Linux Technologies

SUPINFO International University

INSTITUTE OF INFORMATION TECHNOLOGY

Datacenter Solutions Coursework

Project

Implementing a highly available secure mail server

Version 1.0
Last update: 09/12/2014
Use: Students
Author: Samuel CUELLA

TABLE OF CONTENTS

1 OBJECTIVES

This project is a research project that will help you improving your overall Linux skills. You will explore course topics beyond the initial in-class course scope.

Your final goal is to implement a Highly Available mail infrastructure along with support services, with a strong emphasis on security. Here is a non-limitative list of involved services/technologies:

- Pacemaker
- Postfix
- Courrier
- iSCSI
- DRBD
- SELinux

2 THE PROJECT

Your assignment is to implement to following topology.

2.1 SERVERS / SERVICES

2.1.1 Support services

As you're going to setup a mail server, you need to install support services first.

2.1.1.1 DNS

Configure DNS to name resolution for the utopia.net domain.

The DNS should provide name resolution for all hosts and servers. Be sure to also add reverse resolution entries for servers.

2.1.2 Mail server

The mail server should accept mail for the utopia domain, and provide access to the mail boxes

through:

- IMAP(S)
- POP3(S)

All these services should be highly available. The mailboxes themselves should be stored on a iSCSI volume which should also be highly available.

Needless to say, the server should be configured will all appropriate authentication and security options.

2.1.2.1 Security

The mail services should not be able to access files or do any operation beside their normal expected behavior.

Create appropriate SELinux components to enforce strict observance of that rule.

2.1.3 iSCSI SAN

Your solution should also include a SAN in the form of a highly-available iSCSI volume.

3 CONDITIONS AND DELIVERY

You're free to use as much (or as less) virtual machines as you want. The only requirement is to have a dedicated virtual machine to act as a network client. However you're expected to be able to explain how to span services across different machines.

Although you can perfectly do this project on your own if you decide to do so, this project has been designed to be done by a group of 3-4 students. There is no need to declare your group before the delivery: Will be considered part of the group all students mentioned in the final delivery. All members of the group present in the delivery will get the same mark.

You have to hand back the following items to your local trainer:

- Modified configuration files for each service/virtual machine
- MD5 Checksum of all your virtual machines hard disks. Give a list of all virtual machines disk files names (vmdk if you're using VMware) and checksums.
- A list of the group members

You will show your work and do a live demonstration during orals.

Warning: You're going to send checksums of your virtual machine disks. Don't power up the virtual machine after the checksum.

3.1 VIRTUAL CAMPUS

Exact same rules apply for all students, including those of the Virtual Campus. However, for obvious reasons, Virtual Campus students won't be evaluated through "live" viva, but remotely via Skype screen sharing to do their demonstration.

They will also send their delivery directly to the local trainer.

4 DEADLINE

You must have sent items from section 4 to your local trainer by the **15 of January 2015, 23h59 GMT+1**.

5 GRADED ITEMS

Item	Points
Highly available Postfix	5
Highly available access (IMAP/POP3)	3
Highly available SAN	3
SELinux policy for mail services	9
Total	20