Domaine et contrôleur de domaine

1. Définition

Domaine : ensemble d’ordinateurs qui partagent des informations. C’est pu être une zone géographique, une entreprise ou un service d’une entreprise

godefroy

Sio

Sidoine.com

.jbdelasalle.com

Contrôle de domaine : Grere toutes machines de notre domainen authentification des utilisateurs, GPO : stratégie de sécurité du domaine

1. Services

DNS

DHCP

Service WEB (IIS/Apache)

Base de données (MySQL, SQL Server)

1. Identité et accées

Règlementer les accès aux données, ressources

ACL , ACE (windows)

ACL : lisre des droits associés aune ressource

ACE : Un droit (une ligne) dans une ACL

SID : identifiant des sécurités d’une ressources, un utilisateur, une machine

**SID** a le format suivant : **S-1-5-12–7623811015-3361044348-030300820-1013**

1. Authentifier, autoriser, gérer le compte

Nom d’utilisatateur (login)

Mot de passe

Station : SAM

Serveur : SAM (utilisateur locaux)

Serveur CD : Active directory (utilisateurs du domaine)

1. Active directory

Base de donnée LDAP

|  |
| --- |
| Schéma (structure de la base de données) |
| Configuration domaine |
| Data Store (utilisateurs, Machines, domaine) |
| DNS (optionnel) |
| Catalogue Globale (données présentes sur toutes la foret) |

C’est anciennement un système d’annuaire

1. arbre

Sio.local

Utilisateurs Machines

Nndaudier amedessi SIO-3807-PRF SIO-3806-PR

1. représentation

DC : domaine component

OU : organizational unit

CN : common Name

DC = sio

OU = utilisateur

CN = nnaudier

* cn = nnaudier, ou = Utilisateurs, DC = sio, DC = local

local

sio

Utilisateurs Machines

Professeurs Eleves 3806 3807

SIO 1 SIO2 Prof Prof

SLAM SISR SLAM SISR

CN = tcaute, OU = SISR, OU = SIO1, OU = Eleves, OU = Utilisateurs, DC = sio, DC = local

Kerberos

1. introduction

Ciffrement asymétrique 🡺 2 clés

* clé publique (source) 🡺 chiffrer
* clé privée (destinataire) 🡺 déchiffrer

Ksrc (données)

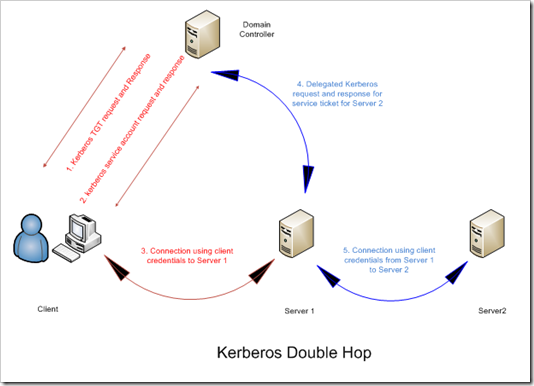
Destinataire

K dest

Source

K src

1. fonctionnement



1. Sécurité

Si les clés sont compromises, tout est compromis

Si on peut intercepter les tickets, on peut usurper l’identité du client

1. Utilisation

Authentification Windows, Unix

Apache (serveur web)

Filezilla (serveur ftp)

Mac OS X 10.2

Windows 2000

Samba (SMB, partage de dossier)

|  |  |  |
| --- | --- | --- |
| Mondomaine.com | NS | Dns1.mondomaine.com |
| Mondomaine.com | NS | Dn2.mondomaine.com |
| Mondomaine.com  Dns1.mondomaine.com | A | 80.113.201.13 |
| Mondomaine.com  Dn2.mondomaine.com | A | 80.113.201.14 |
| Mondomaine.com | A | 80.113.201.16 |
| [www.mondomaine.com](http://www.mondomaine.com) | A | 80.113.201.16 |
| Pop3.mondomaine.com | MX | 80.113.201.15  Mail.mondomaine.com |
| Imap.mondomaine.com | MX | 80.113.201.15  Mail.mondomaine.com |
| Smtp.mondomaine.com | MX | 80.113.201.15  Mail.mondomaine.com |
| [ftp.mondomaine.com](ftp://ftp.mondomaine.com) | CNAME | 80.113.201.16  Mondomaine.com |
| [www.mondomaine.com](http://www.mondomaine.com) | CNAME | 80.113.201.16 |
| [www.mondomaine.com](http://www.mondomaine.com) | CNAME | Mondomaine.com |

NS : Serveur DNS

A : Lie les noms de domaines et les IPs

MX : serveur de messagerie

CNAME : alias

SAUVEGARDE :

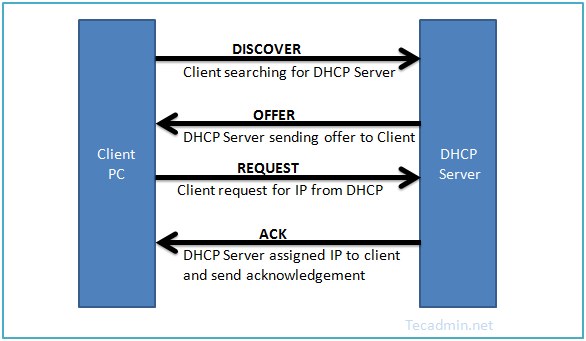
1. Introduction
2. Types de sauvegarde

* Sauvegarde complète
* Différentielle
* Incrémentiel

1. Rotation des supports de stockage

DHCP (Dynamic Host Configuration Protocol)

1. fonctionnement



2. Paramétrage Serveur

* Bail
* Pool (Plage d’adresse IP)

Adresse IP de début

Adresse IP de fin

Masque réseau

* Information supplémentaire (PXE, etc)

3. Paramètre Client

Configurer la carte réseau en mode DHCP

4. Agent Relais DHCP

Linux

Ubuntu/debian/Mint/Kali/Gentoo

Fedora / ArchLinux/ Redhat

Triskal

Slockware

1. Système de fichier

Amorce : MBR ou GPT

GRUB : outil pour le MultiBoot

IDE : HDA1

B

SATA SDA1

B

2. Arboressance du disque

/

/etc (configutation, liste des utilisateurs et mots de passes)

/home ( données utilisateurs)

/user

/root (Données de l’admistrateur)

/bin (logiciels système)

/sbin

/usr (logiciels et environnement graphique)

/opt

/media (CD, USB, Disque Windows, Disque reseau)

/proc (Equipements)

/dev

/lib (Bibliothèque)

/var (Journaux de sécurité)

Linux et les droits de sécurité

Windows :

ACL

Administrateurs

Autres

Groupe

Utilisateurs

Propriétaire

D RWX RWX RWX (Utilisateur(RX), Groupe(R), Autres(R)).

Shell Linux

Bash

1. Script

# !/bin/bash

Echo « Hello World »

2. variables

Echo $message

Message = « Boujour »

Personne[0] = « Gates »

Personne[1] = « Bill »

Echo ${personne[0]}

Echo ${personne[1]}

Echo ${personne[2]}

3. Chaine de texte

Texte = « Mon texte »

Echo $texte

Echo « Mon texte est : $texte » 🡺 Mon texte est : Mon texte

Echo  ‘Mon texte est : $texte ‘ 🡺 Mon texte est : $texte

4. les Tests

If [ -f fichier.txt ], then

Echo « le fichier existe »

fi

If [ -d Mondossier ]; then

Echo « le dossier existe »

fi

if [ -x script.sh ] ; then

|  |  |  |  |
| --- | --- | --- | --- |
| Maths | Français | Anglais | Bash |
| = | Egale | Equal | -eq |
| ≠ <> | Diffèrent | Not equal | -ne |
| < | Inférieur | Lower | -lt |
| ≤ | Inférieur ou égale | Lower or Equal | -le |
| > | Supérieur | Greater | -gt |
| ≥ | Supérieur ou égal | Greater or Equal | -ge |

5. calculs

N1 = 4

N2 = 5

Res = $(($n1 + $n2))

Echo $res

If [ $var –eq 7 ] ; then

Echo « ok »

Else

Echo « pas Ok »

Fi

6. Structure de contrôle

Case (switch)

Case $var in

Start)

Echo « start » ;;

Stop)

Echo « stop » ;;

Restart)

Echo « Restart » ;;

Statue)

Echo « Satue » ;;

\*)

Echo « défaut » ;;

Esac

**Boucle FOR**

For (( i = 0 ; $i –lt 10 ; i = $(( $i + 1)) )) do

Echo $i

Done

For valeur in $liste do

Echo $valeur

Done