

Sécurité et mobilité Windows 8

pour les utilisateurs nomades

UEFI • BitLocker et AppLocker • DirectAccess • VPN
• SmartScreen • Windows Defender...

Arnaud Jumelet
Stanislas Quastana
Pascal Saulière

Préface de Bernard Ourghanlian



Avant-propos

Il y a à peine quelques années, le « poste de travail » portait bien son nom : PC fixe, fidèle au poste, immobile sur le bureau de l'utilisateur. La sécurité était relativement simple à appréhender : il y avait le réseau interne, la périphérie et le reste du monde. Le poste de travail, comme les serveurs, était du bon côté de la barrière.

C'est un lieu commun de dire que l'utilisateur d'aujourd'hui est mobile, travaille chez lui, dans le train ou les aéroports, et pas uniquement sur un PC : la tablette et le smartphone sont plus que des périphériques compagnons d'un PC portable. L'utilisateur a aussi son propre matériel et entend l'utiliser, ou, dans certains cas, fait un usage personnel d'un matériel fourni par la DSI.

Il faut donc tenir compte des appareils variés, maîtrisés ou non, personnels ou non, mobiles dans tous les cas, et toujours en faisant en sorte que le bon niveau de sécurité soit appliqué en fonction des risques. Le contexte étant posé, nous allons exposer dans cet ouvrage les réponses de Windows 8 et quels éléments il apporte dans le nécessaire équilibre à trouver entre les nouveaux usages et la maîtrise des données de l'entreprise.

À qui ce livre s'adresse-t-il ?

Ce livre s'adresse à tous les passionnés des nouvelles technologies Microsoft. Le sujet de la sécurité du poste de travail et du télétravail en situation de mobilité est un sujet récurrent et plus que jamais d'actualité en entreprise.

Ce livre intéressera les directeurs des systèmes d'information, les responsables de la sécurité des systèmes d'information, les ingénieurs systèmes et réseaux, les architectes, les consultants, mais aussi certains chefs de projets.

Travailler en situation de mobilité sur un poste de travail de confiance où les données sont sécurisées est désormais un besoin vital et commun à toutes les entreprises, quelle que soit leur taille (de la TPE à la multinationale).

Le niveau de connaissances requis pour la lecture de cet ouvrage est relativement élémentaire pour une personne impliquée de près ou de loin dans les technologies Microsoft.

Les explications fournies à travers les chapitres démarrent à partir de connaissances généralistes sur les systèmes et architectures basées sur Windows (Active directory, DNS, DHCP...).

Cet ouvrage est donc abordable par toute personne connaissant les fondamentaux de l'informatique et des produits Microsoft. Les sujets traités dans cet ouvrage sont également couverts par plusieurs certifications Microsoft.

Voici la liste de ces certifications :

71-410 - Installing and Configuring Windows Server 2012

70-412 - Configuring Advanced Windows Server 2012 Services

70-413 - Designing and Implementing a Server Infrastructure

70-414 - Implementing an Advanced Server Infrastructure

70-415 - Implementing a Desktop Infrastructure

70-416 - Implementing Desktop Application Environments

70-417 - Upgrading Your Skills to MCSA Windows Server 2012

70-687 - Configuring Windows 8

70-688 - Managing and Maintaining Windows 8

Comment ce livre est-il structuré ?

Ce livre est découpé en deux grandes parties. La première concerne les **mécanismes de sécurité disponibles dans Windows 8** (combiné parfois avec son pendant côté serveur). La seconde expose les **différentes approches technologiques permettant à un utilisateur d'entreprise de travailler en situation de nomadisme**.

Le chapitre 1 propose de faire un **état des lieux du poste de travail nomade moderne** avec ses défis en termes de besoins utilisateur par rapport à la sécurité, à l'administration et au coût.

Les chapitres 2 à 6 sont focalisés sur les aspects sécurité et mécanismes de protection d'un poste de travail fonctionnant avec Windows 8.

- Le chapitre 2 est consacré au rôle du matériel avant, pendant et après le démarrage de Windows 8. Il décrit l'intérêt d'avoir un firmware UEFI et un module de plate-forme sécurisée TPM lors du démarrage de Windows 8. Ce chapitre est sûrement le plus technique de l'ouvrage, puisqu'il expose les arcanes les plus méconnus du système d'exploitation.
- Le chapitre 3 décrit quelques-uns des mécanismes liés à des fonctions de base de la sécurité du système, comme l'authentification des utilisateurs, l'ouverture de session, le contrôle d'accès, le contrôle de compte d'utilisateur et l'isolation des applications Windows 8. Ce chapitre est plutôt technique, mais explique certains aspects du fonctionnement du système.

- Le chapitre 4 présente les services intégrés dans Windows 8 pour la protection et la lutte contre les malwares. Au-delà de Windows Defender, un anti-malware non intrusif, la vraie valeur ajoutée réside certainement dans Windows SmartScreen, qui aide les utilisateurs à prendre la bonne décision face à un programme inconnu et n'ayant aucune réputation.
- Le chapitre 5 est dédié aux applications traditionnelles et modernes. Le maintien en conditions opérationnelles est détaillé avec Windows Update. Il est essentiel de télécharger, appliquer ou mettre à disposition les toutes dernières mises à jour. Enfin, il est expliqué comment contrôler les applications avec AppLocker, c'est-à-dire comment les autoriser ou non à s'installer et à s'exécuter.
- Le chapitre 6 est consacré à la protection des données et au contrôle d'accès. Lorsqu'un ordinateur est électriquement éteint, le fait de chiffrer les données du disque au repos par BitLocker prémunit contre l'accès physique non autorisé. Le contrôle d'accès dynamique est la seconde partie de ce chapitre ; il s'agit du contrôle d'accès moderne avec une prise de décision dynamique en fonction du contexte d'accès.

Les chapitres 7 à 11 sont axés sur l'aspect mobilité et nomadisme des postes de travail d'entreprise.

- Le chapitre 7 a pour objectif d'**aider à démarrer un projet de mise en place d'accès distants au système d'information** en proposant un état des lieux des solutions technologiques possibles, une aide à la décision pour le choix des technologies, un rappel des bonnes pratiques et une vue rapide des solutions existant chez Microsoft. C'est un chapitre peu technique, mais essentiel pour la lecture des chapitres suivants.
- Le chapitre 8 concerne l'**accès distant aux applications et Bureaux distants** pour les postes gérés ou nongérés (personnels). Il détaille notamment les services web et de passerelles présents dans Windows Server 2008 R2 et 2012.
- Le chapitre 9 traite de la mise en œuvre d'**accès distants au travers de réseaux privés virtuels (VPN)** pour les postes gérés ou non gérés. Il comprend l'installation des composants serveurs sur Windows Server 2012 et la configuration de ces connexions sur un poste Windows 8.
- Le chapitre 10 présente les **infrastructures DirectAccess et détaille les mécanismes utilisés** dans cette nouvelle méthode de connexions distantes au système d'information avec Windows 8 couplé à Windows Server 2008 R2 ou, mieux, Windows Server 2012.
- Le chapitre 11 présente **Windows To Go, qui est une installation de Windows 8 Entreprise sur un média amovible**. Ce chapitre détaille les prérequis à respecter, les scénarios d'usage et la méthode pour créer un espace de travail Windows To Go.

Systèmes nécessaires

Il est possible de tester l'ensemble des technologies détaillées dans ce livre sur une plateforme d'intégration.

Pour cela, il faut idéalement se munir d'une machine assez puissante sur laquelle le rôle Hyper-V de Windows Server 2012 sera installé (au minimum 16 Go de RAM). Cela permettra de mettre en œuvre et de tester les différentes technologies et scénarios présentés au sein de cet ouvrage. Il est également possible de mixer des serveurs physiques et virtuels.

Afin de tester les différents scénarios, voici un exemple de configuration :

- un serveur hébergeant les rôles Active Directory, DNS et DHCP ;
- une machine cliente Windows 8 pour effectuer les tests ;
- 1 à 5 serveur(s) pour mettre en œuvre les infrastructures sur lesquelles va se connecter le poste de travail de test ;
- un équipement réseau de type commutateur (*Switch*) ;
- des câbles réseaux Ethernet pour connecter les machines ;
- un support (clé USB, DVD, disque dur USB) afin de stocker éventuellement des données nécessaires à l'accomplissement de certaines parties du livre ;
- une connexion Internet pour télécharger l'ensemble des outils et produits nécessaires.

Les systèmes d'exploitation (Windows 8 et Windows Server 2008 R2 ou Windows Server 2012) présentés dans cet ouvrage sont téléchargeables gratuitement en versions d'évaluation (limitée à 180 jours d'utilisation) sur le centre de téléchargement de Microsoft (www.microsoft.com/fr-fr/download/).

L'histoire d'une aventure de 13 passionnés !

Nous ne pouvions pas vous laisser démarrer la lecture sans vous expliquer comment ce projet a démarré. Ce livre fait partie d'un ensemble de quatre ouvrages consacrés au poste de travail Windows 8. Ce projet a réellement démarré au début de l'année 2012. Les 13 auteurs de ces ouvrages sont des passionnés et experts reconnus dans leurs domaines respectifs.

Voici la liste des ouvrages :

Sécurité et mobilité du poste de travail Windows 8, Arnaud Jumelet, Stanislas Quastana et Pascal Saulière.

Développement Windows 8, Louis-Guillaume Morand, Luc Vo Van et Alain Zanchetta.

Virtualisation du poste de travail Windows 7 et 8, William Bories, Abderrahmane Laachir, Philippe Lafeil, David Thieblemont et François-Xavier Vitrant.

Déploiement et migration Windows 8, par William Bories, Olivia Mirial et Stéphane Papp.

D'autres passionnés chez Microsoft sont venus contribuer à ces ouvrages en apportant une relecture profonde et pragmatique. Certains de ces relecteurs sont également des experts reconnus, ils ont pu nous défier sur notre propre terrain. D'autres relecteurs, n'ayant aucune expertise technique, ont eu la volonté de lire des dizaines de pages pour améliorer la qualité de ces ouvrages. Bref, c'est un projet atypique sur lequel nous avons tous pris beaucoup de plaisir à participer !

En espérant que vous partagerez ce plaisir, je vous souhaite une excellente lecture.

William Bories,
Coordinateur du projet

Remerciements

Comme expliqué précédemment, ce projet d'ouvrages est l'œuvre de nombreux intervenants et c'est pour cette raison que nous souhaitons remercier nos relecteurs avant toute autre personne !

Ils furent nombreux à participer aux relectures, experts techniques ou non. Ils ont su avec brio s'adapter à nos styles respectifs, défier la cohérence globale de cet ouvrage et bien évidemment, corriger la forme et le fond malgré nos relectures personnelles ! Nous remercions ainsi chaleureusement : Guillaume Barry, Christophe Besançon, Philippe Labeil, Sébastien Chavenas, Frédéric Esnouf, Arnaud Lheureux, Ismaël Limbada, Louis-Guillaume Morand, Félix Ndouga, Didier Pilon, Angélique Pichard, Julien Massé et Roxana Garraud.

Les éditions Eyrolles ont également joué un rôle important dans la réussite de cet ouvrage. La qualité des relectures chez cet éditeur a permis à ce livre de s'élever à un tout autre niveau. Merci Muriel, Laurène, Sophie, Géraldine et Éric pour tout ce travail et cette confiance que vous nous avez accordée.

Enfin, nous remercions également Bernard Ourghanlian qui a su, avec toute sa sympathie et sa grande expérience dans l'industrie IT, préfacer notre ouvrage avec brio. Merci Bernard, c'est un honneur de t'avoir en préfacier.

Arnaud Jumelet

J'ai été ravi de participer à ce projet d'écriture avec à bord Stanislas et Pascal, une bonne équipe de geeks, des vrais de vrais ! Merci aussi aux relecteurs et à William pour son enthousiasme contagieux. Nous n'imaginions pas le temps que cela nous prendrait ; heureusement avec de la bonne musique cela devient tout de suite plus agréable.

Je tiens à remercier Anne-Sophie, ma moitié, pour son soutien et sa compréhension tout au long de ce projet et plus particulièrement durant les week-ends !

Pascal Sauliere

Être l'épouse d'un geek n'est pas tous les jours facile, mais quand celui-ci s'essaie à l'écriture, les week-ends deviennent encore plus compliqués. Merci donc à Chantal pour sa patience sans limite. Ce projet étant collectif, que tous ceux qui ont participé soient également remerciés, et en premier lieu Arnaud, Stanislas et nos relecteurs pour leur exigence et leur grande rigueur.

Stanislas Quastana

Pour faire original, je vais remercier mes compagnons d'aventure, Arnaud et Pascal, qui ont relevé avec moi ce défi passionnant, ainsi que les relecteurs techniques qui ont passé du temps à nous aider à améliorer cet ouvrage.

Je remercie également William Bories, coordinateur du projet, qui a su m'embarquer dans ce navire (qui aurait pu devenir rapidement une galère sans son aide précieuse !), ainsi que Louis-Guillaume Morand qui m'a particulièrement poussé sur le style de ma rédaction (et il avait bien raison, fort de sa grande expérience d'auteur !).

Je tiens finalement à remercier mes amis et ma famille, qui m'ont parfois supporté en mode « grognon » durant mes phases de rédaction.