Best Practice - Gestion de l'anti-virus avec Citrix Provisioning Services

Sources :

- CTX124185 - http://support.citrix.com/article/ctx124185
- Créée le 26 mars 2014
- Mise à jour le 02 septembre 2014

Symptômes ou erreurs

Les Serveurs PVS et les Target Devices peuvent rencontrer un ou plusieurs des symptômes suivants si l'anti-virus n'est pas correctement configuré pour votre environnement Provisioning services (PVS) :

- Lenteur sur les Target Devices ou les serveurs PVS.
- Ressources excessives du CPU et mémoire.
- Changement significatif de la mémoire cache en écriture Disk au niveau des performances E/S. Par exemple, lorsque vous utilisez « Perfmon », le pourcentage de temps pour les écritures disque ou la longueur de file d'attente pour les écritures disque augmente de façon significative.
- Etat de réplication incorrect pour un vDisk au niveau de l'inventaire.
- Les Target Devices ne démarrent pas sur le vDisk, mais sur le disque local si existant et affiche un X rouge au niveau du pictogramme vDisk de la barre des tâches du client PVS.
- Lors du démarrage, les performances des Target Devices sont décevantes pendant un laps de temps court même si les définitions AV sont mises à jour.

Les symptômes peuvent considérablement varier et ne sont pas limités à cette liste.

Solution

Limiter les mises à jour des définitions antivirales au niveau des Target Devices.

Créer une méthodologie de mise à jour périodique des vDisks en utilisant les mises à jour manuelles ou automatiques des vDisks. Cela peut réduire considérablement la bande passante réseau et la performance globale. Evitez de scanner les Write Cache et les fichiers de streaming du vDisk (I/O disque) qui forment le système d'exploitation d'une Target Device.

Evitez de scanner les processus et les drivers systèmes suivants sur les Target Devices PVS 6.x\7.x :

- **bndevice.exe** : handles client functions, licensing, etc
- **bnistack6.sys** : IO protocol driver | UDP port 6911-6930
- **CVhdBusP6.sys** : disk enumerator
- **CNicTeam.sys** : network teaming if being used
- **CFsDep2.sys** : system minifilter

Évitez de scanner les processus suivants sur les serveurs PVS 6.x \ 7.x:

- **Streamprocess.exe** : IO delivery | UDP port 6901-6910
- **Streamservice.exe** : watchdog for the streamprocess
- **Soapserver.exe** : handles Database connectivity and AD authentication
- **Inventory.exe** : vDisk Inventory | UDP port 6895
- **MgmtDaemon.exe** : inter-server communication |UDP port 6898
- **Notifier.exe** : inter-server communication | UDP port 6903
- **BNTFTP.exe** : PVS TFTP delivers bootstrap | UDP port 69
- **PVSTSB.exe** : Two Stage Boot delivers bootstrap | UDP port 6969
- **BNPXE.exe** : PVS PXE service | Broadcast Protocol
- **BNAbsService.exe** : PVS Ramdisk Server
- **CdfSvc.exe** : Citrix Diagnostic Facility COM Server

Evitez de scanner les fichiers de Write Cache des vDisks (sur les Target Devices ou les serveurs PVS). Les noms de fichiers de Write Cache pour le cache local des disques des Target Devices sont :

- 6.x : .vdiskcache
- 7.x : vdiskdif.vhdx ou .vdiskcache

La cause des problèmes

En général, la plupart des produits antivirus sont configurés pour analyser tous les fichiers I/O et les processus sur un disque. Comme un système d'exploitation s'exécute localement à son matériel, toutes les opérations d'E/S au niveau du streaming sont soumises à une analyse en temps réel par défaut. Si un programme antivirus analyse le flux actif des données en continu, qui compose le système d'exploitation de la Target Device, une dégradation va entraver le fonctionnement normal de PVS en provoquant des retards sur les I/O disque, des échecs en lecture-écriture, des problèmes de haute disponibilité, et plus encore. Dans les cas extrêmes, la Target Device et le serveur PVS peuvent consommer plus de ressources que nécessaire ou devenir inactif.

Lorsqu'un disque virtuel (vDisk) est en cours d'exécution en mode standard (lecture) et doit être redémarré, il va potentiellement re-télécharger toutes les définitions virales qui étaient précédemment chargées. Ce scénario courant provoque une dégradation sérieuse des performances quand les Target Devices sont redémarrés en masse, car elles causent des goulots d'étranglement côté bande passante pour une brève période de temps. Les Best practices seraient de mettre à jour juste la Target master et de régénérer un vDisk avec la nouvelle définition virale (ou mettre à jour le vDisk).

Ressources supplémentaires

Lors de l'installation ou la mise à niveau du logiciel client antivirus (ou tout autre logiciel qui modifie la pile réseau de la Target Device), PVS 6.x\7.x. vous oblige à d'abord désinstaller le client PVS et de le réinstaller dernière, pour ensuite refaire une image. Le logiciel PVS devient inutilisable quand un logiciel modifie ou interfère avec « BNistack6.sys » de la Target Device ou les I/O des interfaces réseau des serveurs de streaming. Un logiciel antivirus varie d'un fournisseur à l'autre, alors il faut vérifier auparavant les instructions spécifiques sur la configuration des exceptions d'analyse. Comme toujours, il est recommandé de tester le logiciel client anti-virus et sa configuration avant de le placer dans un environnement de Provisioning.