.254 255.255.255.0

ip tcp adjust-mss 1200

duplex auto

speed auto

media-type rj45

no mop enabled

no mop sysid

!

interface GigabitEthernet0/3

ip address 65.32.147.254 255.255.255.0

ip tcp adjust-mss 1200

duplex auto

speed auto

media-type rj45

no mop enabled

no mop sysid

!

interface GigabitEthernet0/4

no ip address

duplex auto

speed auto

media-type rj45

!

interface GigabitEthernet0/5

ip address 18.31.192.254 255.255.255.0

duplex auto

speed auto

media-type rj45

no mop enabled

no mop sysid

!

interface GigabitEthernet0/6

ip address 100.71.60.254 255.255.255.252

ip tcp adjust-mss 1200

duplex auto

speed auto

media-type rj45

no mop enabled

no mop sysid

!

interface GigabitEthernet0/7

ip address 87.250.250.254 255.255.255.0

ip tcp adjust-mss 1200

duplex auto

speed auto

media-type rj45

no mop enabled

no mop sysid

!

router bgp 65000

bgp log-neighbor-changes

neighbor 18.31.192.1 remote-as 65005

neighbor 18.31.192.2 remote-as 65005

neighbor 65.32.147.1 remote-as 65004

neighbor 94.121.72.1 remote-as 65003

neighbor 100.10.9.5 remote-as 65002

neighbor 132.87.2.1 remote-as 65001

!

address-family ipv4

network 1.6.6.6 mask 255.255.255.255

network 8.8.4.4 mask 255.255.255.255

network 8.8.8.8 mask 255.255.255.255

network 18.31.192.0 mask 255.255.255.0

network 65.32.147.0 mask 255.255.255.0

network 87.250.250.0 mask 255.255.255.0

network 94.121.72.0 mask 255.255.255.0

network 100.10.9.4 mask 255.255.255.252

network 100.71.60.252 mask 255.255.255.252

network 132.87.2.0 mask 255.255.255.0

neighbor 18.31.192.1 activate

neighbor 18.31.192.2 activate

neighbor 65.32.147.1 activate

neighbor 94.121.72.1 activate

neighbor 100.10.9.5 activate

neighbor 132.87.2.1 activate

exit-address-family

!