SUPINFO Academic Dept.

SUPINFO International University

INSTITUTE OF INFORMATION TECHNOLOGY

Microsoft Windows Active Directory - Project

Document content

Subject
Delivery

Version 1.0
Last update: 15/11/2018
Use: Students
Author: Judicaël LAPORTE

SUMMARY

1 CONTEXT

You have been hiring recently in an international company ShipTruck. This company is a leader in the shipping service in France and wants to develop its business model in Europe.

This company was created in 1975 and doesn't really take into consideration the benefits of IT for his business.

You are the new IT Administrator of this company and you have a lot of work to obtain a good infrastructure for the entire company.

First of all, you decide to implement a complete Active Directory Architecture to simplify the administration of accounts, printers, computers…

In the same time, you want to implement a complete documentation of your work. Those best practices are essential for you and for the future of your new company.

2 DELIVERY

Your document must be delivered to your trainer as a single zip with all documents and with the main configuration steps, including commented screenshots of your work.

Notation will be mainly based on the presentation that will illustrate your work.
The presentation must be made in **20 minutes**. Please reserve a couple of minutes for questions.

During the presentation, it is mandatory that your architecture is **functional**. You will be evaluated on a running architecture only.
No Screenshots or videos can be considered as a proof.

You can realise this project either by group of **4** students or less.

Upload your zip on **sce.sad.supinfo.com before the deadline**.

Plagiarism and copying are strictly forbidden. Any elements of this kind would result in a 0 grade and the cheater status for all the groups implicated in the fraud.

3 ARCHITECTURE

First of all you must install the entire architecture.

ShipTruck is organized in several agencies to deliver packages over the country. Headquarter is based in Paris and all employees employed in the Direction Department work on the Headquarter site.

Agencies are installed in the main town of France and are managed by several employees.

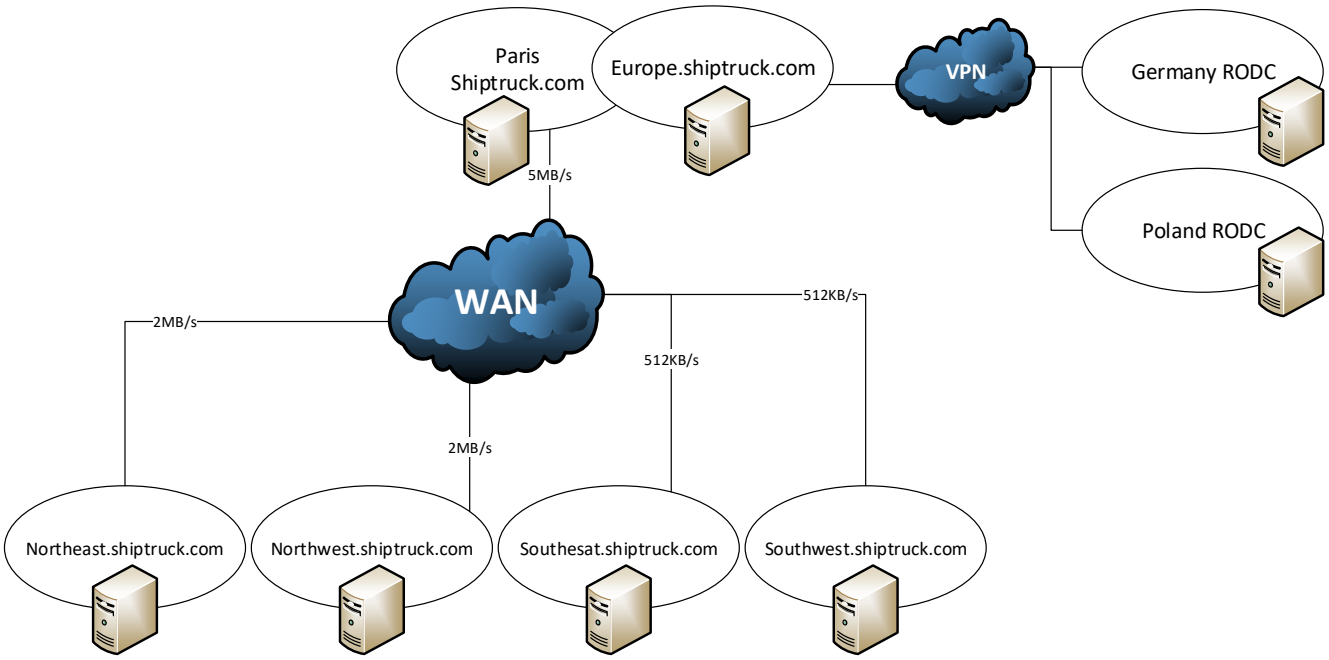
For this documentation, you decide to not develop each agencies configuration but only special configurations.

3.1 ARCHITECTURE INSTALLATION (3 POINTS)

Begin by installing the first domain controller.
The domain name will be shiptruck.lan and the functional level must be Windows server 2016.

This server is the main domain of the architecture and it will be used later for the Headquarter configurations.

Fortunately a WAN network already exists between agencies. It is used for a business software that was installed by an IT service company. But this WAN is linked by region not by agencies according to this scheme:



So to respect this architecture and for financial compliance you will create sub domains by region rather than by agencies.

On this document, you do not detail the configuration of sub domains of France regions.

However, you install a new domain controller with a sub domain named europe.shiptruck.com because it will have different configuration options.

When you present the project to the Direction Department employees, they are satisfied by the improvement brought by the project. But in another hand, they are afraid to install a domain controller in a foreign land. So you must find a solution to improve security of domain controllers that are present in those countries.

You decide to install a read only domain controller. The first country to receive this kind of domain controller is Germany.

3.2 Active Directory hierarchy (5 points)

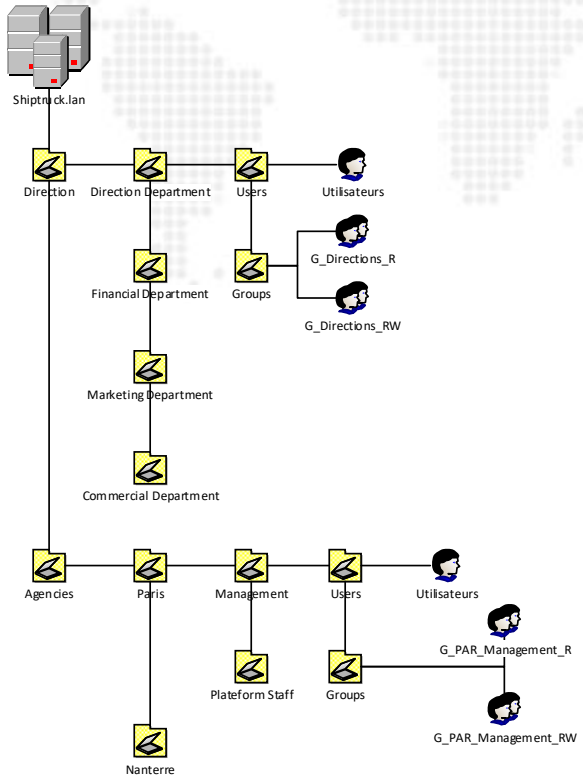
You now have a server architecture but you have to organize your Active Directory and populate it.

All this part must be done by PowerShell script(s).

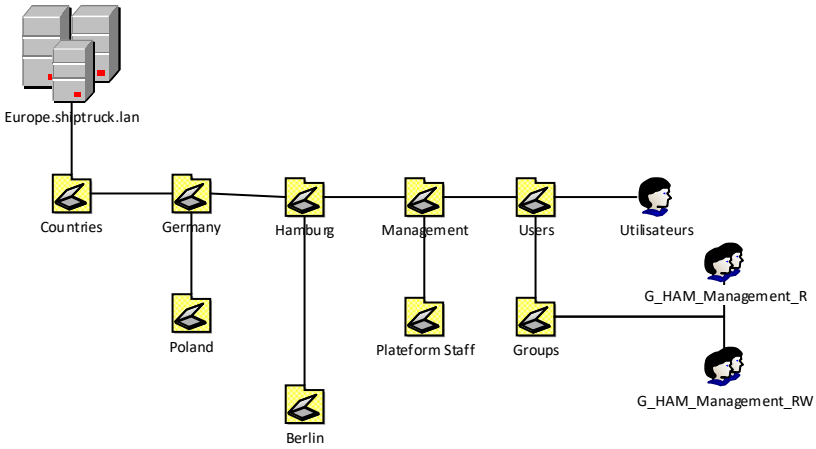
Use the document named organization.xlsx that represents all the employees and where they work in the Company to create accounts, groups and organizational units.

You must create a script that can be reused on other domain controllers or domains.
The script must create the architecture for shiptruck.lan and europe.shiptruck.lan.

The shiptruck.lan architecture must look like:



The europe.shiptruck.lan architecture must look like:



All details are not present on those schemes. For example, all Departments in the Direction organizational unit have the same sub architecture as Direction Department.

Please respect a naming convention like G_HAM_Management_R

- G: it's because it's a group
- HAM: it's the three first letters of the agency town
- Management: it's the full name of the department
- R: it's for rights (R for Read and RW for Read and Write)

By default, all employees of an agency and a department are members of the read group of their department.

Account login must be like pdupont for a person who is named Paul DUPONT.

3.3 SECURITY

3.3.1 RODC Security (2 points)

In case of VPN shut down, accounts located in a foreign land must be replicated on RODC that is running in this country.

In another hand, those servers must have a consolidated password security.
Policy:

- Length: 12
- Complexity: on
- Must be change every 30 days
- Password retention: 10

3.3.2 Others policies (3 points)

All employees must have a policy that includes:

- Computer configuration :
  - Password :
    - Remember 3 passwords
    - Maximum life : 90 days
    - Strong password enable
    - Length : 8
  - Internet explorer :
    - Disable accelerators
    - Disable al tabs (advanced, connexion…)
    - Delete history after browser quit
  - Enable remote desktop
- User
  - The first page of internet explorer must be http://www.microsoft.com

An exception must be made for people who are in the Direction organizational unit. Previous configurations must be applied with those additional options:

- Computer configuration :
  - Password :
    - Remember 5 passwords
    - Maximum life : 30 days
    - Strong password enable
    - Length : 10
  - Account :
    - Account must be locked after 3 bad login
  - Internet Explorer:
    - The content tab must be enable
  - Connect a network drive called IDBOOSTER

Show in your documentation where you apply those policies.

3.4 NETWORK AND REPLICATION (3 POINTS)

You must take care about the network bandwidth of the WAN configuration.

To do this you must configure three sites: North, South, and Europe.

Place domain controllers in the correct site. ShipTruck.com and europ.shiptruck.com in North and the RODC in the Europe site.

You also need to configure site links. The first Active Directory domain controller is in the North site and Europe servers replicate their data with North domain controllers. Bandwidth with Europe sites are very slow due to the VPN connection and many business data are transferring during the working hours. Europe servers are also RODC that don't need synchronisation all the time. So disable replication during the working hours (8H to 20H) and increase the replication interval to 300 min.

3.5 MULTIPLE DOMAIN (4 POINTS)

In France ShipTruck has recently buy another company to be present in more town and increase its competitiveness.

For your POC install a new domain controller that represents this new company, name it bty.lan.

Then you must create a unidirectional approbation between shiptruck.lan and bty.lan. Users that are present in shiptruck.lan subdomains must be able to access to bty.lan resources.