TEST PROJECT IT NETWORK SYSTEM ADMINISTRATION

WSC2017_TP39_ModuleA_actual

Submitted by: Module A group

Danny Meier CH
Andreas Strömgren SE
Avner Santos BR
Jun Tian CN
Janos Csoke HU
Johan M. Kerta ID
Atsuya Kamioka JP
Bart Jaminon NL
Yi-Chen Huang TW
Abdullah Bakhashwain SA

MODULE A

CONTENTS

This Test Project proposal consists of the following documentation/files:

1. WSC2017_TP39_ModuleA_EN_final

INTRODUCTION

The competition has a fixed start and finish time. You must decide how to best divide your time.

Please **carefully read** the following instructions!

When the competition time ends, please leave your station in a running state. The assessment will be done in the state as it is. *No reboot will be initiated as well as powered off machines will not be powered on!*

Please do not touch the VMware configuration as well as the configuration of the VM itself except the CD-ROM / HDD drives

PHYSICAL MACHINE (HOST)

FOLDER PATHS

ISO Images:	VMware ESXi Datastore

LOGIN

Username:	root / skill39 / LDAP-Users
Password:	Skill39
Domain:	wsc17.cloud

SYSTEM CONFIGURATION

Region:	United Arabic Emirates
Locale:	English US (UTF-8)
Key Map:	English US

SYSTEM TOOLS

- Install CURL
- Install SSH daemon and allow root access

LOGIN BANNER

Must be shown before the login prompt. Must appear for local and network logins.

```
********************************
* WorldSkills 2017 - Abu Dhabi *
*           Module A           *
*                              *
*        >>[hostname]<<        *
********************************
```

DESCRIPTION OF PROJECT AND TASKS

You are a system engineer and you have the task to implement a complex Linux based IT environment for an international assembly of professional experts. The requirements are gathered where possible and documented. Please get an overview of the project by studying the physical and logical diagrams at the end of this document.

SYSTEM CONFIGURATION (GENERAL)

All the server and client systems are pre-installed with a basic configuration of Debian Linux. Please use the credentials and settings stated on the introduction page (page 2). You are allowed to change these values to the ones you prefer. But at the end of the day, all the settings must be reverted to its initial values.

Configure all servers with the correct hostname and network settings found in the appendix.

Install on every machine the system tools that has been mentioned in the introduction.

Please use the default configurations if you are not given any details.

For values which do not impact the assessment, such as 'Region' or 'Locale', will result in losing minor points. If the process of assessment is impaired you will lose all points respectively.

The “Internet” network/subnet is connected to the management station. This means that you can leverage PUTTY/SSH to manage your virtual machines, given that your network is properly configured.

GENERAL TASKS

SETTINGS

Configure the system as mentioned in the Module A introduction.

Differences between the pre-installed system and the requested system configuration may exist.

SOFTWARE

Install all the software as mentioned in the Module A introduction.

DMZ ZONE

WSC-D-ABUDHABI

LOAD BALANCER (HAPROXY)

Configure a HTTP/HTTPS load balancer for “www.wsc17.cloud”, which is hosted by wsc-c-saopaulo and wsc-c-leipzig. Connect to backends by using HTTPS and make sure that certificates are fully trusted (no browser or other certificate errors).

DNS

- Install Bind9.
    - Configure a forward zone called “wsc17.cloud”.
        - Create for each host an A record to the respective IP
        - Create a CNAME record for ‘www’ that points to the appropriate host that serves websites for all clients
        - Create a CNAME record for ‘mail’ that points to the mail server
        - Create the appropriate MX records
        - Create a CNAME record for ‘ftp’ that points to the ftp server
        - Create a CNAME record for ‘files’ to access the DFS shares
    - Configure a forward zone called “competition.ae”
        - Create the appropriate records for email to work
    - Configure a reverse zone for the IP range defined in DMZ network.

MAIL

- Install Postfix and Dovecot.
    - Configure SMTPS and IMAPS server for "wsc17.cloud" and “competition.ae” domain using certificates issued by wsc-i-calgary.
    - Configure mail directory in /home/[user]/Maildir.
    - Authentication has to be done through LDAP
        - Make sure that the corresponding local user do not exist
        - Allow only users from the OU “mail”.
    - Enable SMTP submission (TLS tcp/587).
        - Disable port tcp/25
    - Enable secure IMAP (TLS tcp/143)

WSC-D-SAOPAULO AND WSC-D-LEIPZIG

WEBSERVER – APACHE

The marking will be done on either of the two servers. Which one will be decided prior the marking starts by the assessment team. So you have to configure both servers!

- Install Apache
    - Configure a HTTPS-only website for "www.wsc17.cloud" domain and “localhost” using certificates issued by wsc-i-calgary.
    - The website page should display the following message:
        - *“Welcome to the wsc17 cloud on [HOSTNAME]”.*
        - Add the hostname dynamically with PHP
    - Add the HTTP header “X-Served-By” with the server hostname as the value.
    - Install rsync on wsc-d-saopaulo and synchronize /var/www directory (recursive) from wsc-d-saopaulo to wsc-d-leipzig, automatically every minute.

        - To run the script don’t use crontab, solve it within the script only
        - Script must be running while assessing the test project
        - Make the script available in ‘/root/web_sync.sh’

    - Make sure that PHP scripts can be run
        - index.php should be first priority for index files
    - Install the appropriate Redis module for PHP
    - Create a password protected (basic authentication) subfolder “redis”
        - Use user *skill39* with password *Skill39* to authenticate
    - Add a PHP script with the name “index.php” inside the redis folder
        - Add the following content the “index.php”

```
<?php
  $redis = new Redis();
  $redis->connect(<server>);
  $content = $redis->get(<key>);
  echo $content;
?>
```

PROTECTED SERVER ZONE

WSC-I-LONDON

Install and configure the following services. Make sure that all LDAP users in OU “Misc” can login locally, users from other OU must not be allowed to login locally.

SYSTEM

- Configure the disks and partitions
  - Add three disks to the system (chose the appropriate type and size by yourself)
  - Create a RAID 5 array and partition them with EXT4
  - Mount the new array to /files (file access must be possible automatically after system start)

FILE SHARES

- Install and use Samba for the following tasks
  - Authentication is done by “wsc-i-calgary”, local users are not permitted
  - Home directory of the respective user (authenticated user against Samba)
    - Not visible (nobody)
    - Accessible only for the authenticated user through “\\[server]\[user]”
    - The home share is only accessible from the client’s subnet
    - Local data path: /files/users/[user]

DISTRIBUTED FILE SHARE (DFS)

- Configure Samba for DFS
  - Enable DFS
  - DFS should be accessible through “\\wsc-i-london\dfs” for clients
    - Local DFS root: /files/samba/dfs
  - Distribute the share “public” through DFS (\\wsc-i-london\dfs\public)
    - Local data path: /files/samba/public
    - Share is not visible outside the DFS (e.g. \\wsc-i-london\public)
    - Creating a “public” sub-folder inside the DFS share is not allowed (real DFS linking)
    - This share is writable by everyone (authenticated and anonymous)
  - Distribute the share “private” through DFS (\\wsc-i-london\dfs\private)
    - Remote data path: \\wsc-i-calgary\private
    - Creating a “private” sub-folder inside the DFS share is not allowed (real DFS linking)
    - This share is readable / writable for every LDAP user

FTP

- Setup FTP with PureFTP
  - Use a virtual user configuration (not system users)
    - User: skill39-ftp / Password: Skill39
    - Home directory: “/files/users/skill39-ftp”
  - The virtual user has to be mapped to the system user/group “ftpuser/ftpgroup”
  - Per user only one active concurrent session is allowed
  - Only allow explicit SSL / TLS (ftpes://)
  - File renaming is not allowed

WSC-I-CALGARY

LDAP

- Install LDAP service.
  - Configure the directory service of wsc17.cloud.
  - Create users with OU and password specified in the appendix.
  - File Share, Web and Mail services should be available for LDAP users.
  - Create a OU named “wsc-i-london” and use this to grant SSH access to “wsc-i-london”. User not in this group, should be denied access. Root access should not be allowed.
- Create a new second domain “competition.ae”.
  - In this domain create the users as stated in the appendix.

RADIUS

- Install RADIUS service.
  - Use LDAP as the authentication back-end.
  - Add wsc-p-stgallen as RADIUS client and VPN user should be authenticated through this server.
  - Use Skill39 as shared secret

CA

- Configure as CA using OpenSSL.
  - Use /etc/ca as the CA root directory
    - Private key should have minimal permission
  - CA attributes should be set as follows:
    - Country code is set to AE
    - Organization is set to WorldSkills International
    - The common name is set to “WorldSkills 2017 CA”
  - Create a root CA certificate.
  - All certificates required in the test project should be published by CA.

SAMBA

- Install Samba
  - Authentication is done by wsc-i-calgary. Local users are not permitted
  - Distribute the share “private”, which is used for DFS on wsc-i-london
    - Local data path: /files/samba/private
    - Share is not visible outside the DFS (e.g. \\wsc-i-calgary\private)
  - Make sure no other folders are shared (either visible nor hidden)

INTERNAL SERVER ZONE

WSC-I-SHIZUOKA

REDIS

- Install redis server (key-value store)
- Add a new entry to the store with following command line code. Replace the content in brackets with some hard-coded equivalents

```
  >> SET skill39:index "Today is the [date] and in one hour is [current time +1]"
```

CACTI MONITORING

- Install Cacti monitoring service
- Change the administrator's password to "Skill39"
- Add a graph of wsc-d-abudhabi's network traffic

PING MONITORING

- Install Icinga monitoring service, use password "Skill39" as the password for "icingaadmin".
- Setup a basic ICMP ping monitor wsc-i-london.
- When monitoring fails, after 60 seconds send a notification to user3@wsc17.cloud.

SYSTEM

- Create a script (shell or php) with the name 'index_update.*' in the folder '/root'
- The script should update the redis entry (created above) with the current date and the mentioned time. The same command as above can be used for shell scripts or `$content = $redis->get('skill39:index');` if you prefer php
- Schedule the execution of the script
    - Every two minutes where the execution must happen on odd-minutes

- Create a script 'ftp_listing.sh' in the folder '/root' that lists the content of the ftp user

CLIENT ZONE

WSC-I-HELSINKI

Install and configure the following services. Make sure that all LDAP users in OU “Misc” can login locally, users from other OU must not be allowed to login locally.

E-MAIL

- Use Icedove as the e-mail client and configure using the user “skill39”.
  - Configure to use user3@wsc17.cloud
  - Send an email to competitor@competition.ae
  - Use IMAP to connect to the mailbox

WEB

- Use Firefox as the web browser.
  - Make sure that www.wsc17.cloud is accessible.
  - No certificate warning
  - Shows appropriate content

FTP

- Use FileZilla as FTP-client
  - Make sure that a connection to wsc-i-london (ftp.wsc17.cloud) can be established.

SAMBA

- Make sure that users can access the file shares from wsc-i-london
  - Mount DFS share to /mnt/dfs
  - You must be able to access both shares (public, private) through DFS

LOGIN

- Add offline capabilities
- After LDAP is offline, it should still be possible for users to access the host within one minute

Add the wsc17.cloud CA certificate as trusted, so that no certificate warnings are shown for all the above.

WSC-E-SEOUL

E-MAIL

- Use Icedove as the e-mail client and configure using the user “skill39”.
  - Configure to use competitor@competition.ae
  - Send an email to user3@wsc17.cloud
  - Use IMAP to connect to the mailbox

VPN

- Install a VPN client for (L2TP/IPSEC)
  - Connect to WSC-P-STGALLEN using any of the VPN-Users.
  - Create a script on “/root/vpn.sh start | stop” to start and stop the VPN connection.

Add the wsc17.cloud CA certificate as trusted, so that no certificate warnings are shown for all the above.

NETWORK/SECURITY

WSC-P-STGALLEN

SOFTWARE

Install software package *freeradius-utils*

ROUTING

Enable routing. Consider the different VLANs!

FIREWALL

Setup a firewall to protect your intranet (Clients, Internal Servers, Protected Servers, DMZ) networks from outside networks. You must make sure that rules targeting "Internet" match all outside networks and not just 172.16.1.0/24.

- Use IPTABLES.
    - Make sure that firewall operates in stateful mode.
    - Allow all ICMP ping traffic to the local machine.
    - Allow all traffic from Clients network to all networks.
    - Allow access to the following services on wsc-i-calgary from all intranet networks and VPN networks:
        - LDAP
        - RADIUS Authentication and Accounting
    - Allow access to the Redis database on wsc-i-shizuoka from the following sources:
        - Host wsc-d-saopaulo
        - Host wsc-d-leipzig
    - Allow access to the FTP service on wsc-i-london from wsc-i-shizouka
    - Allow access to the following services from Internet to wsc-p-stgallen:
        - VPN (L2TP/IPSEC)
    - Configure source NAT for internet access from Clients network.
        - Create a chain called INTERNET-SNAT to translate all outgoing connections except packets headed towards intranet networks.
        - Jump to the custom chain for all traffic originating from Clients network.
    - Configure NAT to provide DNS services on wsc-p-stgallen:
        - All internal IP addresses on router wsc-p-stgallen should be translated when receiving a connection to the DNS port with either TCP or UDP.
        - The host wsc-d-abudhabi should be used as the backend server.
        - Make sure that all intranet hosts are allowed to use wsc-p-stgallen as a nameserver.
    - Configure DNAT to provide access from the internet to wsc-d-abudhabi.
        - SMTPS, IMAPS, HTTPS, and DNS.
    - Ensure that VPN-clients can access the same services as the client’s network.
    - Make sure that SSH is allowed on each host
    - All other traffic must be dropped by default.

VPN

- Install strongswan and xl2tpd service to provide VPN.
- Use a certificate signed by wsc-i-calgary
- Use address range 10.2.4.100 to 10.2.4.120 for VPN clients.
- Authenticate users upon VPN connection. Authenticate only users from OU “VPN” via RADIUS protocol.

APPENDIX A

LDAP USERS

USERNAME	OU	PASSWORD	DOMAIN
user1	VPN	Skill39	wsc17.cloud
user2	VPN	Skill39	wsc17.cloud
user3	MAIL	Skill39	wsc17.cloud
user4	MAIL	Skill39	wsc17.cloud
user5	WSC-I-LONDON	Skill39	wsc17.cloud
user6 – user99	MISC	Skill39	wsc17.cloud
Competitor	MAIL	Skill39	competition.ae

DNS

Nameserver address should be equal on all hosts (except on the DNS server itself, which instead uses localhost) and point to the same address as the gateway.

If you are unable to setup wsc-p-stgallen properly, use the direct IP address of wsc-d-abudhabi and adjust firewall accordingly. You will lose those points.

WSC-D-ABUDHABI

SETTING	VALUE
IP	10.1.1.10/24
Hostname	wsc-d-abudhabi.wsc17.cloud

WSC-D-SAOPAULO

SETTING	VALUE
IP	10.1.1.20/24
Hostname	wsc-d-saopaulo.wsc17.cloud

WSC-D-LEIPZIG

SETTING	VALUE
IP	10.1.1.30/24
Hostname	wsc-d-leipzig.wsc17.cloud

WSC-I-LONDON

SETTING	VALUE
IP	10.2.1.10/24
Hostname	wsc-i-london.wsc17.cloud

WSC-I-CALGARY

SETTING	VALUE
IP	10.2.1.20/24
Hostname	wsc-i-calgary.wsc17.cloud

WSC-I-SHIZUOKA

SETTING	VALUE
IP	10.2.2.10/24
Hostname	wsc-i-shizuoka.wsc17.cloud

WSC-P-STGALLEN

SETTING	VALUE
IP	10.1.1.1/24 (VLAN10) 10.2.1.1/24 (VLAN20) 10.2.2.1/24 (VLAN30) 10.2.3.1/24 (VLAN40) 10.2.4.100-120 (VPN) 172.16.1.254/24 (Internet)
Hostname	wsc-p-stgallen.wsc17.cloud

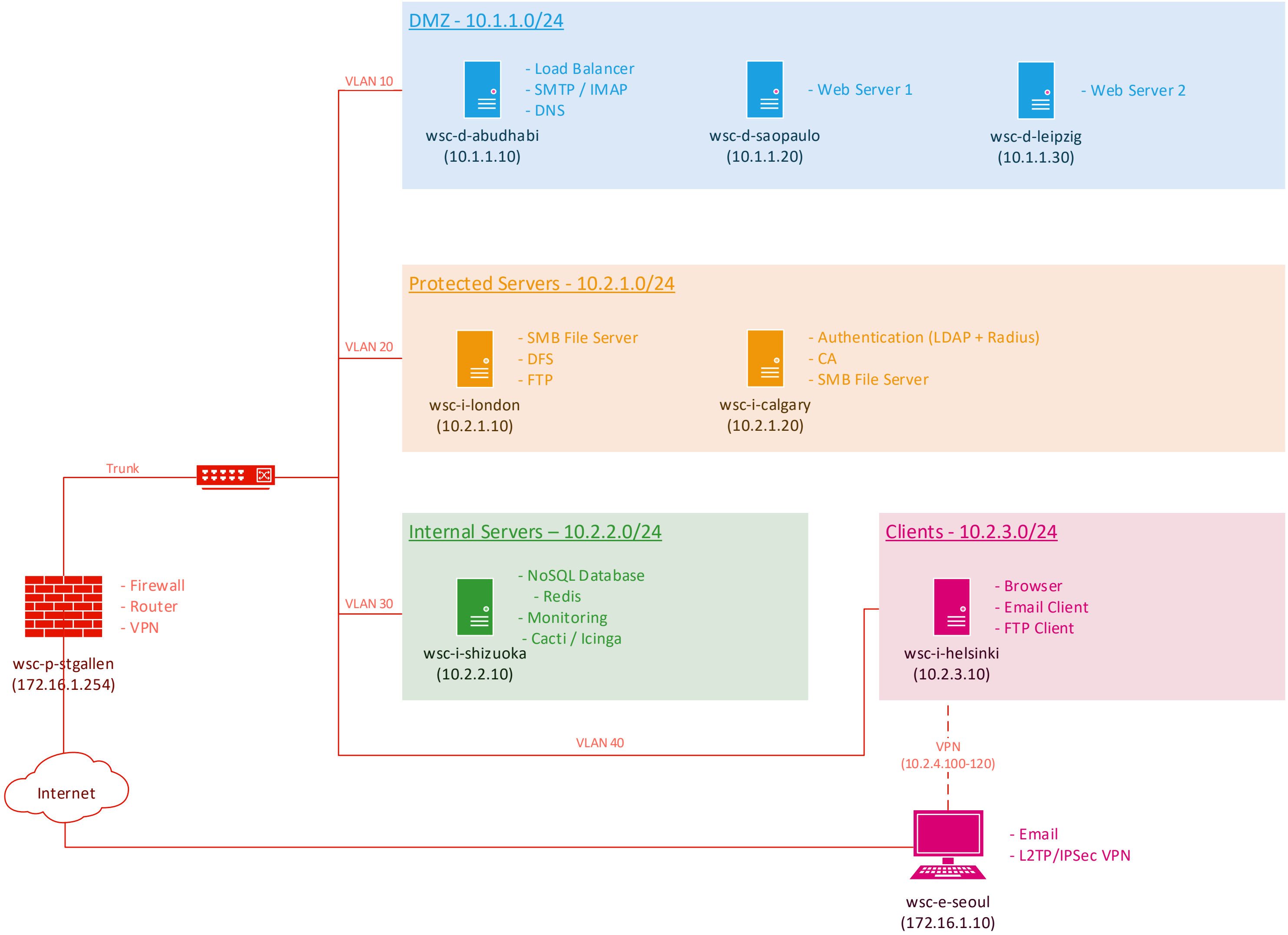
WSC-I-HELSINKI

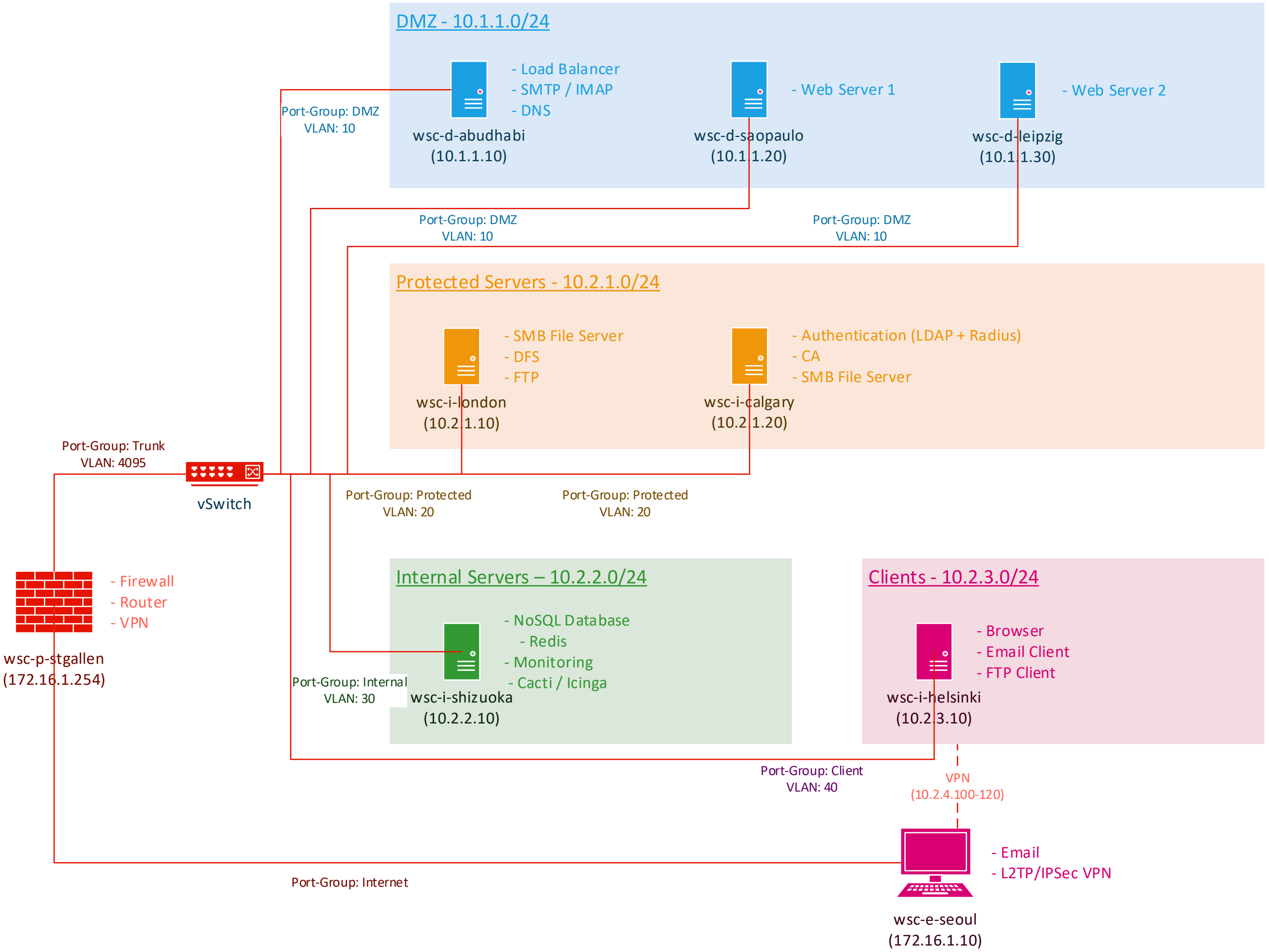
SETTING	VALUE
IP	10.2.3.10/24
Hostname	wsc-i-helsinki.wsc17.cloud

WSC-E-SEOUL

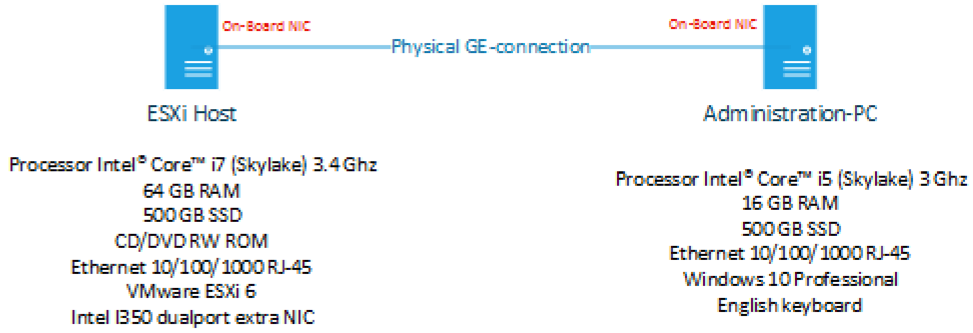
SETTING	VALUE
IP	172.16.1.10/24 (Internet) 10.2.4.1xx (VPN)
Hostname	wsc-e-seoul.wsc17.cloud

APPENDIX B


DMZ - 10.1.1.0/24
- Load Balancer
- SMTP / IMAP
- DNS
wsc-d-abudhabi
(10.1.1.10)
- Web Server 1
wsc-d-saopaulo
(10.1.1.20)
- Web Server 2
wsc-d-leipzig
(10.1.1.30)
VLAN 10
Protected Servers - 10.2.1.0/24
- SMB File Server
- DFS
- FTP
wsc-i-london
(10.2.1.10)
- Authentication (LDAP + Radius)
- CA
- SMB File Server
wsc-i-calgary
(10.2.1.20)
VLAN 20
Trunk
Internal Servers – 10.2.2.0/24
- NoSQL Database
- Redis
- Monitoring
- Cacti / Icinga
wsc-i-shizuoka
(10.2.2.10)
VLAN 30
Clients - 10.2.3.0/24
- Browser
- Email Client
- FTP Client
wsc-i-helsinki
(10.2.3.10)
- Firewall
- Router
- VPN
wsc-p-stgallen
(172.16.1.254)
VLAN 40
VPN
(10.2.4.100-120)
Internet
- Email
- L2TP/IPSec VPN
wsc-e-seoul
(172.16.1.10)



DMZ - 10.1.1.0/24
- Load Balancer
- SMTP / IMAP
- DNS
wsc-d-abudhabi
(10.1.1.10)
- Web Server 1
wsc-d-saopaulo
(10.1.1.20)
- Web Server 2
wsc-d-leipzig
(10.1.1.30)
Port-Group: DMZ
VLAN: 10
Port-Group: DMZ
VLAN: 10
Port-Group: DMZ
VLAN: 10
Protected Servers - 10.2.1.0/24
- SMB File Server
- DFS
- FTP
wsc-i-london
(10.2.1.10)
- Authentication (LDAP + Radius)
- CA
- SMB File Server
wsc-i-calgary
(10.2.1.20)
Port-Group: Trunk
VLAN: 4095
vSwitch
Port-Group: Protected
VLAN: 20
Port-Group: Protected
VLAN: 20
- Firewall
- Router
- VPN
wsc-p-stgallen
(172.16.1.254)
Internal Servers – 10.2.2.0/24
- NoSQL Database
- Redis
- Monitoring
- Cacti / Icinga
Port-Group: Internal
VLAN: 30
wsc-i-shizuoka
(10.2.2.10)
Clients - 10.2.3.0/24
- Browser
- Email Client
- FTP Client
wsc-i-helsinki
(10.2.3.10)
Port-Group: Client
VLAN: 40
VPN
(10.2.4.100-120)
- Email
- L2TP/IPSec VPN
Port-Group: Internet
wsc-e-seoul
(172.16.1.10)



Processor Intel® Core™ i7 (Skylake) 3.4 Ghz
64 GB RAM
500 GB SSD
CD/DVD RW ROM
Ethernet 10/100/1000 RJ-45
VMware ESXi 6
Intel I350 dualport extra NIC

Processor Intel® Core™ i5 (Skylake) 3 Ghz
16 GB RAM
500 GB SSD
Ethernet 10/100/1000 RJ-45
Windows 10 Professional
English keyboard