



Collection

EXPERT IT

DirectAccess

Mobilité et nomadisme

Mise en œuvre
de la solution Microsoft

**Lionel
LEPERLIER**



Microsoft®
Most Valuable
Professional

**Benoît
SAUTIERE**



Microsoft®
Most Valuable
Professional

Téléchargement

www.editions-eni.fr



INFORMATIQUE TECHNIQUE



Collection

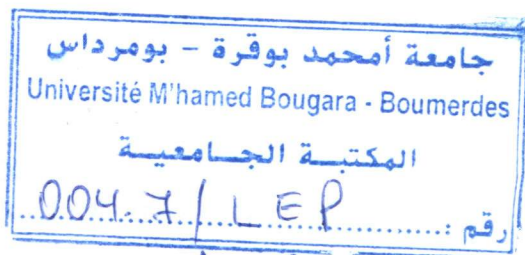
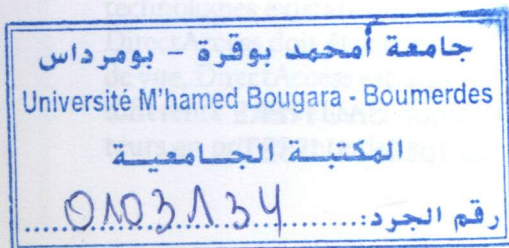
EXPERT IT



Direct Access

Mobilité et nomadisme

Mise en œuvre
de la solution Microsoft



Ne 48.

Les éléments à télécharger sont disponibles à l'adresse suivante :

<http://www.editions-eni.fr>.

Saisissez la référence ENI de l'ouvrage **EIDIRA** dans la zone de recherche et validez. Cliquez sur le titre du livre puis sur le bouton de téléchargement.

Avant-propos

Chapitre 1

DirectAccess pour quoi faire ?

1. Le nomadisme en quelques mots.	15
1.1 Du point de vue de l'utilisateur.	15
1.2 Du point de vue de l'exploitant.	17
2. Objectifs de DirectAccess.	18
2.1 Du point de vue de l'utilisateur.	18
2.2 Du point de vue de l'exploitant.	20
3. Scénarios autour du nomadisme.	20
3.1 Authentification des utilisateurs mobiles.	20
3.2 Gestion du poste de travail en situation de mobilité.	23
3.3 Gestion de la conformité du poste de travail en situation de mobilité.	24
3.4 Contrôle d'accès et isolation logique.	25
3.5 Uniformisation de la politique d'accès à Internet.	27
4. La sécurité de nos réseaux d'entreprise.	28
4.1 Notre réseau d'entreprise est-il sûr ?	28
4.2 Redéfinir le périmètre à protéger.	31
5. Dans le cadre de cet ouvrage.	32
6. Synthèse.	36

Chapitre 2**L'assemblage des technologies**

1. Introduction	37
2. Pourquoi IPv6 ?	37
2.1 Faut-il avoir peur d'IPv6 ?	39
2.2 Pourquoi DirectAccess repose-t-il sur IPv6 ?	40
2.3 Dois-je commencer un projet IPv6 ?	42
3. DirectAccess Windows versus DirectAccess UAG	43
4. Positionnement des technologies pour DirectAccess	45
4.1 IPv4	45
4.2 IPv6	46
4.3 Pare-feu	47
4.4 IPSec	50
4.5 AuthIP	53
4.6 NRPT - Tout part du client	61
4.7 PKI	65
4.8 Network Location Server	66
5. Synthèse	67

Chapitre 3**IPv6**

1. Introduction à IPv6	69
1.1 Synthèse comparative	69
1.2 Espace d'adressage et notation	70
1.3 Notion de préfixe	72
1.4 Synthèse	72
2. Les différents types d'adresses	72
2.1 Link-Local	73
2.2 Unique Local IPv6 Unicast	74
2.3 Global Unicast	74
2.4 MultiCast	75

2.5 Anycast	75
2.6 Special	76
2.7 Synthèse	76
3. Configuration	76
3.1 Configuration manuelle	77
3.2 Configuration automatique	78
3.3 Synthèse	78
4. Cohabitation IPv4	79
4.1 ISATAP	80
4.2 6to4	84
4.3 Teredo	89
4.4 IPHTTPS	95
4.5 DNS64	98
4.6 NAT64	101
5. Synthèse	103

Chapitre 4 Les choix d'architectures

1. Introduction	105
2. Domain Name Server	105
2.1 Zones DNS internes	106
2.2 Serveurs DNS internes	106
2.2.1 DNSQueryBlockList	107
2.2.2 ISATAP	109
2.2.3 Binding IPv6	111
2.3 Zones DNS externes	112
2.4 Exceptions	112
3. Active Directory	114
3.1 Identification des clients nomades	114
3.2 Identification des serveurs DirectAccess	115

Chapitre 5

L'approche projet

1. Introduction	197
2. Les interlocuteurs impliqués	197
2.1 Le chef de projet	198
2.1.1 Son rôle dans le projet	198
2.1.2 Risques à prendre en considération	199
2.2 Le responsable de la sécurité informatique	199
2.2.1 Son rôle dans le projet	200
2.2.2 Risques à prendre en considération	200
2.2.3 Se focaliser avant tout sur l'essentiel	202
2.3 L'équipe en charge du poste de travail	202
2.3.1 Son rôle dans le projet	202
2.3.2 Risques à prendre en considération	202
2.4 L'exploitant de la plateforme Windows	204
2.4.1 Son rôle dans le projet	205
2.4.2 Risques à prendre en considération	205
2.4.3 Le cas des hébergeurs	207
2.5 L'exploitant réseau	209
2.5.1 Son rôle dans le projet	209
2.5.2 Risques à prendre en considération	209
2.6 Support de premier niveau	211
2.6.1 Rôle dans le projet	211
2.6.2 Risques à prendre en considération	211
2.7 Des utilisateurs représentatifs	212
2.7.1 Rôle dans le projet	213
2.7.2 Risques à prendre en considération	213
3. Organisation du projet	214
3.1 Les éventuels sous-projets	215
3.1.1 Authentification forte	215
3.1.2 Haute disponibilité	216
3.1.3 La conformité	219

3.1.4	Gestion du client nomade	221
3.1.5	IPv6	222
3.2	Approche itérative	225
3.2.1	IPD Guides	225
3.2.2	Test Lab Guides	226
3.2.3	Technet	227
3.2.4	Proof of Concept	227
3.2.5	Disposer de plusieurs environnements	228
3.2.6	Développer par itérations	229
4.	La compatibilité des applications	230
4.1	Résolution DNS	231
4.2	Applications client-serveur	231
4.3	Application non compatible avec IPv6	232
5.	Synthèse	233

Chapitre 6

Mise en œuvre de DirectAccess

1.	Introduction	235
2.	Pré-requis communs	235
2.1	Configuration des interfaces réseau	235
2.1.1	Configuration de l'interface réseau LAN	236
2.1.2	Table de routage	240
2.1.3	Configuration de l'interface réseau Internet	241
2.1.4	Binding order	246
2.2	Domaine Active Directory	247
2.2.1	Flux réseau nécessaires	247
2.2.2	Réduire la plage de ports	249
2.2.3	Read Only Domain Controller	249
2.2.4	Autres ports	250
2.3	Certificats	250
2.3.1	IPSec	250

Chapitre 7

Aller plus loin avec DirectAccess

1. Introduction	315
2. Simuler Internet sur un environnement de maquette	315
2.1 Configuration de la machine virtuelle "Simulation Internet"	316
2.1.1 Configuration des rôles ADCS et DNS	316
2.1.2 Configuration du rôle DHCP	327
2.1.3 Configuration du rôle Routage et accès distant	330
2.2 Intégration de la machine virtuelle dans la maquette	331
2.3 NCSI	332
2.4 Synthèse	334
3. Pare-feu	335
3.1 Sur le poste client	335
3.2 Sur le serveur UAG	338
3.3 En amont du serveur DirectAccess/UAG	339
3.4 En aval du serveur DirectAccess/UAG	339
3.5 La DMZ a-t-elle un sens en IPv6 ?	342
3.6 Rupture de protocole avec ISATAP	343
3.7 Synthèse	344
4. Sécurisation UAG	344
4.1 Security Configuration Wizard	344
4.2 Antivirus sur UAG	346
4.3 Les correctifs et les Services Pack UAG/TMG	349
4.3.1 Windows Update	349
4.3.2 TMG	351
4.3.3 UAG	351
4.4 Synthèse	352
5. DirectAccess Connectivity Assistant	352
5.1 Configuration avec Forefront UAG 2010 SP1	354
5.2 Configuration avec Windows Server 2008 R2	358
5.3 Synthèse	360

Annexe

Aller plus loin avec UAG

1. Introduction	491
2. Création d'un portail UAG.....	492
2.1 Web Monitor	502
2.1.1 Création de la publication du Web Monitor.....	502
2.1.2 Section DirectAccess du Web Monitor.....	505
2.2 Fonctionnalités limitées du client Lync	507
2.3 Publication des services Lync.....	510
2.3.1 Création de l'écouteur Web	510
2.3.2 Mise en œuvre de la publication	515
2.3.3 Tests basiques de vérifications	525
3. Bonnes pratiques.....	527
3.1 Environnement de test.....	527
3.1.1 Connectivité Internet.....	527
3.1.2 Test d'accès	528
3.2 Performances.....	528
3.3 Sécurité	528
4. Conclusion	529
Index	531

Benoît SAUTIERE est leader technique spécialiste en infrastructure d'annuaire Active Directory et sécurité des infrastructures. C'est à ce titre qu'il a été reconnu Microsoft MVP (Most Valuable Professional) sur le domaine Enterprise Security. Dans le cadre de ses missions régulières il intervient sur des projets de refonte d'infrastructure d'annuaire ainsi que sur des projets DirectAccess.

Lionel LEPELIER est un spécialiste de la sécurité des infrastructures Microsoft. C'est à ce titre qu'il a été reconnu Microsoft MVP (Most Valuable Professional) sur le domaine Forefront. Il intervient régulièrement sur des projets de protection d'infrastructures de messagerie et d'accès itinérants ainsi que sur des projets DirectAccess.

Benoît SAUTIERE et Lionel LEPELIER ont collaboré à plusieurs éditions des Techdays de Microsoft pour promouvoir DirectAccess et la gamme de produits Microsoft Forefront. Ils connaissent parfaitement les attentes des informaticiens sur ce type de projet et proposent un livre réellement opérationnel avec une démarche progressive aboutissant à la mise en production de la solution DirectAccess.

ISBN 978-2-7460-7112-4



9 782746 071124

€ 39,56

AU 1 01 13

€ 39,00



www.editions-eni.fr

DirectAccess

Mobilité et nomadisme

Mise en œuvre de la solution Microsoft

Ce livre sur DirectAccess s'adresse à tous les intervenants d'un projet DirectAccess (les **équipes réseau, système, support**) ainsi qu'au **responsable du projet**. Cette fonctionnalité native de Windows Server 2008 R2 et Windows 7 Enterprise ou Ultimate révolutionne l'expérience de la mobilité pour l'utilisateur final. Les auteurs accompagnent le lecteur dans la mise en œuvre depuis la **phase de maquettage** jusqu'à la **mise en production** et le **transfert d'expertise** aux exploitants.

Avant de rentrer dans le vif du sujet technique, le premier chapitre s'attachera à répondre à un certain nombre d'interrogations autour de DirectAccess et à présenter **les différents scénarios d'usage**. Le second chapitre fournira **les détails techniques sur DirectAccess** en analysant chaque composant impliqué et les relations entre eux. Le troisième chapitre sera dédié à **l'utilisation d'IPv6** dans DirectAccess. À ce stade de l'ouvrage, nous nous attaquerons à la pratique de **DirectAccess dans le cadre d'un projet**; le quatrième chapitre traitera les aspects techniques et le cinquième se focalisera sur l'aspect purement projet (les intervenants, les attentes, les pièges à éviter). La **mise en œuvre sera détaillée et optimisée** dans les chapitres 6 et 7. Le dernier chapitre sera dédié à **l'exploitation** des plateformes DirectAccess et au **dépannage des clients nomades** et s'adressera donc aux exploitants.

Au terme de cet ouvrage le lecteur aura une vue complète d'un projet DirectAccess. **Horizon Education** maquette opérationnelle.

Des éléments de ce livre sont en téléchargement sur le site www.editions-eni.fr



9782746071124

Les ch DIRECTACCESS - M BOUM

Avant-propos • DirectAccess pour quoi faire ? • L'assemblage des technologies • IPv6 • Les choix d'architectures • L'approche projet • Mise en œuvre de DirectAccess • Aller plus loin avec DirectAccess • Exploitation de la plateforme DirectAccess • Aller plus loin avec UAG



Sur www.editions-eni.fr :

- Informations complémentaires sur DirectAccess sous Windows 8.
- Webographie.

Collection
EXPERT IT