Microsoft Forefront UAG 2010 SP1

Mise en œuvre d'une plateforme DirectAccess pas à pas -DirectAccess

Advanced architecture and Design for DirectAccess



Version 1.2

lundi, 6 juin 2011

Rédigé par benoits@exakis.com MVP Enterprise Security 2010 Benoits@exakis.com



© 2009 Microsoft Corporation. All rights reserved. *MICROSOFT CONFIDENTIAL – FOR INTERNAL USE ONLY*. The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication and is subject to change at any time without notice to you. This document and its contents are provided AS IS without warranty of any kind, and should not be interpreted as an offer or commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The descriptions of other companies' products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

We will not knowingly provide advice that conflicts with local, regional, or international laws, however, it is your responsibility to confirm your implementation of our advice is in accordance with all applicable laws.



Fiche de révision et de signature

Historique des versions

Date	Auteur	Version	Modification
16/01/2011	Benoît SAUTIERE	1.2	Corrections mineures
20/11/2010	Benoît SAUTIERE	1.1	Découpage en parties
06/11/2010	Benoît SAUTIERE	1.0	Création du document

Relecteur

Nom	Version approuvée	Fonction	Date
Benoît SAUTIERE	1.2	MVP Entreprise Security	16/01/2011
Benoît SAUTIERE	1.1	MVP Entreprise Security	20/11/2010
Benoît SAUTIERE	1.0	MVP Entreprise Security	06/11/2010



Sommaire

8	Cor	nfiguration de DirectAccess	. 3
	8.1	Paramétrage coté client de DirectAccess	.4
	8.2	Paramétrage coté serveur de DirectAccess	. 8
	8.3	Paramétrage de la Name Resolution Policy Table	12
	8.4	Checklist de bon fonctionnement	16
9	Qu'	'est ce qui a changé	18



8 **CONFIGURATION DE DIRECTACCESS**

Passons maintenant au plat de résistance avec la configuration de DirectAccess. Tout se passera dans l'interface de configuration d'UAG avec une collection d'interfaces de configuration. Pour éviter de se poser des questions en cours de route, le tableau suivant résume les choix de déploiement qui seront mis en œuvre :

Configuration à mettre en œuvre	Valeur
Scénario de déploiement	Autoriser les clients DirectAccess à se connecter au réseau interne et activer la gestion à distance des clients DirectAccess.
Localisation des clients	Dans le domaine corp.contoso.com
Liaison des stratégies de groupe	A la racine du domaine
Identification des clients DirectAccess	Dans le conteneur « Workstations » localisé à la racine du domaine
Configuration du DirectAccess Connectivity Wizard	Oui
Autoriser les clients à utiliser la résolution de noms DNS locale	Oui
Indicateur de connectivité du DAC	http://app1.corp.contoso.com
Portail à présenter à l'utilisateur en cas de défaillance DirectAccess	http://www.contoso.com/troubleshooting
Nom du portail	Portail d'assistance
Adresse de messagerie du support	Administrateur@contoso.com
Première adresse IPv4 publique	131.107.0.2
Adresse IPv4 privée	192.168.0.1
Identification du certificat IP-HTTPS	Friendly name « IP-HTTPS »
Autorité de certification interne	DC1.CORP.CONTOSO.COM
Authentification double facteur	Non
Prise en charge de NAP avec DirectAccess	Oui
Mode de mise en œuvre de NAP	Monitoring mode
Localisation du serveur HRA	Sur le serveur UAG
URL de dépannage NAP	http://www.contoso.com/troubleshooting.htm
Autorité de certification délivrant les certificats System « Health Authentication »	DC1.CORP.CONTOSO.COM\CORP-DC1-CA.
Gabarit de certificats pour NAP	System Health Authentication



Gestion des flux en partance du poste client	Split Tunneling
Localisation des serveurs UAG	Servers\UAGDA
Network Location Server	https://nls.corp.contoso.com
Méthode de résolution des noms locaux	Fallback to local name resolution
Mode d'accès au réseau interne	End-to-Edge

8.1 Paramétrage coté client de DirectAccess

La première étape de la configuration, c'est l'identification des clients pour lesquels DirectAccess devra être activé, le niveau d'accès de ces clients au système d'information et enfin la configuration optionnelle du DAC. Le DirectAccess Security Configuration Wizard est une interface utilisateur permettant à celui-ci d'être informé de l'état de fonctionnement de DirectAccess. C'est la partie la plus simple de la configuration de DirectAccess.





Clients and GPOs Configuration Clients and GPOs Deployment Model Client Domains Policy Management Client Groups	Solution So	On va conserver la configuration par défaut. Par rapport à la RTM d'UAG, il y a tout de même subtilité. Il n'est plus besoin de configurer la gestion des clients en situation de mobilité. Les exceptions de pare-feu sont déjà intégrées.
Clients and GPOs Configuration Clients and GPOs Deployment Model Client Domains Policy Management Client Groups	Specify the domains in which the client computers allowed to connect using Forefront UAG DirectAccess reside. Policy settings contained in the UAG DirectAccess clients Group Policy object (GPO) will be applied to these computers. Table Corp contoso.com	Par défaut, UAG va positionner la stratégie de groupe de configuration des postes clients dans un seul domaine. Il est donc possible de déployer UAG/DirectAccess dans un scénario de forêt de ressources.
Clients and GPOs Configuration Clients and GPOs Deployment Model Client Domains Policy Management Client Groups	Se Configuration Forefront UAG uses Group Policy Objects (GPOs) to deliver UAG DirectAccess policy settings to client computers, the UAG DirectAccess server, and application servers: UAG DirectAccess can create the GPOs automatically, or you can save policy settings to existing GPOs you have designated for DirectAccess. Automatically generate the following GPOs for DirectAccess policies: GPO Name GPO Name GPO Name Generate the following GPOs for DirectAccess policies: Modify_ Modify_ Save the UAG DirectAccess settings to these existing GPOs: GPO Name Gateway Application Servers Application Se	Dans la version RTM d'UAG, on n'avait pas la possibilité de configurer la liaison des stratégies de groupe. Ici encore, il sera possible de positionner le serveur UAG et les serveurs de ressources dans des forêts distinctes.



Clients and GPOS Conf	iguration 💌	
Deployment Model Client Domains Policy Management Client Groups	From the client computer domains, select organizational units (OU) or security groups containing clients that will be allowed to connect using UAG DirectAccess. Client GPO policy settings are applied to these DirectAccess clients based ore: © Security groups © Organizational units (OU) Bable DirectAccess for clients in these OUs or security groups:	Dans la version RTM, le filtrage s'effectuait uniquement par rapport à l'appartenance à un groupe. Avec le SP1, on peut maintenant filtrer par rapport à un conteneur organisationnel.
Elsosge Time	Access Gateway Management de	On en a fini avec la configuration obligatoire coté client, passons maintenant aux paramétrages optionnels.
Clients and GPOs Conf Client Connectivity Connection Verification Troubleshooting Portal Diagnostic Logging	A specify connectivity and troubleshooting settings for the DirectAccess Connectivity Assistant. Settings are stored in the client GPO, and applied on DirectAccess client computers running the DirectAccess Connectivity Assistant application. Do you want to configure settings for the DirectAccess Connectivity Assistant application? (* Yes, configure application settings) (* No, I do not want to configure application settings at this time	On va configurer le DirectAccess Connectivity Wizard et autoriser l'utilisateur à basculer en résolution de noms locale. L'utilisateur pourra ainsi désactiver DirectAccess si nécessaire. La version 1.5 du client est diponible dans « c:\Program Files\ Microsoft ForeFront Unified Access Gateway\Common\Bin\Da\DA
Learn more	< Back Next > Finish Cancel	С».

Clients and GPOs Configuration	x Assistant Configuration	Le DAC doit être configuré
Client Connectivity Connection Verification Troubleshooting Portal Diagnostic Logging	Select how connectivity between DirectAccess clients and the internal network is automatically verified. When connectivity verification fails, a notification is displayed in the taskbar notification area of the DirectAccess client computer. Connectivity verifiers: Connectivity verifiers: Address Method http://app1.corp.contoso.com HTTP	interne. Dans notre cas, j'ai retenu le site web par défaut hébergé sur le serveur APP1.
	Edit. Remove	En environnement de production, je recommanderai de choisir un autre point de référence, voire même d'en référencer plusieurs.
Learn more	< Back Next > Finish Cancel	
Client Connectivit	y Assistant Configuration	
Client Connectivity Connection Verification Troubleshooting Portal Diagnostic Logging	The DirectAccess client feature notifies users when connectivity is not functioning properly. The notification includes a link to a troubleshooting page. Specify the portal that DirectAccess clients are directed to for troubleshooting: C This UAG portal:	En cas d'indisponibilité, le DAC va informer l'utilisateur
	¥	et le rediriger vers un portail.
	This site (URL): http://www.contoso.com/troubleshooting Example: https://www.contoso.com/troubleshooting Friendly name for URL link: Portail d'assistance	Si on a préalablement configuré le portail UAG, il est même possible de le référencer.
Learn more	< Back Next > Finish Cancel	
Clients and GPOs Configuration	y Assistant Configuration	En cas de défaillance, l'utilisateur peut générer des
Client Connectivity Connection Verification Troubleshooting Portal DiagnosticLogging	With the DirectAccess Connectivity Assistant installed, clients can run diagnostics to collect log information and send it to an e-mail address. You can also specify an additional script to run during diagnostics. Script output is appended to the log file. Send client log files to: administrateur@contoso.com Example: administrator@contoso.com	traces que l'on va envoyer par messagerie à l'équipe de support.
	Specify the path and name of the diagnostics script (optional): Example: C/Windows/System32/DADiag-LIDC_DCA.bat The script should be stored on the DirectAccess client computer in a location that is accessible only with elevated permissions.	ll est même possible d'utiliser un script de diagnostic personnalisé.
Learn more	< <u>B</u> ack <u>Next</u> > <u>Einish</u> Cancel	

8.2 Paramétrage coté serveur de DirectAccess

Deuxième étape, la configuration de DirectAccess à proprement parlé. A ce stade, on va :

- Indiquer à UAG quelle est l'interface interne
- Indiquer à UAG quelle est l'interface externe (avec ses deux adresses IPv4 publiques consécutives)
- Spécifier le certificat qui sera utilisé pour le protocole de transition IP-HTTPS
- Spécifier l'autorité de certification qui sera utilisée pour authentifier les tunnels IPSEC

En option, on va pouvoir :

- Spécifier l'usage de la carte à puce ou d'un dispositif OTP au niveau des tunnels IPSEC
- Intégrer la prise en charge de Network Access Protection au sein de DirectAccess
- Spécifier le mode de gestion des flux sortants au niveau du client DirectAccess
- Spécifier la localisation des serveurs UAG DirectAccess

International Unified Access Gateway Management Image: Method Mesange Help Image: Method Mesange Help Image: Method Mesange Help Image: Mesange Help Image: Mesange Help Image: Mesange: Method Mesange Help Image: Mesange Help Image: Mesange: Method Mesange Help Image: Mesange Help Image: Mesange: Mesange: Mesange Image: Mesange Help Iman: Mesange: Mesange Image: Me	onfiguration du client est ntenant terminée. sons à la configuration erveur.
Apply Policy Epport Policy Activate Disable DirectAccess Message Time Message Type Message Ready Ready	
	ce stade, pas de ngement, il faut indiquer AG quelle est l'interface rne et l'interface externe. oter que comme pour la I, l'interface refusera de rsuivre si les prérequis ont pas respectés.



UAG DirectAccess Server Confid Network Access R NAP Enforcement HRA and NPS NAP Certification Authority	Protection Configuration Forefront UAG DirectAccess can verify the health of client computers using Network Access Protection (NAP) policies located on a Network Policy Server (NPS). Specify how NAP policies are enforced. Use NAP to verify DirectAccess client computers are compliant with network health policies Select the NAP mode used for UAG DirectAccess clients: Monitoring mode. Both compliant and non-compliant DirectAccess clients can connect. Forforcement mode. Only compliant DirectAccess clients can connect. keath	NAP était déjà intégré à la configuration de DirectAccess sauf qu'il fallait intervenir sur la stratégie de groupe coté serveur pour configurer le mode de NAP. Dans notre maquette, nous allons commencer par le mode « Monitoring ».
UAG DirectAccess Server Confid Network Access F NAP Enforcement HRA and NPS NAP Certification Authority	Protection Configuration To verify DirectAccess client health using Network Access Protection (NAP), specify the location of a Health Registration Authority (HRA) server, and a Network Policy Server (NPS). The NPS and HRA roles are installed on this UAG server (UAG configures settings automatically). To use autoremediation to automatically update non-compliant computers Clients can link to this URL for troubleshooting compliance issues (optional): Inttp://www.contoso.com/troubleshooting.htm Example: http://www.contoso.com/troubleshooting.htm The A and NPS are installed on another server (administrator configures settings manually). To or or more HRA servers are not accessible from the Internet.	Dans la version RTM d'UAG, il n'était pas possible d'héberger le rôle « Health Registration Authority » sur le serveur UAG. C'est maintenant possible avec le SP1. En plus, il le configure pour nous !
UAG DirectAccess Server Config Network Access F NAP Enforcement HRA and NPS NAP Certification Authority	Protection Configuration Specify the certification authority (CA) used by the HRA server. The HRA server validates the credentials of a compliant DirectAccess client computer, and obtains a health certificate from the CA on its behalf. Specify the NAP CA server: DCL.corp.contoso.com/corp.DCL-CA Add Remove Image: Select the authenticated compliant certificate template: SystemiticalthAuthentication If you have specified an enterprise CA, you must select a certificate template. < Back	La configuration de NAP implique de désigner l'autorité de certification qui va délivrer les certificats de type System Health Authentication.

UAG RTM ne permettait pas de configurer l'encapsulation ou non des flux en partance du client. Dans notre cas, nous allons conserver le mode par défaut.
Note : Le mode « Force Tunneling » intègre des nouveautés dans le SP1 d'UAG 2010 par rapport à la version RTM.
Tout comme pour les clients, il est possible de filtrer l'application de la stratégie de groupe concernant le ou les serveurs UAG à un conteneur Active Directory précis.

8.3 Paramétrage de la Name Resolution Policy Table

Dans cette troisième étape de la configuration de DirectAccess, on va se focaliser sur le contenu de la « Name Resolution Policy Table ». Pour rappel, cette table référence des suffixes DNS et des hôtes pour lesquels il ne faut pas utiliser la résolution de noms d'hôtes Internet. Pour chaque référence, on peut :

- Spécifier un ou plusieurs serveurs DNS IPv6
- Faire traiter la requête par le mécanisme de transition DNS64/NAT64
- Refuser de traiter la résolution DNS

Pour rappel, notre Network Location Server ne doit pas être accessible depuis Internet. Pour cela l'hôte DNS va être référencé comme refusé à la résolution dans la NRPT. Il est essentiel de bien référencer tous les suffixes DNS référencés dans l'entreprise. Sinon, ils ne pourront pas être adressés depuis l'extérieur.





Infrastructure Server Configure Infrastructure Server Network Location Server DNS Suffixes Authentication Domains Management Servers	tion X ver Configuration Enter the name suffixes and IP addresses of internal DNS servers used to resolve DNS suffix queries. Name Suffix IP address of DNS Server • corp.contos.com (DNS64) • sop.contos.com (Excluded) * Double-click here to add Excluded • only use local name resolution option: • Only use local name resolution if the name does not exist in DNS (most restrictive) • fail back to local name resolution if the name does not exist in DNS or the DNS servers are unreachable when the client computer is on a private network (recommended) • Fail back to local name resolution for any kind of DNS resolution error (least secure)	On constate bien la présence de l'exception ainsi que de la prise en charge du suffixe DNS pour la zone DNS relative au domaine Active Directory.
Infrastructure Server Configura Infrastructure Server DNS Suffixes Authentication Domains Management Servers	tion ▼ Ver Configuration Specify the domains that contain user accounts of clients connecting using DirectAccess. Also, specify any domains containing management servers that require DirectAccess clients to authenticate using Kerberos. O Domain controllers in the specified domains are automatically added to the management servers list. Eatable DirectAccess for user accounts in these domains: I Client Domains Add. Remove	A ce stade, il est possible de spécifier les domaines Active Directory additionnels à prendre en charge, aussi bien pour les clients que les ressources auxquels ils accèdent.
Infrastructure Server Configura Infrastructure Ser Network Location Server DNS Suffixes Authentication Domains Management Servers	tion ver Configuration DirectAccess management servers provide services to DirectAccess clients. Add internal management servers to discoverable built-in groups, and user-defined groups. Image: Configuration of the server of the serv	Nouveauté d'UAG 2010 SP1, la détection automatique des contrôleurs de domaine et « Health Registration Authority », à condition qu'ils soient localisés dans le même domaine que le serveur UAG.

Sumfrastructure Server Configura	tion X	
Network Location Server DNS Suffixes Authentication Domains Management Servers	Discoverable groups were last refreshed on Wednesday, October 27, 2010 1037 PM.	Déclarer le serveur HRA est essentiel car il doit être accessible par le client dans le tunnel infrastructure, donc avant l'ouverture de session.
Learn more		
The view Adm Messages hep	Arron 1 d Access Gateway 2020 UAG DirectAccess front d Access Gateway 2020 UAG DirectAccess for this page to enable and configure UAG DirectAccess for your organization d teck UAG dedivormet and alternang guides Step 3 Step 1 Step 2 Clients and GPOS Learning: DirectAccess Server policies for the UAG DirectAccess Server. Lient Ministructure alternation and management server. a setting: DirectAccess Server policies for the UAG DirectAccess Server. Internation Configure on the UAG DirectAccess Server. Set Pai Access Learning Server. a setting: Direct Turneting Server. Extend to Access Learn more Learning Extend to Access Learn more Learning policies for the UAG DirectAccess Extend to Access Learn more Learning Extend to Access Learn more Learning policies for the UAG DirectAccess Extend to Access Learn more Learning Extend to Access Learn more Learning policies for the UAG DirectAccess Extend to Access Learning Extend to Access Learn more Learning	This the end, …
End-to-End Authentic End-to-End Authentic By default, traffic between using IPsec. You can also applications servers. Authenticate traffic between Select the security grown Select the security grown You can edit the encry and the application s Edit IPSec cryptograp	Authentication and Encryption Configuration A DirectAccess clients and the UAG DirectAccess server is authenticated and encrypted authenticate and encrypt traffic between DirectAccess clients and selected internal etween DirectAccess clients and selected application servers: Add Remove uption settings for traffic between DirectAccess clients ervers. Hy settings	Presque car cette étape de configuration est optionnelle. Par défaut, le déploiement s'effectue en mode « End-to- Edge », ce qui signifie que l'utilisateur a accès à l'intégralité du réseau car son ou ses tunnels se terminent sur le serveur UAG.





8.4 Checklist de bon fonctionnement

Configurer DirectAccess est certes un challenge. Maintenant, il faut que cela fonctionne. Pour cela, on va travailler à plusieurs niveaux :

- La console « UAG Activation Monitor » pour suivre l'état d'avancement de la configuration d'UAG
- La « Web Console » pour suivre l'état de santé du serveur UAG et des composants impliqués
- La « Web Console » pour suivre les sessions
- Le Snapin PowerShell livré avec UAG 2010 SP1
- La console « Pare-Feu avancé » du système d'exploitation pour suivre l'établissement des tunnels IPSEC

		Impression écran		Description
Forefront Unified Access G Refresh Options UAG Aray Members VAG1	Severity State State Information Information Information Debugging Debugging Debugging Information Information Information Information	Message Validating configuration settings. Starting activation. Configuring NLB settings. NLB settings were configured successfully. Configuring NLB settings. NLB settings were configured successfully. Configuring the frewall. Allowing outgoing TCP connection for 192.168.0.150002. Allowing outgoing TCP connection for 131.107.0.250002. Allowing outgoing TCP connection for 131.107.0.250002. Allowing outgoing TCP connection for 131.107.0.250002. The frewal was configured successfully. Configuring SSL Network Tunneling (SSTP). The SSL Network Tunneling (SSTP).	ccessfully.	La console « UAG Activation Monitor » permet de suivre l'état d'activation de notre serveur UAG. Notre serveur est bien activé mais on n'en sait pas plus.
Vindows Firewall with Advant File Acton Vew Help Windows Firewall with Advanced Chrobund Rules Outbound Rules Connection Security Rule Monitoring Firewall Connection Security Rule Security Associations Wan Mode Quick Mode	Information State Debugging I I I I I I I I I I I I I I I I I I I	Activating Network Connector. Writing the configuration files. Writing the file [C:\Program Files\Microsoft Forefront Unified Acc rity Rules Profile Endpoint 1 Endpoint 2 as Gateway - Clents Access Privat 2002;836b Any ss Gateway - Clents Corp Tu Privat 2002;836b Any	ess Gateway\von\conf\Repoter xr Actions Connection Security Rules Refresh Export List., Refresh Help	On doit pouvoir constater la présence de règles IPSEC actives dans la console de pare-feu du serveur UAG 2010. La stratégie de groupe a bien été prise en charge par notre serveur.
<u> </u>				



9 QU'EST CE QUI A CHANGE

La question est vaste. Coté serveur UAG, le script de configuration a effectué beaucoup de travail :

- Configuration du serveur UAG comme routeur ISATAP propageant un préfixe IPv6 dans l'organisation
- Configuration du serveur UAG comme routeur IPv6
- Configuration du serveur UAG comme routeur 6to4
- Configuration du serveur UAG comme relai et routeur Teredo
- Configuration du serveur UAG comme routeur IP-HTTPS
- Configuration du HRA sur le site web d'UAG
- Création d'une stratégie de groupe pour la configuration des clients DirectAccess
- Création d'une stratégie de groupe pour la configuration des serveurs UAG



Impression écran	Description
Administrator: Command Prompt Microsoft Windows [Version 6.1.7600] Copyright (c) 2009 Microsoft Corporation. All rights reserved. C:\Users\administrator.CORP>ipconfig Windows IP Configuration Ethernet adapter Local Area Connection* 9: Media State Media disconnected Connection-specific DNS Suffix .: Ethernet adapter LAN: Connection-specific DNS Suffix .: corp.contoso.com Link-local IPv6 Address	Coté UAG, on pourrait penser que rien n'a changé. On ne constate même pas d'adresses IPv6 ?



Administrator: Command Prompt				
Tunnel adapter 6TO4 Adapter:	Ben non, on a bien plusieurs interfaces (6to4, Teredo, IP- HTTPS). Certaines interfaces sont désactivées car non nécessaires. C'est donc			
Connection-specific DNS Suffix .: contoso.com IPv6 Address				
Tunnel adapter Teredo Tunneling Pseudo-Interface:				
Connection-specific DNS Suffix .: Link-local IPv6 Address : fe80::8000:f227:7c94:fffdx15 Default Gateway :				
Tunnel adapter isatap.contoso.com:				
Connection-specific DNS Suffix .: contoso.com Link-local IPv6 Address : fe80::200:5efe:131.107.0.2x16 Link-local IPv6 Address : fe80::200:5efe:131.107.0.3x16 Default Gateway :				
Tunnel adapter isatap.corp.contoso.com:	normal d'avoir une interface			
Connection-specific DNS Suffix .: corp.contoso.com IPv6 Address	ISATAP désactivée coté Internet.			
Tunnel adapter IPHTTPSInterface:				
Connection-specific DNS Suffix .: IPv6 Address				
Tunnel adapter isatap.{DED4B6DC-A20D-421C-8F9B-A3081C6F7F91}:				
Media State				
C:\Users\administrator.CORP>				
Administrator Command Promot				
Administrator: Command Prompt				
Administrator: Command Prompt C:\Users\Administrator>>ipconfig /all Hindows IB Configuration				
Administrator: Command Prompt C:\Users\Administrator>ipconfig /all Windows IP Configuration Host Name				
Image: State Stat	Coté contrôleur de domaine, on constate la présence			
Image: State Stat	Coté contrôleur de domaine, on constate la présence d'une interface ISATAP qui			
Administrator: Command Prompt C:\Users\Administrator>ipconfig /all Windows IP Configuration Host Name	Coté contrôleur de domaine, on constate la présence d'une interface ISATAP qui s'est automatiquement			
Administrator: Command Prompt C:\Users\Administrator>ipconfig /all Windows IP Configuration Host Name	Coté contrôleur de domaine, on constate la présence d'une interface ISATAP qui s'est automatiquement configurée.			
Administrator: Command Prompt C:\Users\Administrator>ipconfig /all Windows IP Configuration Host Name Corp.contoso.com Node Type	Coté contrôleur de domaine, on constate la présence d'une interface ISATAP qui s'est automatiquement configurée.			
Administrator: Command Prompt	Coté contrôleur de domaine, on constate la présence d'une interface ISATAP qui s'est automatiquement configurée.			
Administrator: Command Prompt C:\Users\Administrator>ipconfig /all Windows IP Configuration Host Name	Coté contrôleur de domaine, on constate la présence d'une interface ISATAP qui s'est automatiquement configurée. Si nécessaire on dispose de			
Standaministrator: Command Prompt C:\Users\Administrator>ipconfig /all Windows IP Configuration Host Name	Coté contrôleur de domaine, on constate la présence d'une interface ISATAP qui s'est automatiquement configurée. Si nécessaire on dispose de la commande « SC.EXE			
<pre>Standministrator: Command Prompt C:\Users\Administrator>ipconfig /all Windows IP Configuration Host Name Corp.contoso.com Node Type</pre>	Coté contrôleur de domaine, on constate la présence d'une interface ISATAP qui s'est automatiquement configurée. Si nécessaire on dispose de la commande « SC.EXE CONTROL IPHLPSVC			
Standministrator: Command Prompt X C:\Users\Administrator>ipconfig /all Windows IP Configuration Host Name	Coté contrôleur de domaine, on constate la présence d'une interface ISATAP qui s'est automatiquement configurée. Si nécessaire on dispose de la commande « SC.EXE CONTROL IPHLPSVC PARAMCHANGE » pour			
Administrator: Command Prompt C:\Users\Administrator>ipconfig /all Windows IP Configuration Host Name Corp.contoso.com Mode Type	Coté contrôleur de domaine, on constate la présence d'une interface ISATAP qui s'est automatiquement configurée. Si nécessaire on dispose de la commande « SC.EXE CONTROL IPHLPSVC PARAMCHANGE » pour actualiser le paramétrage			
Standministrator: Command Prompt C:\Users\Administrator>ipconfig /all Windows IP Configuration Host Name	Coté contrôleur de domaine, on constate la présence d'une interface ISATAP qui s'est automatiquement configurée. Si nécessaire on dispose de la commande « SC.EXE CONTROL IPHLPSVC PARAMCHANGE » pour actualiser le paramétrage IPv6 d'un système			
<pre>C: Administrator: Command Prompt C: \Users\Administrator>ipconfig /all Windows IP Configuration Host Name Corp.contoso.com Node Type</pre>	Coté contrôleur de domaine, on constate la présence d'une interface ISATAP qui s'est automatiquement configurée. Si nécessaire on dispose de la commande « SC.EXE CONTROL IPHLPSVC PARAMCHANGE » pour actualiser le paramétrage IPv6 d'un système d'exploitation.			
<pre>C:\Administrator:Command Prompt C:\Users\Administrator>ipconfig /all Vindows IP Configuration Host Name</pre>	Coté contrôleur de domaine, on constate la présence d'une interface ISATAP qui s'est automatiquement configurée. Si nécessaire on dispose de la commande « SC.EXE CONTROL IPHLPSVC PARAMCHANGE » pour actualiser le paramétrage IPv6 d'un système d'exploitation.			
<pre>S. Administrator: Command Prompt C:\Users\Administrator>ipconfig /all Windows IP Configuration Host Name</pre>	Coté contrôleur de domaine, on constate la présence d'une interface ISATAP qui s'est automatiquement configurée. Si nécessaire on dispose de la commande « SC.EXE CONTROL IPHLPSVC PARAMCHANGE » pour actualiser le paramétrage IPv6 d'un système d'exploitation.			
C: Administrator: Command Prompt C: \Users\Administrator>ipconfig /all Windows IP Configuration Host Name	Coté contrôleur de domaine, on constate la présence d'une interface ISATAP qui s'est automatiquement configurée. Si nécessaire on dispose de la commande « SC.EXE CONTROL IPHLPSVC PARAMCHANGE » pour actualiser le paramétrage IPv6 d'un système d'exploitation.			



Tunnel adapter isatap.internet.fr: Media State	Administrator: C:\Windows\system32\cmd.exe	
Media State	Tunnel adapter isatap.internet.fr:	
Tunnel adapter 6104 Adapter: Connection-specific DNS Suffix : : internet.fr Description	Media State Media disconnected Connection-specific DNS Suffix . : internet.fr Description	
Connection-specific DNS Suffix : internet.fr Description	Tunnel adapter 6T04 Adapter:	
Tunnel adapter iphttpsinterface: 6to4, Teredo, IP-HTTPS). Media State	Connection-specific DNS Suffix .: internet.fr Description : Microsoft 6to4 Adapter Physical Address : 00-00-00-00-00-00-00-E0 DHCP Enabled : No Autoconfiguration Enabled : Yes IPv6 Address : 2002:836b:65::836b:65(Pref Default Gateway : 2002:836b:2::836b:2 DNS Servers : 131.107.0.1 NetBIOS over Tcpip : Disabled	Coté client, même combat. On retrouve les mêmes interfaces IPv6 (ISATAP,
Media State Media disconnected Connection-specific DNS Suffix iphttpsinterface Physical Address 00-00-00-00-00-00-00 DHCP Enabled Runnel adapter Teredo Tunneling Pseudo-Interface: Connection-specific DNS Suffix Connection-specific DNS Suffix : Description Physical Address McConfiguration Enabled McConfiguration Enabled Description Physical Address MCP Enabled McConfiguration Enabled IPv6 Address IPv6 Address Physical I Gadeway	Tunnel adapter iphttpsinterface:	6to4, Teredo, IP-HTTPS).
Tunnel adapter Teredo Tunneling Pseudo-Interface: Connection-specific DNS Suffix .: Description Teredo Tunneling Pseudo-Interface Physical Address	Media State Media disconnected Connection-specific DNS Suffix . : Description : iphttpsinterface Physical Address 00-00-00-00-00-00-E0 DHCP Enabled No Autoconfiguration Enabled Yes	Cependant, certaines sont désactivées car inutiles dans la situation présente.
Connection-specific DNS Suffix : Description	Tunnel adapter Teredo Tunneling Pseudo-Interface:	
NetBIOS over Tcpip : Disabled C:\Users\administrator>	Connection-specific DNS Suffix .: Description	iterface)4:ff9a(Preferre .6(Preferred)
C:\Users\administrator>	NetBIOS over Tcpip : Disabled	
	C:\Users\administrator>	T

Voilà pour les bases du DirectAccess. Pour les plus téméraires, il reste la conclusion ainsi que les possibilités pour améliorer la solution.

