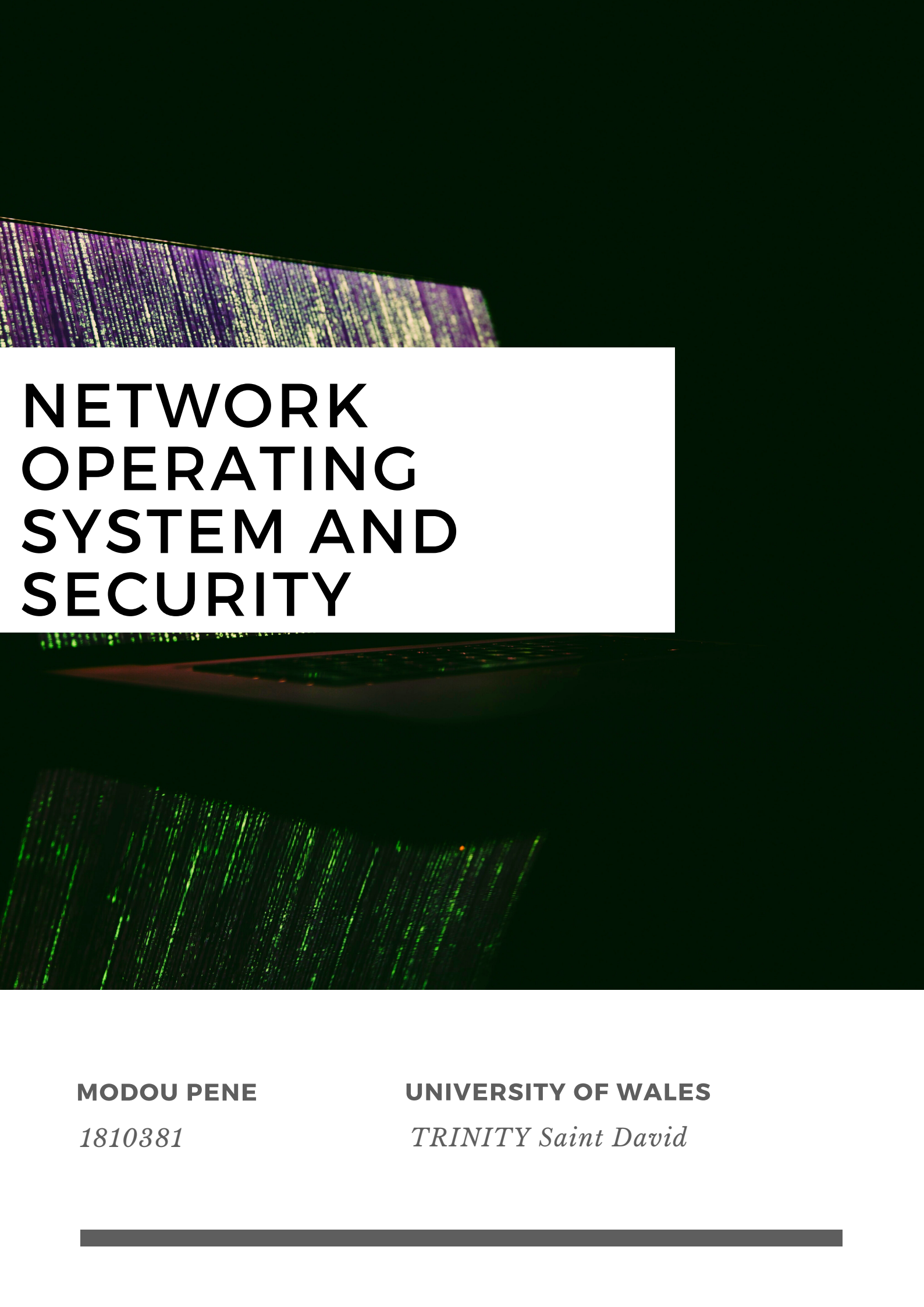




NETWORK OPERATING SYSTEM AND SECURITY

MODOU PENE

1810381

UNIVERSITY OF WALES

TRINITY Saint David

ACTIVE DIRECTORY

Introduction

Active Directory is the heart at the IT infrastructure level, of most companies around the globe is definitely the one of the layer on which to build the part of secure, automate for users and pc. To build the right infrastructure, we don't need to be a magician but it is important to know a some little ways to avoid configuration and security issues.

Active Directory was build over 20 year ago ,, Windows 2000 server introduced in Windows the NT4. The main important of AD is to have a database with all the details related to infrastructure objects (users, computers, groups, etc.) in order to simplify the access and exchange of data. Like any database, other products can read its contents to assess access to various resources.

The most important feature of Active Directory is that we can extend our table to add more columns, properties, and values. Most of the applications, such as Exchange Server, use AD to add elements and functionality. This allows us to consolidate and also avoid inventing other methods to manage mailbox permissions and properties.

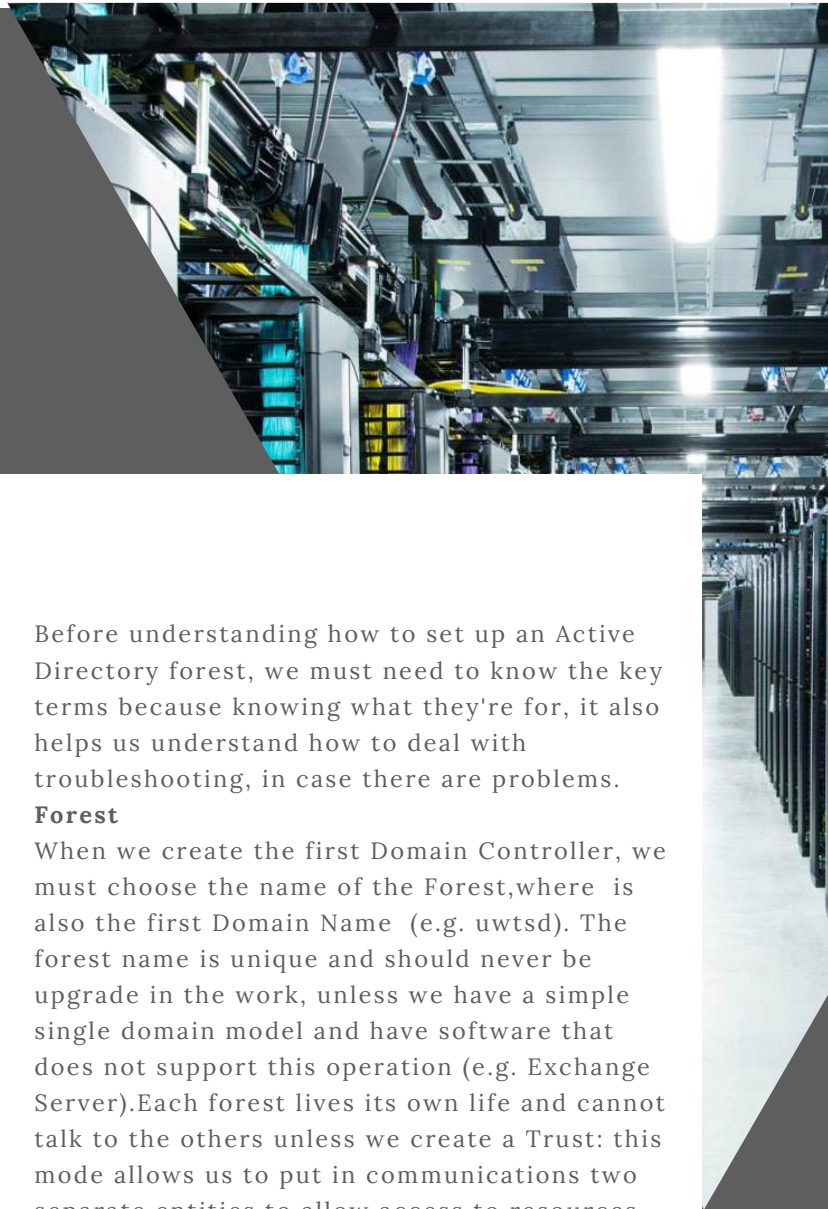
Before understanding how to set up an Active Directory forest, we must need to know the key terms because knowing what they're for, it also helps us understand how to deal with troubleshooting, in case there are problems.

Forest

When we create the first Domain Controller, we must choose the name of the Forest, where is also the first Domain Name (e.g. uwtsd). The forest name is unique and should never be upgrade in the work, unless we have a simple single domain model and have software that does not support this operation (e.g. Exchange Server). Each forest lives its own life and cannot talk to the others unless we create a Trust: this mode allows us to put in communications two separate entities to allow access to resources in a cross-reference; for example, it is a practice used when two companies are merged, since the trust allows the user of domain **A** to access the file server in domain **B** with his credentials.

Domain property

The domain name is one of the main part of the Active Directory when is created, we will choose the domain name and with it the label to apply to each object in our infrastructure. In most AD, forest, and domain models, they are the same name because it reduces the complexity of the infrastructure.





There is the ability to divide the infrastructure model into Child Domain Name, `uwtsd.com`, which are logical entities separated from the root domain that allow you to be managed differently. Some large companies use the top-level domain to place resources (e.g. servers) and use sub-domains to place users and groups. The subdomain requires a dedicated DC, and the Trust must automatically configured with the root domain to allow information to pass.

FSMO

The Flexible Single Master Operation is the set of five roles on which the Active Directory entity rotates when we need to add a new domain Controller, synchronise the time, or add a new object (user or group), it is called. By default, FSMO are assigned to the first Domain Controller you create, but they can be separated on two or more machines. The roles are called as follows:

- Master Schema (Forest)
- Domain Naming Master (Forest)
- Primary Domain Controller (Domain)
- Infrastructure Master (Domain)
- Domain (RID)
- Losing a Domain Controller with one of these roles can reduce some functionality. For example, the loss of the Primary Domain Controller role prevents you from receiving password updates when they are changed.

Global Catalog

The global catalog is a multi-domain catalog that help us for a quick search of objects without having to query within each individual domain. Its purpose is to use partial information or attribute sets to quickly find Active Directory users, computers, and other resources. Required in any infrastructure, this role becomes crucial in complex scenarios (e.g. multi-domain). The GC role is automatically assigned to the first Domain Controller created and is maintained by the ADDS replication system. You can assign this role to other DCs as well, but in some cases, it's not recommended.

Dns

There is no Active Directory without a Domain Name System, which is the tree that allows the transposed between name and IP address. The DNS server manages all physical objects that are part of the AD infrastructure and maintains updates when objects have trust (usually when machines belong to the domain). Without proper DNS configuration, all Active Directory would not work correctly; not surprisingly, in most of the problems encountered in object resolution, or authentication, we find the DNS server as the first suspect. For example, erroneous removal of a Domain Controller can lead to incorrect removal in DNS, which leads to errors in replicas, clients that cannot contact objects, or who can no longer authenticate.



When planning to build an Active Directory infrastructure, it's good to know a few tricks to avoid security and configuration issues:

Rename the Domain Admin – All attacks start with trying to force the administrator account. Our first step should be to rename it, choosing a name other than the standards. For example, it might be called our company: Admin_uwtsdAD.

Strong Password for Domain Admin – The Domain Admin should set a strong and reserved password. Remember that this account has access to everything and therefore once lost, there will be no way to stop it and any object would be at risk.

Dedicated CREDENTIALS for IT – Each IT department member must have separate credentials, one for ordinary operations (PC use) and one for administration operations. In the event of an attack, the classic account will have no access to anything but your PC and this will prevent escalation from a security perspective.

Assign The Right Permissions – If you have multiple administrators, it is good to assign well-defined permissions to each of them. Nominal credentials, in addition to being required by law, are useful to understand who does what. No user should ever go beyond the Domain Admin role to avoid changing the schema or other Areas of Active Directory.

At least Two Domain Controllers – No matter the size of our infrastructure, having two DCs can be a great parachute because the loss of the only Domain Controller could mean the forced shutdown of your entire company.

Naming Convention – Defining a naming convention can help us build a clean, talking infrastructure. This methodology should be applied to clients, servers, but also network devices.

Update DC – Security also goes from applying Windows updates and keeping Domain Controllers aligned helps your business not to be subject to the latest exploits and security flaws.

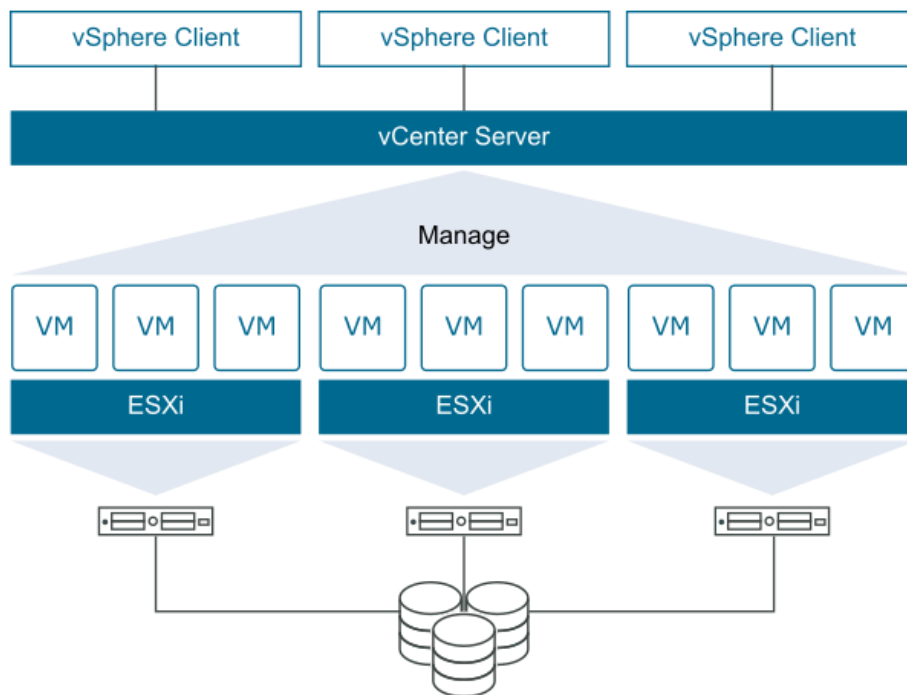
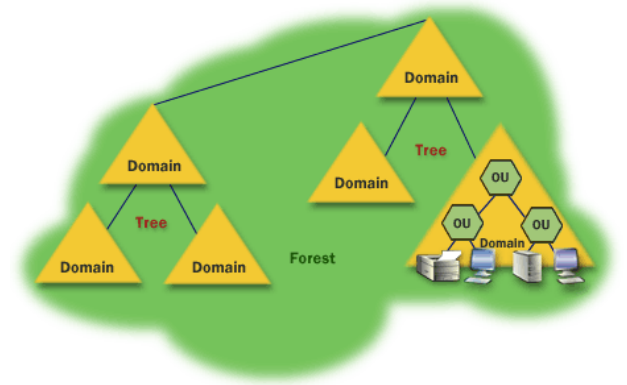
Virtual Machine

We want to implement Active Directory through virtual machines, no problem, but it's good to keep in mind the following considerations:

Virtual DCs are Supported – Starting with Windows Server 2012, with the introduction of a component called VM Generation-ID, we can use a virtual machine as a Domain Controller. With Windows Server 2008 and 2008 R2, it was possible but not supported by Microsoft. Always remember to set the VM to start automatically with a 0-second Start-Time.

No Checkpoint – Although supported, it is best to avoid the creation of checkpoints for Domain Controllers.

VM Replication – Replication should never be used. If we have a Disaster Recovery site, it's good to set up a Domain Controller and use Active Directory tools to replicate, which is definitely more functional.



Conclusion

As we've seen, having all the informations about how to configuration Active Directory can help us to decide best to implement our infrastructure to avoid configuration errors and to keep it up the level of security.

References

D. Kiwior and S. Zabele, "Active Resource allocation in Active Networks", IEEE JSAC, vol. 19, no. 3, pp. 452-459, March 2001.

Ramachandran, R. Pandey and S.-H. Chan, "Fair Resource Allocation in Active Networks", Proceedings of the IEEE International Conference on Computer Communications and Networks (ICCCN), pp. 468-475, Oct 16-18, 2000.