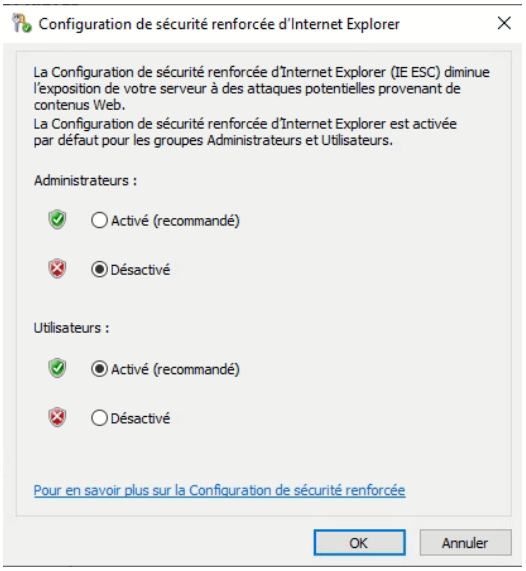
PARAMÉTRAGE DE WINDOWS SERVEUR

#1 - UTILISATION D'INTERNET EXPLORER / INSTALLATION DE EDGE -

Pour sécuriser le serveur « **la configuration de sécurité renforcée d'Internet Explorer** » est « **Actif** ».

Désactiver la configuration de sécurité renforcée d'Internet Explorer » que pour les administrateurs pour utiliser normalement le navigateur Internet.

Antivirus Windows Defender	Protection en temps réel : activée
Commentaires et diagnostics	Paramètres
Configuration de sécurité renforcée d'Internet Explorer	Inactif
Fuseau horaire	(UTC+01:00) Bruxelles, Copenhague, Madrid, Paris
ID de produit (Product ID)	Non activé



Installer le navigateur **EDGE**

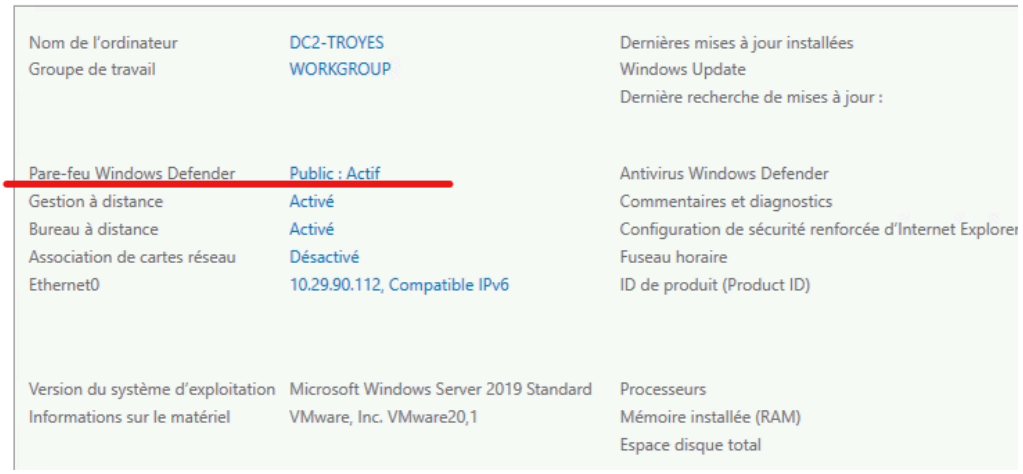
#3 – COMMUNICATION ENTRE LE CLIENT ET LE SERVEUR

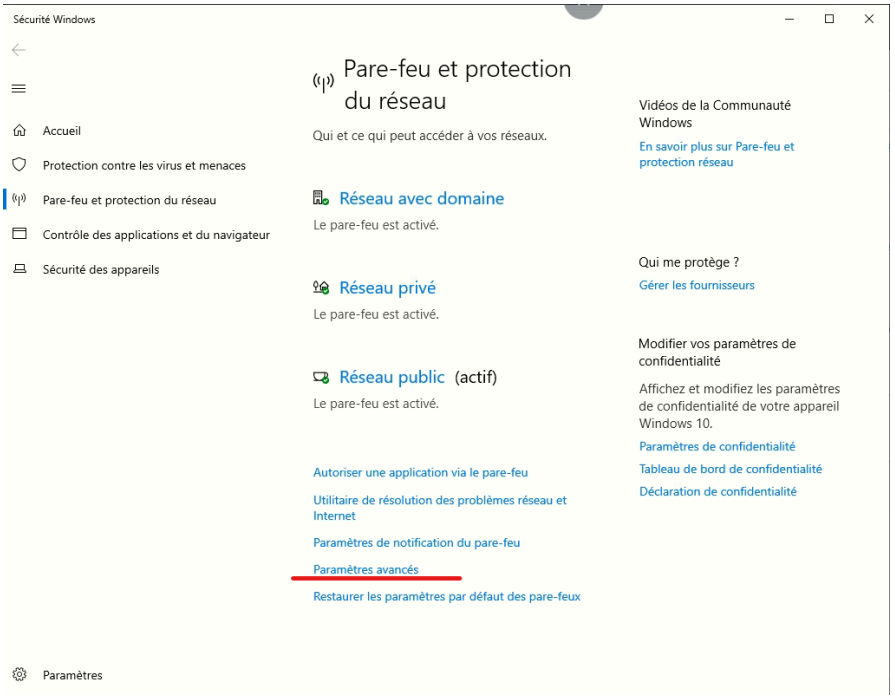
```
C:\Users\admin1>ping 10.29.90.112

Envoi d'une requête 'Ping'  10.29.90.112 avec 32 octets de données :
Réponse de 10.29.90.112 : octets=32 temps<1ms TTL=128
Réponse de 10.29.90.112 : octets=32 temps<1ms TTL=128
Réponse de 10.29.90.112 : octets=32 temps<1ms TTL=128
Réponse de 10.29.90.112 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 10.29.90.112:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

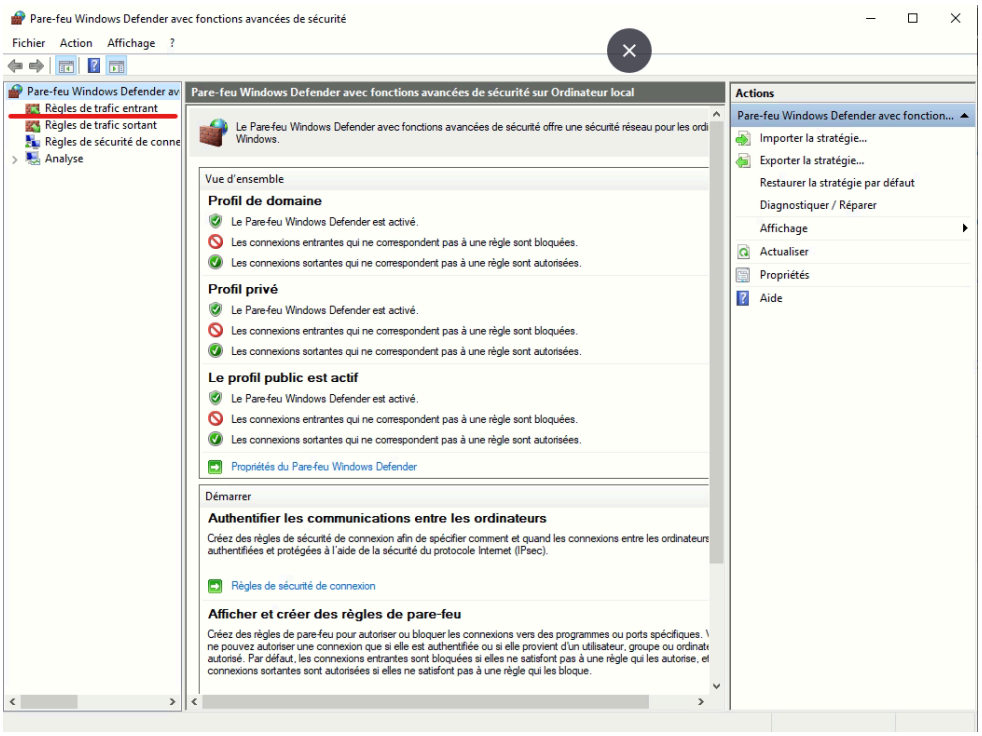
Le ping depuis le client windows 11.

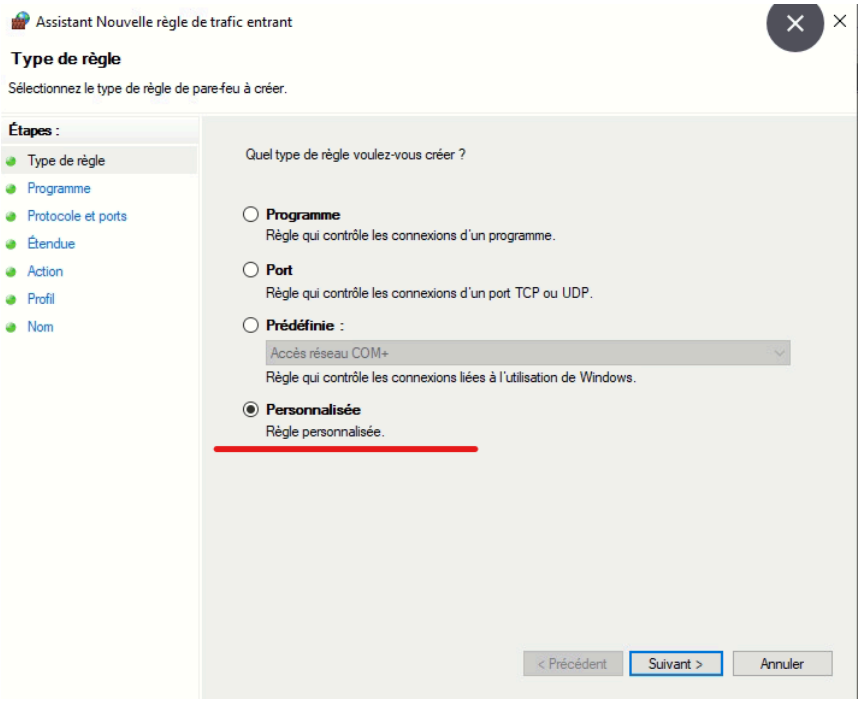
```
C:\Users\Administrateur>ping 10.29.90.99

Envoi d'une requête 'Ping'  10.29.90.99 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 10.29.90.99:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),

C:\Users\Administrateur>
```

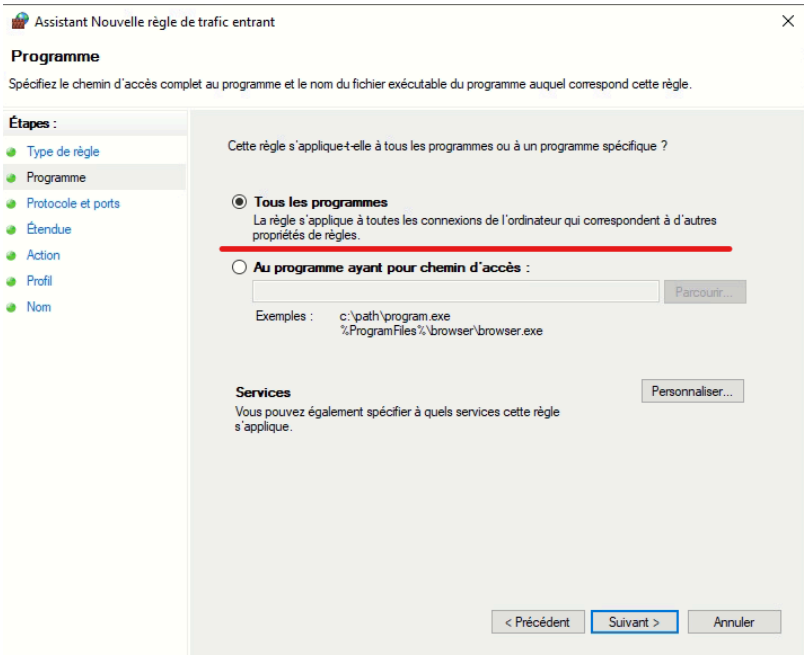
Le ping ne s'effectue pas du serveur vers le client.

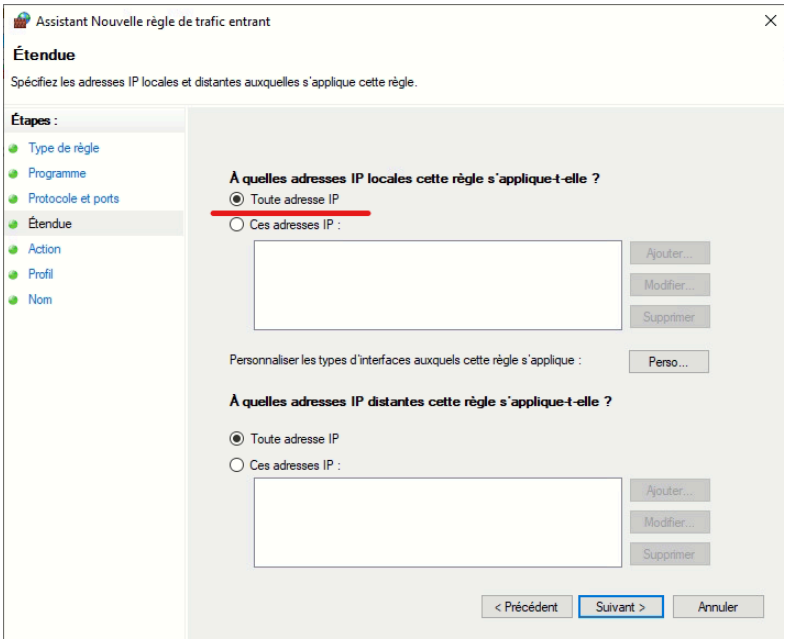


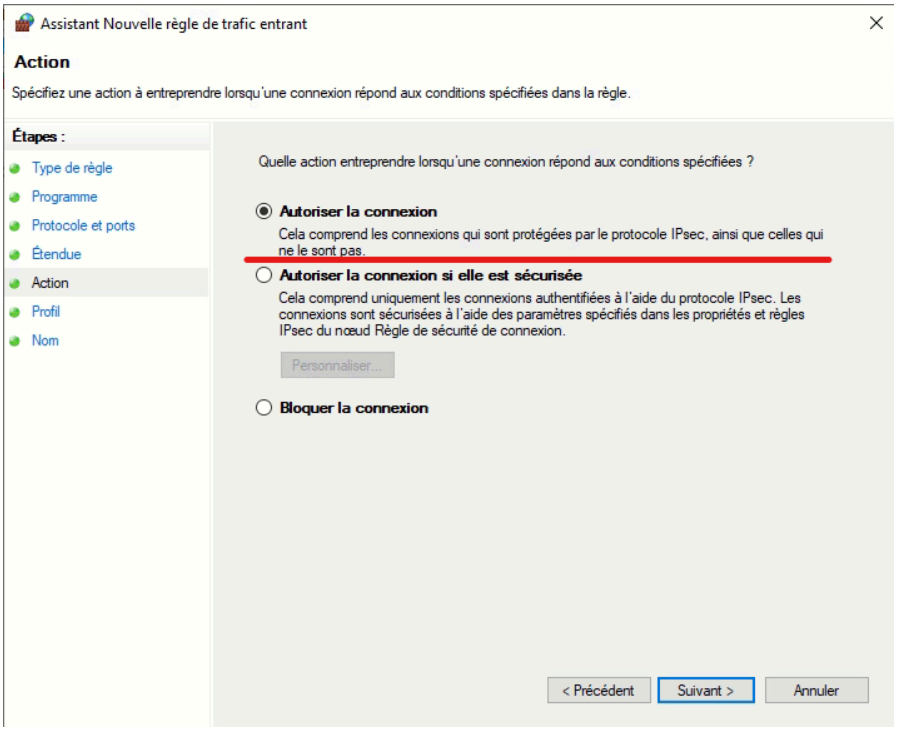

Sécurité Windows
Pare-feu et protection du réseau
Qui et ce qui peut accéder à vos réseaux.
Accueil
Protection contre les virus et menaces
Pare-feu et protection du réseau
Contrôle des applications et du navigateur
Sécurité des appareils
Paramètres
Réseau avec domaine
Le pare-feu est activé.
Réseau privé
Le pare-feu est activé.
Réseau public (actif)
Le pare-feu est activé.
Autoriser une application via le pare-feu
Utilitaire de résolution des problèmes réseau et Internet
Paramètres de notification du pare-feu
Paramètres avancés
Restaurer les paramètres par défaut des pare-feux
Vidéos de la Communauté Windows
En savoir plus sur Pare-feu et protection réseau
Qui me protège ?
Gérer les fournisseurs
Modifier vos paramètres de confidentialité
Affichez et modifiez les paramètres de confidentialité de votre appareil Windows 10.
Paramètres de confidentialité
Tableau de bord de confidentialité
Déclaration de confidentialité

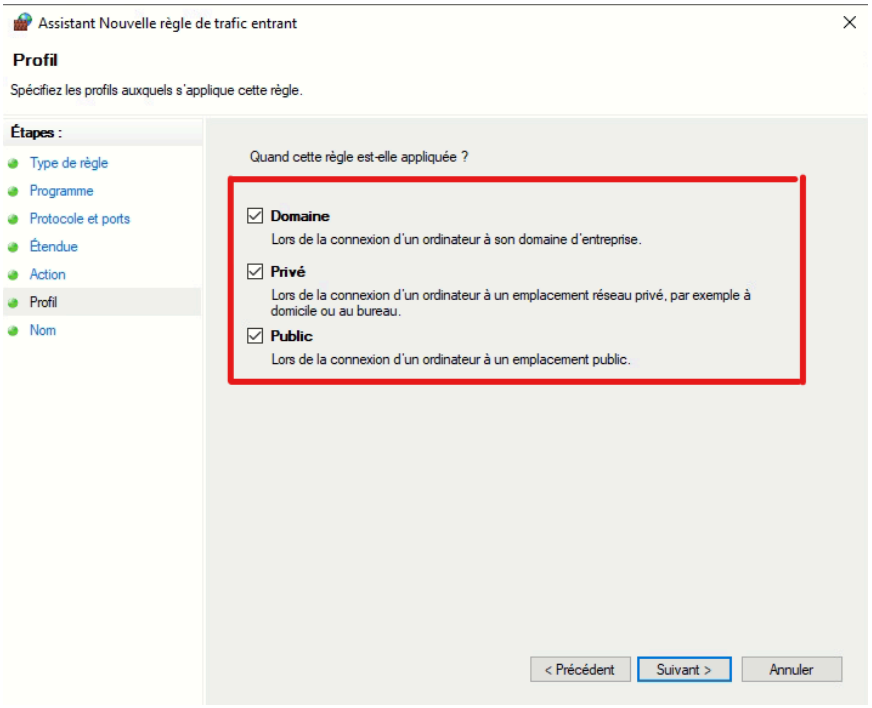

Pare-feu Windows Defender avec fonctions avancées de sécurité
Fichier Action Affichage ?
Pare-feu Windows Defender av
Règles de trafic entrant
Règles de trafic sortant
Règles de sécurité de conne
Analyse
Pare-feu Windows Defender avec fonctions avancées de sécurité sur Ordinateur local
Vue d'ensemble
Profil de domaine
Le Pare-feu Windows Defender est activé.
Les connexions entrantes qui ne correspondent pas à une règle sont bloquées.
Les connexions sortantes qui ne correspondent pas à une règle sont autorisées.
Profil privé
Le Pare-feu Windows Defender est activé.
Les connexions entrantes qui ne correspondent pas à une règle sont bloquées.
Les connexions sortantes qui ne correspondent pas à une règle sont autorisées.
Le profil public est actif
Le Pare-feu Windows Defender est activé.
Les connexions entrantes qui ne correspondent pas à une règle sont bloquées.
Les connexions sortantes qui ne correspondent pas à une règle sont autorisées.
Propriétés du Pare-feu Windows Defender
Démarrer
Authentifier les communications entre les ordinateurs
Règles de sécurité de connexion
Afficher et créer des règles de pare-feu
Actions
Pare-feu Windows Defender avec fonction...
Importer la stratégie...
Exporter la stratégie...
Restaurer la stratégie par défaut
Diagnostiquer / Réparer
Affichage
Actualiser
Propriétés
Aide

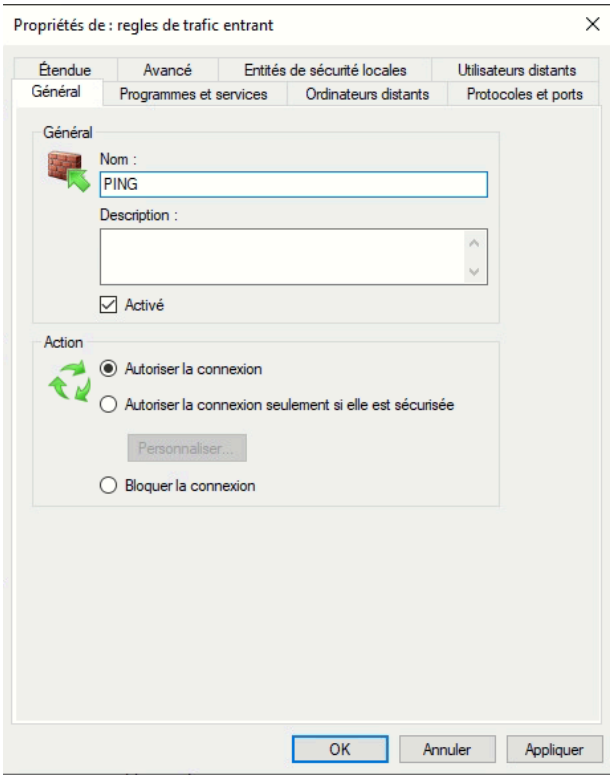

Assistant Nouvelle règle de trafic entrant
Type de règle
Sélectionnez le type de règle de pare-feu à créer.
Étapes :
Type de règle
Programme
Protocole et ports
Étendue
Action
Profil
Nom
Quel type de règle voulez-vous créer ?
Programme
Règle qui contrôle les connexions d'un programme.
Port
Règle qui contrôle les connexions d'un port TCP ou UDP.
Prédéfinie :
Accès réseau COM+
Règle qui contrôle les connexions liées à l'utilisation de Windows.
Personnalisée
Règle personnalisée.
< Précédent
Suivant >
Annuler


Assistant Nouvelle règle de trafic entrant
Programme
Spécifiez le chemin d'accès complet au programme et le nom du fichier exécutable du programme auquel correspond cette règle.
Étapes :
Type de règle
Programme
Protocole et ports
Étendue
Action
Profil
Nom
Cette règle s'applique-t-elle à tous les programmes ou à un programme spécifique ?
Tous les programmes
La règle s'applique à toutes les connexions de l'ordinateur qui correspondent à d'autres propriétés de règles.
Au programme ayant pour chemin d'accès :
Parcourir...
Exemples : c:\path\program.exe
%ProgramFiles%\browser\browser.exe
Services
Personnaliser...
Vous pouvez également spécifier à quels services cette règle s'applique.
< Précédent
Suivant >
Annuler


Assistant Nouvelle règle de trafic entrant
Étendue
Spécifiez les adresses IP locales et distantes auxquelles s'applique cette règle.
Étapes :
Type de règle
Programme
Protocole et ports
Étendue
Action
Profil
Nom
À quelles adresses IP locales cette règle s'applique-t-elle ?
Toute adresse IP
Ces adresses IP :
Ajouter...
Modifier...
Supprimer
Personnaliser les types d'interfaces auxquels cette règle s'applique :
Perso...
À quelles adresses IP distantes cette règle s'applique-t-elle ?
Toute adresse IP
Ces adresses IP :
Ajouter...
Modifier...
Supprimer
< Précédent
Suivant >
Annuler


Assistant Nouvelle règle de trafic entrant
Action
Spécifiez une action à entreprendre lorsqu'une connexion répond aux conditions spécifiées dans la règle.
Étapes :
Type de règle
Programme
Protocole et ports
Étendue
Action
Profil
Nom
Quelle action entreprendre lorsqu'une connexion répond aux conditions spécifiées ?
Autoriser la connexion
Cela comprend les connexions qui sont protégées par le protocole IPsec, ainsi que celles qui ne le sont pas.
Autoriser la connexion si elle est sécurisée
Cela comprend uniquement les connexions authentifiées à l'aide du protocole IPsec. Les connexions sont sécurisées à l'aide des paramètres spécifiés dans les propriétés et règles IPsec du nœud Règle de sécurité de connexion.
Personnaliser...
Bloquer la connexion
< Précédent
Suivant >
Annuler

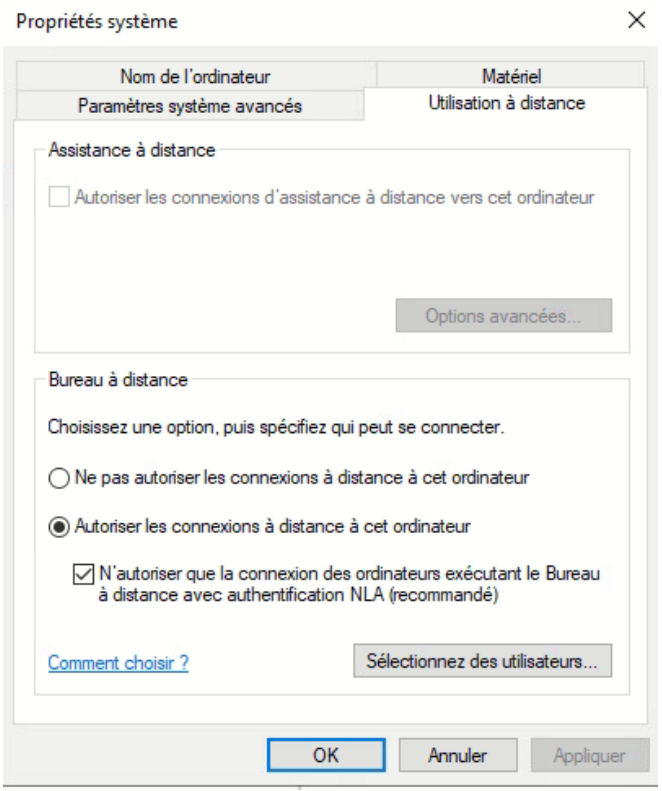

Assistant Nouvelle règle de trafic entrant
Profil
Spécifiez les profils auxquels s'applique cette règle.
Étapes :
Type de règle
Programme
Protocole et ports
Étendue
Action
Profil
Nom
Quand cette règle est-elle appliquée ?
Domaine
Lors de la connexion d'un ordinateur à son domaine d'entreprise.
Privé
Lors de la connexion d'un ordinateur à un emplacement réseau privé, par exemple à domicile ou au bureau.
Public
Lors de la connexion d'un ordinateur à un emplacement public.
< Précédent
Suivant >
Annuler

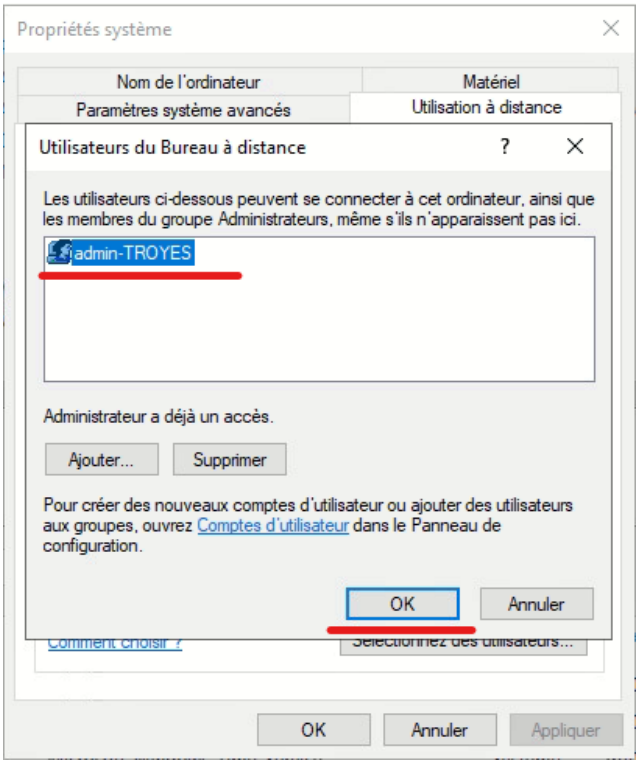

Propriétés de : regles de trafic entrant
Étendue
Avancé
Entités de sécurité locales
Utilisateurs distants
Général
Programmes et services
Ordinateurs distants
Protocoles et ports
Général
Nom :
PING
Description :
Activé
Action
Autoriser la connexion
Autoriser la connexion seulement si elle est sécurisée
Personnaliser...
Bloquer la connexion
OK
Annuler
Appliquer

```
C:\Users\admin1>ping 10.29.90.112

Envoi d'une requête 'Ping'  10.29.90.112 avec 32 octets de données :
Réponse de 10.29.90.112 : octets=32 temps<1ms TTL=128
Réponse de 10.29.90.112 : octets=32 temps<1ms TTL=128
Réponse de 10.29.90.112 : octets=32 temps<1ms TTL=128
Réponse de 10.29.90.112 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 10.29.90.112:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Le ping vers le serveur fonctionne bien.

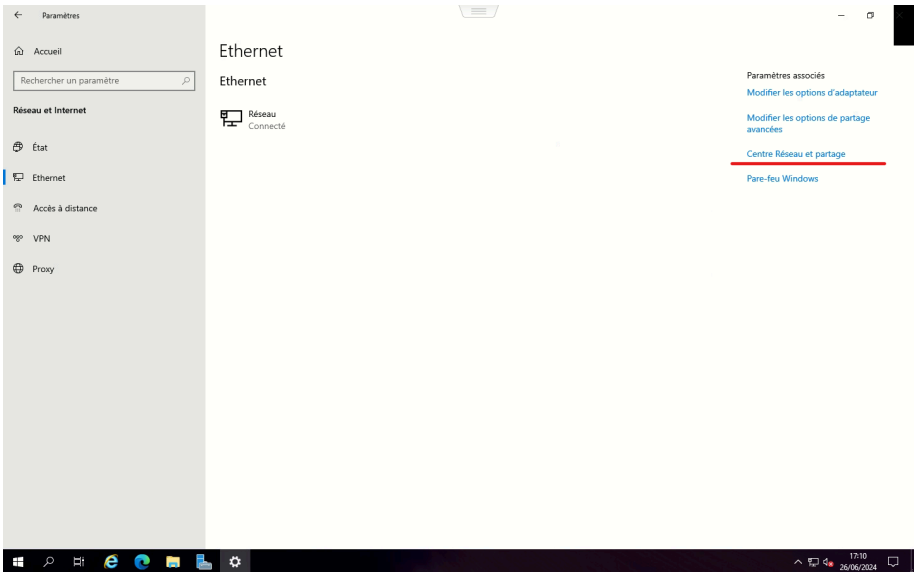
#4 - Connexion bureau à distance -

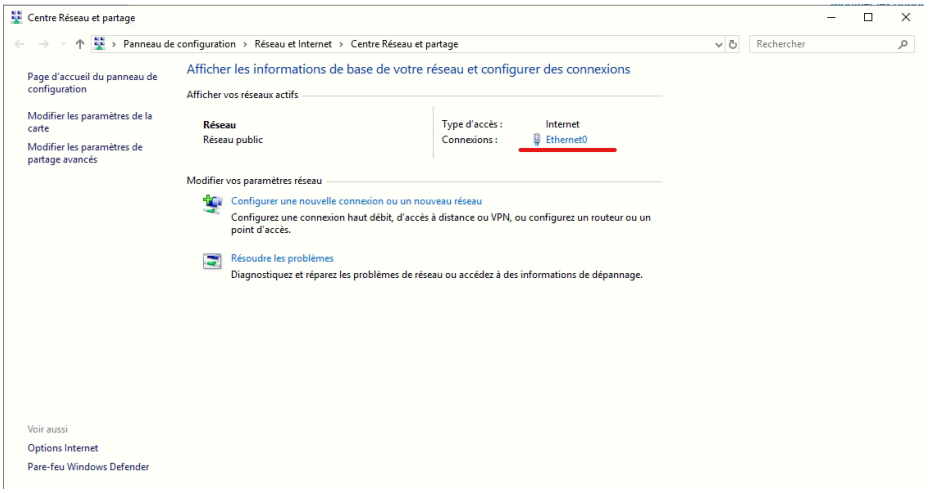


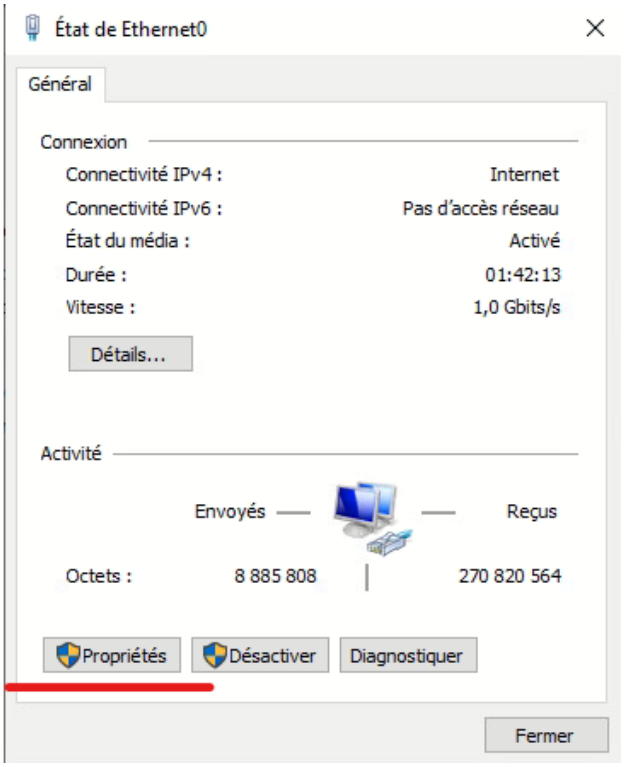


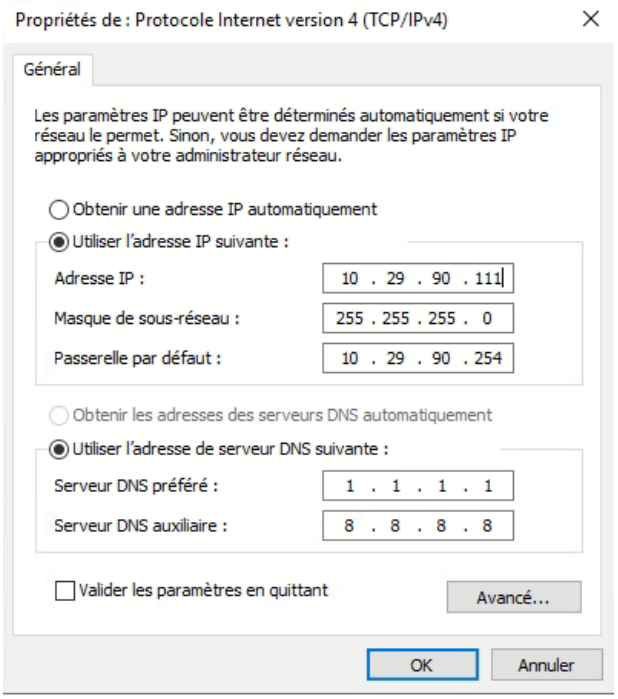
#5 - Changement des propriétés TCP/IP du Serveur Windows -

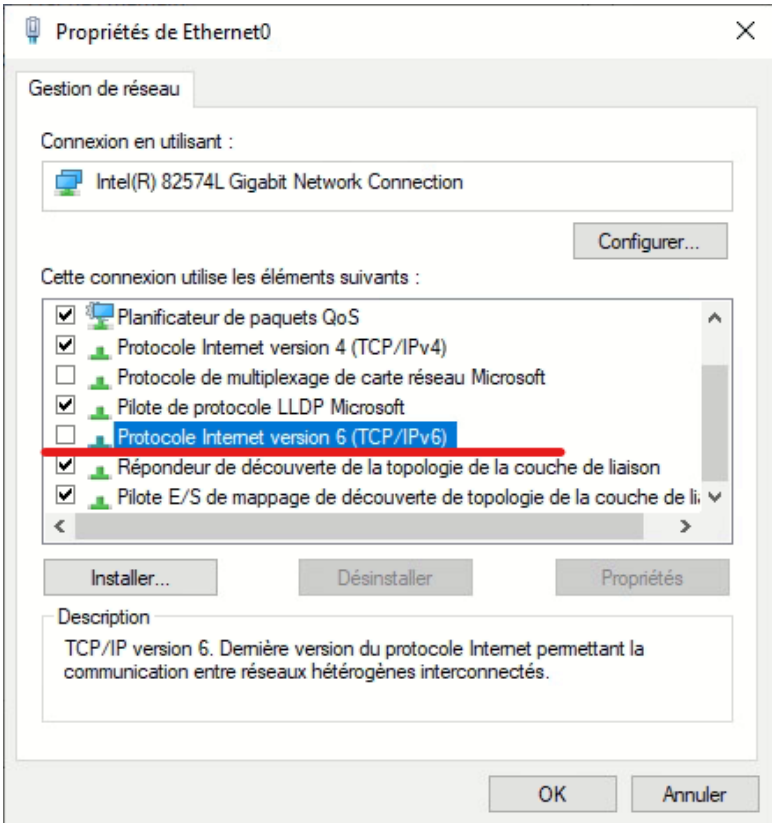
Configurer les propriétés TCP/IPv4 conformément aux instructions fournies.
Désactiver Protocole Internet version 6(TCP/IPv6)





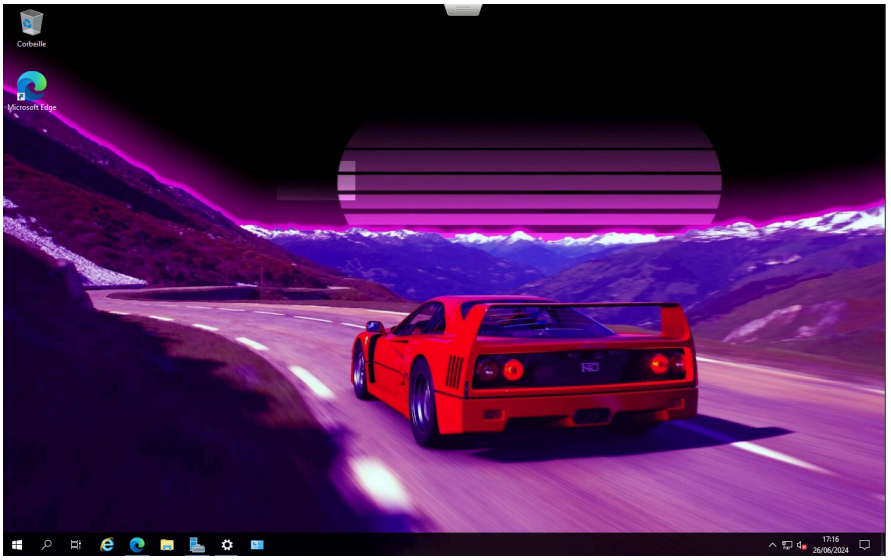

État de Ethernet0
Général
Connexion
Connectivité IPv4 : Internet
Connectivité IPv6 : Pas d'accès réseau
État du média : Activé
Durée : 01:42:13
Vitesse : 1,0 Gbits/s
Détails...
Activité
Envoyés
Reçus
Octets : 8 885 808 270 820 564
Propriétés
Désactiver
Diagnostiquer
Fermer


Propriétés de : Protocole Internet version 4 (TCP/IPv4)
Général
Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.
Obtenir une adresse IP automatiquement
Utiliser l'adresse IP suivante :
Adresse IP : 10 . 29 . 90 . 111
Masque de sous-réseau : 255 . 255 . 255 . 0
Passerelle par défaut : 10 . 29 . 90 . 254
Obtenir les adresses des serveurs DNS automatiquement
Utiliser l'adresse de serveur DNS suivante :
Serveur DNS préféré : 1 . 1 . 1 . 1
Serveur DNS auxiliaire : 8 . 8 . 8 . 8
Valider les paramètres en quittant
Avancé...
OK
Annuler



#6 – Fond d'écran -

Changer le fond d'écran de votre serveur



#7 – Installation BGInfo -

Télécharger et installer le logiciel « Bginfo »

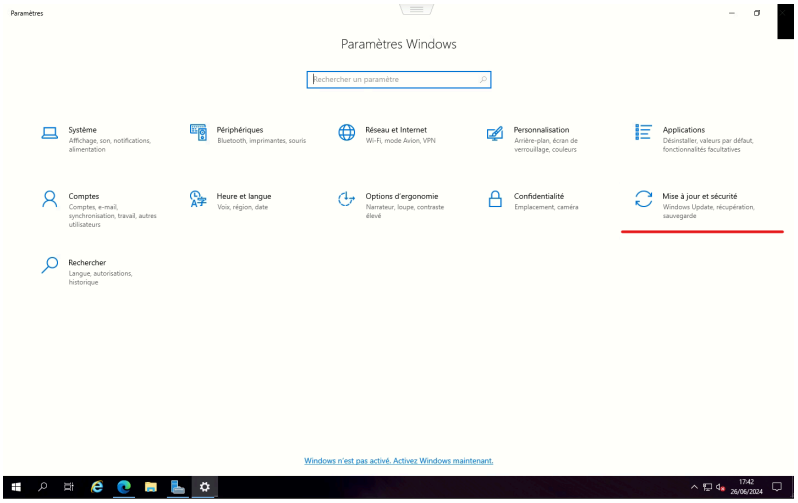
Paramétrer Bginfo pour afficher :

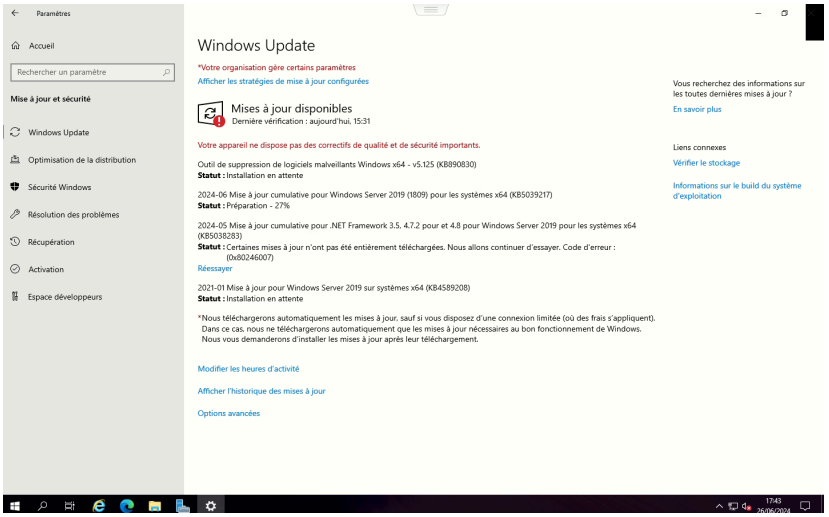
- Date et heure
- Nom du serveur :
- Adresse IP :
- Espace Disque Libre
- Domaine
- Système d'exploitation
- Nom d'utilisateur

Renommé les différents champs comme sur la liste ci-dessus.

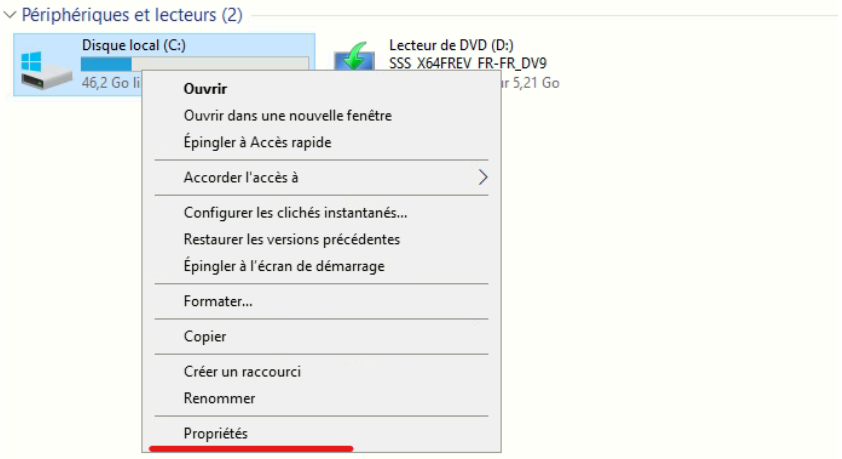
Placer les informations en bas à droite

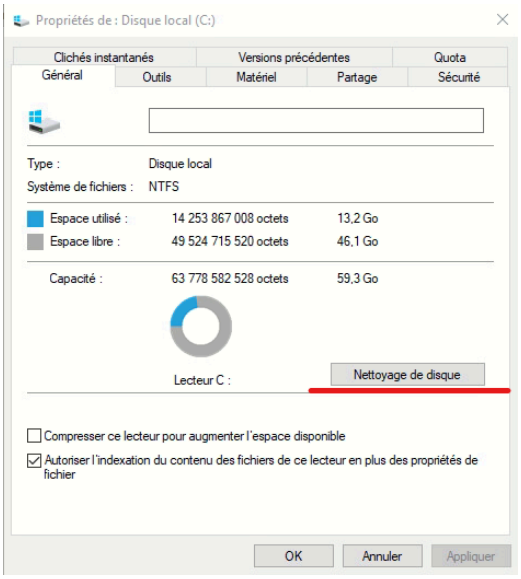
#8 - INSTALLATION DES MISES À JOURS -





#9 - Effectuer le nettoyage de disque





#10 - QUESTIONS -

1. Quelle est la **commande PowerShell** qui permet d'ouvrir la fenêtre de « **Connexions réseau** »

La commande PowerShell pour ouvrir la fenêtre de « Connexions réseau » est `Start-Process ncpa.cpl`.

2. A quoi servent les **VMware Tools**

Les VMware Tools améliorent les performances et la gestion des machines virtuelles en offrant des pilotes optimisés et des fonctionnalités supplémentaires.

3. Quels sont les serveur DNS **127.0.0.1** et **1.1.1.1** et quel est le serveur DNS de **Google**

127.0.0.1 est l'adresse de loopback locale, souvent utilisée pour tester et résoudre les problèmes DNS sur la machine elle-même.
1.1.1.1 est un serveur DNS public fourni par Cloudflare, connu pour sa rapidité et sa confidentialité.
8.8.8.8 est un serveur DNS public de Google, également largement utilisé pour sa fiabilité et sa rapidité.

4. Pourquoi doit-on faire un **nettoyage de disque après l'installation des mises à jour**

-Libérer de l'espace : Supprimer les fichiers temporaires et de mise à jour qui ne sont plus nécessaires.
-Améliorer les performances : Éviter que le disque dur soit encombré, ce qui peut ralentir le système.
-Réduire les conflits : Éliminer les anciens fichiers qui pourraient causer des problèmes avec les nouvelles mises à jour.

5. Pourquoi doit-on mettre une **IP fixe aux Serveurs**

On met une IP fixe aux serveurs pour garantir leur accessibilité et leur fiabilité sur le réseau.