Sécuriser un minimum un ordinateur Windows

Désactivation de NETBIOS sur les serveurs Windows 1

Activer l'authentification au niveau du réseau (NLA) 1

Activer l'authentification au niveau du réseau (NLA) via les GPO 2

Désactiver la découverte automatique de proxy - Windows 10 3

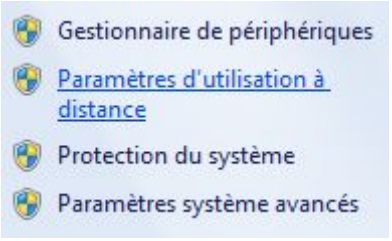
Désactiver le protocole LLMNR sous Windows 4

Désactivation de NETBIOS sur les serveurs Windows

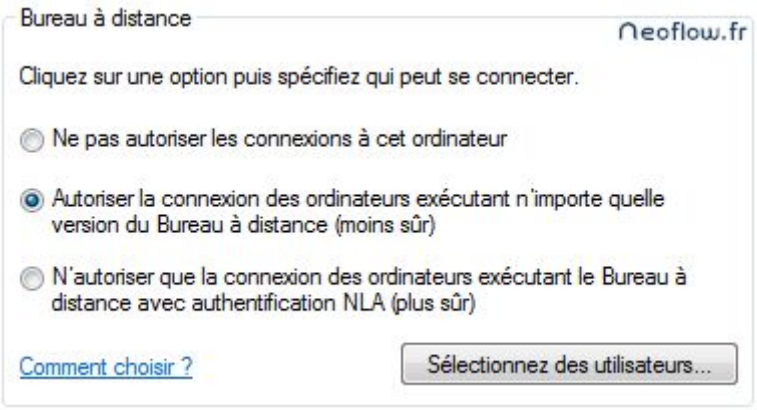
1. Sélectionnez **Panneau de configuration** > **Réseau et Internet** > **Centre Réseau et partage**.
2. Cliquez sur **Modifier les paramètres de la carte**.
3. Cliquez avec le bouton droit de la souris sur **Connexion au réseau local** puis cliquez sur **Propriétés**.
4. Sélectionnez **Protocole Internet version 4 (TCP/IPv4)**, cliquez sur **Propriétés** puis sur **Avancé**.
5. Cliquez sur l'onglet WINS et, dans la section Paramètre NetBIOS, cliquez sur **Désactiver NetBIOS avec TCP/IP**. Cliquez sur **OK** pour fermer la fenêtre des propriétés.
6. Sélectionnez **Outils d'administration** > **Services**, cliquez avec le bouton droit de la souris sur **Assistance TCP/IP NetBIOS** puis cliquez sur **Arrêter**.
7. Cliquez avec le bouton droit de la souris sur **Assistance TCP/IP NetBIOS**, cliquez sur **Propriétés** et, dans la liste Type de démarrage, sélectionnez **Désactivé**. Cliquez sur **OK**.
8. Fermez les fenêtres de propriétés réseau restantes.

Activer l'authentification au niveau du réseau (NLA)

Démarrer, Clic droit sur **Ordinateur** ou **Poste de travail**, **Propriétés**, **Paramètres d'utilisation à distance**

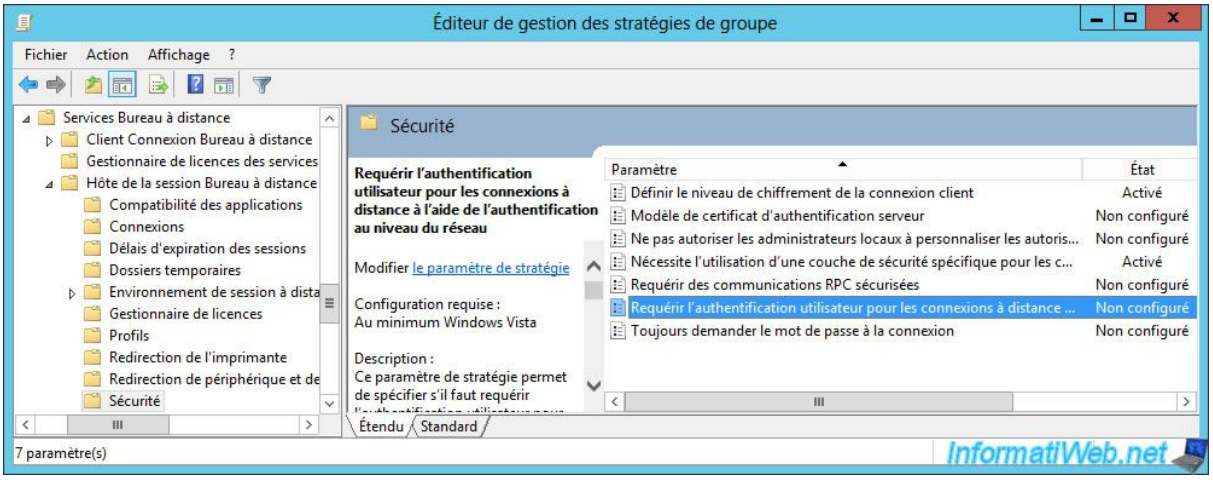


Sélectionner “ N’autoriser que la connexion des ordinateurs exécutant le Bureau à distance avec authentification NLA (plus sûr)

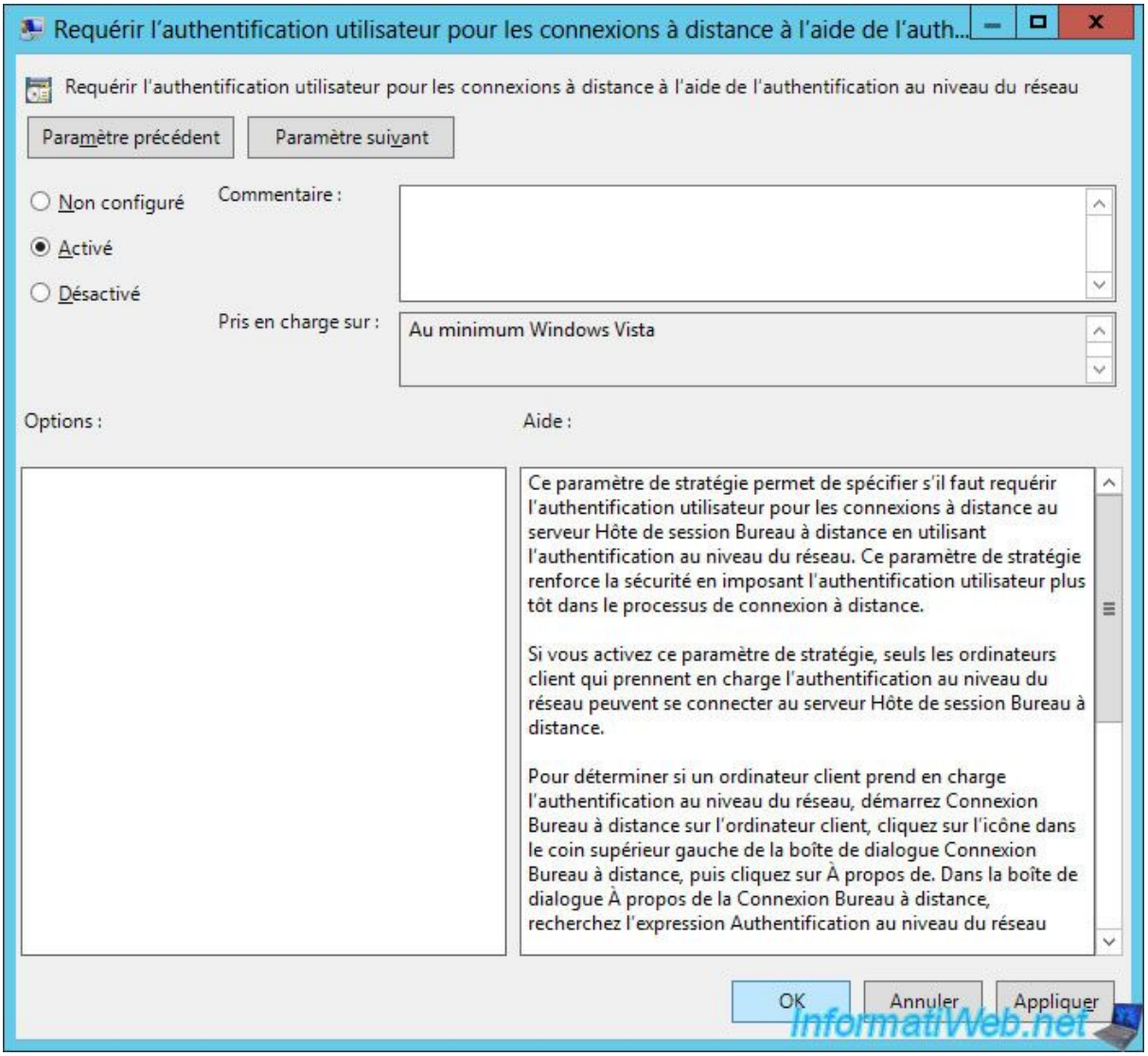


Activer l'authentification au niveau du réseau (NLA) via les GPO

Pour activer l'authentification au niveau du réseau (NLA) via les stratégies de groupe, vous devez activer la stratégie : Requérir l'authentification utilisateur pour les connexions à distance à l'aide de l'authentification au niveau du réseau.
Cette stratégie est disponible dans : Configuration ordinateur -> Stratégies -> Modèles d'administration -> Composants Windows -> Services Bureau à distance -> Hôte de la session Bureau à distance -> Sécurité.



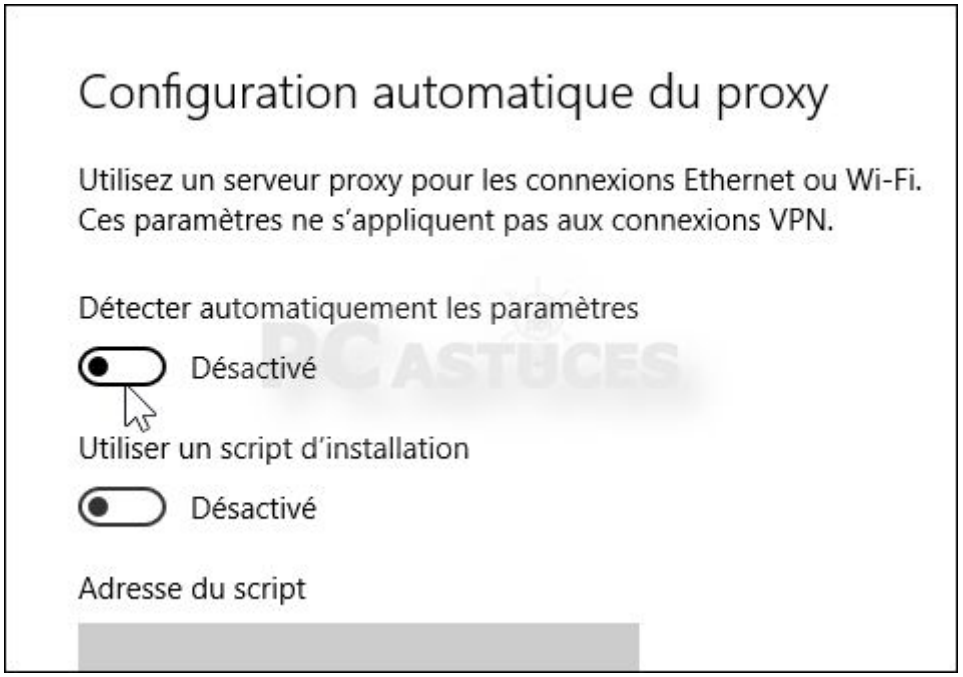
Activez la stratégie, puis quittez l'éditeur de stratégies de groupe et forcez la mise à jour de la stratégie de vos serveurs hôtes de sessions.



Désactiver la découverte automatique de proxy - Windows 10

Cliquez sur le bouton Démarrer puis sur **Paramètres** > **Réseau et Internet** > colonne de gauche **“Proxy”**

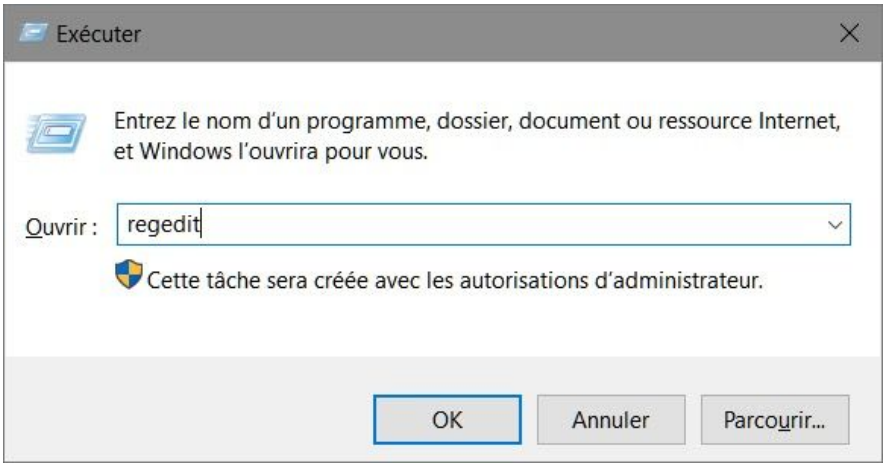
Désactivez alors l'option **Détecter automatiquement les paramètres.**



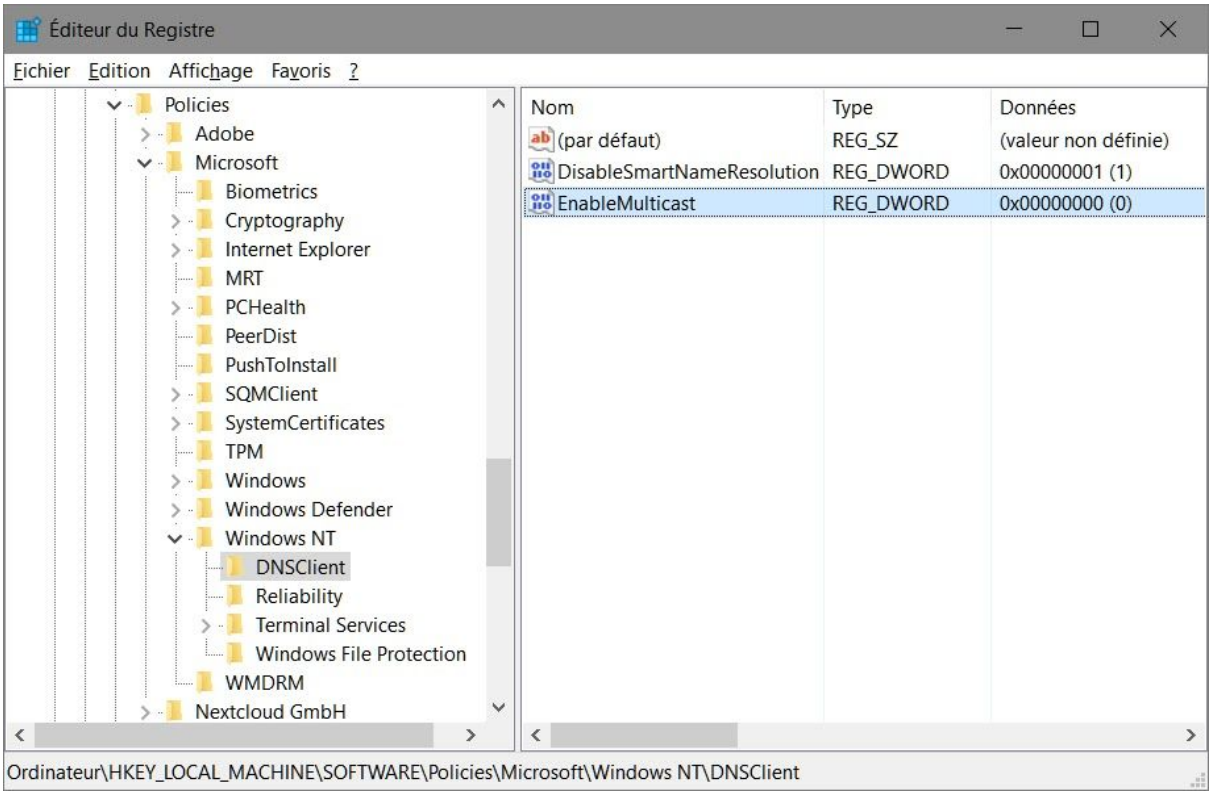
Désactiver le protocole LLMNR sous Windows

Le protocole LLMNR (Local Link Multicast Name Resolution) assure la résolution de noms, en absence de résolution DNS, dans le cas où les machines du réseau local n'ont pas été enregistrés dans un serveur DNS manuellement ou bien au travers d'un serveur DHCP. Ce protocole est excessivement verbeux. Il convient, dans le cadre du fonctionnement normal d'un réseau local, de le désactiver sur toutes les machines Windows. Il écoute sur le port Udp/5355. Il est d'ailleurs utilisé par les FAI pour détecter les machines présentes sur votre réseau local : ordinateurs, tablettes et téléphones mobiles.

Lancer la commande regedit, à partir de menu Démarrer (Windows+R).



Si elle n'existe pas, créez la clé HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient, et affectez la valeur 0 au paramètre EnableMulticast (DWORD 32 bits) .



L'autre solution est d'utiliser la console gpedit.msc : Configuration ordinateur -> Modèles d'administration -> Réseau -> Client DNS -> Désactiver la résolution de noms multidiffusion.