# Installation du serveur ESET Endpoint Antivirus

Installation

## Base

1. Créez une zone DNS "antivirus.domaine.ch" sans mises à jour dynamique avec un hôte pointant sur le serveur ESET Endpoint en interne et créez cette entrée sur le DNS externe avec l'IP publique
2. Ouvrez les ports 2221 et 2222 sur le firewall et faire un NAT sur ce serveur
3. Ouvrez les ports 2221 et 2222 en TCP/UDP sur le firewall de Windows pour tous les profiles avec pour nom "ESET Endpoint Remote Server TCP" et "ESET NOD32 Remote Server UDP"
4. Ouvrez les ports 2223 et 2224 en TCP/UDP sur le firewall de Windows pour tous les profiles avec pour nom "ESET Endpoint Remote Installer TCP" et "ESET NOD32 Remote Installer UDP"
5. Installez le rôle IIS avec l'authentification basique et les outils d'administration
6. Téléchargez sur le site de ESET (<http://www.eset.com/>) les paquets suivants :
   1. ESET Remote Administrator Server
   2. ESET Remote Administrator Console
   3. ESET Endpoint Antivirus 4 32bits + 64bits
7. Exécutez l'installation de "ESET Remote Administrator Server"
   1. Laissez la sélection de tous les composants
   2. Choisissez le mode avancé
   3. Choisissez la licence principale
   4. Laissez "Local System Account"
   5. Choisissez le nom du serveur "antivirus.domaine.ch"
   6. Définissez les mots de passe :
      1. Password for Console (Administrator Access) -> ESET NOD32 Console Password
      2. Password for Console (Read-Only Access) -> ESET NOD32 Console Password
      3. Remote installer password (Agent) -> ESET NOD32 Remote Installer
      4. Password for Clients (ESET Security Products) -> ESET NOD32 Client/Server Communication
      5. Password for Replication -> Rien
   7. Ne pas utiliser de serveurs SMTP
   8. Choisissez le port "44301" pour le protocole HTTPS
8. Exécutez l'installation de "ESET Remote Administrator Console"
   1. Choisissez le mode avancé
   2. Utilisez le nom du serveur localhost
9. Ouvrez la console NOD32
   1. Allez dans "Remote Install" puis "Manage Packages"
      1. Créez un paquet "ESET Endpoint Antivirus English" et "ESET Endpoint Antivirus French"
         1. Ajoutez les paquets 32bits et 64bits
         2. Récupérez le fichier modèle XML "DefaultStrategies.xml"
         3. Passez en revue tous les éléments préconfigurés, notamment :
            1. Modifiez les liens sur le serveur antivirus.domaine.ch et introduisez le mot de passe "ESET NOD32 Client/Server Communication"
            2. Introduisez le mot de passe de protection du setup "ESET NOD32 Client Configuration"
            3. Modifiez le serveur de mise à jour antivirus.domaine.ch ainsi que le mot de passe du compte AD "antivirusupdate"
            4. Modifiez l'utilisateur et le mot de passe pour les mises à jour chez ESET
      2. Cliquez sur "Export to Folder or Logon Script" et exporter les configurations pour les installations via le VPN ainsi que les installations manuelles
   2. Allez dans "Server Options"
      1. Désactivez l'accès sans authentification pour les clients
      2. Choisissez "Create update mirror", ne pas choisir de serveur http
      3. Cliquez sur "Update Now"

*Créez des comptes ordinateurs dans l'AD dans les OU "Computers" si elles sont vides afin que les OU soient synchronisées avec la console ESET. Ensuite les objets doivent être détruits.*

* 1. Allez dans "Group Manager", "Active Directory Synchronization"
     1. Synchronize groups : All Groups
     2. Synchronization type : AD Groups Import
     3. Synchonisez automatiquement toutes les 4 heures
     4. Lancez la synchronization
  2. Supprimez les OU qui ne sont plus nécessaires dans la console ESET (ne garder que Computers et Servers)
  3. Allez dans "Group Manager", "Active Directory Synchronization"
     1. Synchronize groups : Only Groups Containing ERA Server Clients
     2. Synchronization type : AD Groups Import
  4. Allez dans "Policy Manager"
     1. Sous "Default Parent Policy", cliquez sur "Add New Child Policy"
        1. Policy name : DefaultStrategies
        2. Copy policy configuration from .xml file : Choisissez la stratégie crée avec le paquet de déploiement automatique
     2. Dans "Policy Rules", cliquez sur "New"
        1. Name : DefaultStrategies
        2. Rule 1 : FROM Primary Server
        3. Rule 2 : ERA Groups IN : Choisissez l'OU des ordinateurs dans l'AD
        4. Policy : DefaultStrategies (Antivirus.domaine.ch)

1. Créez un nouveau site web dans IIS
   1. Site name : ESET Endpoint Mirror
   2. Physical path : C:\Documents and Settings\All Users\Application Data\ESET\ESET Remote Administrator\Server\Mirror
   3. Type : http, port 2221
   4. Dans "MIME Types", ajoutez le type "application/octet-stream" pour l'extension "\*"
   5. Désactivez l'authentification anonyme et activez l'authentification basique en spécifiant le domaine "domaine.local"
   6. Créez un utilisateur "antivirusupdate" et ajoutez le droit de lecture sur le site web crée (garder l'héritage)
2. Déployez via la console les anti-virus sur les serveurs (sauf DC qui doit être déployé via einstaller.exe)
3. Créez les GPO suivantes selon les rapports enregistrés :
   1. Computers - NOD32 deployment \*copiez le fichier einstaller.exe crée précédemment

*Vous pouvez pousser les installations via la console, par GPO ou avec l'exécution d'einstaller.exe depuis le LAN ou le VPN. Ne pas oublier les exclusions sur les serveurs (SQL, BackupExec, WSUS, …). Ne pas Installer ESET Mail Security for Microsoft Exchange Server sur le serveur Exchange car il crée des problèmes avec la carte réseau.*

*Si le paquet doit être redéployé, par ex après une désinstallation manuelle du produit, il faut supprimer les clés de registre suivantes : HKEY\_LM\SOFTWARE\Wow6432Node\ESET et HKEY\_LM\SOFTWARE\ESET.*