



PROJET 3.2

M2L



Loïc Bonnin

Aziz Ouattara

Youva Ait Hadi

Eva Gonzalez-Burga

Administration réseau (Serge RIBA)

Mission 1.1 – supervision du parc réseau

Installation de Eyes Of Network et implémentation dans le réseau de la M2L

Dans le cas suivant l'installation de EON est effectué sur une VM mais dans le réseau de la M2L il est déployée sur une Machine physique.

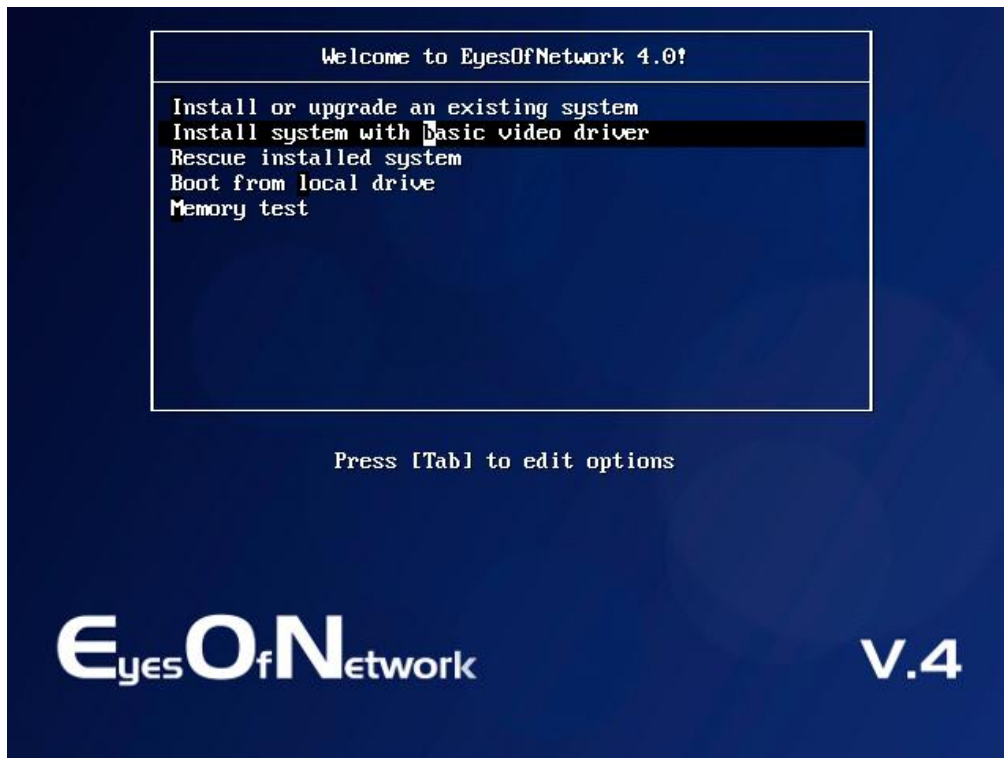
Ce tuto est organisé de la façon suivante :

1. l'installation et la configuration de Eon
2. L'installation de NS++ sur un poste client et activation du protocole snmp sous WINDOWS 7
3. L'activation du protocole SNMP sur le commutateur et le routeur Cisco
4. La présentation de l'interface graphique WEB administrateur de EON

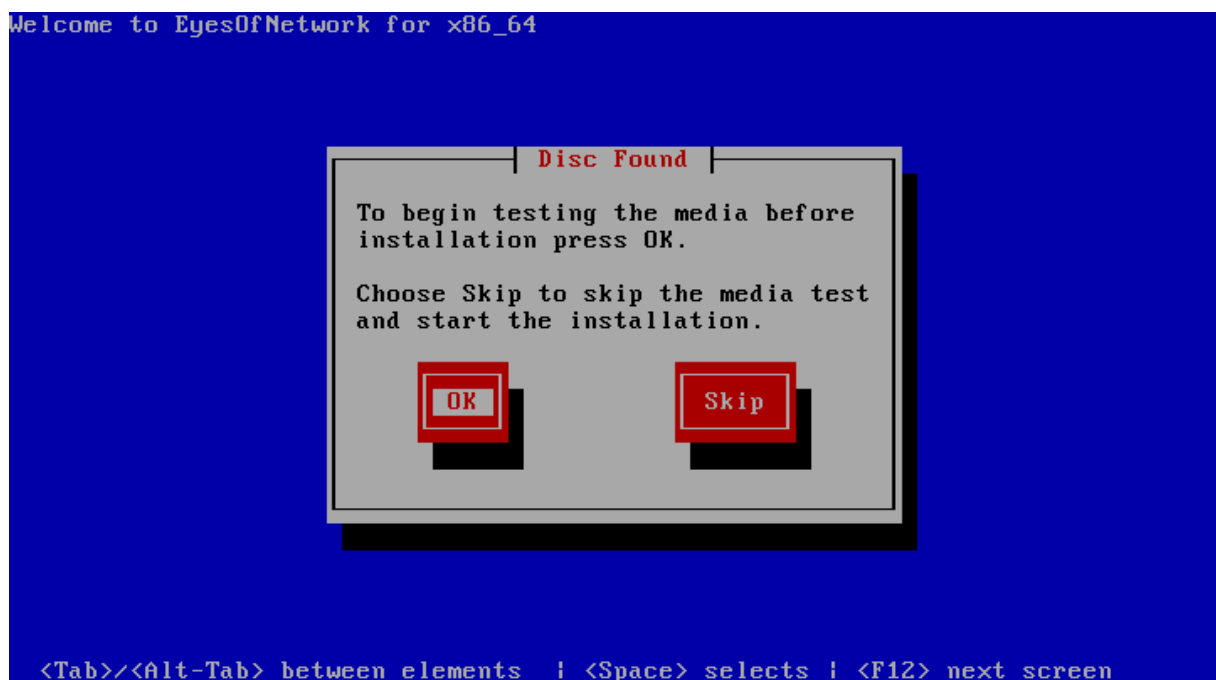
Installation et la configuration de Eon

Rendez vous sur le site officielle de Eon et Télécharger la dernière version de EON

https://www.eyesofnetwork.com/?page_id=48&lang=fr



Dans notre cas nous installerons EON avec l'interface graphique



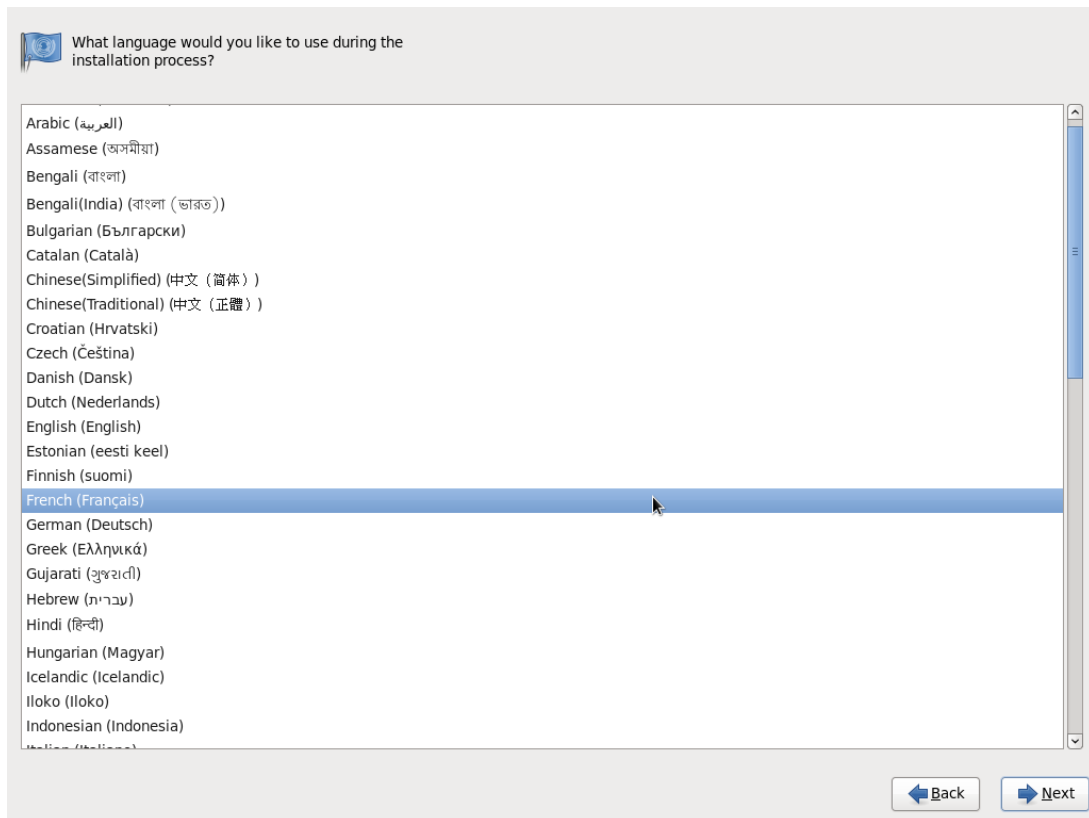
L'installation commence EON vous propose de testé votre image pour être sûr qu'elle est complète et sans erreur avant l'installation

E_{yes}**ON**_fNetwork

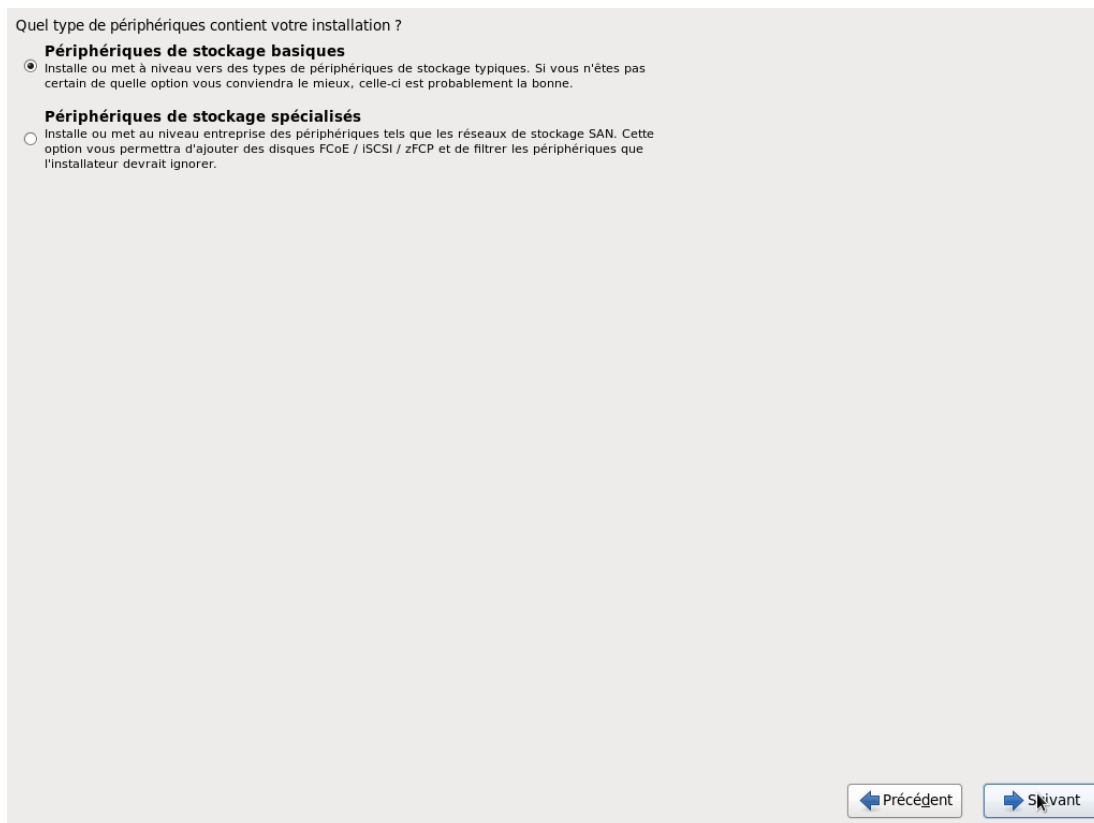
V.4

← Back


Next →



Choix de la langue « Français » 😊




Nous allons utiliser un Disque dure classique pour effectuer l'installation

 Veuillez nommer cet ordinateur. Le nom d'hôte identifie l'ordinateur sur le réseau.

Nom d'hôte :

Nous allons nommer notre serveur EyesOfNetwork

 Le compte « root » est utilisé pour administrer le système. Saisissez un mot de passe pour l'utilisateur « root ».

Mot de passe « root » :

Confirmation :

Ceci est la Configuration du Mot de passe d'administration

Quel type d'installation souhaitez-vous ?

- Utiliser tout l'espace**
Supprime toutes les partitions sur le(s) périphérique(s) sélectionné(s). Cela inclut les partitions créées par d'autres systèmes d'exploitation.
Astuce : Cette option supprimera les données du (ou des) périphérique(s) sélectionné(s). Assurez-vous de bien faire des copies de sauvegarde.
- Remplacement du (ou des) système(s) Linux existant(s)**
Supprime uniquement les partitions Linux (créées depuis une installation Linux précédente). Ceci ne supprimera pas les autres partitions que vous pourriez avoir sur votre (ou vos) périphérique(s) de stockage (tel que VFAT ou FAT32).
Astuce : Cette option supprimera les données du (ou des) périphérique(s) sélectionné(s). Assurez-vous de bien faire des copies de sauvegarde.
- Réduire la taille du système actuel**
Réduire les partitions existantes afin de créer de l'espace pour le partitionnement par défaut.
- Utiliser l'espace libre**
Conserve vos données et partitions actuelles et n'utilise que l'espace non-partitionné sur le(s) périphérique(s) sélectionné(s), en supposant que vous possédez suffisamment d'espace disponible.
- Créer un partitionnement personnalisé**
Créer manuellement votre propre partitionnement personnalisé sur le(s) périphérique(s) sélectionné(s) à l'aide de l'outil de partitionnement.

Chiffrer le système
 Revoir et modifier le schéma de partitionnement

Nous allons utiliser tout l'espace du disque dure ce qui est recommandé pour une installation propre

L'installation par défaut de EyesOfNetwork est une installation minimale. Vous pouvez optionnellement sélectionner un jeu de logiciels différents.

Minimal

Merci de sélectionner les dépôts que vous souhaitez utiliser pour l'installation des logiciels.

EyesOfNetwork

Vous pouvez personnaliser la sélection des logiciels maintenant, ou après l'installation via l'application de gestion des logiciels.

Personnaliser ultérieurement Personnaliser maintenant

! ATTENTION !

Cocher la case Personnaliser Maintenant

Pour installer les options supplémentaires pour la prise en charge de Nagios et autre

EyesOfNetwork Supervision	<input checked="" type="checkbox"/> Base
EyesOfNetwork Production	<input checked="" type="checkbox"/> Options
	<input checked="" type="checkbox"/> Shinken (BETA)

Paquetages fournissant Shinken en remplacement expérimental de Nagios.

Paquets optionnels sélectionnés : 4 sur 4

Cocher toutes les cases proposées

EyesOfNetwork Supervision	<input checked="" type="checkbox"/> Gestion des incidents
EyesOfNetwork Production	<input checked="" type="checkbox"/> Inventaire

Paquetages fournissant le support pour l'inventaire.

Paquets optionnels sélectionnés : 9 sur 9

Paquets optionnels

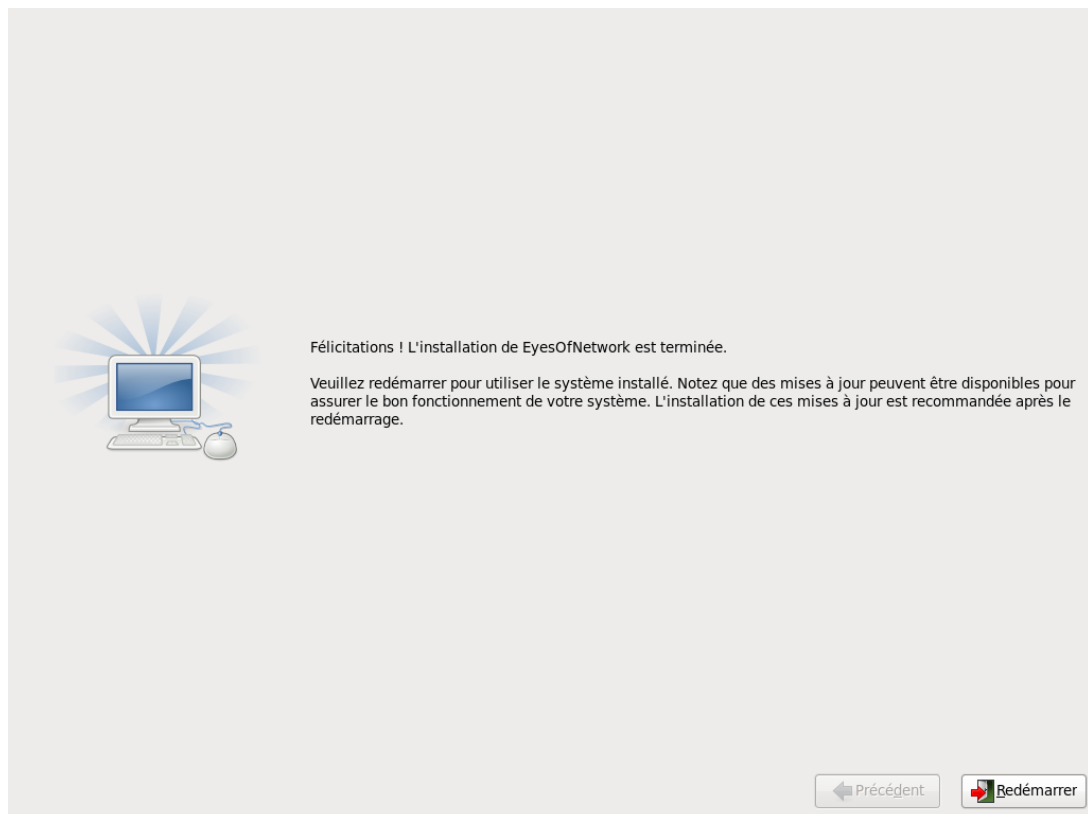
← Précédent Suivant →

N'oubliez pas l'onglet production



Voilà L 'installation de EON est en cour cella prend un certain temps

Prenez un café ☺



L'installation fini redémarré votre machine

```
EyesOfNetwork release 4.0 (Charly)
Kernel 2.6.32-358.11.1.el6.x86_64 on an x86_64

EyesOfNetwork access : http:///
EyesOfNetwork website : http://www.eyesofnetwork.com/

EyesOfNetwork login: _
```

Voici le terminal de commande EON n'a pas d'interface graphique
Loguez-vous avec root et le mot de passe configuré précédemment
Dans notre cas « nagios » comme demandé dans le cahier des charges

2) Configuration de EON

```
EyesOfNetwork release 4.0 (Charly)
Kernel 2.6.32-358.11.1.el6.x86_64 on an x86_64

EyesOfNetwork access : http:///
EyesOfNetwork website : http://www.eyesofnetwork.com/

EyesOfNetwork login: root
Password:
[root@EyesOfNetwork ~]# nano /etc/sysconfig/network-scripts/ifcfg-eth0_
```

Configuration de la carte réseau Eth0

Ouvrir le fichier de configuration `etc/sysconfig/network-scripts/ifcfg-eth0`

```
GNU nano 2.0.9 Fichier : /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
HWADDR=08:00:27:42:14:FF
TYPE=Ethernet
UUID=8ed84d01-339b-48a5-b000-8dd21a3922d0
ONBOOT=no
NM_CONTROLLED=yes
BOOTPROTO=dhcp

[ Lecture de 7 lignes ]
^G Aide      ^O Écrire    ^R Lire fich.^Y Page préc.^K Couper     ^C Pos. cur.
^X Quitter   ^J Justifier ^W Chercher  ^U Page suiv.^U Coller    ^T Orthograp.
```

Le fichier d'origine n'est pas configuré

Il faut donc modifier et ajouter les configuration réseau

```
GNU nano 2.0.9 Fichier : /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
HWADDR=08:00:27:9D:38:D2
TYPE=Ethernet
UUID=7a02e164-7aca-477c-8b75-146c381818f5
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=static
IPADDR=172.16.2.56
NETMASK=255.255.255.192
NETWORK=172.16.2.0
BROADCAST=172.16.2.63

[ Lecture de 12 lignes ]
^G Aide      ^O Écrire    ^R Lire fich.^Y Page préc.^K Couper     ^C Pos. cur.
^X Quitter   ^J Justifier ^W Chercher  ^U Page suiv.^U Coller    ^T Orthograp.
```

Voilà le fichier configuré avec le réseau de la M2I

Ne pas oublier de redémarré la carte réseau pour appliquer les paramètres

Avec la commande `ifdown eth0` puis `ifup eth0`

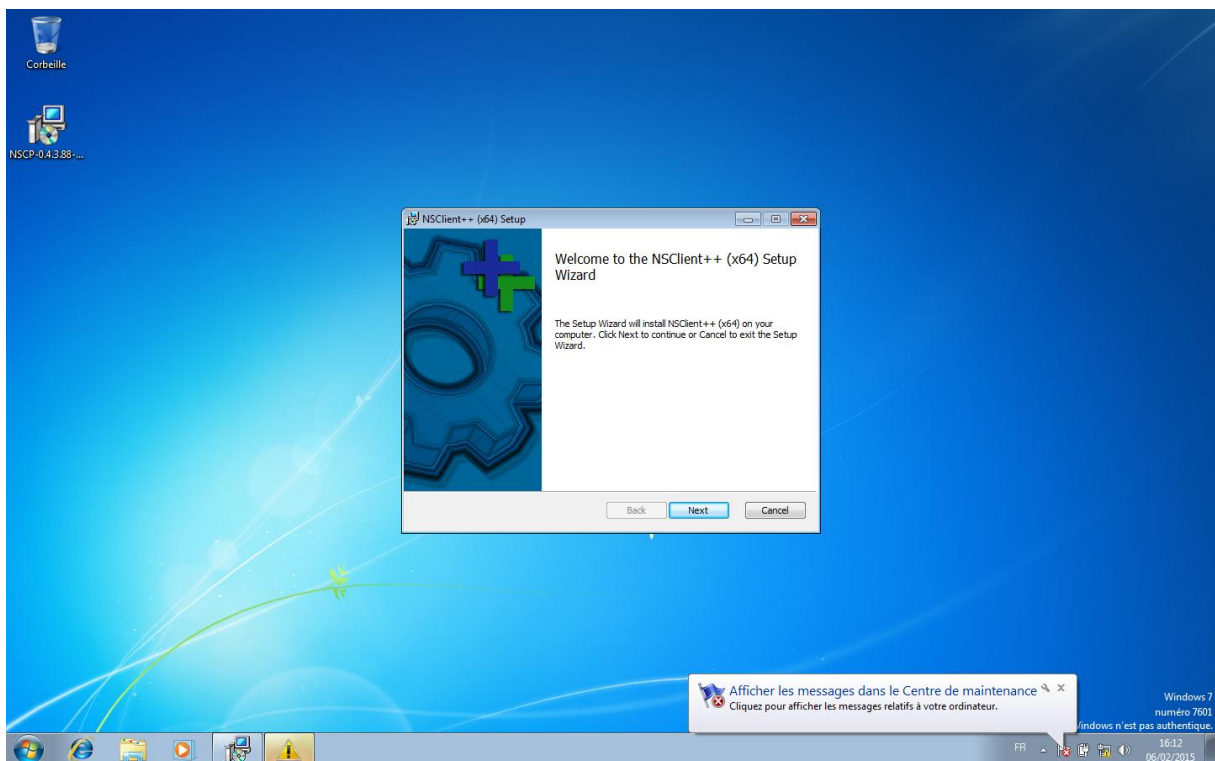
La configuration de Nagios est finie

Installation de NS++ sur un poste client et activation du protocole snmp sous WINDOWS 7

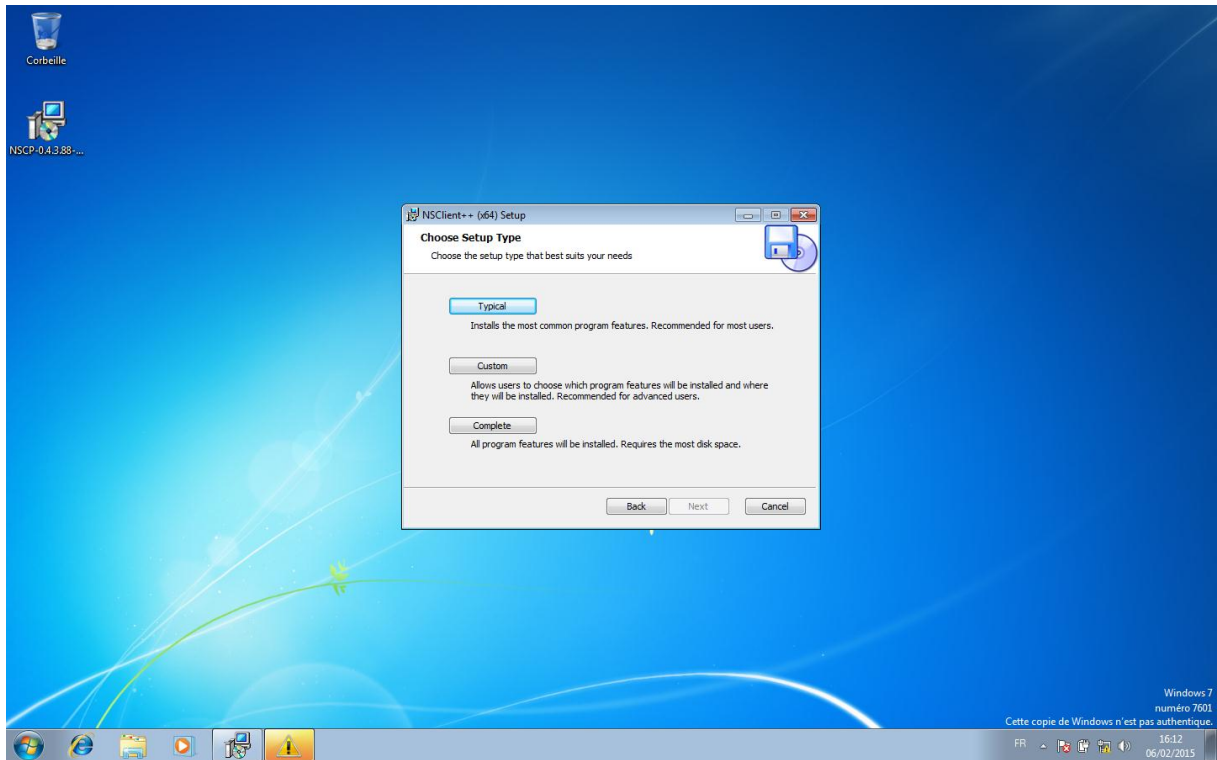
En premier lieu rendez-vous sur le site <http://www.nsclient.org/>

Pour télécharger le client NsCilent ++

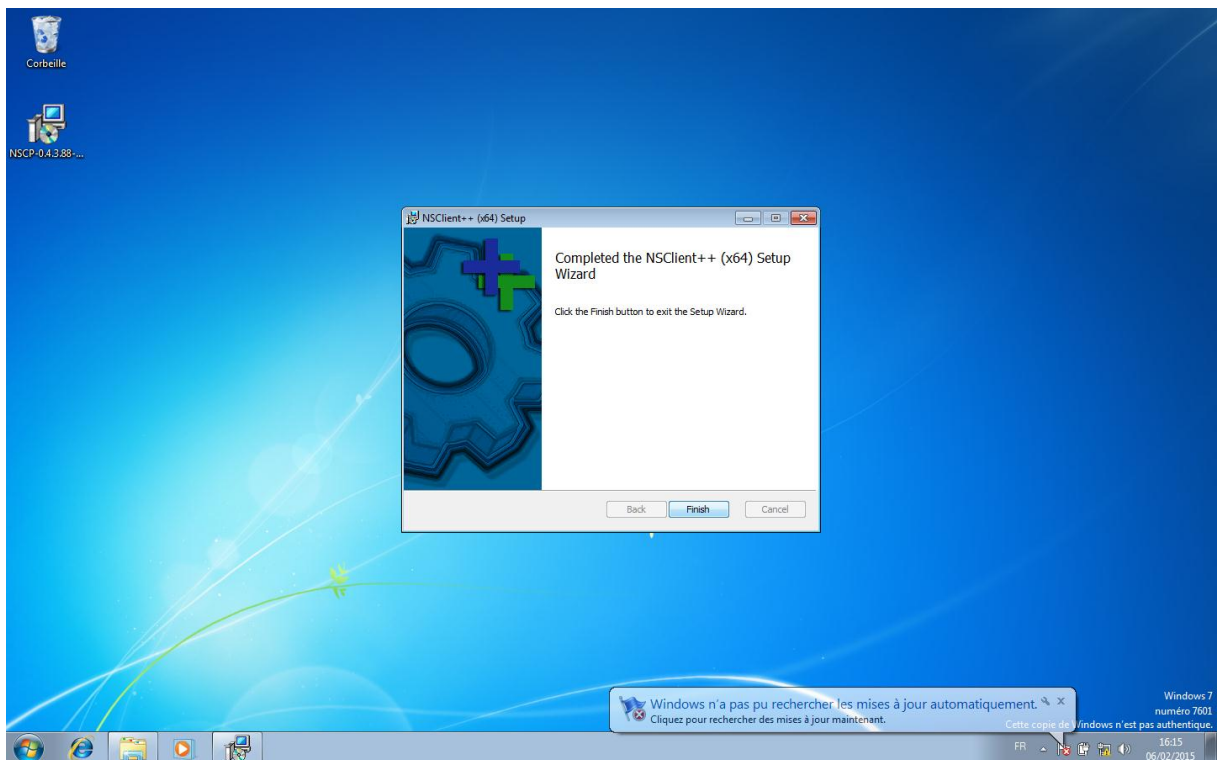
Nous allons commencer par l'installation du client Ns++ sur le poste client Windows 7



Exécuté NsCilent ++ et suivre les étapes jusqu'à :

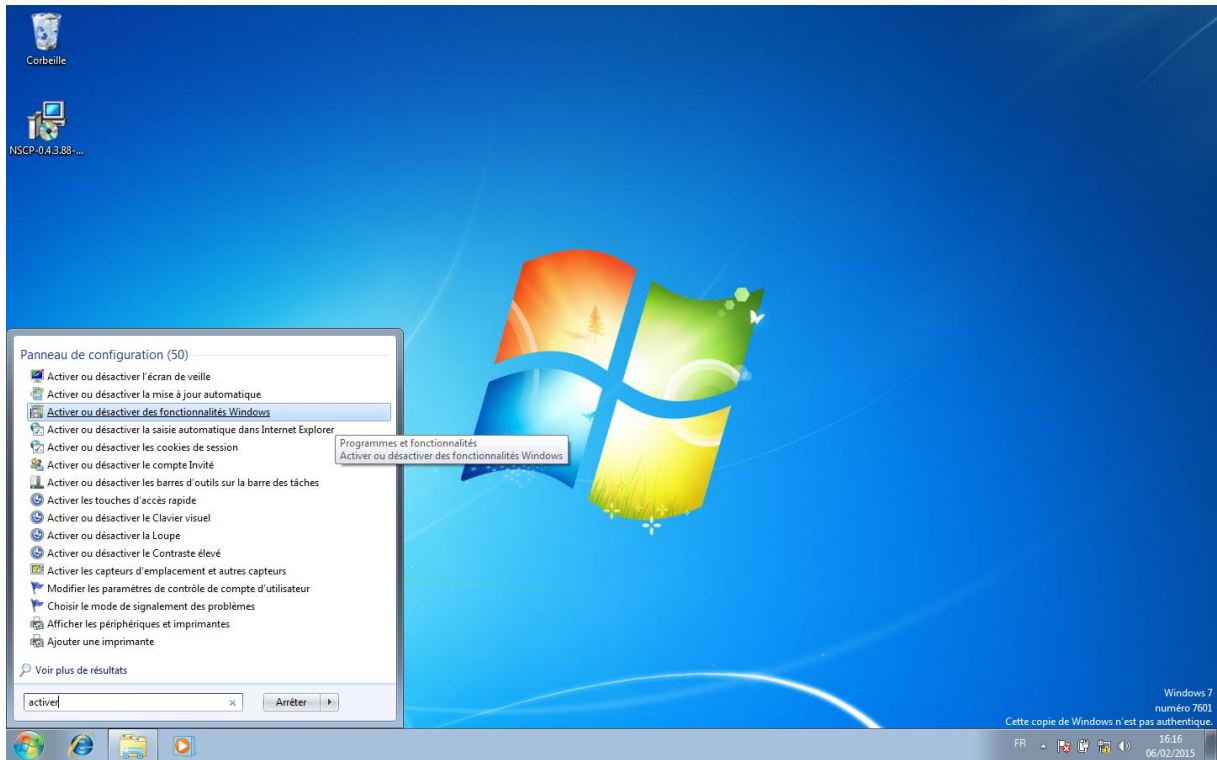


NsClient vous demande de choisir le type d'installation choisir COMPLETE

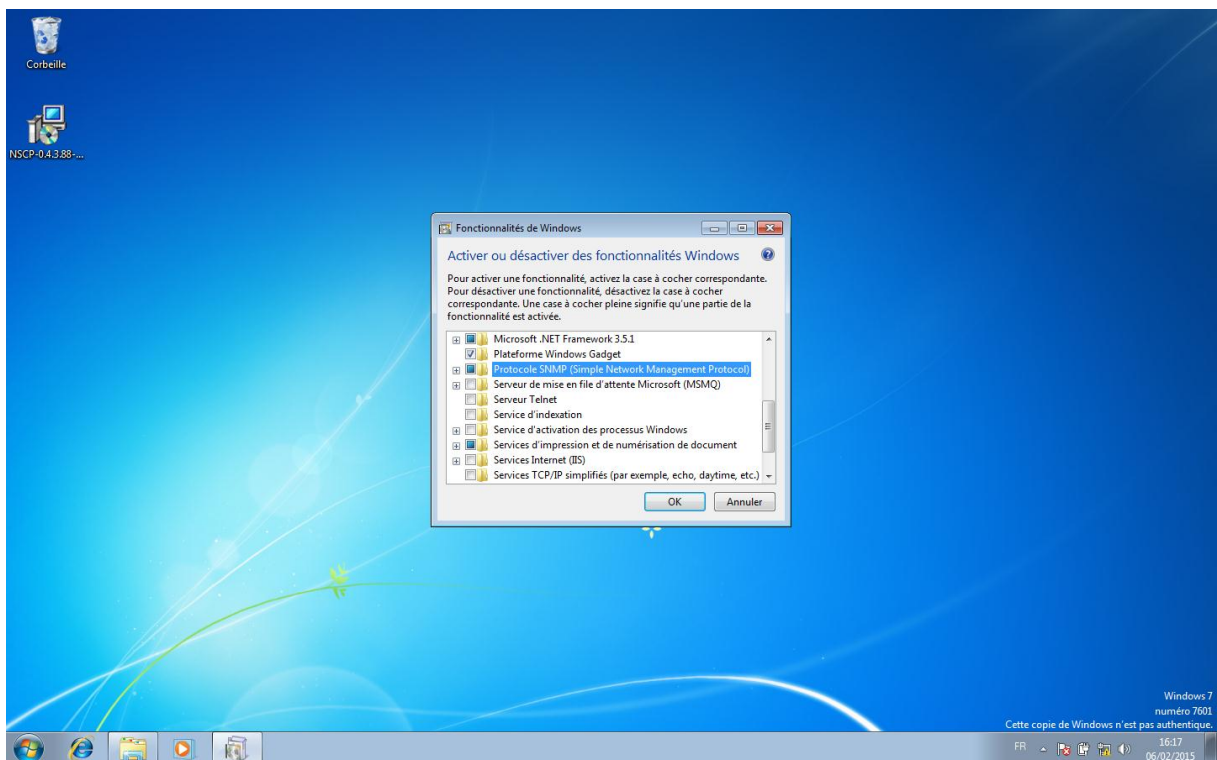


Voilà le client est installé

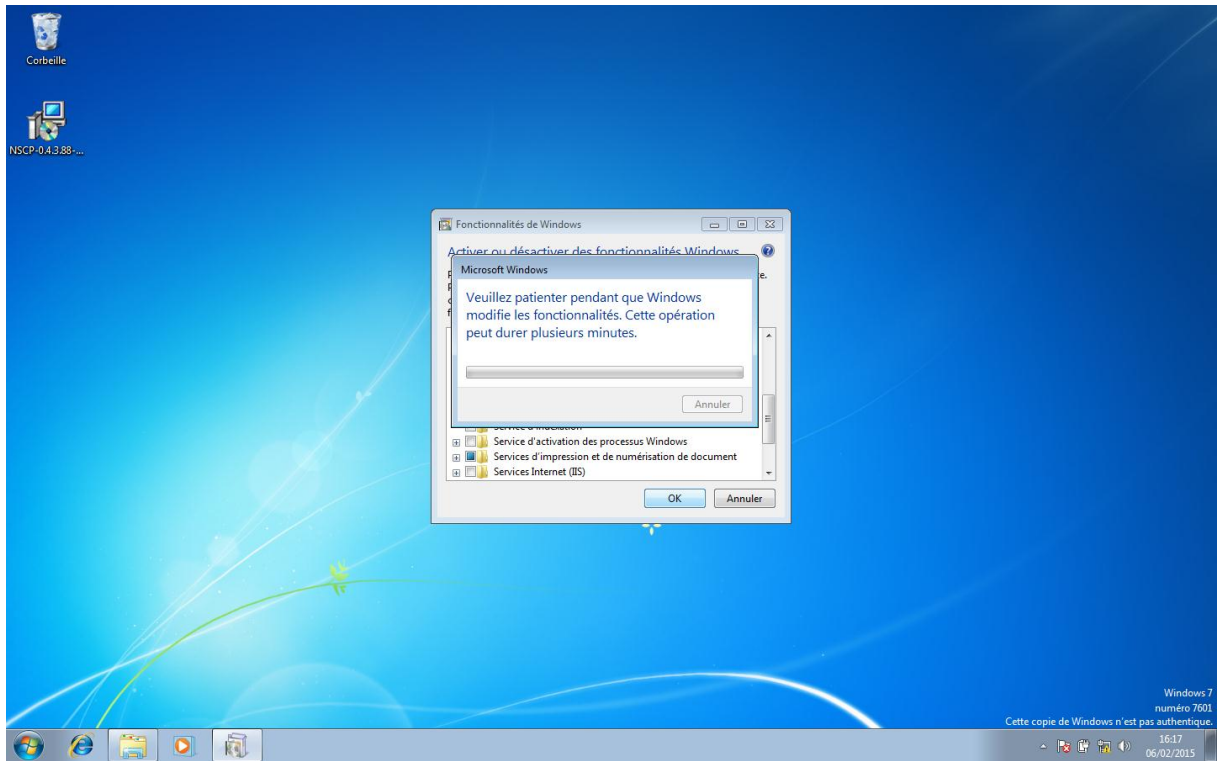
Mais il ne fonctionnera pas si le protocole SNMP n'est pas activé



Pour l'activer rendez-vous dans le menu démarré et recherché
Activer ou désactiver les fonctionnalités Windows



Une petite fenêtre s'ouvre et chercher la fonctionnalité Protocole SNMP puis activer la 😊

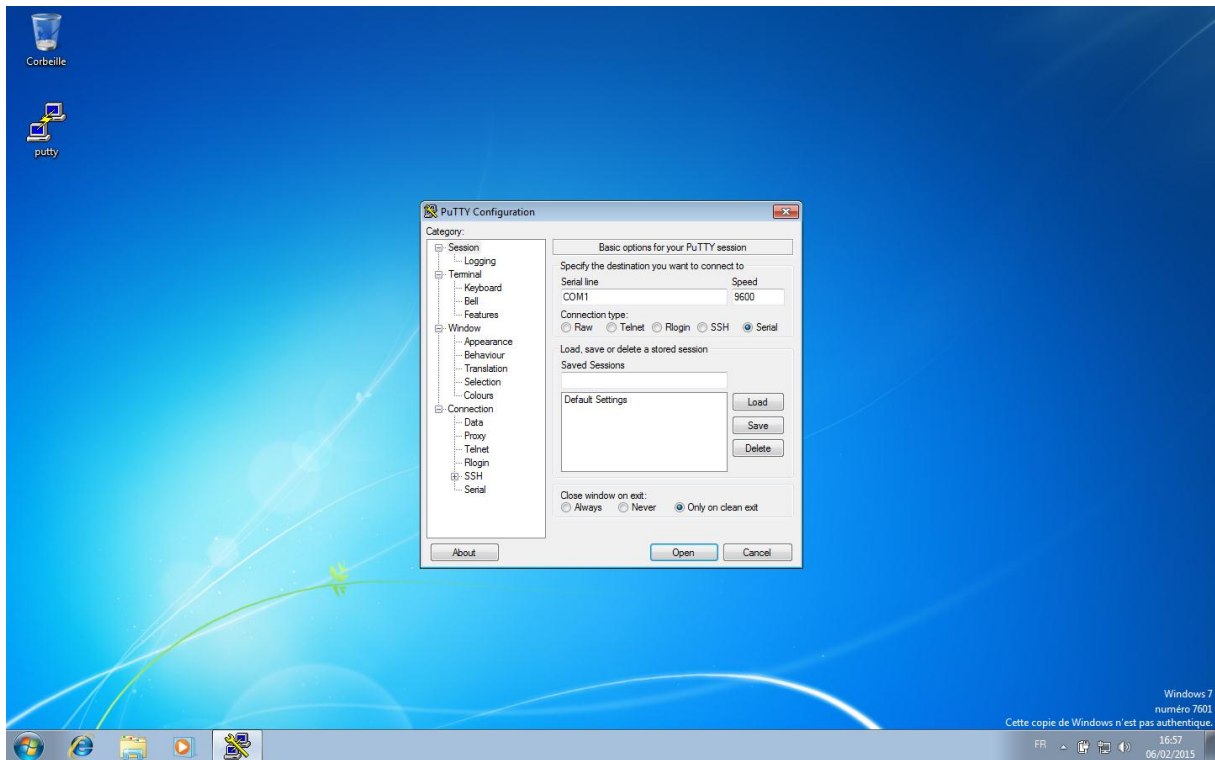


Voilà le protocole SNMP est activé il pourra donc communiquer avec notre serveur EON

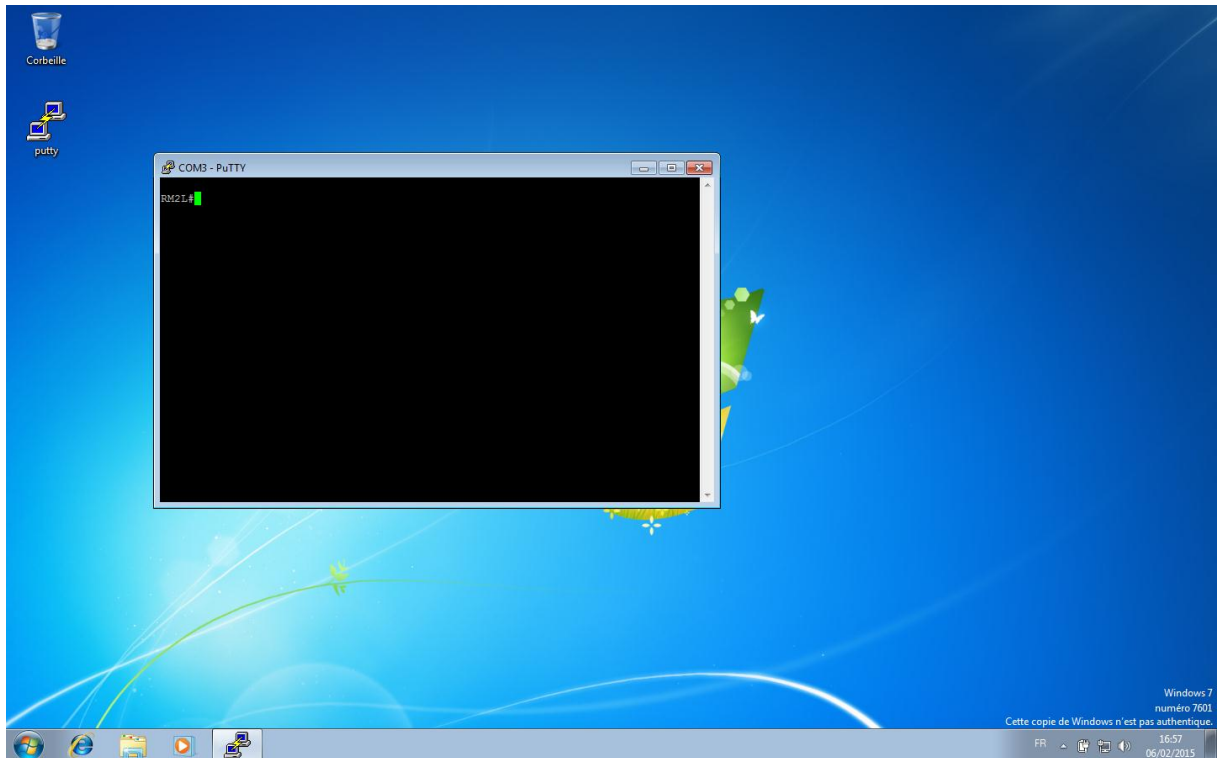
Activation du protocole SNMP sur le commutateur et le routeur Cisco

Pour activé le Protocole Snmp sur le matérielle CISCO

Il nous faut administrer le matérielle avec le câble console via Putty



Router :



Ajouter les commandes suivantes pour activer le protocole snmp

Router :

`conf t` « pour entrer en mode configuration »

`snmp-server community EyesOfNetwork RO` « Accès lecture seule au serveur EON »

`snmp-server host 172.16.2.56 EyesOfNetwork` « destinataire des messages SNMP »

Le reste des options de communication snmp :

`snmp-server enable traps flash insertion removal`

`snmp-server enable traps cpu threshold`

`snmp-server enable traps envmon fan shutdown supply temperature status`

`snmp-server enable traps snmp warmstart linkdown linkup coldstart`

`snmp-server enable traps hsrp`

`snmp-server enable traps ospf state-change`

`snmp-server enable traps config`

`snmp-server enable traps config-copy`

Switch :

`snmp-server community EyesOfNetwork RO`« Accès lecture seule au serveur EON »

`snmp-server host 172.16.2.56 EyesOfNetwork`« destinataire des messages SNMP »

Le reste des options de communication snmp :

`snmp-server enable traps snmp authentication warmstart linkdown linkup coldstart`

`snmp-server enable traps config`

`snmp-server enable traps config-copy`

`snmp-server enable traps flash insertion removal`

`snmp-server enable traps c2900`

`snmp-server enable traps vlancreate`

`snmp-server enable traps vlandelete`

`snmp-server enable traps envmon fan shutdown supply temperature status`

Mission 1.2 – WIFI et sécurisation

Configuration point d'accès Wi-Fi

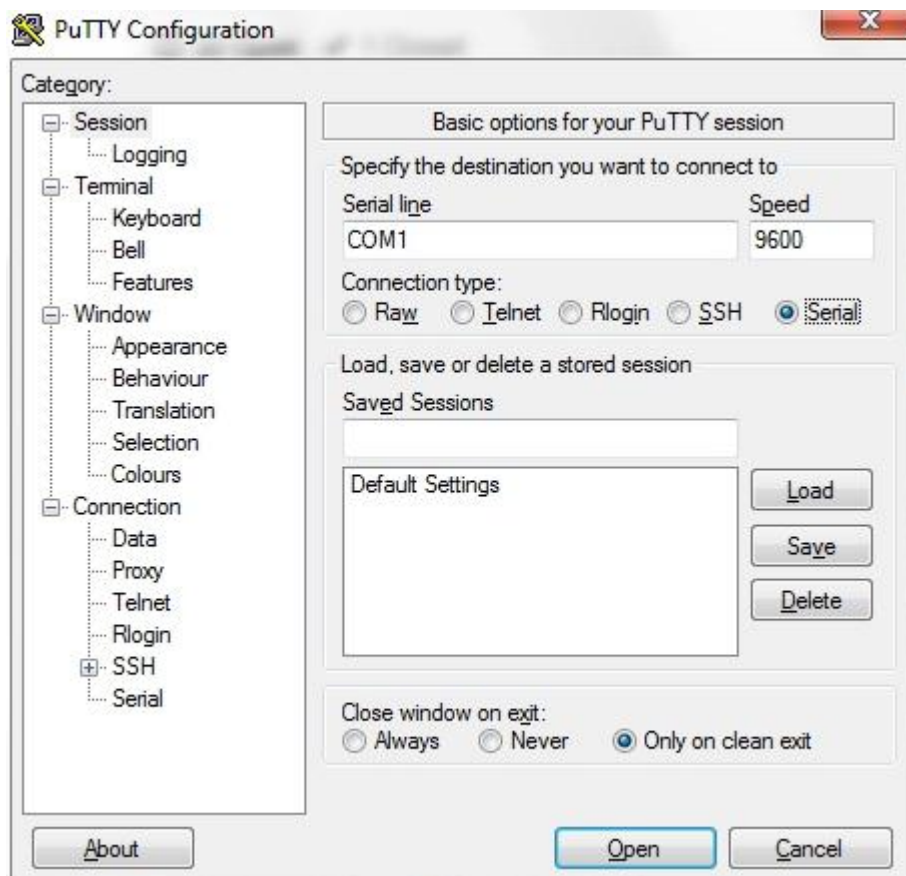
Brancher le point d'accès wifi avec le câble console au PC pour affecter une adresse IP à l'interface du point d'accès.

Factory reset : Brancher l'alimentation tout en restant appuyé 15 secondes sur le bouton reset.

avec Putty :

Connection type : serial

Open



. Dans Putty, configuration de l'interface:

```
En
Password Cisco
Conf t
Hostname AP
Interface bvi1
IP address 172.16.99.30 255.255.255.224
```

```
ap>
ap>en
Password:
ap#
*Mar 1 00:13:43.729: %LINK-3-UPDOWN: Interface BVI1, changed state to up
*Mar 1 00:13:44.729: %LINEPROTO-5-UPDOWN: Line protocol on Interface BVI1, changed state to up
*Mar 1 00:13:48.600: %LINK-3-UPDOWN: Interface BVI1, changed state to down
*Mar 1 00:13:49.600: %LINEPROTO-5-UPDOWN: Line protocol on Interface BVI1, changed state to down
ap#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ap(config)#no
ap(config)#hostname AP
AP(config)#in
AP(config)#interface b
AP(config)#interface bVI 1
AP(config-if)#ip
AP(config-if)#ip a
AP(config-if)#ip ad
AP(config-if)#ip address
*Mar 1 00:15:03.731: %LINK-3-UPDOWN: Interface BVI1, changed state to up
*Mar 1 00:15:04.731: %LINEPROTO-5-UPDOWN: Line protocol on Interface BVI1, changed state to up1
% Incomplete command.

AP(config-if)#ip address 172
*Mar 1 00:15:08.600: %LINK-3-UPDOWN: Interface BVI1, changed state to down
*Mar 1 00:15:09.600: %LINEPROTO-5-UPDOWN: Line protocol on Interface BVI1, changed state to down.
% Incomplete command.

AP(config-if)#ip address 172.16.99.30
% Incomplete command.

AP(config-if)#ip address 172.16.99.30 255.255.255.224
AP(config-if)#no shutdown
AP(config-if)#
```

Configurer l'adressage IP du pc afin qu'il puisse se connecter au point d'accès, par exemple :

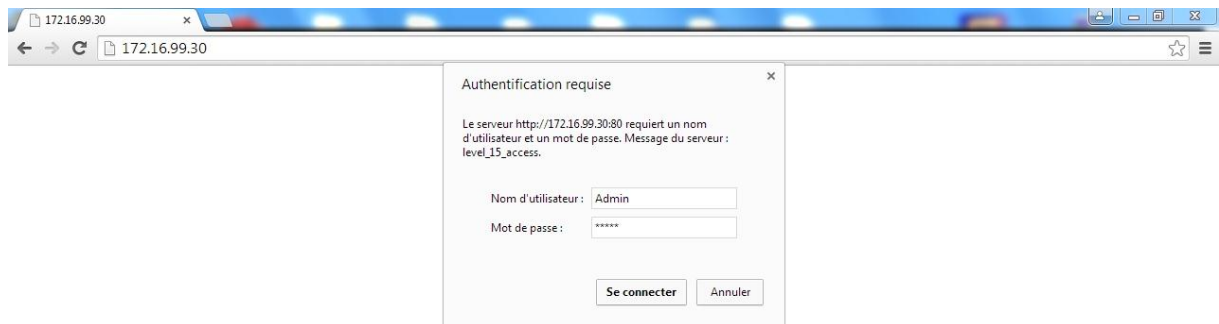
```
IP : 172.16.99.29
Masque : 255.255.255.224
172.16.99.31
```

Sur le navigateur web :

Se connecter avec l'adresse IP choisi précédemment (172.16.99.30)

Login : Admin

Password : Cisco



Etant donné que nous allons configurer deux SSID, nous ferons deux parties distinctes résumant la configuration de ces deux SSID.

SSID Public :

Express security

SSID : public

Broadcast SSID in beacon : coché

Enable VLAN ID: 101

Sécurité : no security

Apply

Warning : ok

The screenshot shows the configuration page for a Cisco Aironet 1200 Series Access Point. The browser address bar shows the URL `172.16.99.30/ap_express-security.shtml`. The page title is "Cisco Aironet 1200 Series Access Point". The main content area is titled "Express Security Set-Up" and includes a navigation menu on the left with options like HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The configuration is for Hostname AP, with an AP uptime of 28 minutes. The "Express Security Set-Up" section is divided into three parts: 1. SSID Configuration, where the SSID is "Public" and "Broadcast SSID in Beacon" is checked; 2. VLAN Configuration, where "Enable VLAN ID: 101" is selected; and 3. Security Configuration, where "No Security" is selected. There are also fields for RADIUS Server and RADIUS Server Secret. At the bottom, there is an "SSID Table" with columns for SSID, VLAN, Encryption, Authentication, Key Management, Native VLAN, and Broadcast SSID. The table is currently empty.

Services

VLAN

Current VLAN : cliquer sur VLAN 101

Create VLAN

VLAN ID : 101

VLAN name : VLANpublic

Apply

The screenshot shows the configuration page for a Cisco Aironet 1200 Series Access Point. The browser address bar shows the URL `172.16.99.30/ap_services_vlan.shtml`. The page title is "Cisco Aironet 1200 Series Access Point". The host is named "AP" and has been up for 26 minutes.

The "Services: VLAN" section is active. Under "Global VLAN Properties", the "Current Native VLAN" is set to "Management VLAN 1".

The "Assigned VLANs" section shows a "Current VLAN List" with "VLAN 101" selected. To the right, the "Create VLAN" form is filled out with "VLAN ID: 101" and "VLAN Name (optional): VLANPublic". There are checkboxes for "Native VLAN" and "Enable Public Secure Packet Forwarding", both of which are currently unchecked. "Apply" and "Cancel" buttons are visible at the bottom right of this section.

The "VLAN Information" section shows a table for "View Information for: VLAN 101".

	FastEthernet Packets	Radio0-802.11G Packets
Received	0	0
Transmitted	0	0

At the bottom right of the page, there is a "Refresh" button. The footer contains the text "Close Window" and "Copyright (c) 1992-2005 by Cisco Systems, Inc."

SSID Employes :

Express security

SSID : Employes

Broadcast SSID in beacon : non

Enable VLAN ID: 100

Sécurité : no security

Apply

Warning : ok

Hostname AP AP uptime is 35 minutes

Express Security Set-Up

SSID Configuration

1. SSID Broadcast SSID in Beacon

2. VLAN

No VLAN Enable VLAN ID: (1-4094) Native VLAN

3. Security

No Security

Static WEP Key

Key 1 128 bit

EAP Authentication

RADIUS Server: (Hostname or IP Address)

RADIUS Server Secret:

WPA

RADIUS Server: (Hostname or IP Address)

RADIUS Server Secret:

SSID Table

Delete	SSID	VLAN	Encryption	Authentication	Key Management	Native VLAN	Broadcast SSID
<input type="radio"/>	Employes	none	none	open	none		✓
<input checked="" type="radio"/>	Public	none	none	open	none		✓

Services

VLAN

Current VLAN : cliquer sur VLAN 100

Create VLAN

VLAN ID : 100

VLAN name : VLANEmployes

Apply

The screenshot shows the configuration interface for a Cisco Aironet 1200 Series Access Point. The browser address bar shows the URL `172.16.99.30/ap_services_vlan.shtml`. The page title is "Cisco Aironet 1200 Series Access Point". The host is named "AP" and has been up for 36 minutes.

The "Services: VLAN" section is active. Under "Global VLAN Properties", the "Current Native VLAN" is set to "Management VLAN 1".

The "Assigned VLANs" section shows a "Current VLAN List" with "VLAN 100" selected. The "Create VLAN" form is filled with "VLAN ID: 100" and "VLAN Name (optional): VLANEmployes". There are checkboxes for "Native VLAN" and "Enable Public Secure Packet Forwarding", both of which are currently unchecked. "Apply" and "Cancel" buttons are present.

The "VLAN Information" section shows "View Information for: VLAN 100". A table displays statistics for FastEthernet and Radio0-802.11G packets:

	FastEthernet Packets	Radio0-802.11G Packets
Received	0	0
Transmitted	0	0

At the bottom right, there is a "Refresh" button. The footer contains "Close Window" and "Copyright (c) 1992-2005 by Cisco Systems, Inc."

Security

Encryption manager

Set encryption mode and keys for VLAN : 100

Encryption modes:

Cipher AES CCMP + TKIP*

Apply

Warning : ok

The screenshot displays the configuration interface for a Cisco Aironet 1200 Series Access Point, specifically the 'Security: Encryption Manager' section for VLAN 100. The interface includes a navigation menu on the left, a main configuration area, and a bottom bar with 'Apply' and 'Cancel' buttons.

Security: Encryption Manager

Set Encryption Mode and Keys for VLAN: 100 [Define VLANs](#)

Encryption Modes

- None
- WEP Encryption Optional
Cisco Compliant TKIP Features: Enable Message Integrity Check (MIC) Enable Per Packet Keying (PPK)
- Cipher AES CCMP + TKIP

Encryption Keys

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 2:	<input checked="" type="radio"/>	<input type="text"/>	128 bit
Encryption Key 3:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 4:	<input type="radio"/>	<input type="text"/>	128 bit

Global Properties

Broadcast Key Rotation Interval: Disable Rotation Enable Rotation with Interval: (10-10000000 sec)

WPA Group Key Update: Enable Group Key Update On Membership Termination Enable Group Key Update On Member's Capability Change

AP uptime is 42 minutes

Apply Cancel

SSID manager

Current SSID list:

Selectionner "Employes"

SSID : Employes

VLAN : NONE

Interface : cocher "Radio0-802.11G"

Client authenticated key management:

Key management : mandatory

Cocher : WPA

WPA pre-shared key : m21123456

The screenshot shows the configuration page for a Cisco Aironet 1200 Series Access Point, specifically the 'Security: Global SSID Manager' section. The page is titled 'Cisco Aironet 1200 Series Access Point' and shows the 'SSID Properties' for the 'Employes' SSID. The 'Current SSID List' includes '< NEW >', 'Employes', and 'Public'. The 'SSID' is set to 'Employes', 'VLAN' is '< NONE >', and 'Interface' is checked for 'Radio0-802.11G'. The 'Network ID' is '(0-4096)'. Under 'Client Authentication Settings', 'Methods Accepted' includes 'Open Authentication' (checked), 'Shared Authentication', and 'Network EAP'. 'Server Priorities' are set to 'Use Defaults' for both 'EAP Authentication Servers' and 'MAC Authentication Servers'. 'Client Authenticated Key Management' is set to 'Key Management: Mandatory' and 'WPA' is checked. The 'WPA Pre-shared Key' is 'm21123456' and 'Hexadecimal' is selected. The page also shows 'Accounting Settings' at the bottom.

Network interfaces

Radio-802.11G

Dans l'onglet setting

Enable radio : enable

Vérifier que nous sommes bien en mode « access point »

* aes ccmp + tkip : cryptage en AES et TKIP est un Protocol qui fait changer la clé toutes les secondes

The screenshot shows the Cisco Aironet 1200 Series Access Point configuration page for the Radio0-802.11G interface. The page is divided into several sections: Configuration, Interface Statistics, and Error Statistics. The radio is currently disabled, and the hardware status is down. The interface statistics show zero activity, and the error statistics show zero errors.

Network Interfaces: Radio0-802.11G Status			
Configuration			
Software Status	Disabled	Hardware Status	Down
Operational Rates	1.0, 2.0, 5.5, 6.0, 9.0, 11.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0 Mb/sec	Basic Rate	1.0, 2.0, 5.5, 11.0 Mb/sec
Aironet Extensions	Enabled	Carrier Set	EMEA
Current Radio Channel	0 MHz Channel 0	Transmitter Power CCK/OFDM	50 mW / 30 mW
Role in Network	Access Point		
Interface Statistics			
Interface Resets	0		
Receive / Transmit Statistics			
Receive		Transmit	
5 Min Input Rate (bits/sec)	0	5 Min Output Rate (bits/sec)	0
5 Min Input Rate (packets/sec)	0	5 Min Output Rate (packets/sec)	0
Time Since Last Input	never	Time Since Last Output	never
Total Packets Input	0	Total Packets Output	0
Total Bytes Input	0	Total Bytes Output	0
Error Statistics			
Receive		Transmit	
Total Input Errors	0	Total Output Errors	0
Throttles	0	Last Output Hang	never



Cisco Aironet 1200 Series Access Point

- HOME
- EXPRESS SET-UP
- EXPRESS SECURITY
- NETWORK MAP +
- ASSOCIATION +
- NETWORK INTERFACES
- IP Address
- FastEthernet
- Radio0-802.11G
- Radio1-not installed
- SECURITY +
- SERVICES +
- WIRELESS SERVICES +
- SYSTEM SOFTWARE +
- EVENT LOG +

RADIO0-802.11G STATUS DETAILED STATUS SETTINGS CARRIER BUSY TEST Hostname AP AP uptime is 51 minutes

Network Interfaces: Radio0-802.11G Settings

Enable Radio: Enable Disable

Current Status (Software/Hardware): Disabled ▼ Down ▼

Role in Radio Network:

- Access Point
- Access Point (Fallback to Radio Shutdown)
- Access Point (Fallback to Repeater)
- Repeater

- Root Bridge
- Non-Root Bridge
- Root Bridge with Wireless Clients
- Non-Root Bridge with Wireless Clients

- Workgroup Bridge
- Scanner

Data Rates: Best Range Best Throughput Default

1.0Mb/sec	<input checked="" type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
2.0Mb/sec	<input checked="" type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
5.5Mb/sec	<input checked="" type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
* 6.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
* 9.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
11.0Mb/sec	<input checked="" type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
* 12.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
* 18.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
* 24.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
* 36.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
* 48.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
* 54.0Mb/sec	<input type="radio"/> Require	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable

* OFDM Rates

CCK Transmitter Power (mW): 1 5 10 20 30 50 Max

Ensuite il faut brancher le point d'accès sur le switch :

Sur le switch :

Créer les vlans 101 et 100 sur le switch

```
En
Conf t
Vlan 100
Name Employes
Exit
Vlan 101
Name Public
Exit
```

Créer des ports trunks sur deux interfaces (1 pour le point d'accès et 1 autre pour le routeur)

```
En
Conf t
Int fa 0/1 – 2
Switch(config-if)#switchport trunk encapsulation dot1Q
Switch(config-if)#switchport mode trunk
```

Sur le routeur :

Configurer 2 étendues DHCP (une pour chaque sous réseau)

```
En
Conf t
Interface fa 0/1
No shutdown
Exit
Interface fa 0/1.100
Encapsulation dot1Q 100
Ip address 172.16.100.30 255.255.255.224
Exit
Interface fa 0/1.101
Encapsulation dot1Q 101
Ip address 172.16.101.254 255.255.255.0
Exit
End
```

Configuration du serveur DHCP interne au routeur

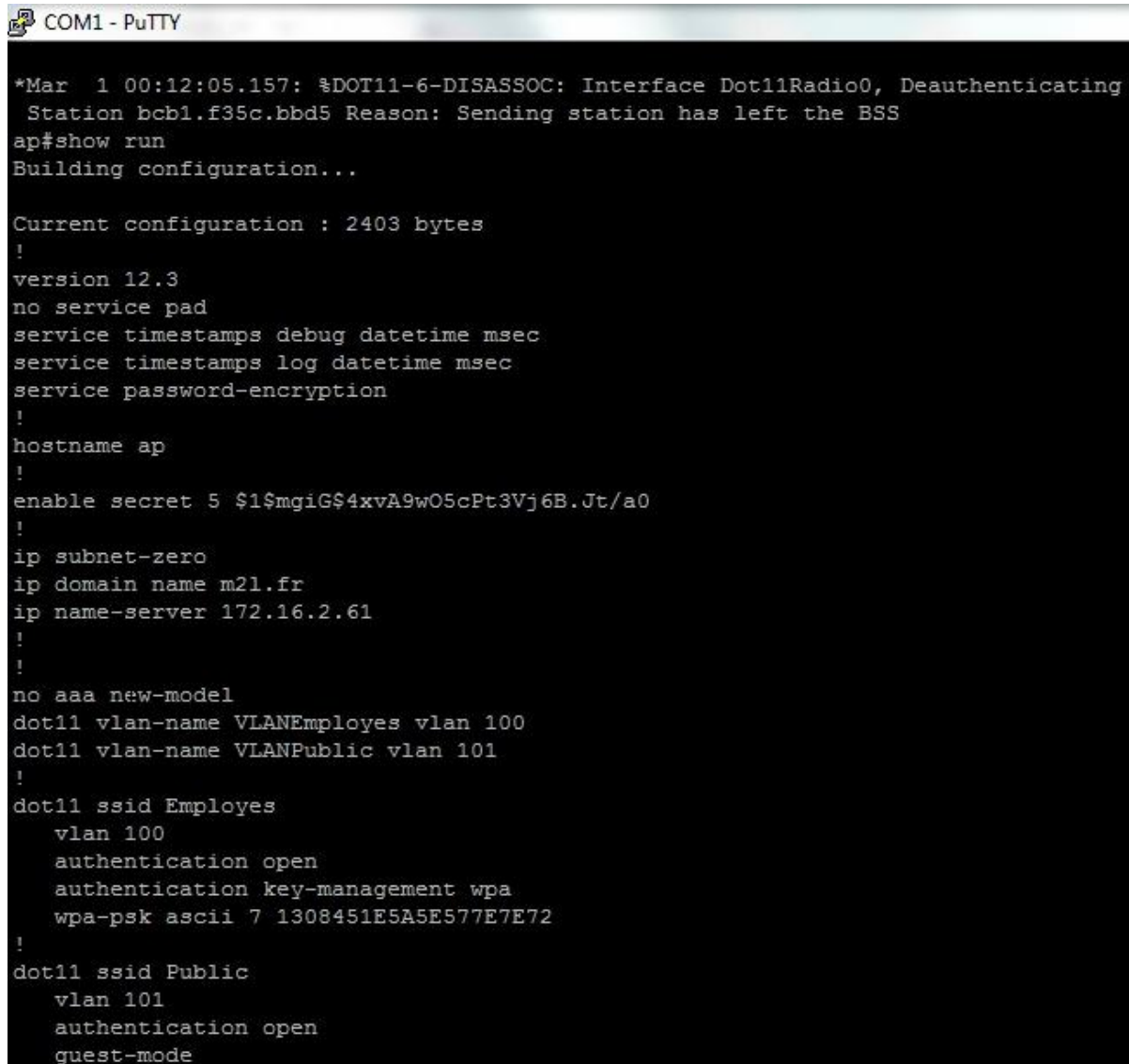
```
En
Conf t
Service dhcp
Ip dhcp excluded-address 172.16.101.245 172.16.101.254
Ip dhcp excluded-address 172.16.100.25 172.16.100.30
Ip dhcp pool Public
Network 172.16.101.0 255.255.255.0
Default-router 172.16.101.254
Option @IP du serveur TFTP
Dns-server 172.16.2.61
```



```
Lease 0 2 45
Ip dhcp pool Employes
Network 172.16.100.0 255.255.255.224
Default-router 172.16.101.30
Option @IP du serveur TFTP
Dns-server 172.16.2.61
Lease 6 0 0
Exit
```

Configurer le routage dynamique OSPF

```
En
Conf t
Router ospf 1
Network 172.16.100.0 0.0.0.255
Network 172.16.101.0 0.0.0.31
End
```



```
COM1 - PuTTY
*Mar  1 00:12:05.157: %DOT11-6-DISASSOC: Interface Dot11Radio0, Deauthenticating
  Station bcb1.f35c.bbd5 Reason: Sending station has left the BSS
ap#show run
Building configuration...

Current configuration : 2403 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
enable secret 5 $1$mgiG$4xvA9wO5cPt3Vj6B.Jt/a0
!
ip subnet-zero
ip domain name m21.fr
ip name-server 172.16.2.61
!
!
no aaa new-model
dot11 vlan-name VLANEmployes vlan 100
dot11 vlan-name VLANPublic vlan 101
!
dot11 ssid Employes
    vlan 100
    authentication open
    authentication key-management wpa
    wpa-psk ascii 7 1308451E5A5E577E7E72
!
dot11 ssid Public
    vlan 101
    authentication open
    guest-mode
```

Administration système (Mohammed KARROUM)

Contexte

Conformément à sa politique d'administration consistant à automatiser au maximum les installations en réseau, l'administrateur vous confie la mission permettant de superviser les clients Nagios/EON (Serveurs, clients Windows, Linux, etc.), les activités processeurs, disques, etc), les applications. Ce qui lui permettra de gagner du temps, de réduire les coûts d'exploitation et d'uniformiser les traitements.

Mission 1.1 : Déploiement de clients Nagios/EON par stratégie de groupe

Si vous avez plusieurs postes sur lesquels vous devez installer NSClient++, il peut être utile d'utiliser un script permettant d'automatiser cette installation.

Pour cela il vous faut :

le .msi permettant l'installation du logiciel (comme le .exe), disponible sur le site de NSClient++.

Un fichier de configuration du logiciel (soit le nsclient.ini pour les versions 4.0 ou NSC.ini pour les versions 3.9 et moins) correctement configuré (le mieux est d'installer NSClient ++ sur un poste, d'entrer l'adresse de votre serveur de supervision, le mot de passe et les plugins que vous allez utiliser et de récupérer le fichier de configuration une fois l'installation terminée).

Pour les étapes suivantes, il faut accepter les termes de la licence et de la configuration typique.

L'emplacement d'installation est par défaut.

Nous avons ensuite renseigné L'IP du serveur Nagios, laisser le champ du mot de passe vide et cocher tous les modules

Un dossier partagé (optionnel) si vous voulez éviter de devoir copier/coller les deux fichiers précédents sur chacune des machine sur laquelle vous allez faire l'installation.

Pour la suite, utiliser le script ci-dessous.

Le script :

```
NET USE Z: \\srv-ad\script /PERSISTENT:NO
msiexec /i "z:\nsclient++.msi" /quiet
xcopy "z:\nsclient.ini" "C:\Program Files\NSClient++" /y
NET USE Z: /DELETE /YES
Net stop nscp
Net start nscp
```

Explications :

NET USE Z: \\srv-ad\script /PERSISTENT:NO -> Monte le lecteur réseau Z : (obligatoire si le script est stockés sur un dossier partagé).

msiexec /i "z:\nsclient++.msi" /quiet -> lance l'installation de NSClient en mode silencieux.

xcopy "z:\nsclient.ini" "C:\Program Files\NSClient++" /y -> Copie le fichier de configuration dans le répertoire d'installation de NSClient++ et ne demande pas de confirmation lors de l'écrasement du précédent fichier.

NET USE Z: /DELETE /YES -> Démonte le lecteur réseau précédemment créé.

Net stop nscp -> Arrête le service nscp (NSClient++)

Net start nscp -> Démarre le service nscp (NSClient++)

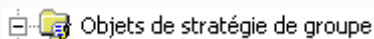
Maintenant, il faut déployer le script via une GPO

Création de la GPO

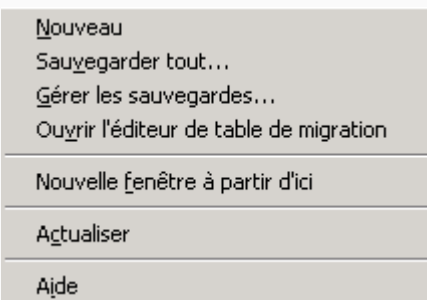
Rendez-vous sur votre serveur Contrôleur de domaine.

Exécutez la console d'administration « Gestion des stratégies de groupe » que vous trouverez dans les outils d'administration de votre serveur.

Ensuite cherchez l'onglet « Objets de stratégie de groupe »



Cliquez droit et sélectionnez « nouveau »



Saisissez le nom que vous souhaitez donner à la GPO

Une fois créé, faites un clic droit dessus et cliquez sur « Modifier »

Dans l'éditeur d'objets de stratégie de groupe, rendez-vous dans la partie :

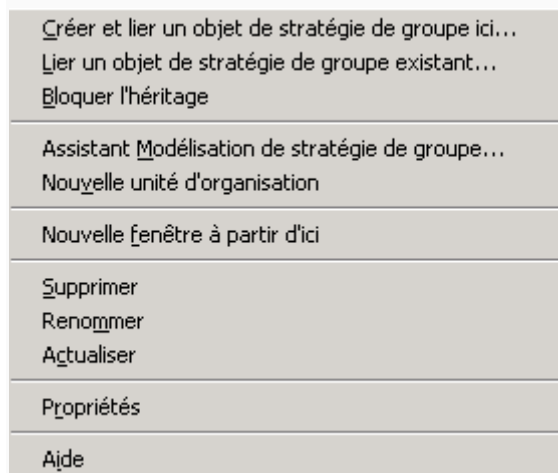
Configuration utilisateur => Paramètres Windows => Scripts (ouverture/fermeture de session)

Copiez le script que vous avez précédemment créé dans le répertoire affiché puis fermez la fenêtre.

Cliquez maintenant sur « Ajouter... » Et saisissez l'emplacement de votre script.

Votre script est maintenant bien configuré dans la GPO, il ne vous reste plus qu'à appliquer la GPO à une OU de vos utilisateurs.

Pour appliquer la GPO, toujours dans la console d'administration « Gestion des stratégies de groupe ». Cliquez droit sur l'OU sur laquelle vous souhaitez appliquer votre GPO, puis sur « Lier un objet de stratégie de groupe existant... »



Choisissez bien le domaine, ainsi que la GPO que vous avez précédemment créé. Une fois appliquée il ne vous reste plus qu'à cliquer sur celle-ci.

Votre GPO n'est pour le moment pas encore appliquée à l'OU, pour remédier à cela cliquez droit sur l'OU puis sur « appliqué »

Vous pouvez également choisir à quel utilisateur vous souhaitez que la GPO soit appliquée, par défaut, elle sera appliquée à tout utilisateur authentifiés.

Il vous suffit juste de jouer avec les boutons « Ajouter » et « Supprimer ».

Configuration Nagios

Nous allons installer Nagios sur une machine nouvellement créée grâce à la commande « apt-get install nagios3 »

Nagios
 Current Network Status
 Last Updated: Tue Apr 1 15:47:07 CEST 2014
 Updated every 90 seconds
 Nagios® Core™ 3.4.1 - www.nagios.org
 Logged in as nagiosadmin

Host Status Totals
 Up Down Unreachable Pending
 9 0 0 0
 All Problems All Types
 0 9

Service Status Totals
 Ok Warning Unknown Critical Pending
 38 0 0 1 0
 All Problems All Types
 1 39

Service Overview For All Host Groups

All Servers (all)				Debian GNU/Linux Servers (debian-servers)				HTTP servers (http-servers)			
Host	Status	Services	Actions	Host	Status	Services	Actions	Host	Status	Services	Actions
brandon	UP	4 OK		localhost	UP	6 OK		localhost	UP	6 OK	
dns-dhcp	UP	4 OK									
impression	UP	4 OK									
localhost	UP	6 OK									
ocs-glob	UP	4 OK									
renan	UP	4 OK									
raync	UP	4 OK									
sgbd	UP	4 OK 1 CRITICAL									
valerie	UP	4 OK									
SSH servers (ssh-servers)											
localhost	UP	6 OK									
sgbd	UP	4 OK 1 CRITICAL									

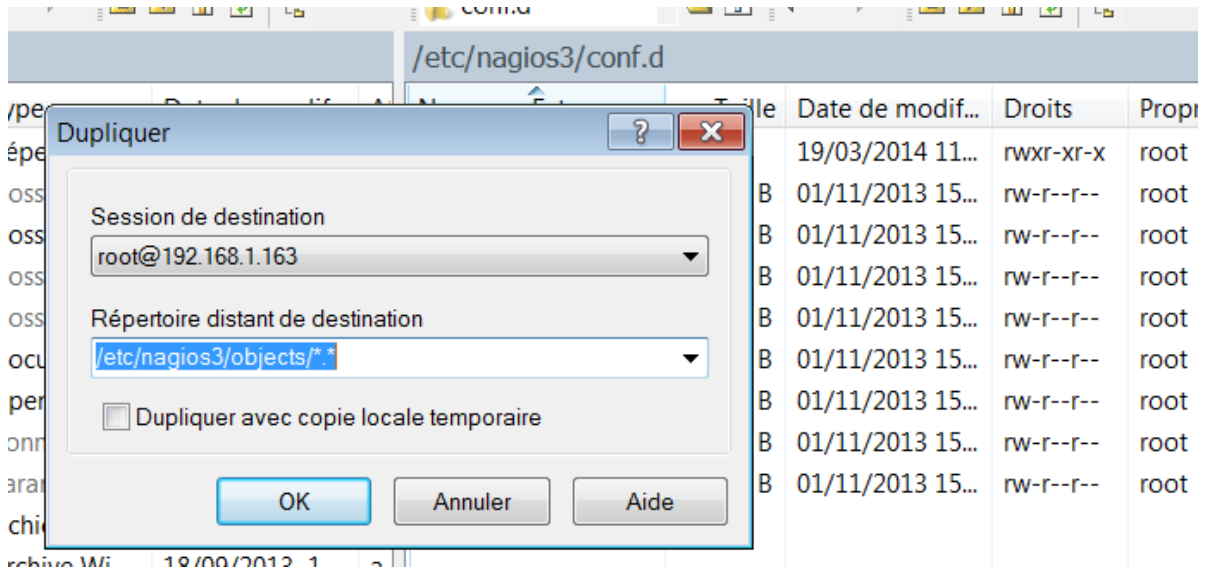
On va ensuite passer à la configuration de Nagios :

Une fois le paquet installé, nous allons nous diriger vers WinSCP qui va nous permettre de configurer plus rapidement le serveur.

Dans etc/nagios3/ créer un dossier nommé «objects»

Nom	Ext	Taille	Date de modif...	Droits	Propri
..			13/03/2014 14...	rwxr-xr-x	root
conf.d			13/03/2014 14...	rwxr-xr-x	root
objects			19/03/2014 11...	rwxr-xr-x	root
stylesheets			13/03/2014 14...	rwxr-xr-x	root
apache2.conf		1 986 B	01/11/2013 15...	rw-r--r--	root
cgi.cfg		12 479...	24/11/2013 16...	rw-r--r--	root
commands.cfg		2 443 B	01/11/2013 15...	rw-r--r--	root
htpasswd.users		50 B	13/03/2014 14...	rw-r--r--	root
nagios.cfg		44 222...	01/11/2013 15...	rw-r--r--	root
resource.cfg		1 293 B	01/11/2013 15...	rw-r-----	root

Il faut ensuite aller dans etc/nagios3/conf.d/ pour copier le fichier localhost et mettre la copie dans objects avec un clic droit sur le fichier « localhost ».



Aller dans ect/objects et nous aloons maintenant renommer le fichier localhost en windows.cfg.

Nous allons ensuite définir tous les hôtes windows de notre réseau comme ci-dessous :

```

define host{
    use                generic-host          ; Name of host template to use
    host_name          valerie
    alias              valerie
    address            192.168.1.11
}

define host{
    use                generic-host          ; Name of host template to use
    host_name          brandon
    alias              brandon
    address            192.168.1.10
}

# Define a service to check the disk space of the root partition
# on the local machine. Warning if < 20% free, critical if
# < 10% free space on partition.

define service{
    use                generic-service       ; Name of service temp
    host_name          localhost,renan,valerie,brandon,dns-dhcp
    service_description Disk Space
    check_command      check_all_disks!20%!10%
}

# Define a service to check the number of currently logged in
# users on the local machine. Warning if > 20 users, critical
# if > 50 users.

define service{
    use                generic-service       ; Name of service temp
    host_name          localhost,renan,valerie,brandon,dns-dhcp
    service_description Current Users
    check_command      check_users!20!50
}

# Define a service to check the number of currently running procs
# on the local machine. Warning if > 250 processes, critical if
# > 400 processes.

define service{
    use                generic-service       ; Name of service temp
    host_name          localhost,renan,valerie,brandon,dns-dhcp

```

De même pour les services à surveiller (checks).

Ensuite on édite le fichier nagios.cfg où nous allons dé commenter la ligne :

```

# Definitions for monitoring a Windows machine
cfg_file=/etc/nagios3/objects/windows.cfg

```

Les hôtes windows apparaissent maintenant sur la page web nagios.

Il nous faut maintenant déclarer les serveurs linux, pour cela, il faut créer le dossier /etc/nagios3/servers, dans lequel nous allons créer un fichier servers.cfg contenant les serveurs linux à déclarer et les services :

```

define host{
    use                generic-host          ; Name of host template to use
    host_name          ocs-glpi
    alias              ocs-glpi
    address             192.168.1.30
}

define host{
    use                generic-host          ; Name of host template to use
    host_name          sgbd
    alias              sgbd
    address             192.168.1.32
}

define host{
    use                generic-host          ; Name of host template to use
    host_name          impression
    alias              impression
    address             192.168.1.33
}

# Define a service to check the disk space of the root partition
# on the local machine. Warning if < 20% free, critical if
# < 10% free space on partition.

define service{
    use                generic-service       ; Name of service temp
    host_name          localhost,ocs-glpi,sgbd,impression,rsync
    service_description Disk Space
    check_command      check_all_disks!20%!10%
}

# Define a service to check the number of currently logged in
# users on the local machine. Warning if > 20 users, critical
# if > 50 users.

define service{
    use                generic-service       ; Name of service temp
    host_name          localhost,ocs-glpi,sgbd,impression,rsync
    service_description Current Users
    check_command      check_users!20!50
}

# Define a service to check the number of currently running procs
# on the local machine. Warning if > 250 processes, critical if
# > 400 processes.

define service{
    use                generic-service       ; Name of service temp
    host_name          localhost,ocs-glpi,sgbd,impression,rsync
    service_description Total Processes
    check_command      check_procs!250!400
}

|

# Define a service to check the load on the local machine.

define service{
    use                generic-service       ; Name of service temp
    host_name          localhost,ocs-glpi,sgbd,impression,rsync
    service_description Current Load
    check_command      check_load!5.0!4.0!3.0!10.0!6.0!4.0
}

```


































Il faut ensuite déclarer ce fichier dans nagios.cfg en dé commentant la ligne :







```

# You can also tell Nagios to process all config files (with a .cfg
# extension) in a particular directory by using the cfg_dir
# directive as shown below:
cfg_dir=/etc/nagios3/servers
#cfg_dir=/etc/nagios3/printers
#cfg_dir=/etc/nagios3/switches
#cfg_dir=/etc/nagios3/routers

```

Les serveurs linux et les services sont maintenant apparent sur la page Web de nagios
 « 192.168.1.35/nagios3/ »

All Servers (all)				Debian GNU/Linux Servers (debian-servers)				HTTP servers (http-servers)			
Host	Status	Services	Actions	Host	Status	Services	Actions	Host	Status	Services	Actions
brandon	UP	4 OK	  	localhost	UP	6 OK	  	localhost	UP	6 OK	  
dns-dhcp	UP	4 OK	  								
impression	UP	4 OK	  								
localhost	UP	6 OK	  								
ocs-glpi	UP	4 OK	  								
renan	UP	4 OK	  								
rsync	UP	4 OK	  								
sgbd	UP	4 OK 1 CRITICAL	  								
valerie	UP	4 OK	  								

SSH servers (ssh-servers)			
Host	Status	Services	Actions
localhost	UP	6 OK	  
sgbd	UP	4 OK 1 CRITICAL	  

Il faut maintenant passer à la phase d'envois des notifications en cas de panne, pour cela, il faut déclarer dans /etc/nagios3/conf.d/contact_nagios.cfg, les contacts et les groupes de contacts qu'il faut alerter :

```
define contact{
    contact_name          valerie
    alias                 Valerie
    service_notification_period 24x7
    host_notification_period 24x7
    service_notification_options w,u,c,r
    host_notification_options d,r
    service_notification_commands notify-service-by-email
    host_notification_commands notify-host-by-email
    email                 chao.valerie@gmail.com
}

#####
#####
#
# CONTACT GROUPS
#
#####
#####

# We only have one contact in this simple configuration file, so there is
# no need to create more than one contact group.

define contactgroup{
    contactgroup_name    admins
    alias                Nagios Administrators
    members              root,valerie,renan,brandon
}

```

Il faut, après cela, modifier les templates utilisés (generic-host et generic-service en général) dans le dossier /etc/nagios3/conf.d pour que cela coïncide avec le groupe à contacter :


```

# Generic host definition template - This is NOT a real host, just a template!

define host{
    name                generic-host    ; The name of this host template
    notifications_enabled 1            ; Host notifications are enabled
    event_handler_enabled 1            ; Host event handler is enabled
    flap_detection_enabled 1           ; Flap detection is enabled
    failure_prediction_enabled 1       ; Failure prediction is enabled
    process_perf_data     1            ; Process performance data
    retain_status_information 1        ; Retain status information across progra
    retain_nonstatus_information 1     ; Retain non-status information across p
        check_command      check-host-alive
        max_check_attempts 10
        notification_interval 0
        notification_period 24x7
        notification_options d,u,r
        contact_groups      admins
register 0                ; DONT REGISTER THIS DEFINITION - ITS NO
}

```

Il faut maintenant installer exim4 en général déjà installé mais si ce n'est pas le cas, il faut appliquer la commande « apt-get install exim »

Il faut ensuite passer la commande « dpkg-config exim-config » puis poursuivre la configuration en suivant les indications du service, en faisant attention à respecter le nom de domaine « naga.fr ».

Ensuite, il faut tester l'envoi d'email avec la commande :

« echo « ... » | mail -s « sujet de test » <adresse mail à joindre> » normalement un mail arrivera dans la boîte mail concernée.

Il faut pour finir, tester en situation réelle, il faut pour cela couper un service par exemple SSH sur un hôte, chez nous sgbd.

Au bout de quelques secondes, sur le site de nagios sera affiché une erreur « critical » au niveau du service SSH du serveur sgbd :

Limit Results: 100 ▾

Host ↕	Service ↕	Status ↕	Last Check ↕	Duration ↕	Attempt ↕	Status Information
sgbd	Current Load	OK	2014-04-01 16:38:50	0d 6h 37m 33s	1/4	OK - Charge moyenne: 0.00, 0.01, 0.05
	Current Users	OK	2014-04-01 16:39:53	0d 6h 41m 38s	1/4	UTILISATEURS OK - 1 utilisateurs actuellement connectés
	Disk Space	OK	2014-04-01 16:40:56	0d 6h 43m 11s	1/4	DISK OK
	SSH	CRITICAL	2014-04-01 16:39:19	0d 1h 6m 7s	4/4	Connexion refusée
	Total Processes	OK	2014-04-01 16:42:00	0d 6h 40m 34s	1/4	PROCS OK: 81 processus

Results 1 - 5 of 5 Matching Services

Nous recevons alors quelques secondes plus tard encore, le mail d'alerte en question sur tous les contacts à avertir :

De: **nagios@nagios.naga.fr** Microsoft SmartScreen a classé ce message comme indésirable.
Envoyé: mar. 01/04/14 13:39
À: **renan.du95200@hotmail.fr**

Microsoft SmartScreen a marqué ce message comme indésirable. Il sera supprimé dans 10 jours.
[Ce message est sûr!](#)

***** Nagios *****

Notification Type: PROBLEM

Service: SSH
Host: sgbd
Address: 192.168.1.32
State: CRITICAL

Date/Time: Tue Apr 1 15:39:26 CEST 2014

Additional Info:

Connexion refusée

La notification à bien été envoyée, le serveur fonctionne.