Installation de Windows 7 SP1 avec WDS

William Sayer

29/06/2014

Table des matières

Résumé

La plateforme WDS est une application client/serveur vu comme un rôle serveur qui a été intégré au système d'exploitation à partir des distributions de Windows server 2008 et qui a remplacé les services d'installation à distances (Remote Installation Services ou RIS) dans le service Pack 2 de Windows Server 2003. Ma réflexion pour mettre en œuvre cette plateforme a commencé au cours de l'année 2010. Elle intègre la technologie PXE et un serveur TFTP permettant le chargement d'une image de démarrage sur une machine cliente.
En 2012, lors d'une journée 2RCE à Montbélliard, un de mes homologues présentait l'application MDT (Microsoft Deployment Toolkit). Il utilisait ce logiciel pour déployer les systèmes d'exploitation sans utiliser la couche PXE donc sans l'aide de WDS. Je me suis rendu compte que cet outil était la clé manquante à mon projet pour réaliser les déploiements de plusieurs machines hétérogènes en utilisant une seule image.
En effet, WDS est l'homologue d'Acronis à la sauce Microsoft puisqu'il permet de récupérer une machine, où l'on a appliqué l'utilitaire sysprep, et de la convertir en une image wim exploitable ensuite par la plateforme WDS. Cette image que l'on appelle le master, correspond à un type de machine bien précis, comme par exemple un Dell precision T3610. Celle-ci est ensuite diffusée sur d'autres machines en vue d'un déploiement massif. Il faut donc autant d'image disque WIM qu'il y a de machines types dans un parc informatique, stations de travail et portables inclus. Ce mécanisme a un inconvénient majeur, vous avez besoin d'espace disque conséquent. En effet, la compatibilité d'une image disque dépend de son contrôleur disque (SCSI, PATA, SATA), en tenant compte aussi de la taille des partitions, du chipset, du processeur (Intel x86 ou x64 ou autres architectures comme AMD) et du contrôleur de mémoire (DDR SDRAM, DDR2 SDRAM ou DDR3 SDRAM). En somme, il est préférable d'avoir le même matériel identique afin d'éviter un écran bleu de la mort ou un dysfonctionnement dû à un pilote non approprié. C'est pourquoi, MDT est la solution à tous ces problèmes, annulant la contrainte de l'espace disque sur un serveur et en rationalisant les différentes images disques pour devenir des profils de machine autour d'une seule et même image. Voir le synoptique d'une architecture MDT.

1 Introduction :

Au sein de notre laboratoire, l'infrastructure réseau est composée de deux mécanismes de déploiement de systèmes d'exploitation. Un serveur SYSLINUX destiné au déploiement des distributions CentOS et Debian, et un serveur WDS (Windows Deployement Services) dédié au déploiement des distributions Windows 7 SP1 et Windows 8.1. Ces deux systèmes utilisent chacun leur propre serveur de transport et serveur DHCP sur des réseaux différents. La solution SYSLINUX est sur le réseau de production du laboratoire, le vlan 700 (194.214.124.0/24) et la solution WDS est sur le réseau interne, le vlan 702 (172.22.52.0/24). Ce dernier réseau n'est pas routable vers l'extérieur car il n'est pas référencé dans le monde de l'internet. Il fait partie des réseaux privés dédiés uniquement aux réseaux locaux (voir la RFC 1597). Ce réseau, au sein de l'ATILF, est utilisé pour la gestion des onduleurs, des commutateurs réseaux manageables, pour les imprimantes, les photocopieurs et pour le serveur de déploiement WDS.

Pourquoi avoir choisi d'utiliser deux serveurs de transport et deux serveurs DHCP ?
Pour la simple et bonne raison que la cohabitation est très difficile, voire peut-être impossible d'utiliser deux serveurs TFTP sur un même réseau avec une infrastructure DHCP basé sous LINUX pour deux raisons élémentaires :

- La première raison est qu'il faut paramétrer les options destinées aux serveurs de déploiement dans le même fichier de configuration du serveur DHCP. C'est là que ça coince ! Je n'ai pas abandonné l'idée, je suis toujours dans la réflexion pour trouver la solution miracle qui me permettra d'avoir deux solutions de déploiement multiplateforme en utilisant uniquement les services réseaux existants sous linux. Il existe toutefois un moyen de combiné les deux mais cela fonctionne sur une architecture Windows. Je n'ai pas essayé de la mettre en place, c'est à tester.

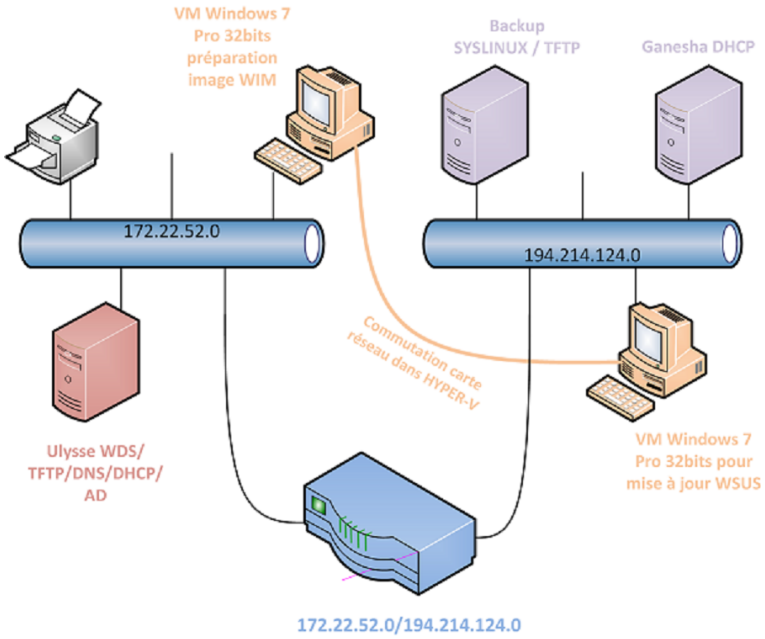
- La seconde raison est qu'une fois sur quatre, c'est le serveur TFTP linux qui réponds le plus rapidement. On pourrait dire dans ce sens, que la machine Windows est plus puissante que la machine Linux, mais ce n'est pas le cas. On pourrait dire aussi que c'est la couche applicative Windows où le traitement des requête qui est plus lent que sous Linux. Pourquoi ? Parce que Windows est plus bavard que Linux, est donc c'est une perte de temps à ce niveau là.[1]

[1] Rejouer la séquence avec un scanner Wireshark

2 Infrastructure de la plateforme WDS :

Les tests réalisés, pour la mise en œuvre d'un déploiement d'une distribution Windows 7 Pro 32 bits, ont été effectués sur une plateforme de virtualisation HYPER-V de Microsoft. L'installation se fait par le biais du réseau en utilisant l'environnement de démarrage PXE (Preboot eXecution Environnement). Dans la mmc Hyper-V, le choix de booter sur le réseau est configurable dans les Paramètres de la future station de travail virtuelle, dans la section BIOS, en positionnant la carte réseau héritée en premier choix de boot.
Le serveur WDS, une machine Hewlett Packard Z800, est configuré avec 3 cartes réseaux. L'une est dédiée uniquement au serveur WDS configurée sur le réseau 172.22.52.0/24. Elle ne doit pas être virtualisée. Concernant les deux autres cartes, ce sont des cartes réseaux que l'on virtualise pour nos futures machines virtuelles. L'une est dédiée pour le vlan 702 (172.22.52.0/24), elle permet d'effectuer la préparation des futures images WIM afin de déployer les futures machines physiques sous Windows 7 Professional. Et l'autre carte réseau est dédiée pour le vlan 700 (194.214.124.0/24), afin d'effectuer toutes les mises à jour des futures images WIM préparée précédemment sur le réseau 172.22.52.0/24. La bascule se fait manuellement dans la mmc HYPER-V, dans la partie réseau, en choisissant l'une ou l'autre carte ETHERNET.

2.1 Schéma architectural pour la création des images WIM dans WDS :

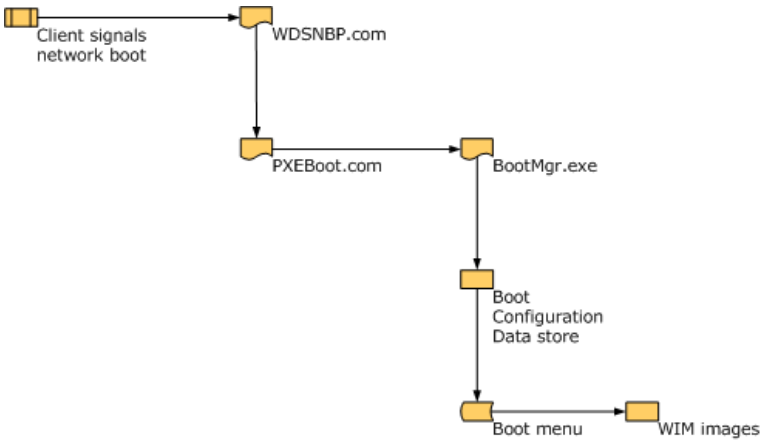


3 Principe de fonctionnement de la technologie PXE :

Le Preboot Execution Environment est une invention d'Intel Corp. Lorsqu'un démarrage de l'environnement de l'exécution de prédémarrage (PXE) est lancé, la PROM de la carte réseau possédant la technologie PXE (port 4011) demande une adresse IP à un serveur DHCP (Dynamic Host Configuration Protocol), en utilisant le processus de découverte DHCP normal. Dans le cadre de la demande de découverte DHCP initiale, l'ordinateur client s'identifie comme étant compatibles PXE, et qui indique au serveur PXE que le client doit être pris en charge. Le serveur de démarrage PXE est un petit fichier qui contient des instructions de logiciels qui doivent être chargés sur l'ordinateur client. Une fois que le client a obtenu une adresse IP valide à partir d'un serveur DHCP, le client tente de localiser et d'établir une connexion avec le serveur PXE pour télécharger un programme d'amorçage réseau (NBP). NBP est le premier fichier téléchargé et exécuté dans le cadre du processus de démarrage d'environnement de l'exécution de prédémarrage (PXE). Le NBP détermine si le client peut démarrer à partir du réseau, si le client doit appuyer sur F12 pour lancer l'amorçage et l'image de démarrage que le client recevra par l'intermédiaire du serveur TFTP (port 69). le NBP est une application 16 bits en mode réel.
Par défaut, le serveur PXE de Windows, Windows Deployment Services (WDS), n'a pas besoin d'être autorisé à desservir les ordinateurs clients. Tou-

tefois, vous pouvez activer l'autorisation DHCP qui est également connue sous le nom de la détection. Cela signifie que les contrôles d'autorisation ont lieu uniquement dans les scénarios dans lesquels les Services de déploiement Windows s'exécutent sur un ordinateur sans le client DHCP. Si les Services de déploiement Windows et DHCP s'exécutent sur le même ordinateur physique, cela signifie que le serveur DHCP est à l'écoute sur le port 67 (dhcpd) et est chargé d'assurer l'autorisation.
PXE est étroitement liée à DHCP qui attribue des adresses IP à l'ordinateur pendant le processus de démarrage. Des paquets de message PXE sont une extension de l'ensemble de commandes DHCP. PXE ne peut fonctionner sans la présence d'un serveur DHCP.

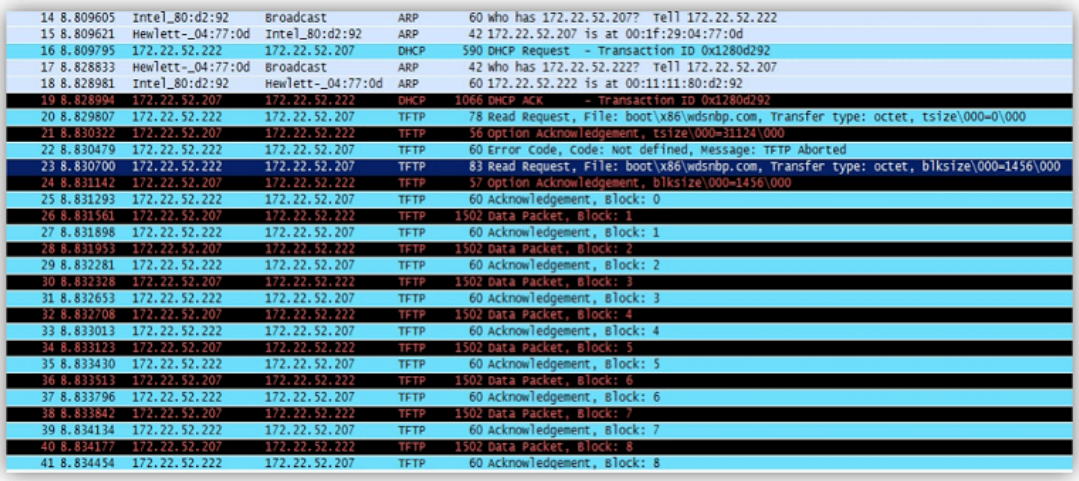
3.1 Schéma du chargement d'un NBP dans WDS :



4 Les différentes étapes du processus de démarrage en réseau :

Les différentes requêtes effectuées par la station de travail sur le réseau à l'aide de l'environnement de démarrage d'ordinateur en réseau (PXE) sont caractérisées par l'exécution de plusieurs protocoles de la couche TCP/IP. Ces tests ont été réalisés en utilisant la réservation d'adresse IP du serveur DHCP.
Voici les différentes étapes du processus pour démarrer à partir d'une image de démarrage d'un serveur WDS. Dans un premier temps un broadcast est émis par la machine en utilisant le protocole ARP pour se faire connaître d'un serveur PXE sur le réseau local. A ce moment précis, un serveur lui répond en lui indiquant son adresse MAC de la carte réseau. Ensuite, La station de travail, par l'intermédiaire de la PROM de la carte réseau contenant la technologie PXE, effectue un broadcast en utilisant le protocole DHCP

pour faire une demande d'adresse IP. Comme la station de travail possède une réservation d'une adresse IP sur le serveur DHCP, le serveur, avant de lui attribuer l'adresse IP, s'assure par l'intermédiaire du protocole ARP que l'adresse MAC est bien celle configurée sur le serveur DHCP. Après la vérification, le serveur attribue l'adresse IP à la machine via le protocole DHCP. Pour finaliser, les deux machines communiquent sur le réseau via le protocole TFTP, chargement de l'image de démarrage . La station de travail récupère ainsi une image de démarrage (boot.wim) à partir du serveur de déploiement. Si vous avez un firewall d'activer, il faudra autoriser les ports 4011 (PXE) et 69 (TFTP).



14	8.809605	Intel_80:d2:92	Broadcast	ARP	60 Who has 172.22.52.207? Tell 172.22.52.222
15	8.809621	Hewlett-_04:77:0d	Intel_80:d2:92	ARP	42 172.22.52.207 is at 00:1f:29:04:77:0d
16	8.809795	172.22.52.222	172.22.52.207	DHCP	590 DHCP Request - Transaction ID 0x1280d292
17	8.828833	Hewlett-_04:77:0d	Broadcast	ARP	42 Who has 172.22.52.222? Tell 172.22.52.207
18	8.828981	Intel_80:d2:92	Hewlett-_04:77:0d	ARP	60 172.22.52.222 is at 00:11:11:80:d2:92
19	8.828994	172.22.52.207	172.22.52.222	DHCP	1066 DHCP ACK - Transaction ID 0x1280d292
20	8.829807	172.22.52.222	172.22.52.207	TFTP	78 Read Request, File: boot\x86\wdsnbp.com, Transfer type: octet, tsize\000=0\000
21	8.830322	172.22.52.207	172.22.52.222	TFTP	56 Option Acknowledgement, tsize\000=31124\000
22	8.830479	172.22.52.222	172.22.52.207	TFTP	60 Error Code, Code: Not defined, Message: TFTP Aborted
23	8.830700	172.22.52.222	172.22.52.207	TFTP	83 Read Request, File: boot\x86\wdsnbp.com, Transfer type: octet, blksize\000=1456\000
24	8.831142	172.22.52.207	172.22.52.222	TFTP	57 Option Acknowledgement, blksize\000=1456\000
25	8.831293	172.22.52.222	172.22.52.207	TFTP	60 Acknowledgement, Block: 0
26	8.831561	172.22.52.207	172.22.52.222	TFTP	1502 Data Packet, Block: 1
27	8.831898	172.22.52.222	172.22.52.207	TFTP	60 Acknowledgement, Block: 1
28	8.831953	172.22.52.207	172.22.52.222	TFTP	1502 Data Packet, Block: 2
29	8.832281	172.22.52.222	172.22.52.207	TFTP	60 Acknowledgement, Block: 2
30	8.832328	172.22.52.207	172.22.52.222	TFTP	1502 Data Packet, Block: 3
31	8.832653	172.22.52.222	172.22.52.207	TFTP	60 Acknowledgement, Block: 3
32	8.832708	172.22.52.207	172.22.52.222	TFTP	1502 Data Packet, Block: 4
33	8.833013	172.22.52.222	172.22.52.207	TFTP	60 Acknowledgement, Block: 4
34	8.833123	172.22.52.207	172.22.52.222	TFTP	1502 Data Packet, Block: 5
35	8.833430	172.22.52.222	172.22.52.207	TFTP	60 Acknowledgement, Block: 5
36	8.833513	172.22.52.207	172.22.52.222	TFTP	1502 Data Packet, Block: 6
37	8.833796	172.22.52.222	172.22.52.207	TFTP	60 Acknowledgement, Block: 6
38	8.833842	172.22.52.207	172.22.52.222	TFTP	1502 Data Packet, Block: 7
39	8.834134	172.22.52.222	172.22.52.207	TFTP	60 Acknowledgement, Block: 7
40	8.834177	172.22.52.207	172.22.52.222	TFTP	1502 Data Packet, Block: 8
41	8.834454	172.22.52.222	172.22.52.207	TFTP	60 Acknowledgement, Block: 8

FIG. 1 : wireshark, capture réalisée sur le serveur ulysse

Voici ci-dessus une capture wireshark à partir de la carte réseau du serveur WDS configuré avec l'adresse IP en 172.22.52.207. La station de travail virtuelle utilisée possède l'adresse IP en 172.22.52.222 configuré sur le serveur DHCP Windows de manière statique, c'est une réservation qui repose sur l'adresse MAC. On peut visualiser toutes les transactions entre les deux machines expliquées précédemment.

Si la station de travail est sur le réseau 194.214.124.0, c'est le serveur DHCP sous Linux qui lui répondra pour l'attribution de l'adresse IP. Dans le fichier dhcp.conf est référencé le serveur de transport SYSLINUX. La transaction TFTP permettra à la station de travail de charger le noyau de démarrage en mémoire vive. Pour l'installation des CentOS, le programme d'installation permet l'utilisation du protocole « http » sur le port 80. Il faut saisir l'adresse de l'url de l'image d'installation de la distribution. SYSLINUX permet également l'exécution d'outils technique pour la maintenance d'une machine en utilisant le protocole « tftp » sur le port 4011. Pour l'installation d'un système d'exploitation via le réseau, il est préférable d'utiliser le protocole « http » plutôt que le protocole « tftp » pour des raisons de souplesse, de rapidité et de rigidité. En effet, le protocole « http » s'appuie sur le protocole TCP pour le transport des paquets qui intègre un CRC, un contrôle d'erreur. Il s'avère donc plus fiable que le protocole « udp », qui est utilisé par le protocole « tftp ».

5 Mise en oeuvre de WDS :

5.1 Pré-requis pour la plateforme WDS

5.2 Installation du service de rôle WDS

Je peux faire des sous sections.

6 Conclusion

Je termine mon premier exemple LaTeX