SUPINFO Academic Dept.

SUPINFO International University

INSTITUTE OF INFORMATION TECHNOLOGY

3LIN - Datacenter Solutions Project - Breaking Smartly Lazy

Contents

Version 1.0
Last update: 27/11/2017
Use: Students
Author: Laurent SANSELME

TABLE OF CONTENTS

1. Objectives 3
2. Project 4
    2.1. Big Freaking First Server 4
    2.2. Big Freaking Second Server 6
3. Conditions And Delivery 7
4. Deadline 8
5. Graded Items 9

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.

Some notions have been seen in earlier courses like 1LIN or 2LIN. Don't hesitate to refer to them if necessary.

Your final goal is detailed in the "Project" chapter.

2. Project

You're a sysadmin employed at "Big Freaking Company". After a lot of years of meritorious and loyal services, the old managerial organization decided to retire and a new team has been employed.

One of the many "Big Freaking Changes" the company decided to establish is the authorization of teleworking. To do so, they want to give the opportunity to any employee who asks to work from home to securely access the company's resources.

You're a really good sysadmin but most of the work you have to do right now has already be done before. So you mostly troubleshoot actual installation and the idea to have to manually give a personal access to numerous employees looks tedious to you.

As a smart lazy employee, you decide to make a specific installation that will allow you to do all your work au-to-ma-ti-ca-lly. That's "Big Freaking Smart".

Needless to say, everything you're going to do will have the appropriate authentication and security options (strong passwords, strong certificates, …) because bad security = more work a day or an other.

2.1. Big Freaking First Server

This server will be the essential part of your installation.

2.1.1. VPN Server

That's the core feature wanted by your hierarchy. So that has to be implemented and functional. The best choice for this is of course OpenVPN.

You want every user to connect to the internal company's network from anywhere. For that, your server has an open incoming port on the global router's company. You can pick whichever you want.

Your server has a second Ethernet card that allows the direct redirection from the internal VPN Network to the company's network.

Everybody must have a unique certificate so you can change it quickly if necessary (computer loss, compromised certificate, ...) and to allow them to connect from anywhere.

Your CA will contain the name of the company. You are free to elect the encryption system you want but be sure to have a key length big enough to ensure security.

You will store a copy of every certificate emitted for archival purpose.

2.1.2. DRBD

As you're dealing with certificates, it's mandatory to have a second storage in case of Big Freaking Disk Failure or Big Freaking Motherboard Burn.

You decide to implement a DRBD service on a distant second server that will contain any data you will create with this set up. Therefore you will apply it on the entire isolated partition containing anything.

2.1.3. Mail Server

To ask for a distant access, people will have to ... contact you. So why not by mail. On a specific address. With their "**FirstName.LastName@BFC.com**" address.

You decide to use an entire domain name for this benefit and you name it "**teleworking.BFC.com.**"

Note

For the demo, you won't have, unless you want to, to implement the DNS server to give this access. You can just do it with a "host" file modification. For the project, you consider that the DNS server is already managed in the company and that you will just have to add an entry and not manage an entire new zone.

You don't want to base your certificate creation on an object or a content because you know people may forget to follow any specific convention. So you allow them to tell you absolutely anything.

You think of 3 kind of request:

2.1.3.1. Ask for a new certificate

When an employee wants a certificate, he has to send an email on the "**request.access@teleworking.BFC.com**".

You will than create a certificate and send back to him all the files (certificates, keys, ...) he needs to be able to connect.

2.1.3.2. Problem with a certificate

When an employee has a problem with his certificate (corrupt certificate, loss, ...) he can ask to revoke the old one and ask to create another just by sending an email to "**certificate.problem@teleworking.BFC.com**"

You will confirm him by mail that his request has been taken into account and you will send him his new set of files.

2.1.3.3. Revocation of the certificate

When an employee leaves the company, his access must be quickly blocked to avoid any data leak. So when an employee leaves, you will revoke his old certificate definitively.

Only the human resources have this power so you will control that emails you receive on the "**definitive.departure@teleworking.BFC.com**" come from "**hr@BFC.com**"

You will confirm to the HR department every revocation once done.

2.1.4. Scripting

Here comes the laziest and smartest part of your Big Freaking Plan.

You will develop scripts to make the work for you. You have implemented a process that allows you to differentiate easily everybody and what they want. Time to make the machines do the work for you. Skynet only exists in terminator.

Your script or set of scripts will drive the certificate creation and revocation every 5 minutes. To do so, you will read the newly received emails on the different mailboxes and do the action/s they are meant for.

2.1.5. Quality Of Service

As you use new resources that were unused at this time, you anticipate the fact that someday you may have to provide new services on this machine, so you will implement quality of service to hold half the bandwidth for the mails you have to send.

2.2. Big Freaking Second Server

This server is your backup solution in case of failure.

2.2.1. DRBD

This server will have the second part of the DRBD service you installed on your first server. It must be in passive mode as you think that maybe some day you will install an high availability system.

3. Conditions And Delivery

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 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 on the https://sce.sad.supinfo.com/ platform in a ZIP file:

- Configuration files for each service/virtual machine
- Source code of your script(s)
- SHA1 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. For that purpose, you will have different users to show how everything work fine and anticipate to be able to run your script manually so your evaluator won't have to wait for 5 minutes.

Warning

You're going to send checksums of your virtual machine disks. Don't power up the virtual machine after the checksum, only do it when asked by your instructor.

4. Deadline

You must have sent items from Chapter 3 in a ZIP file on the http://sce.sad.supinfo.com/ platform before the date given on the 3LIN exam section. It may vary depending on your location.

5. Graded Items

Table 5.1.

Services	Description	Points	Total Points
VPN	VPN Server configuration (CA, Network access, etc.)	4	5
	VPN Certificate generation	1	
DRBD	DRBD replication on both servers	2	2
Mail	Every account created	2	3
	Mail can be sent and received	1	
Scripting	Can create certificate on mail reception	4	8
	Can delete and create a new certificate on mail reception	1	
	Can revoke definitively a certificate on mail reception	2	
	Run every 5 minutes	1	
QoS	Bandwidth correctly holded	2	2
Total			20