

Radius Linux

- [Doc technique et install radius](#)
- [Procédure Mise A Jour Version Linux](#)
- [Procédure retour arriere radius](#)

Doc technique et install radius

Configuration et installation d'un serveur Radius

La configuration s'effectue en plusieurs étapes :

1 - Installation de NPS Windows 2022

2 - Installation de serveurs de certification

3 - Configuration dans la console Meraki (switchs et bornes wifi)

La première partie consiste à installer 4 serveurs Windows 2022 ainsi que 3 serveurs de certification (actuellement il en existe déjà un sur le domaine Vincennes, SP87).

La répartition de ces derniers est la suivante :

2 serveurs NPS pour l'authentification radius des agents en filaire et en wifi + 1 serveur de certification.

2 serveurs NPS pour l'authentification radius des écoles + 2 serveurs de certification

La seconde partie consiste à configurer tous les éléments dans la console web Meraki (switchs et bornes wifi)

Nous avons configuré les 2 serveurs suivants : SP124 et SP125(NPS) dans le vlan système pour l'authentification sur le domaine Vincennes.fr.

1. Récupération de l'autorité de certification :

Certificats - Utilisateur actuel	Délicivré à	Délicivré par	Date d'expirati...	Rôles prévus	Nom convivial	Statut	Modèle de cert...
Personnel	AAA Certificate Services	AAA Certificate Services	01/01/2029	Authentification du...	Sectigo (AAA)		
Autorisés de certification raci	AddTrust External CA Root	AddTrust External CA Root	30/05/2020	Authentification du...	Sectigo (AddTrust)		
Certificats	CertVincennes	CertVincennes	23/08/2011	<Tout>	<Aucun>		Autorité de cer...
Confiance de l'entreprise	Umbrella Root CA	Cisco Umbrella Root CA	28/06/2036	<Tout>	<Aucun>		
Autorisés de certification intermédiaires	Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	02/08/2028	Authentification du...	VeriSign Class 3 Pu...		
Objet utilisateur Active Direct	Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	31/12/1999	Enregistrement des ...	Microsoft Timesta...		
Éditeurs approuvés	DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	10/11/2031	Authentification du...	DigiCert		
Certificats non autorisés	DigiCert Global Root CA	DigiCert Global Root CA	10/11/2031	Authentification du...	DigiCert		
Autorisés de certification raci	DigiCert Global Root G2	DigiCert Global Root G2	15/01/2038	Authentification du...	DigiCert Global Roo...		
Personnes autorisées	DigiCert Global Root G3	DigiCert Global Root G3	15/01/2038	Authentification du...	DigiCert Global Roo...		
Émetteurs d'authentification	DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	10/11/2031	Authentification du...	DigiCert		
Racines de confiance de carte	DigiCert Trusted Root G4	DigiCert Trusted Root G4	15/01/2038	Authentification du...	DigiCert Trusted Ro...		
	FG3H0E3917903740	FG3H0E3917903740	12/03/2028	<Tout>	<Aucun>		
	GlobalSign	GlobalSign	18/03/2029	Authentification du...	GlobalSign Root CA...		
	GlobalSign Root CA	GlobalSign Root CA	28/01/2028	Authentification du...	GlobalSign Root CA...		
	ManageEngineCA	ManageEngineCA	10/01/2124	<Tout>	<Aucun>		
	ManageEngineCA-DS-CA	ManageEngineCA-DS-CA	10/01/2124	<Tout>	<Aucun>		
	Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	01/01/2000	Messengerie électro...	Microsoft Authenti...		
	Microsoft ECC Product Root Ce...	Microsoft ECC Product Root Certi...	27/02/2043	<Tout>	Microsoft ECC Prod...		
	Microsoft ECC TS Root Certifica...	Microsoft ECC TS Root Certificate ...	27/02/2043	<Tout>	Microsoft ECC TS R...		
	Microsoft Identity Verification R...	Microsoft Identity Verification Ro...	16/04/2045	Signature du code, ...	Microsoft Identity V...		
	Microsoft Root Authority	Microsoft Root Authority	31/12/2020	<Tout>	Microsoft Root Aut...		
	Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	10/05/2021	<Tout>	Microsoft Root Cert...		
	Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	23/06/2035	<Tout>	Microsoft Root Cert...		
	Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	22/03/2036	<Tout>	Microsoft Root Cert...		
	Microsoft Time Stamp Root Cer...	Microsoft Time Stamp Root Certif...	22/10/2039	<Tout>	Microsoft Time Sta...		
	NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 Ve...	08/01/2004	Enregistrement des ...	VeriSign Time Stam...		
	Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile Root ...	15/03/2032	Signature du code	<Aucun>		
	Thawte Timestamping CA	Thawte Timestamping CA	01/01/2021	Enregistrement des ...	Thawte Timestampi...		
	VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary Ce...	17/07/2036	Authentification du...	VeriSign		
	vincennes-SP87-CA	vincennes-SP87-CA	01/07/2031	<Tout>	<Aucun>		Autorité de cer...

1. Ajout du rôle NPS (Network Policy Server)

← →
▶
Gestionnaire de serveur ▶ Tableau de bord

Tableau de bord

- Serveur local
- Tous les serveurs
- Services de fichiers et d... ▶
- Services de stratégie et...

BIENVENUE DANS GESTIONNAIRE DE SERVEUR

DÉMARRAGE RAPIDE

NOUVEAUTÉS

- 1 Configurer ce serveur local
- 2 Ajouter des rôles et des fonctionnalités
- 3 Ajouter d'autres serveurs à gérer
- 4 Créer un groupe de serveurs
- 5 Connecter ce serveur aux services cloud

Sélectionner le type d'installation

SERVEUR DE DESTINATION
SP124.vincennes.fr

- Type d'installation
- Sélection du serveur
- Rôles de serveurs
- Fonctionnalités
- Confirmation

Sélectionnez le type d'installation. Vous pouvez installer des rôles et des fonctionnalités sur un ordinateur physique ou virtuel en fonctionnement, ou sur un disque dur virtuel hors connexion.

- Installation basée sur un rôle ou une fonctionnalité**
 Configurez un serveur unique en ajoutant des rôles, des services de rôle et des fonctionnalités.
- Installation des services Bureau à distance**
 Installez les services de rôle nécessaires à l'infrastructure VDI (Virtual Desktop Infrastructure) pour déployer des bureaux basés sur des ordinateurs virtuels ou sur des sessions.

Sélectionner le serveur de destination

SERVEUR DE DESTINATION
SP124.vincennes.fr

- Avant de commencer
- Type d'installation
- Sélection du serveur**
- Rôles de serveurs
- Fonctionnalités
- Confirmation
- Résultats

Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

- Sélectionner un serveur du pool de serveurs
- Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :		
Nom	Adresse IP	Système d'exploitation
SP124.vincennes.fr	172.27.0.13	Microsoft Windows Server 2022 Datacenter

Choisir « Serveur de stratégie et d'accès réseau » puis installer

Sélectionner des rôles de serveurs

SERVEUR DE DESTINATION
SP124.vincennes.fr

- Avant de commencer
- Type d'installation
- Sélection du serveur
- Rôles de serveurs**
- Fonctionnalités
- Confirmation
- Résultats

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

Rôles

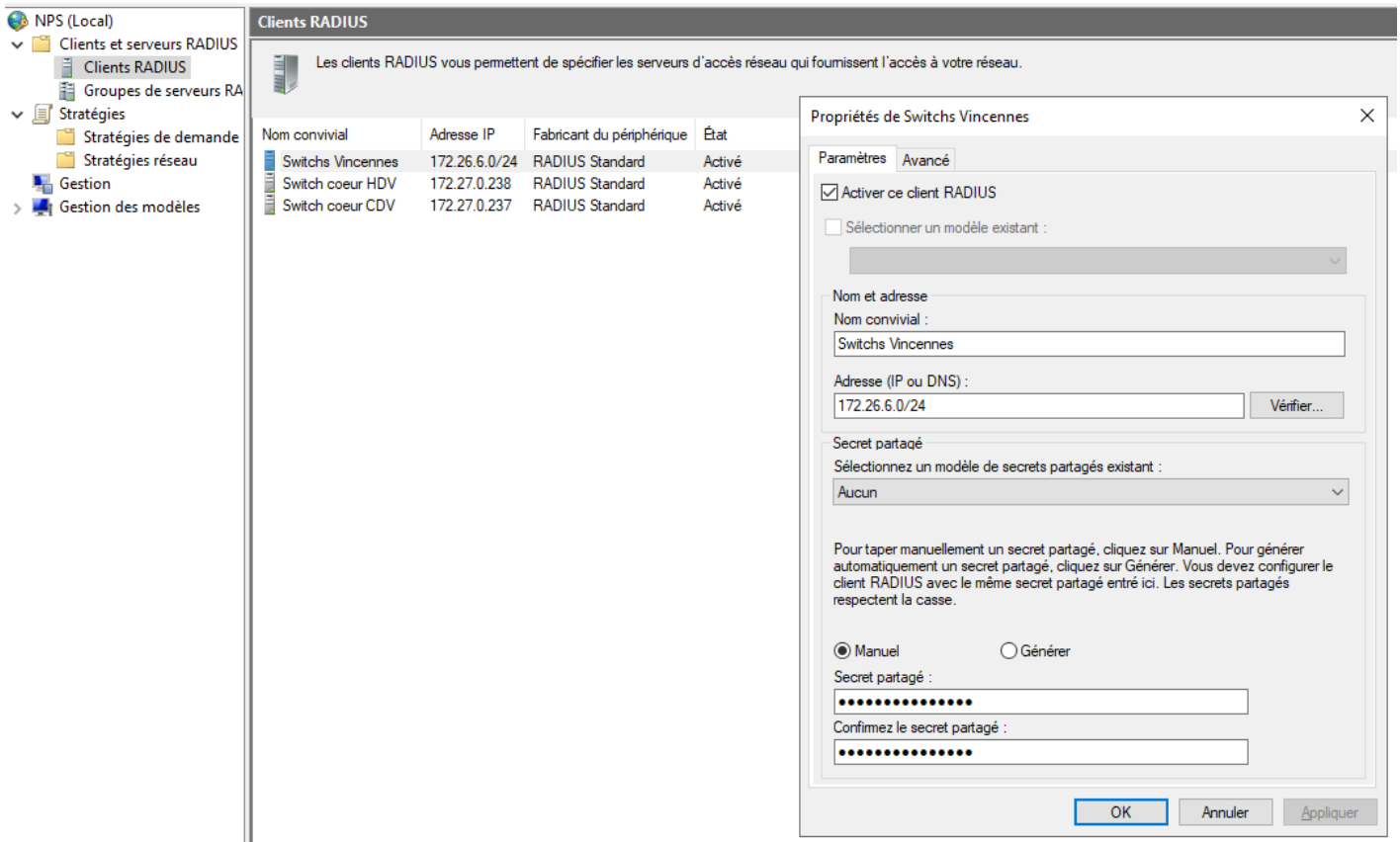
- Contrôleur de réseau
- Hyper-V
- Serveur de télécopie
- Serveur DHCP
- Serveur DNS
- Serveur Web (IIS)
- Service Guardian hôte
- Services AD DS
- Services AD LDS (Active Directory Lightweight Directory Services)
- Services AD RMS (Active Directory Rights Management Services)
- Services Bureau à distance
- Services d'activation en volume
- Services d'impression et de numérisation de documents
- Services de certificats Active Directory
- Services de fédération Active Directory (AD FS)
- Services de fichiers et de stockage (1 sur 12 installés)
- Services de stratégie et d'accès réseau (Installé)
- Services WSUS (Windows Server Update Services)
- Windows Deployment Services

Description

Les services de stratégie et d'accès réseau fournissent un serveur NPS (Network Policy Server) qui contribue à garantir la sécurité de votre réseau.

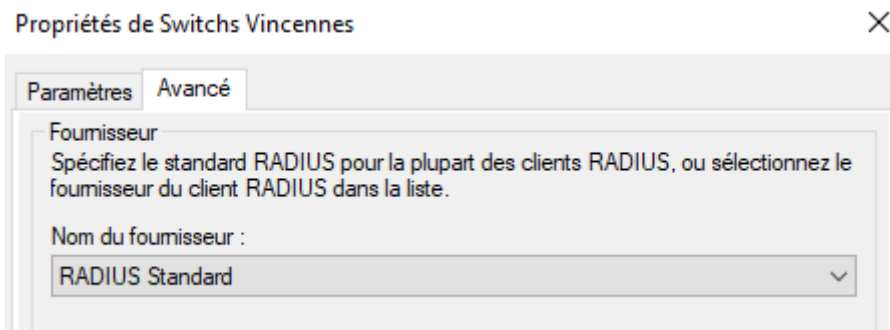
1. Configuration du NPS :

Configurer les clients radius (réseau sur lequel se trouvent les switchs et les bornes wifi)



A noter que le secret partagé se trouve dans le keypass.

Onglet « Avancé »



Configuration de demande de connexion : s'applique aux éléments actifs (switchs et borne wifi)

- NPS (Local)
 - Clients et serveurs RADIUS
 - Clients RADIUS
 - Groupes de serveurs RADIUS distants
 - Stratégies
 - Stratégies de demande de connexion**
 - Stratégies réseau
 - Gestion
 - Gestion des modèles

Stratégies de demande de connexion

Les stratégies de demande de connexion vous permettent de spécifier si les demandes de connexion sont traitées

Nom de la stratégie	État	Ordre de traitement	Source
AP 802.1x	Activé	1	Non spécifié
Utiliser l'authentification Windows pour tous les utilisateurs	Désactivé	2	Non spécifié

AP 802.1x

Conditions - Si les conditions suivantes sont réunies :

Condition	Valeur
Type de port NAS	Ethernet OU Sans fil - IEEE 802.11

Paramètres - Les paramètres suivants sont appliqués :

Paramètre	Valeur
Fournisseur d'authentification	Ordinateur local
Remplacer l'authentification	Désactivé

Les stratégies réseaux sont configurées de manière à orienter les réseaux vers lesquels les agents vont se connecter en fonction du groupe auxquels ils appartiennent.

Les groupes sont configurés dans l'AD :

- Groupes globaux
 - Groupes locaux
 - Acces
 - de test
 - Imprimantes
 - Ordinateur par plage DHCP
 - Ordinateurs
 - Organisation
 - Radius**
 - Utilisateurs
 - SSRPM

- ACCES_RADIUS_DINSI
- ACCES_RADIUS_TEST
- ACCES_RADIUS_VILLE

- Groupes globaux
 - Groupes de sécurité - Global
 - Groupes de sécurité - Domaine local
 - Groupes de sécurité - Global

Sur les serveurs NPS du domaine Vincennes.fr, nous avons configuré 3 stratégies réseaux dans un premier temps :

ToIP, 802 1X_ADMIN et 802 1X_VILLE

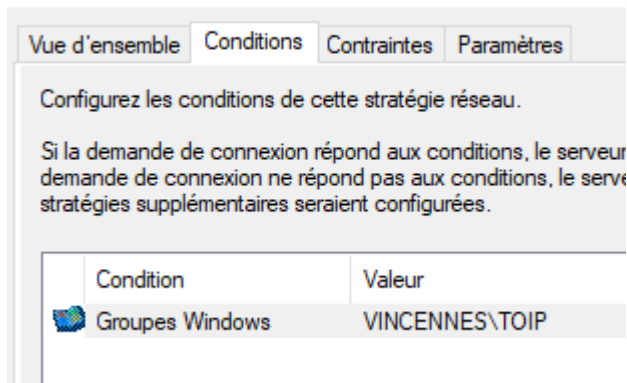


Nom de la stratégie	État	Id	Action	Commentaire
meraki_8021x_test	Activé	1	Accorder l'accès	Non spécifié
ToIP	Activé	2	Accorder l'accès	Non spécifié
802.1x_ADMIN	Activé	3	Accorder l'accès	Non spécifié
802.1x_VILLE	Activé	4	Accorder l'accès	Non spécifié
802.1x_ECOLES	Activé	5	Accorder l'accès	Non spécifié
Connexions au serveur Microsoft de Routage et Accès distants	Désactivé	999998	Refuser l'accès	Non spécifié
Connexions à d'autres serveurs d'accès	Désactivé	999999	Refuser l'accès	Non spécifié

Stratégie ToIP :

Comme son nom l'indique, elle permet aux téléphones de s'authentifier au serveur Radius via son ID de vlan (224) et via la méthode MD5-challenge activée sur ce dernier.

Propriétés de ToIP



Vue d'ensemble Conditions Contraintes Paramètres

Configurez les conditions de cette stratégie réseau.

Si la demande de connexion répond aux conditions, le serveur demande de connexion ne répond pas aux conditions, le serveur stratégies supplémentaires seraient configurées.

Condition	Valeur
Groupes Windows	VINCENNES\TOIP

Propriétés de ToIP

Vue d'ensemble Conditions **Contraintes** Paramètres

Configurez les contraintes de cette stratégie réseau.
Si la demande de connexion ne répond pas à toutes les contraintes, l'accès réseau est refusé.

Contraintes :

Contraintes

- Méthodes d'authentification**
- Délai d'inactivité
- Délai d'expiration de session
- ID de la station appelée
- Restrictions relatives aux jours et aux heures
- Type de port NAS

Autorisez l'accès uniquement aux clients qui s'authentifient à l'aide des méthodes spécifiées.

Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.

Types de protocoles EAP :

MD5-Challenge

Monter

Descendre

Ajouter... Modifier... Supprimer

Méthodes d'authentification moins sécurisées :

- Authentification chiffrée Microsoft version 2 (MS-CHAP v2)
 - L'utilisateur peut modifier le mot de passe après son expiration
- Authentification chiffrée Microsoft (MS-CHAP)
 - L'utilisateur peut modifier le mot de passe après son expiration
- Authentification chiffrée (CHAP)
- Authentification non chiffrée (PAP, SPAP)
- Autoriser les clients à se connecter sans négocier une méthode d'authentification

Propriétés de ToIP

Vue d'ensemble Conditions Contraintes **Paramètres**

Configurez les paramètres de cette stratégie réseau.
Si la demande de connexion répond aux conditions et contraintes, et si la stratégie accorde l'accès, les paramètres sont appliqués.

Paramètres :

Attributs RADIUS

- Standard**
- Spécifiques au fournisseur

Routage et accès à distance

- Liaisons multiples et protocole BAP (Bandwidth Allocation Protocol)
- Filtres IP
- Chiffrement
- Paramètres IP

Pour envoyer des attributs supplémentaires aux clients RADIUS, sélectionnez un attribut RADIUS standard, puis cliquez sur Modifier. Si vous ne configurez pas d'attribut, celui-ci n'est pas envoyé aux clients RADIUS. Consultez la documentation de votre client RADIUS pour connaître les attributs nécessaires.

Attributs :

Nom	Valeur
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID	224
Tunnel-Type	Virtual LANs (VLAN)

Ajouter... Modifier... Supprimer

Propriétés de ToIP

Vue d'ensemble Conditions Contraintes Paramètres

Configurez les paramètres de cette stratégie réseau.
Si la demande de connexion répond aux conditions et contraintes, et si la stratégie accorde l'accès, les paramètres sont appliqués.

Paramètres :

- Attributs RADIUS
 - Standard
 - Spécifiques au fournisseur
- Routage et accès à distance
 - Liaisons multiples et protocole BAP (Bandwidth Allocation Protocol)
 - Filtres IP
 - Chiffrement
 - Paramètres IP

Pour envoyer des attributs supplémentaires aux clients RADIUS, sélectionnez un attribut spécifique au fournisseur, puis cliquez sur Modifier. Si vous ne configurez pas d'attribut, celui-ci n'est pas envoyé aux clients RADIUS. Consultez la documentation de votre client RADIUS pour connaître les attributs nécessaires.

Attributs :

Nom	Fournisseur	Valeur
Cisco-AV-Pair	Cisco	device-traffic-class=voice, subscriber:command=reauth

Informations d'attribut



Nom de l'attribut :
Cisco-AV-Pair

Numéro de l'attribut :
5000

Format de l'attribut :
String

Valeurs d'attribut :

Fournisseur	Valeur
Cisco	device-traffic-class=voice
Cisco	subscriber:command=reauthenticate
Cisco	audit-session-id

Ajouter...

Modifier...

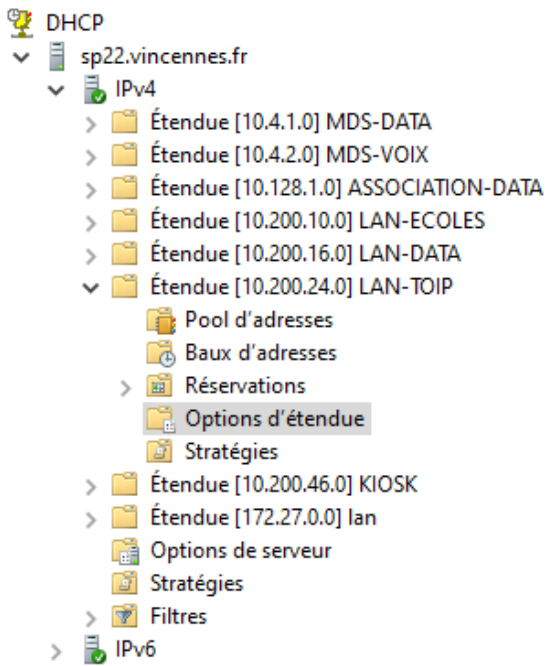
Supprimer

Monter

Descendre

A noter qu'un fichier .reg a été créé afin de rajouter une configuration supplémentaire non incluse dans les paramètres classiques.

Il a été ajouté également l'option 43 sur le Lan-Toip avec la valeur 3a 02 00 e0 dans le serveur DHCP.



Nom d'option	Fournisseur	Valeur
003 Routeur	Standard	10.200.24.1
006 Serveurs DNS	Standard	172.27.0.186, 172.27.0.42
015 Nom de domaine DNS	Standard	vincennes.fr
043 Informations spécifique...	Standard	3a 02 00 e0
066 Nom d'hôte du serveu...	Standard	10.200.0.3
067 Nom du fichier de dé...	Standard	none
004 Serveur de temps	Standard	172.27.0.42

« 3a 02 » correspondant a Alcatel et « 00 e0 » a l'ID du vlan voix en hexadecimal (224).

Cela permet au téléphone de se monter sans avoir l'ID du vlan de cocher dans les paramètres IP.

Stratégie ADMIN :

Cette stratégie permet l'accès du réseau aux administrateurs. La configuration du PC admin doit être en DHCP avec réservation MAC et le vlan d'admin (205) sera monté automatiquement.

802.1x_ADMIN	Activé	3	Accorder l'accès	Non spécifié
802.1x_VILLE	Activé	4	Accorder l'accès	Non spécifié
802.1x_ECOLES	Activé	5	Accorder l'accès	Non spécifié
Connexions au serveur Microsoft de Routage et Accès distants	Désactivé	999998	Refuser l'accès	Non spécifié
Connexions à d'autres serveurs d'accès	Désactivé	999999	Refuser l'accès	Non spécifié

802.1x_ADMIN

Conditions - Si les conditions suivantes sont réunies :

Condition	Valeur
Groupes d'ordinateurs	VINCENNES\ACCES_RADIUS_DINSI

Paramètres - Les paramètres suivants sont appliqués :

Paramètre	Valeur
Configuration du protocole EAP (Extensible Authentication Protocol)	Configuré
Autorisation d'accès	Accorder l'accès
Méthode EAP (Extensible Authentication Protocol)	Microsoft: PEAP (Protected EAP)
Méthode d'authentification	Protocole EAP
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical format)
Tunnel-Pvt-Group-ID	205
Tunnel-Type	Virtual LANs (VLAN)
Pourcentage de capacité du protocole BAP	Réduisez les liaisons multiples si le serveur atteint 50% pour 2 minutes

Le groupe AD dans lequel les PC Admins devront être sont ACCES_RADIUS_DINSI

Propriétés de 802.1x_ADMIN

Vue d'ensemble Conditions Contraintes Paramètres

Configurez les conditions de cette stratégie réseau.

Si la demande de connexion répond aux conditions, le serveur NPS utilise cette demande de connexion ne répond pas aux conditions, le serveur NPS ignore ces stratégies supplémentaires seraient configurées.

Condition	Valeur
Groupes d'ordinateurs	VINCENNES\ACCES_RADIUS_DINSI

Propriétés de 802.1x_ADMIN

Vue d'ensemble Conditions **Contraintes** Paramètres

Configurez les contraintes de cette stratégie réseau.
Si la demande de connexion ne répond pas à toutes les contraintes, l'accès réseau est refusé.

Contraintes :

Contraintes

- Méthodes d'authentification**
- Délai d'inactivité
- Délai d'expiration de session
- ID de la station appelée
- Restrictions relatives aux jours et aux heures
- Type de port NAS

Autorisez l'accès uniquement aux clients qui s'authentifient à l'aide des méthodes spécifiées.

Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.

Types de protocoles EAP :

Microsoft: PEAP (Protected EAP)

Monter
Descendre

Ajouter... Modifier... Supprimer

Méthodes d'authentification moins sécurisées :

- Authentification chiffrée Microsoft version 2 (MS-CHAP v2)
 - L'utilisateur peut modifier le mot de passe après son expiration
- Authentification chiffrée Microsoft (MS-CHAP)
 - L'utilisateur peut modifier le mot de passe après son expiration
- Authentification chiffrée (CHAP)
- Authentification non chiffrée (PAP, SPAP)
- Autoriser les clients à se connecter sans négocier une méthode d'authentification

Propriétés de 802.1x_ADMIN

Vue d'ensemble Conditions Contraintes **Paramètres**

Configurez les paramètres de cette stratégie réseau.
Si la demande de connexion répond aux conditions et contraintes, et si la stratégie accorde l'accès, les paramètres sont appliqués.

Paramètres :

Attributs RADIUS

- Standard**
- Spécifiques au fournisseur

Routage et accès à distance

- Liaisons multiples et protocole BAP (Bandwidth Allocation Protocol)
- Filtres IP
- Chiffrement
- Paramètres IP

Pour envoyer des attributs supplémentaires aux clients RADIUS, sélectionnez un attribut RADIUS standard, puis cliquez sur Modifier. Si vous ne configurez pas d'attribut, celui-ci n'est pas envoyé aux clients RADIUS. Consultez la documentation de votre client RADIUS pour connaître les attributs nécessaires.

Attributs :

Nom	Valeur
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID	205
Tunnel-Type	Virtual LANs (VLAN)

Ajouter... Modifier... Supprimer

Stratégie LAN-DATA :

Cette stratégie permet aux utilisateurs standard de se connecter sur le réseau (vlan 216)

Nom de la stratégie	État	Ordre de traitement	Type d'accès	Source
meraki_8021x_test	Activé	1	Accorder l'accès	Non spécifié
ToIP	Activé	2	Accorder l'accès	Non spécifié
802.1x_ADMIN	Activé	3	Accorder l'accès	Non spécifié
802.1x_VILLE	Activé	4	Accorder l'accès	Non spécifié
802.1x_ECOLES	Activé	5	Accorder l'accès	Non spécifié

802.1x_VILLE

Conditions - Si les conditions suivantes sont réunies :

Condition	Valeur
Groupes d'ordinateurs	VINCENNES\ACCES_RADIUS_VILLE

Paramètres - Les paramètres suivants sont appliqués :

Paramètre	Valeur
Cisco-AV-Pair	audit-session-id, subscriber:command=reauthenticate
Configuration du protocole EAP (Extensible Authentication Protocol)	Configuré
Autorisation d'accès	Accorder l'accès
Méthode EAP (Extensible Authentication Protocol)	Microsoft: PEAP (Protected EAP)
Méthode d'authentification	Protocole EAP
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical format)
Tunnel-Pvt-Group-ID	216
Tunnel-Type	Virtual LANs (VLAN)
Pourcentage de capacité du protocole BAP	Réduisez les liaisons multiples si le serveur atteint 50% pour 2 minutes

Accès aux utilisateurs qui se trouvent dans le groupe ACCES_RADIUS_VILLE

Propriétés de 802.1x_VILLE

Vue d'ensemble Conditions **Contraintes** Paramètres

Configurez les conditions de cette stratégie réseau.

Si la demande de connexion répond aux conditions, le serveur NPS utilise cette demande de connexion ne répond pas aux conditions, le serveur NPS ignore ces stratégies supplémentaires seraient configurées.

Condition	Valeur
Groupes d'ordinateurs	VINCENNES\ACCES_RADIUS_VILLE

Propriétés de 802.1x_VILLE

Vue d'ensemble Conditions **Contraintes** Paramètres

Configurez les contraintes de cette stratégie réseau.
Si la demande de connexion ne répond pas à toutes les contraintes, l'accès réseau est refusé.

Contraintes :

Contraintes

- Méthodes d'authentification
- Délai d'inactivité
- Délai d'expiration de session
- ID de la station appelée
- Restrictions relatives aux jours et aux heures
- Type de port NAS

Autorisez l'accès uniquement aux clients qui s'authentifient à l'aide des méthodes spécifiées.

Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.

Types de protocoles EAP :

Microsoft: PEAP (Protected EAP)

Monter
Descendre

<
>

Ajouter...
Modifier...
Supprimer

Méthodes d'authentification moins sécurisées :

- Authentification chiffrée Microsoft version 2 (MS-CHAP v2)
 - L'utilisateur peut modifier le mot de passe après son expiration
- Authentification chiffrée Microsoft (MS-CHAP)
 - L'utilisateur peut modifier le mot de passe après son expiration
- Authentification chiffrée (CHAP)
- Authentification non chiffrée (PAP, SPAP)
- Autoriser les clients à se connecter sans négocier une méthode d'authentification

Propriétés de 802.1x_VILLE

Vue d'ensemble Conditions Contraintes **Paramètres**

Configurez les paramètres de cette stratégie réseau.
Si la demande de connexion répond aux conditions et contraintes, et si la stratégie accorde l'accès, les paramètres sont appliqués.

Paramètres :

Attributs RADIUS

- Standard
- Spécifiques au fournisseur

Routage et accès à distance

- Liaisons multiples et protocole BAP (Bandwidth Allocation Protocol)
- Filtres IP
- Chiffrement
- Paramètres IP

Pour envoyer des attributs supplémentaires aux clients RADIUS, sélectionnez un attribut RADIUS standard, puis cliquez sur Modifier. Si vous ne configurez pas d'attribut, celui n'est pas envoyé aux clients RADIUS. Consultez la documentation de votre client RADIUS pour connaître les attributs nécessaires.

Attributs :

Nom	Valeur
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...)
Tunnel-Pvt-Group-ID	216
Tunnel-Type	Virtual LANs (VLAN)

Ajouter...
Modifier...
Supprimer

Vue d'ensemble Conditions Contraintes Paramètres

Configurez les paramètres de cette stratégie réseau.
Si la demande de connexion répond aux conditions et contraintes, et si la stratégie accorde l'accès, les paramètres sont appliqués.

Paramètres :

Attributs RADIUS

- Standard
- Spécifiques au fournisseur

Routage et accès à distance

- Liaisons multiples et protocole BAP (Bandwidth Allocation Protocol)
- Filtres IP
- Chiffrement
- Paramètres IP

Pour envoyer des attributs supplémentaires aux clients RADIUS, sélectionnez un attribut spécifique au fournisseur, puis cliquez sur Modifier. Si vous ne configurez pas d'attribut, celui-ci n'est pas envoyé aux clients RADIUS. Consultez la documentation de votre client RADIUS pour connaître les attributs nécessaires.

Attributs :

Nom	Fournisseur	Valeur
Cisco-AV-Pair	Cisco	audit-session-id, subscriber:command=reauthentic...

Informations d'attribut

Nom de l'attribut :
Cisco-AV-Pair

Numéro de l'attribut :
5000

Format de l'attribut :
String

Valeurs d'attribut :

Fournisseur	Valeur
Cisco	audit-session-id
Cisco	subscriber:command=reauthenticate

Ajouter...
Modifier...
Supprimer
Monter
Descendre

Stratégie LAN_ECOLES :

2 serveurs ont été créés sur le domaine des écoles, il s'agit de SP129 et SP130.

2 serveurs de certification ont également été créés, il s'agit de SP131 et SP132.

Cette stratégie s'applique à tout le réseau des postes des écoles (Elèves, enseignants et directeur) sauf les postes des infirmeries, des gardiens ou du personnel des centres de loisirs.

ToIP	Activé	1	Accorder l'accès	Non spécifié
802.1x_ECOLE	Activé	2	Accorder l'accès	Non spécifié
802.1x_ECOLES	Désactivé	3	Accorder l'accès	Non spécifié
Connexions au serveur Microsoft de Routage et Accès distants	Désactivé	4	Refuser l'accès	Non spécifié
Connexions à d'autres serveurs d'accès	Désactivé	5	Refuser l'accès	Non spécifié

802.1x_ECOLE

Conditions - Si les conditions suivantes sont réunies :

Condition	Valeur
Groupes d'ordinateurs	ECOLES\ECOLES.ORDINATEURS

Paramètres - Les paramètres suivants sont appliqués :

Paramètre	Valeur
Cisco-AV-Pair	audit-session-id, subscriber:command=reauthenticate
Configuration du protocole EAP (Extensible Authentication Protocol)	Configuré
Autorisation d'accès	Accorder l'accès
Méthode EAP (Extensible Authentication Protocol)	Microsoft: PEAP (Protected EAP)
Méthode d'authentification	Protocole EAP
Framed-Protocol	PPP

Service-Type	Framed
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical format)
Tunnel-Pvt-Group-ID	210
Tunnel-Type	Virtual LANs (VLAN)
Pourcentage de capacité du protocole BAP	Réduisez les liaisons multiples si le serveur atteint 50% pour 2 minutes

Le groupe AD dans lequel les PCs des écoles devront être est le suivant :

Propriétés de 802.1x_ECOLES

Vue d'ensemble Conditions Contraintes Paramètres

Configurez les conditions de cette stratégie réseau.

Si la demande de connexion répond aux conditions, le serveur NPS utilise c
demande de connexion ne répond pas aux conditions, le serveur NPS igno
stratégies supplémentaires seraient configurées.

Condition	Valeur
Groupes d'ordinateurs	ECOLES\ECOLES.ORDINATEURS

Propriétés de 802.1x_ECOLES

Vue d'ensemble Conditions **Contraintes** Paramètres

Configurez les contraintes de cette stratégie réseau.
Si la demande de connexion ne répond pas à toutes les contraintes, l'accès réseau est refusé.

Contraintes :

Contraintes

- Méthodes d'authentification**
- Délai d'inactivité
- Délai d'expiration de session
- ID de la station appelée
- Restrictions relatives aux jours et aux heures
- Type de port NAS

Autonisez l'accès uniquement aux clients qui s'authentifient à l'aide des méthodes spécifiées.

Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.

Types de protocoles EAP :

Monter
Descendre

Méthodes d'authentification moins sécurisées :

- Authentification chiffrée Microsoft version 2 (MS-CHAP v2)
 - L'utilisateur peut modifier le mot de passe après son expiration
- Authentification chiffrée Microsoft (MS-CHAP)
 - L'utilisateur peut modifier le mot de passe après son expiration
- Authentification chiffrée (CHAP)
- Authentification non chiffrée (PAP, SPAP)
- Autoriser les clients à se connecter sans négocier une méthode d'authentification

Propriétés de 802.1x_ECOLES

Vue d'ensemble Conditions Contraintes **Paramètres**

Configurez les paramètres de cette stratégie réseau.
Si la demande de connexion répond aux conditions et contraintes, et si la stratégie accorde l'accès, les paramètres sont appliqués.

Paramètres :

Attributs RADIUS

- Standard**
- Spécifiques au fournisseur

Routage et accès à distance

- Liaisons multiples et protocole BAP (Bandwidth Allocation Protocol)
- Filtres IP
- Chiffrement
- Paramètres IP

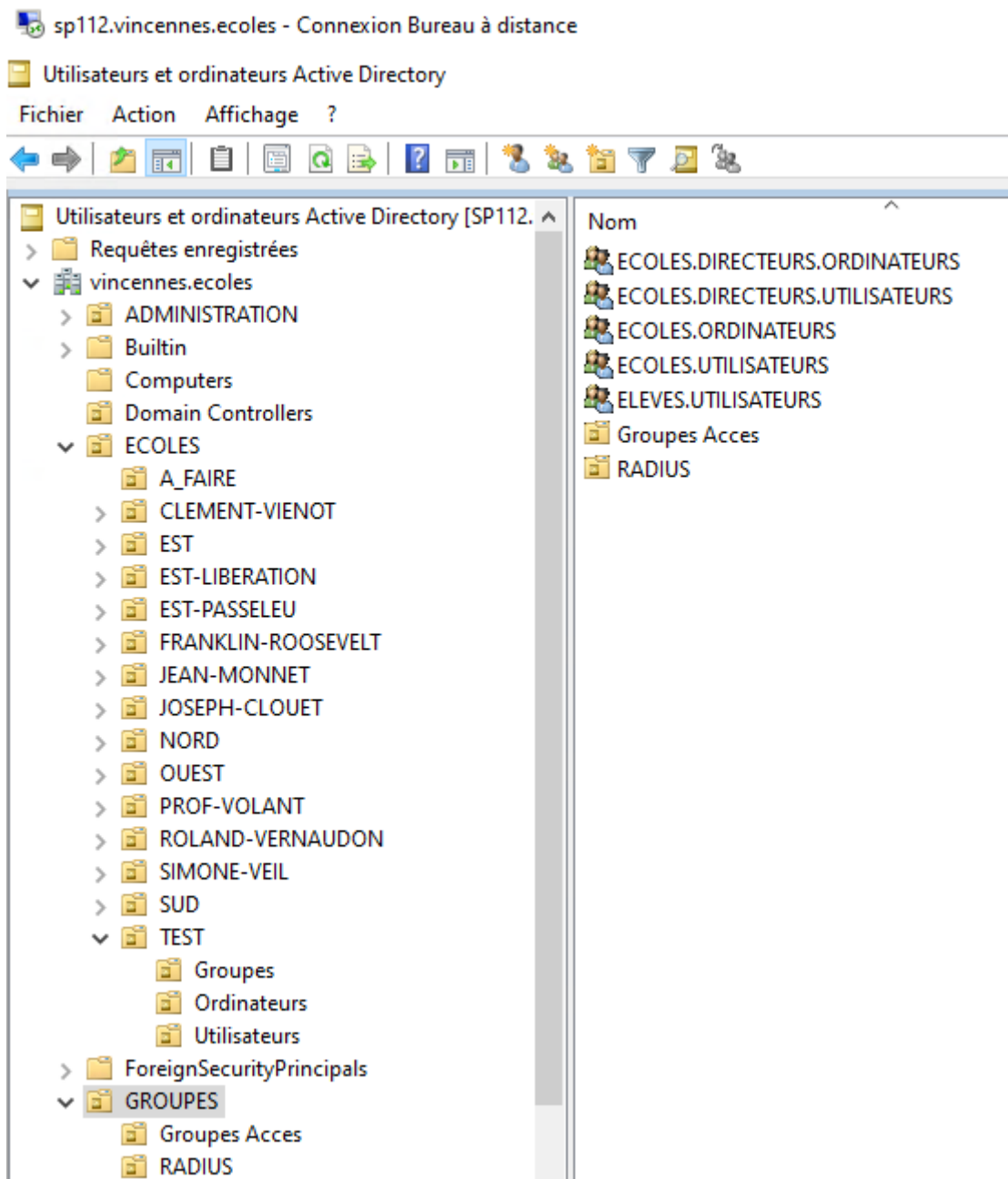
Pour envoyer des attributs supplémentaires aux clients RADIUS, sélectionnez un attribut RADIUS standard, puis cliquez sur Modifier. Si vous ne configurez pas d'attribut, celui-ci n'est pas envoyé aux clients RADIUS. Consultez la documentation de votre client RADIUS pour connaître les attributs nécessaires.

Attributs :

Nom	Valeur
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID	210
Tunnel-Type	Virtual LANs (VLAN)

Configuration sur le serveur AD des écoles :

Le PC doit être dans le groupe ECOLES.ORDINATEURS



Stratégie de groupe permettant l'activation du radius sur la carte réseau :

Activation 802.1X

Étendue Détails Paramètres Délégation État

Activation 802.1X

Données recueillies le : 19/03/2025 15:58:49

[masquer tout](#)

Général

[masquer](#)

Détails

[masquer](#)

Domaine	vincennes.ecoles
Propriétaire	ECOLES\Admins du domaine
Créé le	13/03/2025 19:33:58
Modifié le	13/03/2025 19:55:26
Révisions utilisateur	0 (AD), 0 (SYSVOL)
Révisions ordinateur	15 (AD), 15 (SYSVOL)
ID unique	{56010EC8-D562-4531-9F05-E5BE38160241}
État GPO	Activé

Liaisons

[masquer](#)

Emplacement	Appliqué	État du lien	Chemin d'accès
ECOLES	Non	Activé	vincennes.ecoles/ECOLES

Cette liste ne contient que les liaisons du domaine de l'objet de stratégie de groupe.

Filtrage de sécurité

[masquer](#)

Les paramètres de cet objet GPO ne s'appliquent qu'aux groupes, utilisateurs et ordinateurs suivants :

Nom

ECOLES\Ordinateurs du domaine

Délégation

masquer

Ces groupes et utilisateurs ont l'autorisation spécifiée pour cet objet de stratégie de groupe.

Nom	Autorisations acceptées	Hérité
AUTORITE NT\ENTREPRISE DOMAIN CONTROLLERS	Lecture	Non
AUTORITE NT\Systeme	Modifier les paramètres, supprimer, modifier la sécurité	Non
ECOLES\Administrateurs de l'entreprise	Modifier les paramètres, supprimer, modifier la sécurité	Non
ECOLES\Admins du domaine	Modifier les paramètres, supprimer, modifier la sécurité	Non
ECOLES\Ordinateurs du domaine	Lecture (à partir du filtrage de sécurité)	Non

Configuration ordinateur (activée)

masquer

Stratégies

masquer

Paramètres Windows

masquer

Paramètres de sécurité

masquer

Services système

masquer

Configuration automatique de réseau câblé (Mode de démarrage : Automatique)

masquer

Autorisations

Aucune autorisation spécifiée

Audit

Aucun audit spécifié

Stratégies de réseau câblé (802.3)

masquer

802.1X

masquer

Nom	802.1X
Description	Exemple de description

Paramètres globaux

masquer

Paramètre	Valeur
Utiliser des services réseau LAN câblés Windows pour les clients	Activé
Informations d'identification partagées pour l'authentification réseau	Désactivé

Profil réseau

masquer

Paramètres de sécurité

masquer

Activer l'utilisation de l'authentification IEEE 802.1X pour l'accès réseau	Activé
Forcer l'utilisation de l'authentification IEEE 802.1X pour l'accès réseau	Désactivé

Paramètres IEEE 802.1X

masquer

Mettre en mémoire cache les informations utilisateur pour les futures connexions à ce réseau	Désactivé
Authentification de l'ordinateur	Ordinateur uniquement
Nombre maximal d'échecs d'authentification	1
Nombre maximal de messages EAPOL-Start envoyés	
Période de maintien (secondes)	

Période de démarrage (secondes)

Période d'authentification (secondes)

Propriétés de la méthode d'authentification du réseau

masquer

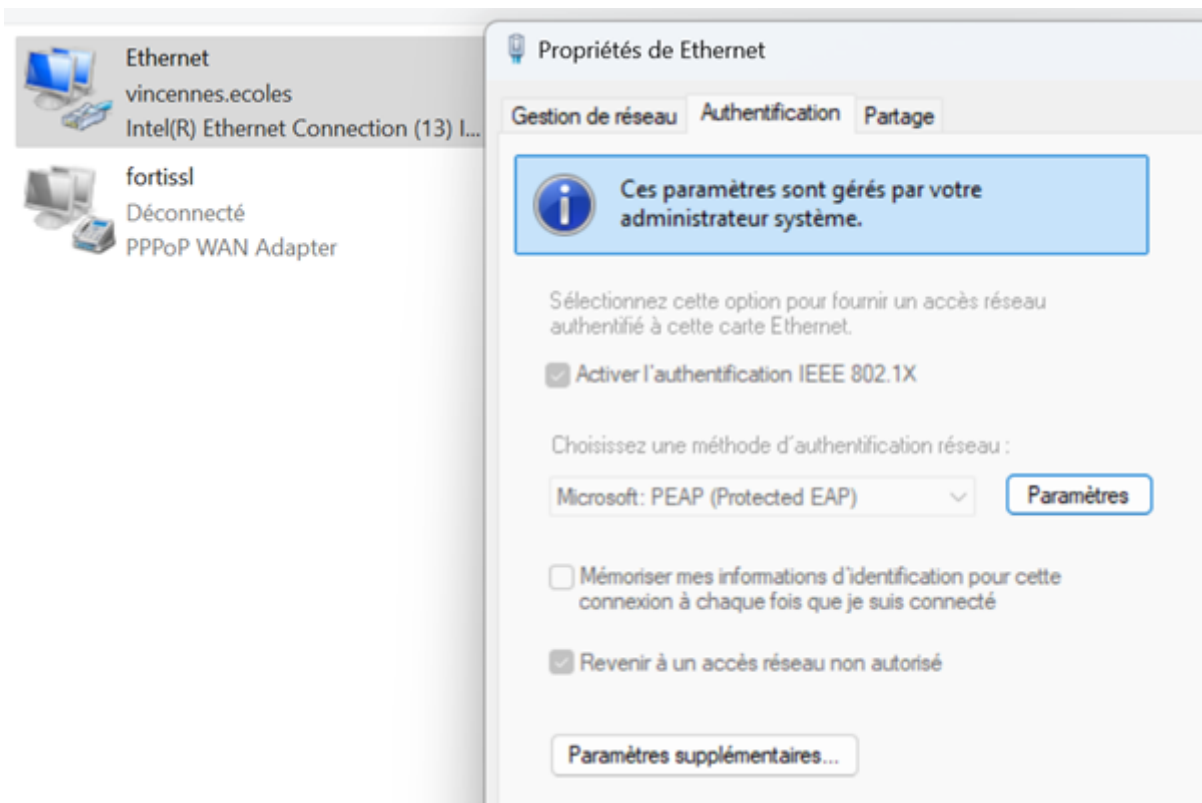
Méthode d'authentification	PEAP (Protected EAP)
Valider le certificat du serveur	Désactivé
Activer la reconnexion rapide	Activé
Déconnect. si le serveur ne présente pas TLV de liaison de chiff.	Désactivé
Appliquer la protection d'accès réseau	Désactivé

Configuration de la méthode d'authentification

masquer

Méthode d'authentification	Mot de passe sécurisé (EAP-MSCHAP version 2)
Utiliser automatiquement mon nom et mon mot de passe Windows d'ouverture de session (et éventuellement le domaine)	Activé

L'onglet « Authentification » apparaît suite à l'activation de la GPO « activation 802.1x »



Vue de l'autorisation d'accès depuis l'observateur d'évènement :

Général | Détails

Le serveur NPS a accordé l'accès à un utilisateur.

Utilisateur :

- ID de sécurité : VINCENNES\LAPTOP-PRO-176\$
- Nom de compte : host/LAPTOP-PRO-176.vincennes.fr
- Domaine de compte : VINCENNES
- Nom de compte complet : vincennes.fr/VINCENNES.FR/MACHINES/LAPTOP-PRO-176

Ordinateur client :

- ID de sécurité : NULL SID
- Nom de compte : -
- Nom de compte complet : -
- Identificateur de la station appelée : B8-AB-61-EF-12-6C:
- Identificateur de la station appelante : 50-EB-F6-8C-80-B3

Serveur NAS :

- Adresse IPv4 du serveur NAS : 172.26.6.181
- Adresse IPv6 du serveur NAS : -

Journal : Sécurité

Source : Microsoft Windows security | Connecté : 19/03/2025 15:49:02

Événement : 6272 | Catégorie : Network Policy Server

Niveau : Information | Mots-clés : Succès de l'audit

Utilisateur : N/A | Ordinateur : SP124.vincennes.fr

Configuration sur la console web Meraki

Il faut dans un premier temps ajouter les serveurs Radius dans la console via le menu « Organization » puis « Settings »

RADIUS servers

Reusable RADIUS servers for access policies across this organization.

Name	Server	Auth Port	Acct Port	Applied networks
SP129	10.200.11.223	1812	1813	Ville de Vincennes LAN - switch
SP130	10.200.11.224	1812	1813	Ville de Vincennes LAN - switch
SP124	172.27.0.13	1812	1813	Ville de Vincennes LAN - switch
SP125	172.27.0.14	1812	1813	Ville de Vincennes LAN - switch

+ Add a RADIUS server

Ensuite il faut ajouter une politique d'accès via le menu « Switching » puis « Access policies »

Access policies

Q Search

2 policies

Policy name	Affected ports	Host mode
∨ RADIUS Ville	29	Multi-Domain
Authentication method	my RADIUS server	Host 172.27.0.13:1812 (radius role: Auth) 172.27.0.14:1812 (radius role: Auth) 172.27.0.13:1813 (radius role: Acct) 172.27.0.14:1813 (radius role: Acct)
Policy type	Hybrid authentication	
∨ RADIUS Ecoles	1	Multi-Domain
Authentication method	my RADIUS server	Host 10.200.11.223:1812 (radius role: Auth) 10.200.11.224:1812 (radius role: Auth) 10.200.11.223:1813 (radius role: Acct) 10.200.11.224:1813 (radius role: Acct)
Policy type	Hybrid authentication	

Lorsque l'on clique sur la policy, on rentre dans les détails de celle-ci :

Radius Ville :

Access Policy Detail 29 switch ports

Name

Authentication method

RADIUS servers

- RADIUS Server testing ⓘ
- RADIUS CoA support ⓘ
- Enable RADIUS accounting servers

#	Name	Host	Secret	Auth	Port	Accounting	Port
1	SP124	<input type="text" value="172.27.0.13"/>	<input type="text" value="••••••••••"/>	<input checked="" type="checkbox"/>	<input type="text" value="1812"/>	<input checked="" type="checkbox"/>	<input type="text" value="1813"/>
2	SP125	<input type="text" value="172.27.0.14"/>	<input type="text" value="••••••••~"/>	<input checked="" type="checkbox"/>	<input type="text" value="1812"/>	<input checked="" type="checkbox"/>	<input type="text" value="1813"/>

+ [Add a server](#)

RADIUS attribute specifying group policy name

Connection

Policy Type ⓘ

Host mode ⓘ

802.1X control direction

Re-authentication interval ⓘ

Concurrent Authentication

Options

- Voice auth ⓘ
- Suspend port bounce ⓘ

Critical Auth VLAN ⓘ **Data** ⓘ **Voice** ⓘ

Guest VLAN ⓘ

Failed Auth VLAN ⓘ

URL redirect walled garden

RADIUS caching ⓘ

Caching timeout ⓘ

[Save](#) [Cancel](#) Please allow 1-2 minutes for changes to take effect.

Radius Ecoles :

Access Policy Detail 1 switch ports

Name

Authentication method

RADIUS servers

- RADIUS Server testing ⓘ
- RADIUS CoA support ⓘ
- Enable RADIUS accounting servers

#	Name	Host	Secret	Auth	Port	Accounting	Port
1	SP129	<input type="text" value="10.200.11.223"/>	<input type="text" value="••••••••"/>	<input checked="" type="checkbox"/>	<input type="text" value="1812"/>	<input checked="" type="checkbox"/>	<input type="text" value="1813"/>
2	SP130	<input type="text" value="10.200.11.224"/>	<input type="text" value="••••••••"/>	<input checked="" type="checkbox"/>	<input type="text" value="1812"/>	<input checked="" type="checkbox"/>	<input type="text" value="1813"/>

+ [Add a server](#)

RADIUS attribute specifying group policy name

Connection

Policy Type ⓘ

Host mode ⓘ

802.1X control direction

Re-authentication interval ⓘ

Concurrent Authentication

Options

- Voice auth ⓘ
- Suspend port bounce ⓘ

Critical Auth VLAN ⓘ **Data** ⓘ **Voice** ⓘ

Guest VLAN ⓘ

Failed Auth VLAN ⓘ

URL redirect walled garden

RADIUS caching ⓘ

Caching timeout ⓘ

[Save](#) [Cancel](#) Please allow 1-2 minutes for changes to take effect.

Concernant la partie wireless, nous avons configuré un SSID de test nommé « Test 802.1x » dans le network Ville de Vincennes.

Test 802.1x

enabled ▾

[rename](#)

[edit settings](#)

802.1X with custom RADIUS

None

unlimited

Local LAN

no

no

111

Disabled

no

n/a

n/a

Access control

SSID

Test 802.1x

Basic info

SSID (name)

Test 802.1x

SSID status

Enabled

Disabled

Hide SSID

Security WPA1/2 Enterprise with 1 RADIUS server and 1 accounting server

Open (no encryption)
Any user can associate

Opportunistic Wireless Encryption (OWE)
Any user can associate with data encryption

Password
Users must enter a passphrase to associate ⓘ

MAC-based access control (no encryption)
RADIUS server is queried at association time

Enterprise with
my RADIUS server ▾

User credentials are validated with 802.1X at association time

Identity PSK with RADIUS

MAC-based Authentication ▾

RADIUS server is queried at association time to obtain a passphrase for a device based on its MAC address

Wi-Fi Personal Network (WPN) ⓘ

Enabled

Disabled

WPA encryption ⓘ

WPA1 and WPA2 ▾



802.11r is disabled due to RADIUS CoA being enabled

802.11r ⓘ

Enabled

Adaptive

Disabled

802.11w ⓘ

Enabled (allow unsupported clients)

Required (reject unsupported clients)

Disabled (never use)



Traffic from static IP address clients will be blocked on this SSID.

Mandatory DHCP

Enabled

Disabled

Splash page *None*



Not all splash authentication methods are compatible with WPA2-Enterprise authentication

None (direct access)

Users can access the network as soon as they associate

Click-through

Users must view and acknowledge your splash page before being allowed on the network

Sponsored guest login

Guests must enter a valid sponsor and own email address before being allowed on the network

Sign-on with

Meraki Cloud Authentication ▾

Users must enter a username and password before being allowed on the network

Sign-on with SMS Authentication

Users enter a mobile phone number and receive an authorization code via SMS.

After a trial period of 25 texts, you will need to connect with your Twilio account on the [Network-wide settings](#) page.

Cisco Identity Services Engine (ISE) Authentication ⓘ

Users are redirected to the Cisco ISE web portal for device posturing and guest access

Endpoint management enrollment ⓘ

Only devices enrolled in endpoint management can access this network

RADIUS 1 RADIUS server, 1 accounting server - CoA supported

RADIUS servers

#	Host IP	Auth port	Secret	RadSec ⓘ	Test
1	172.27.0.13	1812	●●●●●●●●●●●●●●●●	<input type="checkbox"/>	<button>Test</button>

[Add server](#) 3 max.

RADIUS accounting servers

#	Host IP	Acct port	Secret	RadSec ⓘ
1	172.27.0.13	1813	●●●●●●●●●●●●●●●●	<input type="checkbox"/>

[Add server](#) 3 max.



Enabling RADIUS CoA disables the fast roaming features PMKsa caching, OKC, and 802.11r

- RADIUS testing ⓘ
- RADIUS CoA support ⓘ

RADIUS attribute specifying group policy name ⓘ

Advanced RADIUS settings

(NAS ID, Called-station-ID, DAS clients, EAP timers)

Called-station-ID

#	Category
1	AP MAC address
2	SSID name

[Add identifier](#) 4 max.

NAS ID

#	Category
1	AP MAC address
2	SSID number

[Add identifier](#) 4 max.

EAP timers

EAP timeout second(s)

EAP max retries time(s)

EAP identity timeout second(s)

Client IP and VLAN Bridge mode

- Meraki AP assigned (NAT mode)
Clients receive IP addresses in an isolated 10.0.0.0/8 network. Clients cannot communicate with each other, but they may communicate with devices on the wired LAN if the [SSID firewall settings](#) permit.

- External DHCP server assigned
Meraki devices operate transparently (do not perform NAT or DHCP). Wireless clients will receive DHCP leases from a server on the LAN or use static IPs. Use this for wireless clients requiring seamless roaming, shared printers, and wireless cameras.

Bridged

Tunneled

- Layer 3 roaming

RADIUS override ⓘ

Override VLAN tag

Ignore VLAN attribute

RADIUS guest VLAN ⓘ

Disabled

Bonjour forwarding

Bridge mode only

Enabled

Disabled

VLAN tagging ⓘ

VLAN ID

#	Access point tags	VLAN ID
	Default	111

[+ Add VLAN ID](#)

Le vlan assigné est le 111 ce qui correspond au wifi publique. Nous avons également pu tester en mettant le vlan 216 ce qui correspond au vlan data et cela fonctionne parfaitement.

Il faut cependant par ailleurs configurer la borne pour qu'elle accepte la politique radius ce qui a été fait en taggant le SSID (Radius) puis en assignant le TAG au switch sur lequel la borne est connectée ce qui permet sa diffusion.

SSID availability

SSID:

Visibility

Hide this SSID

Per access point
availability ⓘ

Enabled on some access points...

Only enable on access points with any of the following tags:

Radius x

57 access points matched

Scheduled availability

disabled

HDV_DSI_4E	ac:17:c8:04:21:4d	<div style="width: 100%; height: 10px; background-color: green;"></div>	Q2KD-DAH3-B9FY	172.26.6.80	MR42	public Radius HDV
HDV_DSI_RDC	ac:17:c8:04:20:cf	<div style="width: 100%; height: 10px; background-color: green;"></div>	Q2KD-9V23-S32C	172.26.6.81	MR42	public Radius HDV

Ensuite, il faut aller sur le port de connexion de la borne wifi (ici le port 43 du switch que nous avons taggé précédemment) et le configurer avec le vlan correspondant au SSID.

Il faut ensuite ajouter ce vlan sur le port ou est connecté la borne comme cela :

● HDV-DINSI-LT1-01

MS130-48P 6c:c3:b2:0e:46:ea



Set a location for this switch

Add an address below and check Move marker to update its location

ADDRESS 

LAN IP 

172.26.6.185 (statically assigned)

VLAN

106

PUBLIC IP

159.180.242.30

GATEWAY

172.26.6.254

DNS

8.8.8.8

8.8.4.4

LAN IPV6 

Not configured

SERIAL NUMBER

Q3LU-RJUJ-LYBA

TAGS 

Summary **Ports** Power Event log

Port 43: Borne wifi DINSI RDC [Return to port list](#)



Historical data for the last day ▾

Port traffic



Configuration

Port status	Enabled
Type	Trunk
Native VLAN	106
Allowed VLANs	103,106,110-112,205,216
Access policy	Open
Link negotiation	Auto negotiate (1 Gbps)
RSTP	Enabled (Forwarding)

La configuration concernant les ports filaires se font de la manière suivante avec l'Access Policy et le vlan :

L'utilisateur doit absolument être intégré au bon groupe si nous voulons que la stratégie se monte correctement.

Switch / Port

HDV-DINSI-RDC-01 / 23

Name

Port status

Enabled **Disabled**

Link negotiation

Auto negotiate ▼

Port schedule

Unscheduled ▼

Tags

Port profile name

▼

Type

Trunk **Access**

Access policy ⓘ

RADIUS Ville ▼

VLAN

1 ▼

Voice VLAN

224 ▼

Procedure_Mise_A_Jour_Version_Linux

PROCEDURE MISE A JOUR LINUX

MREMOTENG 2

SNAPSHOT 2

LINUX 4

Update and upgrade 4

Processus de mise à jour 4

VERIFICATION 7

Prérequis :

- Vsphere
- MremoteNG

MREMOTENG

Installer logiciel prise en main en ligne de commande car plus pratique

Renseigner l'host, mot de passe et ID root, changer le protocole en SSH version 2

Configuration	
Affichage	
Nom	ST39
Description	
Icône	mRemoteNG
Panneau	General
Connexion	
Nom d'hôte / IP	192.168.201.43
Nom d'utilisateur	root
Mot de passe	••••••••
Protocole	
Protocole	SSH version 2
Port	22
Session PuTTY	Default Settings
Autre	

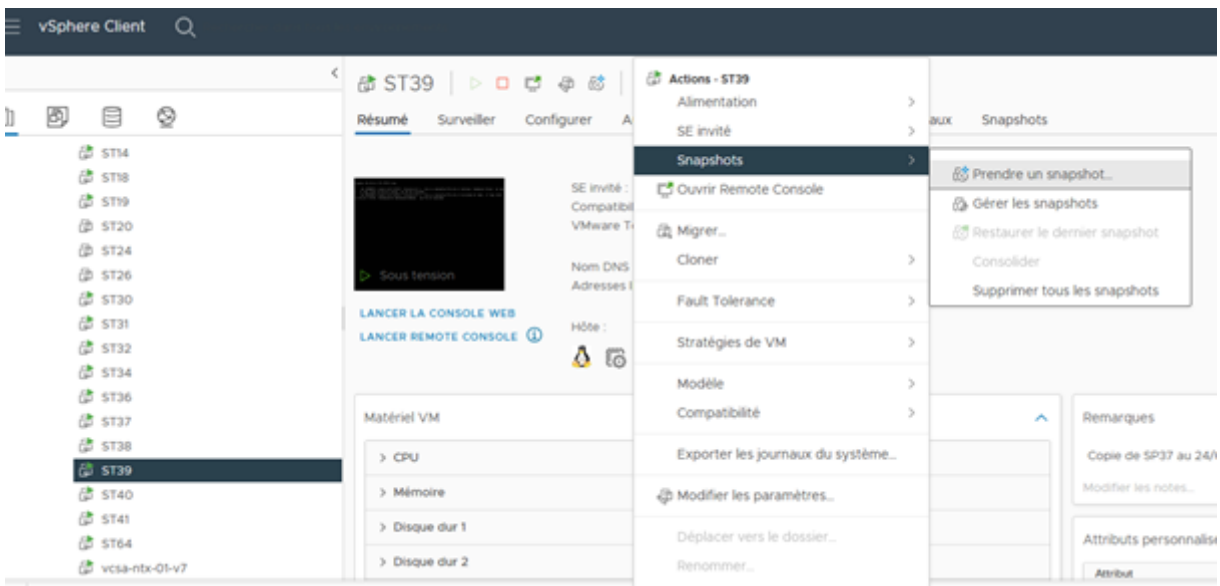
SNAPSHOT

Il est **IMPORTANT** de toujours faire une snapshot avant de commencer la mise à jour du serveur.

Se rendre sur le serveur visé sur vSphere : [Vsphere](#)

Dans section Inventaire, aller dans Vincennes -> MEDIATHEQUE puis rechercher le serveur.

Cliquer sur **ACTION** >> *Snapshots* >> *prendre un snapshot* >> créer



Prendre un snapshot

Nom Snapshot de VM 17/09/2025 14:17:54

Description

Inclure la mémoire de la machine virtuelle

Mettre au repos le système de fichiers invité (nécessite les outils VM)

Par précaution, il est conseillé de s'assurer que la snapshot a bien été prise.

ST39 | | ACTIONS

Résumé Surveiller Configurer Autorisations Banques de données Réseaux **Snapshots**

Snapshot de VM 17/09/2025 14:17:54

Vous êtes ici

LINUX

Update and upgrade

Se connecter à la VM

Puis faire la commande `apt update && apt upgrade -y` (update et upgrade du Linux)

```
Last login: Wed Sep 17 11:52:00 2025 from 10.200.5.27
root@ST39:~# apt update && apt upgrade -y
```

Quand la maj se termine, redémarrer le serveur avec la commande `reboot`

```
Found linux image: /boot/vmlinuz-5.4.0-208-generic
Found initrd image: /boot/initrd.img-5.4.0-208-generic
done
Traitement des actions différées (« triggers ») pour initramfs-tools (0.136ubuntu6.8) ...
update-initramfs: Generating /boot/initrd.img-5.4.0-216-generic
root@ST39:~# reboot
```

Processus de mise à jour

Après redémarrage, faire un do-release-upgrade pour débiter le processus de l'upgrade de la version.

```
Lecture du cache
Vérification du gestionnaire de paquets
Continuer dans une session SSH ?

Cette session semble tourner à travers SSH. Il n'est actuellement pas
recommandé de faire une mise à niveau à travers SSH car en cas
d'échec, il est plus difficile d'effectuer une réparation.

Si vous continuez, un nouveau service SSH va être lancé sur le port «
1022 ».
Voulez-vous continuer ?

_Continuer [oN] █
```

Faire o (oui) pour continuer

```
Lecture du cache
Vérification du gestionnaire de paquets
Continuer dans une session SSH ?

Cette session semble tourner à travers SSH. Il n'est actuellement pas
recommandé de faire une mise à niveau à travers SSH car en cas
d'échec, il est plus difficile d'effectuer une réparation.

Si vous continuez, un nouveau service SSH va être lancé sur le port «
1022 ».
Voulez-vous continuer ?

_Continuer [oN] █
```

Appuyer entrer continuer mise à jour

```
Lecture du cache

Vérification du gestionnaire de paquets

Continuer dans une session SSH ?

Cette session semble tourner à travers SSH. Il n'est actuellement pas
recommandé de faire une mise à niveau à travers SSH car en cas
d'échec, il est plus difficile d'effectuer une réparation.

Si vous continuez, un nouveau service SSH va être lancé sur le port «
1022 ».
Voulez-vous continuer ?

_Continuer [oN] █
```

Entrée une nouvelle fois

```
Lecture du cache

Vérification du gestionnaire de paquets

Continuer dans une session SSH ?

Cette session semble tourner à travers SSH. Il n'est actuellement pas
recommandé de faire une mise à niveau à travers SSH car en cas
d'échec, il est plus difficile d'effectuer une réparation.

Si vous continuez, un nouveau service SSH va être lancé sur le port «
1022 ».
Voulez-vous continuer ?

_Continuer [oN] █
```

Continuer avec o (oui)

NOTE :

Des pop-ups apparaitront à certains moments en fonction des applications présente dans celle-ci, par précaution, les laisser par défaut.

Exemple :

Dire NON en cas de perte de configuration :

```
Configuring libseccomp

There are services installed on your system which need to be restarted when certain
libraries, such as libseccomp, libseccomp, and libseccomp, are upgraded. Since these
restarts may cause interruptions of service for the system, you will normally be
prompted on each upgrade for the list of services you wish to restart. You can
choose this option to avoid being prompted; instead, all necessary restarts will be
done for you automatically so you can avoid being asked questions on each library
upgrade.

Restart services during package upgrades without asking?
<Tab>  Yes
```

```
Running services and programs that are using NSS need to be restarted, otherwise they might not be able to do lookup or authentication any more (for services such as ssh, this can affect your ability to login). Please review the following space-separated list of last-d scripts for services to be restarted now, and correct it if needed.

Note: restarting sshd/teletsd should not affect any existing connections.

Services to restart for GNU libc library upgrade:

Need libnsl0
```

```
Configuration de openssh-server

Une nouvelle version (/tmp/tmp.lEwLQbCyVM) du fichier de configuration /etc/ssh/sshd_config est disponible mais la version actuellement utilisée a été modifiée localement.

Action souhaitée pour le fichier de configuration modifié sshd_config :

    Installer la version du responsable du paquet
    Garder la version actuellement installée
    Montrer les différences entre les versions
    Montrer côte à côte les différences entre les versions
    Montrer les différences entre les trois versions du fichier
    Fusionner les différences entre les trois versions du fichier
    Lancer un shell pour examiner la situation

<Ok>
```

```
Fichier de configuration « /etc/snmp/snmpd.conf »
==> Modifié (par vous ou par un script) depuis l'installation.
==> Le distributeur du paquet a fourni une version mise à jour.
Que voulez-vous faire ? Vos options sont les suivantes :
  Y ou I : installer la version du responsable du paquet
  N ou O : garder votre version actuellement installée
  D      : afficher les différences entre les versions
  Z      : suspendre ce processus pour examiner la situation
L'action par défaut garde votre version actuelle.
*** snmpd.conf (Y/I/N/O/D/Z) [défaut=N] ?
```

Laisser les fichiers de configuration par **DEFAUT (N)** si demandé

```
Recherche de logiciels obsolètes
Lecture des informations d'état... Done

Supprimer les paquets obsolètes ?

36 paquets vont être supprimés.

Continuer [oN] Détails [d]
```

OPTIONNEL mais supprimer les données inutiles, Continuer avec o.

```
La mise à niveau du système est terminée.

Redémarrage nécessaire de l'ordinateur

Un redémarrage est nécessaire pour terminer la mise à niveau.
Si vous choisissez « o », le système sera redémarré.

Continuer [oN]
```

Redémarrage nécessaire, oui (o)

VERIFICATION

Regarder si la version s'est bien appliqué avec la commande lsb_release - a

```
root@ST39:~# lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 22.04.5 LTS
Release:        22.04
Codename:       jammy
root@ST39:~#
```


Mise à jour terminé, faire ensuite la même chose sur les prochains serveurs à mettre à jour.

Procédure retour arriere radius


Problème avec radius


En cas de dysfonctionnement lié au serveur radius, il sera peut-être nécessaire de rebasculer en arrière la configuration actuellement en place.


Exemple de configuration sur le port 1 du switch :


GSM-AC-1E-03 

MS130-48P bc:33:40:b7:90:2c

 Port not forwarding traffic due to access policy.

 Port not forwarding traffic due to access policy.

 Port not forwarding traffic due to access policy.



École J. Bonnet
Square Robert de Cotte
Crèche Multi Accueil Du Domaine Du Bois

ADDRESS
19 avenue Murs du Parc 94300 Vincennes

LAN IP
172.26.6.138 (statically assigned)

VLAN
106

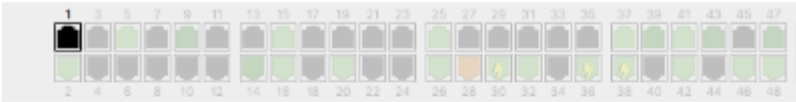
PUBLIC IP
159.180.242.30

GATEWAY
172.26.6.254

DNS
8.8.8.8
8.8.4.4


Summary Ports


Port 1: Lan Ecole [Return to port list](#)



Historical data for the last month ▾

Port traffic




Configuration 

Port status	Enabled
Type	Access
VLAN	1
Voice VLAN	224
Access policy	RADIUS Ecoles
Link negotiation	Auto negotiate
RSTP	Enabled
Port schedule	Unscheduled
Port Isolation	Disabled
Trusted DAI	Disabled

Update 1 port

Switch / Port	GSM-AC-1E-03 / 1
Name	<input type="text" value="Lan Ecole"/>
Port status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Link negotiation	<input type="text" value="Auto negotiate"/>
Port schedule	<input type="text" value="Unscheduled"/>
Tags	<input type="text" value="+"/> <input type="text"/>
Port profile name	<input type="text"/>
Type	<input type="radio"/> Trunk <input checked="" type="radio"/> Access

Access policy 	<input type="text" value="RADIUS Ecoles"/>
VLAN	<input type="text" value="1"/>
Voice VLAN	<input type="text" value="224"/>

Modifier l'entrée « Access Policy » et la mettre sur « Open »

Modifier l'entrée VLAN et mettre l'ID du vlan ecole (210) ou VLAN DATA (216)

Valider