MonitorPack solutions

TECK SYSTEM SOFT

Démarrage rapide MonitorPack

1 - Téléchargez la dernière version 2
2 - Créez un compte de service 2
3 - Liez le compte de service au service MonitorPack Windows 3
4 - Data Execution Prevention 4
5 - Activer la supervision des compteurs de Performance 5
6 - Désactiver l'UAC 5
7 - Update GPO to allow MonitorPack Windows machine(s) 9
8 - Groupes locaux pour superviser les compteurs de performance a distance 12
9 - Windows 10 limitation des droits sur les Dossiers 12

Introduction

Ce document est un guide d'installation rapide à destination des administrateurs afin d'implémenter rapidement nos solutions MonitorPack et créer votre première alarme.
L'équipe support reste à la disposition des abonnés par e-mail par téléphone si nécessaire.

Vous avez reçu votre abonnement, vous disposez donc des informations suivantes :

- User Licence.
- Cloud MonitorPack Server.
- URL pour vous connecter à votre Portail Web.
- Un compte de login pour l'accès au portail web MonitorPack.
- Un mot de passe pour le login du portail web MonitorPack.

MonitorPack Solution

Aucun agent à déployer, ce qui réduit les coûts de transition et vous apporte la simplicité attendue.
Pour compléter la configuration, les processus Windows sont nécessaires pour assurer la sécurité.

Cette procédure consiste à autoriser une seule fois et à partir d'une seule machine, les applications MonitorPack pour toute l'entreprise, cela garantit la sécurité de l'ensemble de la forêt Active Directory. Si vous installez MonitorPack Guard sur plusieurs machines (par exemple dans chaque site AD), vous devrez autoriser toutes les IP de ces machines Windows.

1 - Téléchargez la dernière version

MonitorPack Guard

Page de téléchargement ici http://www.monitorpack.fr/start-monitorpack-guard-fr.php

MonitorPack Asset

Page de téléchargement ici http://www.monitorpack.fr/start-monitorpack-asset-fr.php

Sur quels types de machines

MonitorPack Guard peut être installé sur :

- Windows 2000 Workstation toutes versions.
- Windows 2000 Server toutes versions.
- Windows XP Workstation toutes versions.
- Windows Vista Workstation toutes versions.
- Windows Seven Workstation toutes versions.
- Windows 8 Workstation toutes versions.
- Windows 10 Workstation toutes versions.
- Windows 2003 serveur toutes versions.
- Windows 2008 serveur toutes versions.
- Windows 2012 serveur toutes versions.
- Windows 2016 serveur toutes versions.

2 - Créez un compte de service

Dans Active Directory, créez un compte de service dédié pour la surveillance et l'inventaire de votre infrastructure nommé "svc_monitorpack".
Intégrez ce compte « svc_monitorpack » dans le groupe «Administrateurs» de votre forêt Active Directory.

Comment

Dans la MMC Utilisateurs et ordinateurs Active Directory (dsa.msc), de cette manière le compte de service pourra être désactivé facilement et par cette seule opération.

Quand

Une seule fois si vous êtes dans une forêt Active Directory, sur chaque machine à superviser sui vous êtes en Workgroup.

3 - Liez le compte de service au service MonitorPack Windows

Pourquoi

Le service Windows « MonitorPack Engine » est utilisé par l'application MonitorPack Guard afin d'exécuter des requêtes de mesures auprès d'ordinateurs locaux ou distants depuis une machine MonitorPack Guard, le service fonctionne donc sans aucune session en cours nécessaire.

Comment

1. Sur la machine MonitorPack, exécutez services.msc
2. Dans l'onglet droit, cliquez deux fois sur le service "MonitorPack Engine"
3. Sélectionnez l'onglet Connexion.
4. Cliquez sur le bouton Parcourir et sélectionnez le compte "svc_monitorpack" qui possède les droits d'administrateur sur tous les serveurs et postes de travail que vous allez surveiller.
5. Démarrez les services Windows pour MonitorPack "MonitorPack Engine" et "MonitorPack Control". Lorsque vous installez MonitorPack Guard, les services Windows ne démarrent pas par défaut lors de l'installation.

4 - Data Execution Prevention

Quoi

Depuis Windows Server 2003 SP1, Data Exécution Prévention (DEP) est une fonctionnalité de sécurité qui aide à prévenir les dommages causés par les virus et autres menaces de sécurité en surveillant vos programmes afin de s'assurer qu'ils utilisent la mémoire système en toute sécurité. Il bloque également les produits non Microsoft qui s'exécute sur la machine.

Pourquoi

Pour permettre aux exécutables MonitorPack de s'exécuter localement.

Quand

Lorsque vous installez pour la première fois MonitorPack Guard ou MonitorPack Asset sur une machine Windows.

Ou

Sur la machine Windows où MonitorPack Guard & MonitorPack Asset vont être installés.

Comment

1. Sélectionnez Démarrer > Panneau de configuration.
2. Cliquez sur Sécurité du système.
3. Cliquez sur Advanced System Settings (Paramètres système avancés). La boîte de dialogue Propriétés système s'affiche.
4. Cliquez sur l'onglet "Avancé".
5. Cliquez sur le bouton Paramètres. La boîte de dialogue Options de performance s'affiche.
6. Cliquez sur l'onglet Prévention de l'exécution des données.

Ajoutez ces exécutables à la liste des exceptions:

Pour MonitorPack Guard :

- MonitorPackGuard.exe

- MonitorPackEngine.exe
- MonitorPackControl.exe

Pour MonitorPack Asset :
- MonitorPackAsset.exe

Remarque : Si votre matériel ne prend pas en charge DEP, il se peut que vous ne disposiez pas de cet onglet dans la boîte de dialogue Options de performance. Vous pouvez annuler la procédure maintenant et poursuivre les instructions d'installation.
7. Assurez-vous que le bouton Activer le DEP pour les programmes et services essentiels de Windows est sélectionné.
8. Cliquez deux fois sur OK.

5 - Activer la supervision des compteurs de Performance

Selon le TechNet, le service Windows du Registre à distance doit être en cours d'exécution et son type de démarrage doit être défini sur Automatique pour toutes les machines distantes que vous souhaitez.

6 - Désactiver l'UAC

Quoi

UAC empêche certains outils d'administration utilisant WMI d'être exécutés par un programme de contrôle à distance (comme MonitorPack Guard) parce que les informations d'identification ne sont pas visibles par l'utilisateur distant.

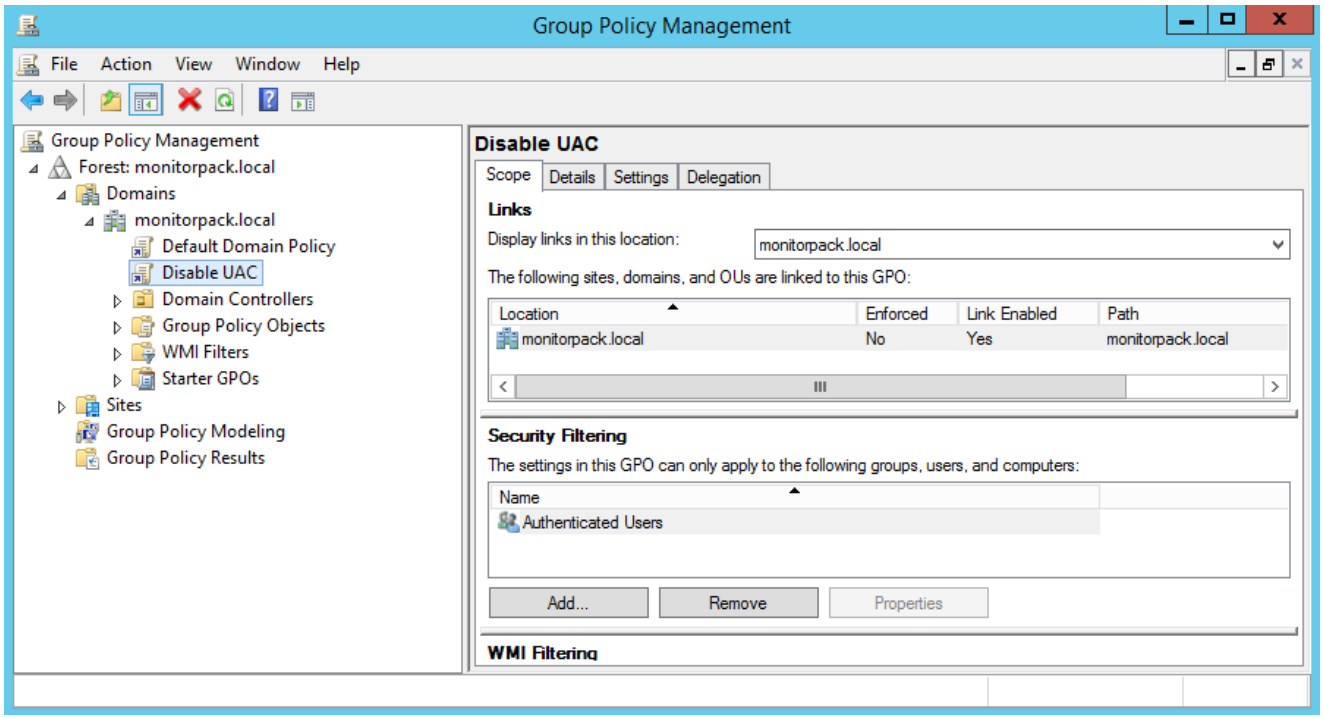
Quand

Lorsque vous installez pour la première fois MonitorPack Guard ou MonitorPack Asset sur dans un foret Active Directory.

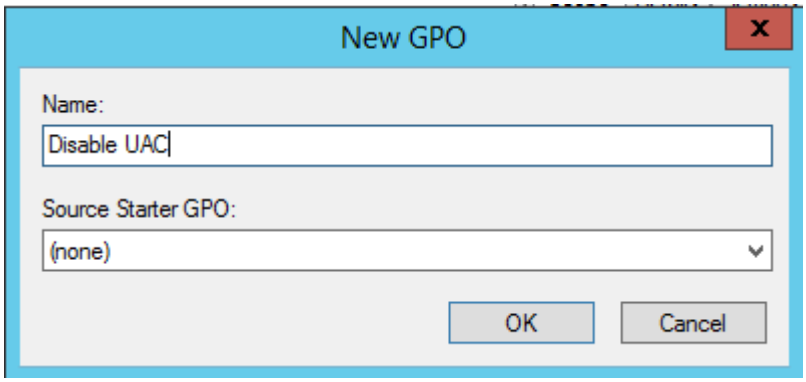
Note : Vous pouvez également décidez de ne désactiver l'UAC que sur les machines que vous allez superviser.

Comment

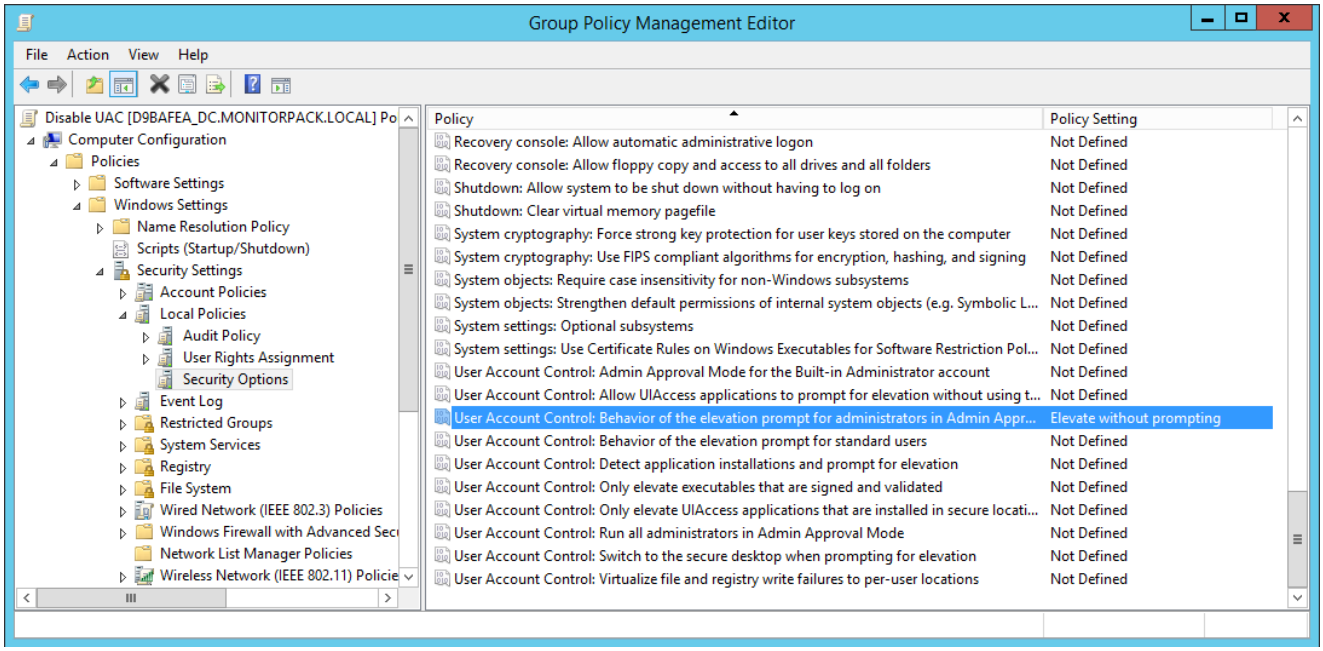
1. Connectez-vous au contrôleur de domaine.
2. Ouvrez la console de gestion des stratégies de groupe en tapant gpmc.msc dans la zone de recherche ou en cliquant sur Outils d'administration > Gestion des stratégies de groupe. (Ignorez le fait que nous avons déjà une GPO pour cela dans la capture d'écran ci-dessous, exécutez simplement cette liste de contrôle pour la créer).



3. Développez Forest > Domain > Domain_Name dans la navigation de gauche pour obtenir une liste des GPO existants. Cliquez avec le bouton droit sur le nom de domaine et sélectionnez Créer un objet de stratégie de groupe dans ce domaine et liez-le ici ... Nommez le GPO "Désactiver UAC" et cliquez sur OK.

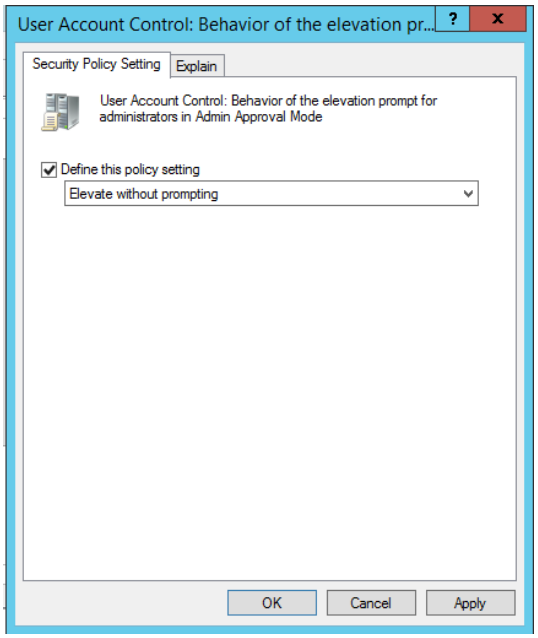


4. Le nouvel objet de stratégie de groupe s'affiche dans la liste. Faites un clic droit dessus et sélectionnez Editez ... Développer Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité

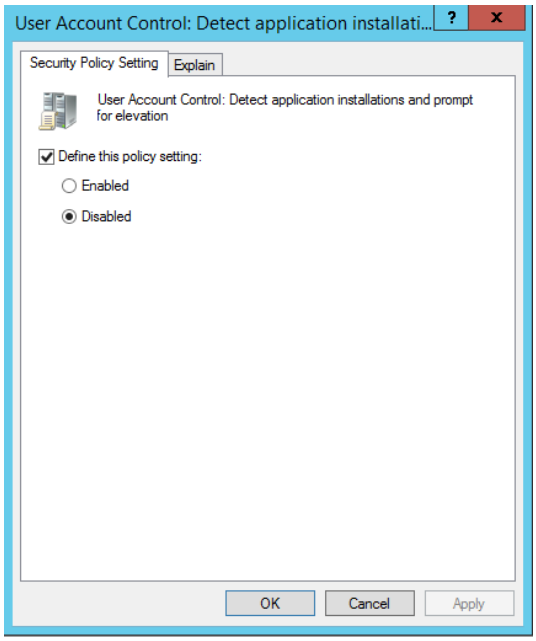


5. Configurez les stratégies suivantes:

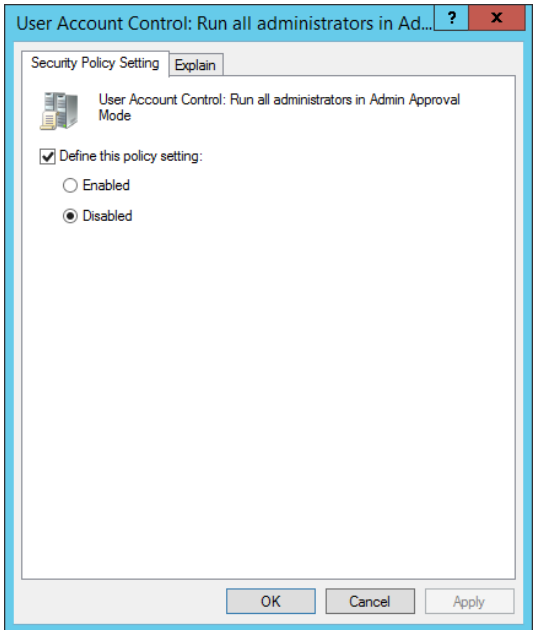
- Contrôle de compte d'utilisateur > comportement de l'invite d'élévation pour les administrateurs en mode d'approbation administrateur : Élévation sans invite.



- Contrôle de compte d'utilisateur > détecter les installations d'application et demander l'élévation: désactivé



- Contrôle de compte d'utilisateur > Exécuter tous les administrateurs en mode d'approbation Admin: Désactivé



Détails de la configuration

User Account Control: Admin Approval Mode for the Built-in Administrator account	Not Defined
User Account Control: Allow UIAccess applications to prompt for elevation without using t...	Not Defined
User Account Control: Behavior of the elevation prompt for administrators in Admin Appr...	Elevate without prompting
User Account Control: Behavior of the elevation prompt for standard users	Not Defined
User Account Control: Detect application installations and prompt for elevation	Disabled
User Account Control: Only elevate executables that are signed and validated	Not Defined
User Account Control: Only elevate UIAccess applications that are installed in secure locati...	Not Defined
User Account Control: Run all administrators in Admin Approval Mode	Disabled
User Account Control: Switch to the secure desktop when prompting for elevation	Not Defined
User Account Control: Virtualize file and registry write failures to per-user locations	Not Defined

6. Exécutez gpudate / force et confirmez que UAC est désactivé.

```
PS C:\Users\Administrator> gpupdate /force
Updating policy...


Computer Policy update has completed successfully.

User Policy update has completed successfully.
```

7 - Update GPO to allow MonitorPack Windows machine(s)

La procédure ci-dessous requiert une connaissance de l'utilisation des utilisateurs, des ordinateurs Active Directory et des outils d'administration de la stratégie de groupe.

Quoi

Les GPO doivent autoriser l'adresse IP de la/des machine(s) MonitorPack où MonitorPack Guard et / ou MonitorPack Asset sont installés) dans la forêt Active Directory.

Pourquoi

La sécurité Microsoft autorise la demande WMI uniquement à partir d'ordinateurs qui sont expressément déclarés avec les droits «Autoriser l'exception d'administration à distance entrante».

Comment

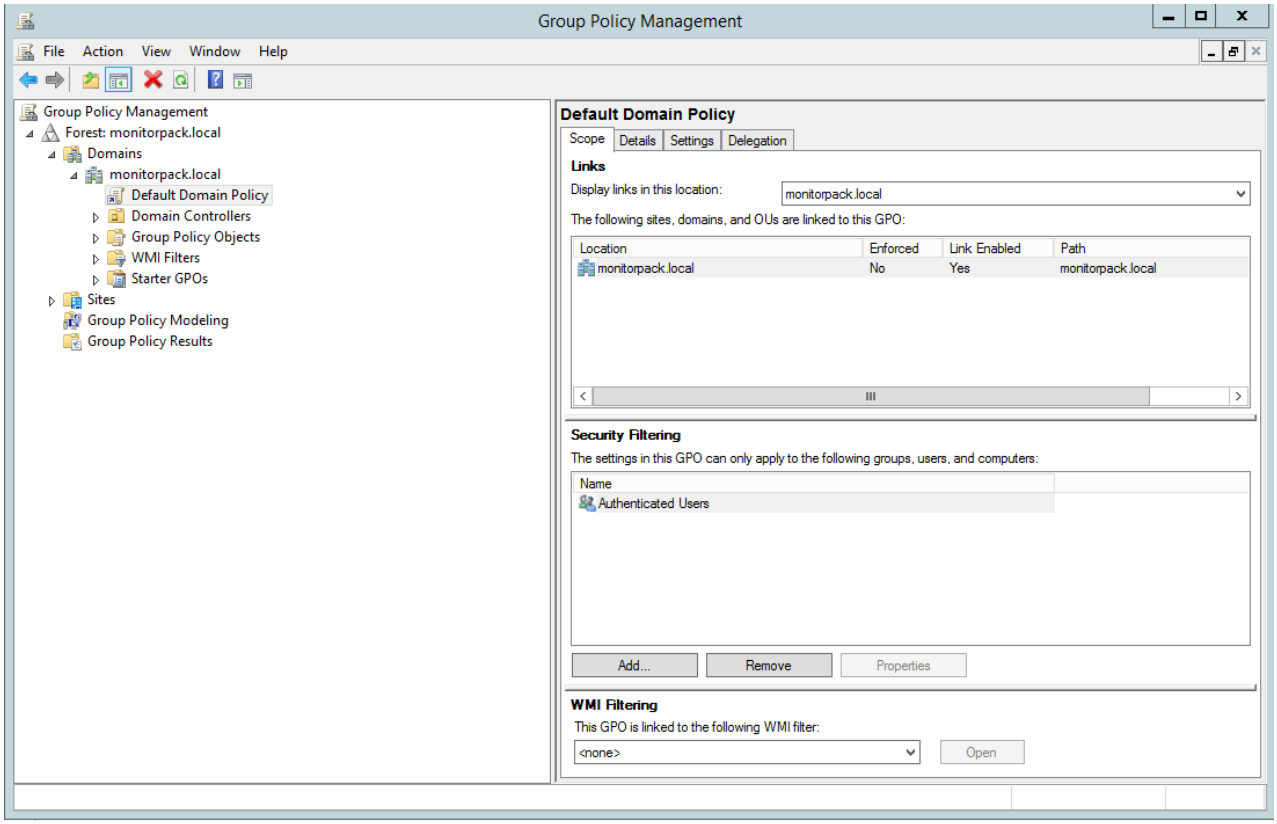
1. Assurez-vous que le compte de service Windows (svc_monitorpack) utilisé sur la machine Windows MonitorPack Guard possède des droits d'administrateur local sur les machines cibles à superviser.

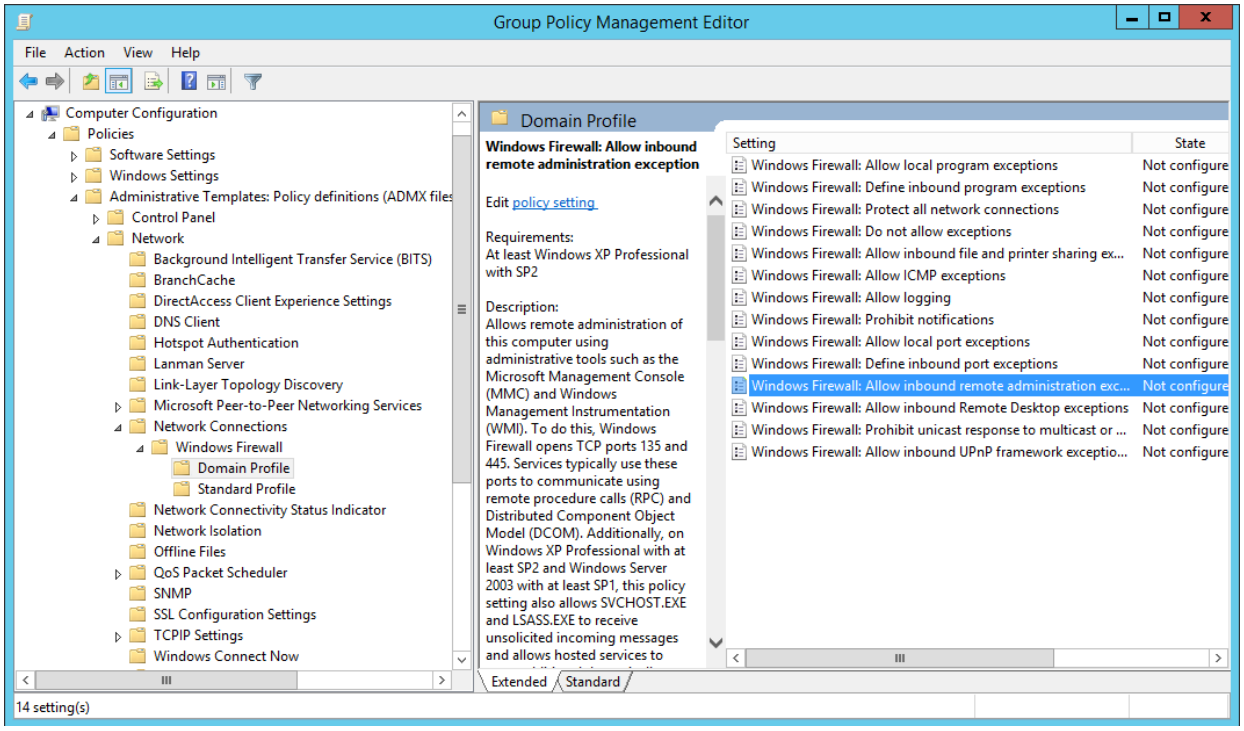
2. Autoriser l'administration à distance sur les ordinateurs cibles comme suit :
Vous pouvez utiliser l'éditeur de stratégie de groupe (Gpedit.msc) pour activer le pare-feu Windows: Avec l'éditeur de stratégie de groupe, utilisez les étapes suivantes dans l'éditeur de stratégie de groupe (Gpedit.msc) pour activer «Autoriser l'administration entrante distante» sur les ordinateurs cibles.

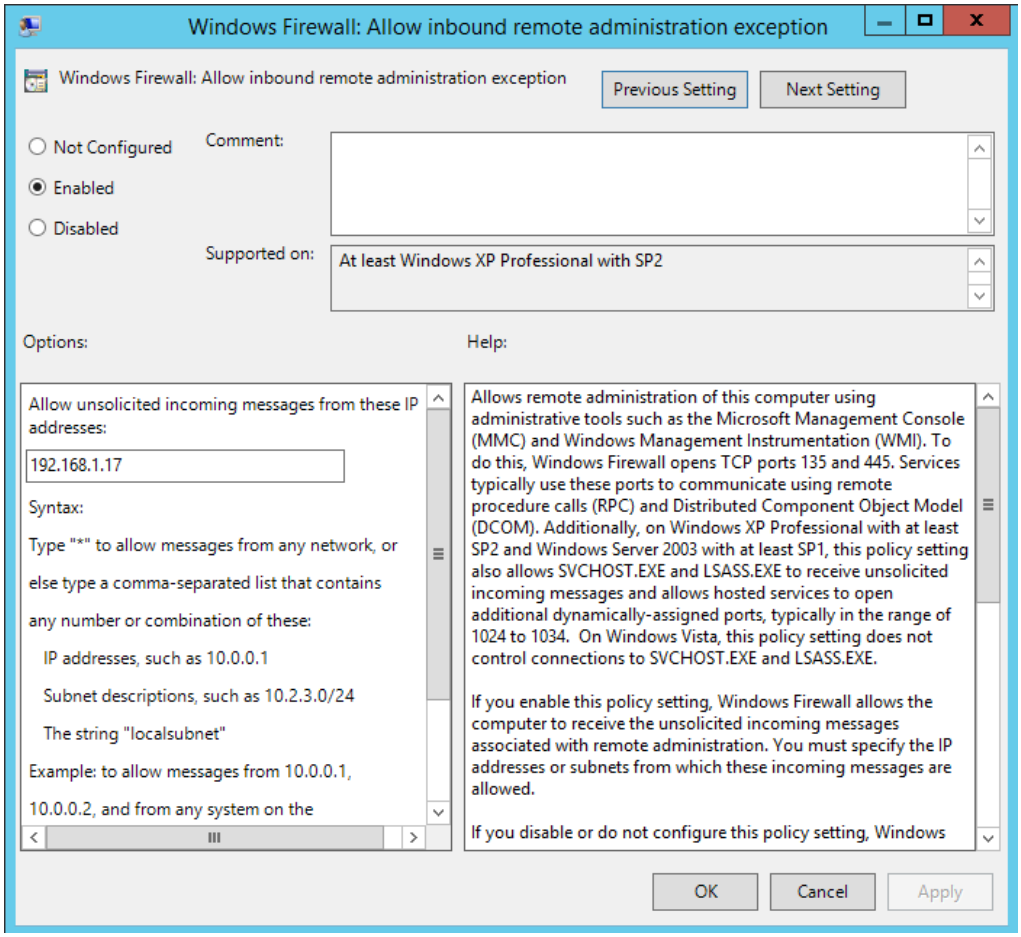
Remarque: En Workgroup, utilisez gpedit.exe sur chaque machine distante à superviser en utilisant le même compte Windows avec le même mot de passe pour toutes les machines.

Avec GPMC

GPMC peut être installé depuis Windows Server 2003 ou Windows XP Professionnel et version supérieures.
Exécutez GPMC avec un compte qui dispose de droits suffisants pour modifier les objets de stratégie de groupe
A - Sous l'en-tête Computer Policy local, double-cliquez sur Computer Configuration.
B - Double-cliquez sur Modèles d'administration, Réseau, Connexions réseau, puis Pare-feu Windows.
C - Si l'ordinateur se trouve dans le domaine, double-cliquez sur Profil de domaine; Dans le cas contraire, double-cliquez sur Profil standard.
D - Cliquez sur Pare-feu Windows: "Autoriser l'exception d'administration à distance entrante".
E - Dans le menu Action, sélectionnez Propriétés.
F - Cliquez sur Activer, indiquez l'adresse IP du (des) machine(s) MonitorPack Guard, puis cliquez sur OK.
G- Pour mettre à jour l'objet GPO, utilisez la commande « Gpupdate / Force »


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: monitorpack.local
Domains
monitorpack.local
Default Domain Policy
Domain Controllers
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Default Domain Policy
Scope Details Settings Delegation
Links
Display links in this location: monitorpack.local
The following sites, domains, and OUs are linked to this GPO:
Location Enforced Link Enabled Path
monitorpack.local No Yes monitorpack.local
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:
Name
Authenticated Users
Add... Remove Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none> Open


Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Administrative Templates: Policy definitions (ADMX files
Control Panel
Network
Background Intelligent Transfer Service (BITS)
BranchCache
DirectAccess Client Experience Settings
DNS Client
Hotspot Authentication
Lanman Server
Link-Layer Topology Discovery
Microsoft Peer-to-Peer Networking Services
Network Connections
Windows Firewall
Domain Profile
Standard Profile
Network Connectivity Status Indicator
Network Isolation
Offline Files
QoS Packet Scheduler
SNMP
SSL Configuration Settings
TCPIP Settings
Windows Connect Now
Domain Profile
Windows Firewall: Allow inbound remote administration exception
Edit policy setting
Requirements:
At least Windows XP Professional with SP2
Description:
Allows remote administration of this computer using administrative tools such as the Microsoft Management Console (MMC) and Windows Management Instrumentation (WMI). To do this, Windows Firewall opens TCP ports 135 and 445. Services typically use these ports to communicate using remote procedure calls (RPC) and Distributed Component Object Model (DCOM). Additionally, on Windows XP Professional with at least SP2 and Windows Server 2003 with at least SP1, this policy setting also allows SVCHOST.EXE and LSASS.EXE to receive unsolicited incoming messages and allows hosted services to
Setting State
Windows Firewall: Allow local program exceptions Not configure
Windows Firewall: Define inbound program exceptions Not configure
Windows Firewall: Protect all network connections Not configure
Windows Firewall: Do not allow exceptions Not configure
Windows Firewall: Allow inbound file and printer sharing ex... Not configure
Windows Firewall: Allow ICMP exceptions Not configure
Windows Firewall: Allow logging Not configure
Windows Firewall: Prohibit notifications Not configure
Windows Firewall: Allow local port exceptions Not configure
Windows Firewall: Define inbound port exceptions Not configure
Windows Firewall: Allow inbound remote administration exc... Not configure
Windows Firewall: Allow inbound Remote Desktop exceptions Not configure
Windows Firewall: Prohibit unicast response to multicast or ... Not configure
Windows Firewall: Allow inbound UPnP framework exceptio... Not configure
Extended Standard
14 setting(s)



8 - Groupes locaux pour superviser les compteurs de performance a distance

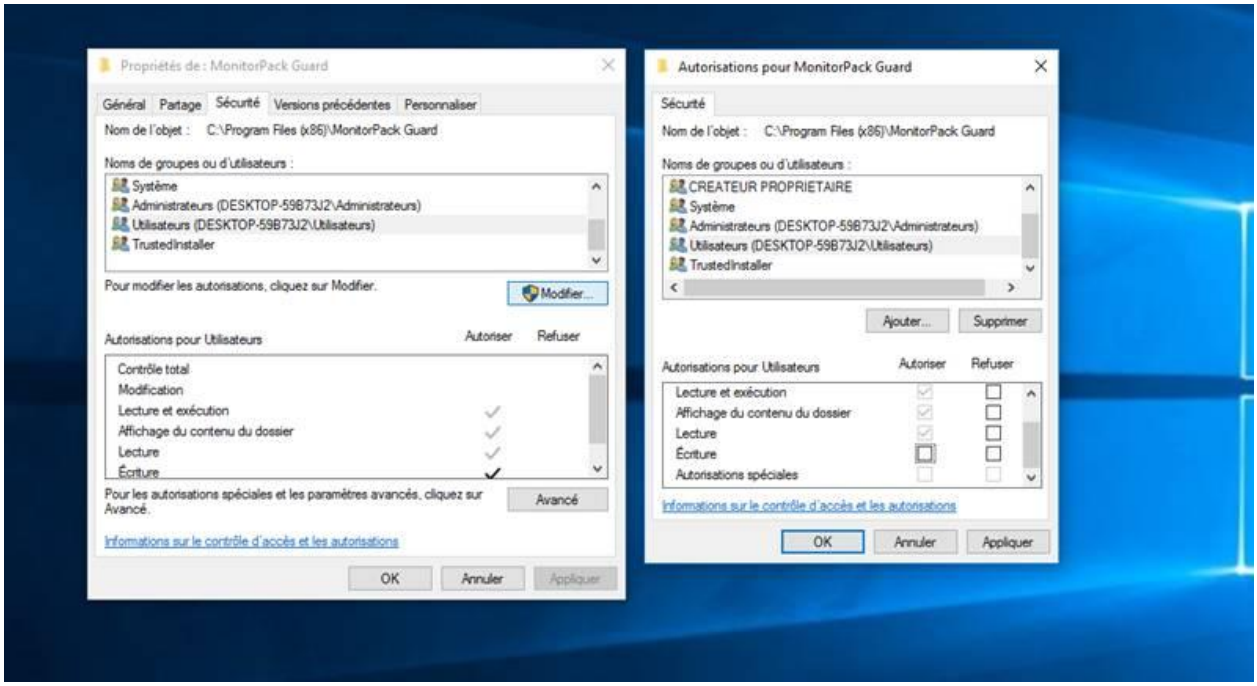
Pourquoi

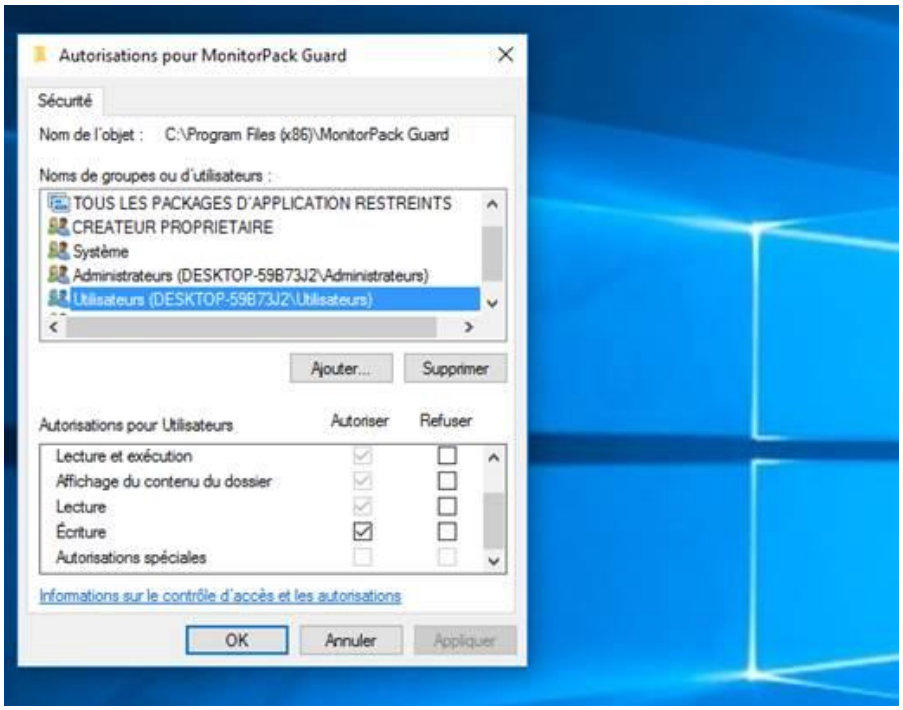
Depuis Windows 2008, Microsoft a augmenté la sécurité pour les demandes WMI, le compte de service Windows MonitorPack Guard utilisé pour MonitorPack Engine Service "svc_monitorpack" doit également être intégré dans les groupes locaux "PLU" ou PMU " Groupe local de chaque Windows Server 2008 ou supérieur surveillé, cela peut être fait serveur par serveur ou à partir de domaine Windows GPO.

9 - Windows 10 limitation des droits sur les Dossiers

Quoi

Après l'installation de MonitorPack Guard ou de MonitorPack Asset sur les versions Windows 10, Microsoft a modifié la sécurité, une fois donc installé vous devez donner le droit d'écriture au groupe local "MyMachine\Utilisateurs " sur le dossier MonitorPack Guard ou MonitorPack Asset.





Nous restons à votre disposition :

- E-mail: support@monitorpack.com
- Base de connaissance en ligne : Online knowledge base
- Par formulaire : Support request