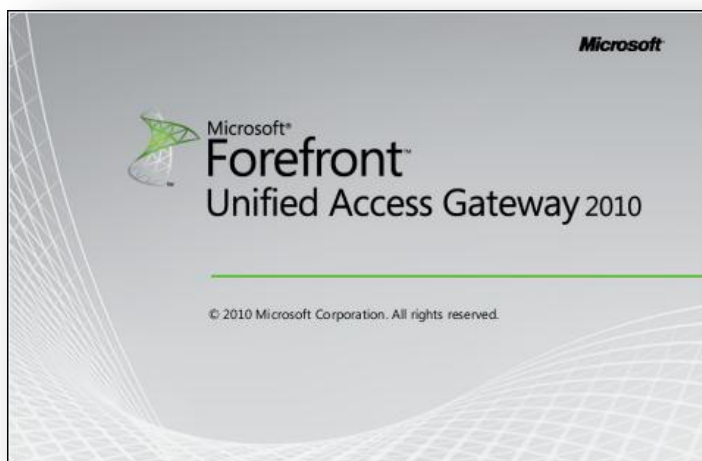


Microsoft Forefront UAG 2010 SP1

Mise en œuvre d'une plateforme DirectAccess pas à pas Pour aller plus loin

Advanced architecture and Design for DirectAccess



lundi, 6 juin 2011

Version 1.2

Rédigé par

benoits@exakis.com

MVP Enterprise Security 2010

Benois@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 Enterprise Security	16/01/2011
Benoît SAUTIERE	1.1	MVP Enterprise Security	20/11/2010
Benoît SAUTIERE	1.0	MVP Enterprise Security	06/11/2010

Sommaire

10	<i>Encore un peu plus ?</i>	3
10.1	Vérifier le bon fonctionnement de NAP	3
10.2	Exploitation des logs en PowerShell	5
10.3	Sécurisation du serveur UAG	6
10.4	Problème de RPC	6
10.5	UAG Best Practices Analyzer (UAGBPA)	7
10.6	La haute disponibilité.....	8
10.7	Gérer la défaillance	8
10.8	Le NAP avancé.....	9
11	<i>Conclusion</i>	10

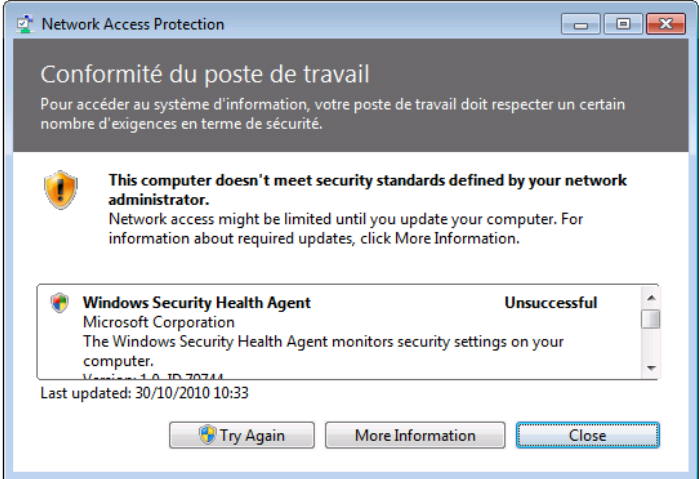


10 ENCORE UN PEU PLUS ?


Maintenant que vous avez lu ce dossier et peut-être même mis en œuvre les étapes décrites, vous voilà presque expert ☺ ! Sachez tout de même que les explications données ici sont prévues pour une maquette de présentation et non de la production. Certains aspects de sécurité ne sont pas abordés.

10.1 Vérifier le bon fonctionnement de NAP

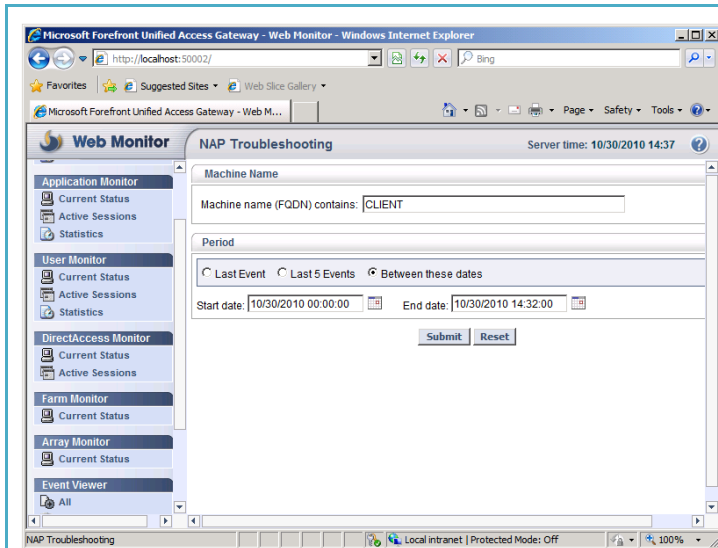
Avec la version RTM, on disposait déjà d'un certain niveau d'intégration avec Network Access Protection. Cependant, il manquait un module de monitoring, module qui est disponible dans la « Web Console » d'UAG 2010 SP1. A noter que les informations relatives aux sessions DirectAccess et Network Access Protection sont consignées dans la base de données SQL Server d'UAG 2010 SP1.



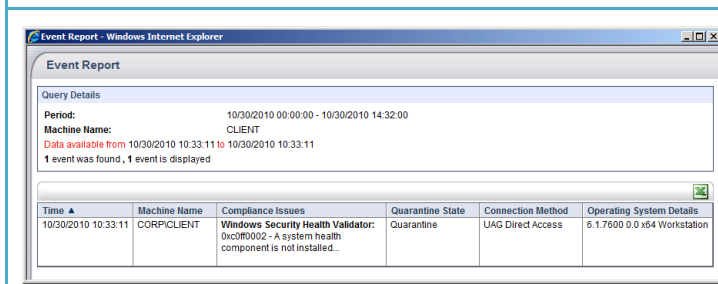
Coté client, la commande « NAPSTAT.EXE » permet d'afficher l'état de santé du poste de travail.



Coté serveur UAG, on peut localiser dans le journal d'évènement « Système » les autorisations et refus du HRA.



Plus simplement, on peut collecter et accéder à ces informations au travers de la « Web Console ».



Il est donc plus facile de suivre ces événements et les exporter vers Excel.

Les journaux de Threat Management Gateway permettent de suivre :

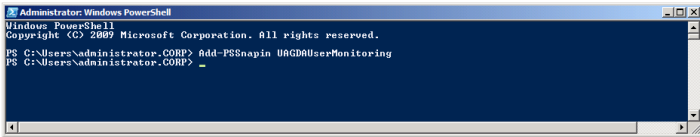
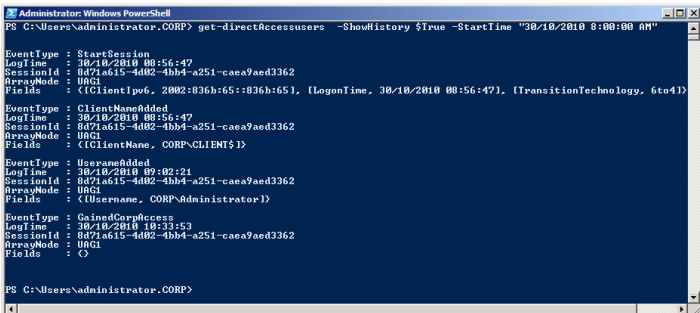


- **L'établissement des sessions IPSEC**
- **La connectivité au réseau interne**
- **L'état de santé**

Ces journaux sont stockés dans la base de données SQL Server de TMG.

10.2 Exploitation des logs en PowerShell

Le Snapin PowerShell pour le Monitoring existait déjà dans la version RTM. Subtilité de la version du SP1. Celui-ci se base maintenant sur les informations relatives aux sessions IPSEC enregistrées dans la base de données de TMG et non plus uniquement sur les sessions journalisées dans le journal de sécurité.

Impression d'écran	Description
 <pre> Administrator: Command Prompt C:\Windows\Microsoft.NET\Framework64\v2.0.50727>InstallUtil.exe "c:\Program Files\Microsoft Forefront Unified Access Gateway\common\bin\da\monitoring\DAUserMonitoringSnapIn.dll" Microsoft (R) .NET Framework Installation utility Version 2.0.50727.4927 Copyright (c) Microsoft Corporation. All rights reserved. Running a transacted installation. Beginning the Install phase of the installation. See the contents of the log file for the c:\Program Files\Microsoft Forefront Unified Access Gateway\common\bin\da\monitoring\DAUserMonitoringSnapIn.dll assembly's progress. The file is located at c:\Program Files\Microsoft Forefront Unified Access Gateway\common\bin\da\monitoring\DAUserMonitoringSnapIn.InstallLog. Installing assembly 'c:\Program Files\Microsoft Forefront Unified Access Gateway\common\bin\da\monitoring\DAUserMonitoringSnapIn.dll'. Affected parameters are: assemblypath = c:\Program Files\Microsoft Forefront Unified Access Gateway\common\bin\da\monitoring\DAUserMonitoringSnapIn.dll logfile = c:\Program Files\Microsoft Forefront Unified Access Gateway\common\bin\da\monitoring\DAUserMonitoringSnapIn.InstallLog logtoconsole = The Install phase completed successfully, and the Commit phase is beginning. See the contents of the log file for the c:\Program Files\Microsoft Forefront Unified Access Gateway\common\bin\da\monitoring\DAUserMonitoringSnapIn.dll assembly's progress. The file is located at c:\Program Files\Microsoft Forefront Unified Access Gateway\common\bin\da\monitoring\DAUserMonitoringSnapIn.InstallLog. Committing assembly 'c:\Program Files\Microsoft Forefront Unified Access Gateway\common\bin\da\monitoring\DAUserMonitoringSnapIn.dll'. Affected parameters are: assemblypath = c:\Program Files\Microsoft Forefront Unified Access Gateway\common\bin\da\monitoring\DAUserMonitoringSnapIn.dll logfile = c:\Program Files\Microsoft Forefront Unified Access Gateway\common\bin\da\monitoring\DAUserMonitoringSnapIn.InstallLog logtoconsole = The Commit phase completed successfully. The transacted install has completed. C:\Windows\Microsoft.NET\Framework64\v2.0.50727> </pre>	<p>N'étant pas installé par défaut, le Snapin Powershell doit être préalable déclaré.</p>
 <pre> Administrator: Windows PowerShell Windows PowerShell Copyright (C) 2009 Microsoft Corporation. All rights reserved. PS C:\Users\Administrator\CORP> Add-PSSnapin UAGDAUserMonitoring PS C:\Users\Administrator\CORP> _ </pre>	<p>Une fois installé, il ne reste plus qu'à importer le Snapin « UAGDAUserMonitoring ».</p>
 <pre> Administrator: Windows PowerShell PS C:\Users\Administrator\CORP> get-directaccessusers -ShowHistory \$true -StartTime "30/10/2010 8:00:00 AM" Event Type : StartSession Log Time : 30/10/2010 08:56:47 Session Id : 8471a615-4d82-4bb4-a251-cae9aed3362 Appx Mode : UAG1 Fields : (ClientIp6, 2002:836b:65::836b:65), (LogonTime, 30/10/2010 08:56:47), (TransitionTechnology, 6to4) Event Type : ClientNameAdded Log Time : 30/10/2010 08:56:47 Session Id : 8471a615-4d82-4bb4-a251-cae9aed3362 Appx Mode : UAG1 Fields : (ClientName, CORP\CLIENT\$1) Event Type : UsernameAdded Log Time : 30/10/2010 09:02:24 Session Id : 8471a615-4d82-4bb4-a251-cae9aed3362 Appx Mode : UAG1 Fields : (Username, CORP\Administrator) Event Type : GainedCompAccess Log Time : 30/10/2010 10:33:53 Session Id : 8471a615-4d82-4bb4-a251-cae9aed3362 Appx Mode : UAG1 Fields : () PS C:\Users\Administrator\CORP> </pre>	<p>Le « Snapin » ne propose qu'un seul « CommandLet » : Get-DirectAccessUsers. Nouveauté du SP1, on peut maintenant avoir l'historique basé sur les négociations de tunnels IPSEC machine et utilisateur.</p>

10.3 Sécurisation du serveur UAG

Depuis Windows 2003 SP1, le système d'exploitation dispose d'un module « Security Configuration Wizard ». Celui-ci permet de sécuriser un système d'exploitation mis en œuvre dans un scénario donné. Toutes les équipes produits ont livré leur fichier XML de description de configuration, l'équipe UAG n'échappe pas à la règle, c'est disponible à l'adresse suivante : <http://www.microsoft.com/downloads/en/details.aspx?FamilyID=120C81D5-B4D5-40C1-9213-20FE957C2B8F>. Le processus de sécurisation va :

- Définir l'état des services et leur mode de démarrage
- Imposer la signature des communications SMB
- Imposer NTLMv2 pour la communication cotée client
- Positionner des permissions sur le système de fichiers NTFS et le registre



Attention, la sécurisation peut avoir un impact sur d'autres services mutualisés sur ce serveur UAG.

Les informations complémentaires concernant la sécurisation d'UAG 2010 sont disponibles à cette adresse : <http://technet.microsoft.com/en-us/library/ee861146.aspx>.

10.4 Problème de RPC

UAG 2010 est déjà bien sécurisé par défaut, parfois même trop. Il en arrive même à bloquer certains mécanismes du système d'exploitation, à savoir les RPC. Les certificats présents sur notre serveur UAG, expireront un jour. Le système d'exploitation va tenter de les renouveler avant expiration. Problème, lors du renouvellement, on tombera sur une erreur RPC que l'on peut reproduire dans la console de certificats.



Ce mécanisme repose sur DCOM qui repose lui-même sur les RPC. Le problème se trouve bien au niveau des RPC mais plus précisément au niveau de la configuration de TMG qui bloque le protocole si les données sont chiffrées. Pour adresser cette problématique, deux possibilités :

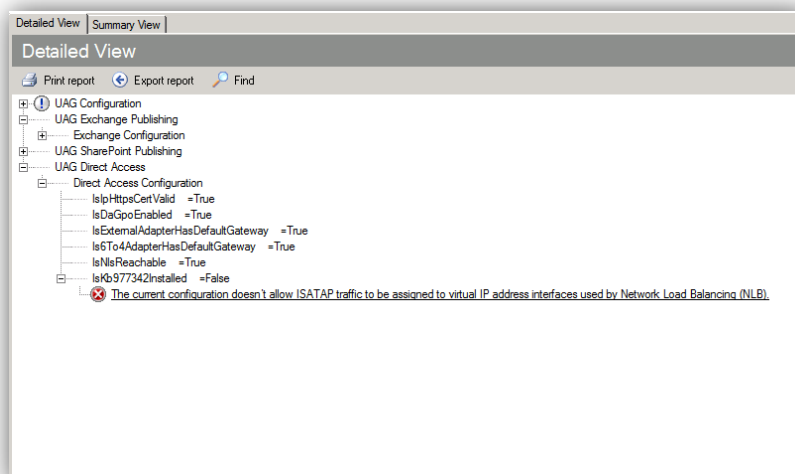
- Suivre la démarche proposée par Tom Shinder sur son blog: <http://blogs.technet.com/b/edgeaccessblog/archive/2010/04/22/deep-dive-into-uag-directaccess-certificate-enrollment.aspx>
- Tout simplement utiliser les extensions « Web Services Enrollment Web Service » et « Enrollment Policy Web Service » du rôle ADCS inclus avec Windows 2008 R2

Personnellement je préfère la seconde méthode, nettement plus élégante.

10.5 UAG Best Practices Analyzer (UAGBPA)

Tout comme pour beaucoup de produits de Microsoft, UAG dispose de son outil d'analyse de configuration : UAG Best Practices Analyzer. Une fois installé celui-ci prend en charge l'analyse des différents scénarios proposés par UAG dont celui de DirectAccess avec les vérifications suivantes :

- Valider que le certificat IP-HTTPS est bien présent et valide
- Valider que l'interface réseau publique dispose bien d'une adresse IPv4 comme passerelle par défaut
- Valider que l'interface réseau publique dispose bien d'une adresse IPv6 comme passerelle par défaut
- Que le correctif [KB977342](#) est bien installé pour adresser la problématique ISATAP dans le scénario de ferme UAG.
- Valider que l'URL pour IP-HTTPS est bien accessible
- Valider que la stratégie de groupe prévue s'applique bien au serveur UAG
- Valider que dans un ferme UAG, tous les nœuds ont bien convergés
- Valider que le site web du Network Location Server est bien accessible



Le Best Practices Analyzer est disponible à cette adresse : <http://www.microsoft.com/downloads/en/details.aspx?FamilyID=D24994EF-8670-4324-957A-805D35F1244E&displaylang=en>.

10.6 La haute disponibilité

UAG 2010 propose des fonctionnalités de « Scale in » et de « Scale out » au travers de son mode d'installation en ferme. La configuration d'UAG 2010 est alors stockée dans un annuaire ADLDS commun. Une ferme peut contenir jusqu'à huit serveurs UAG 2010. Dans ce mode de fonctionnement, l'équilibrage de charge réseau peut être porté par le Network Load Balancing du système d'exploitation ou externalisé auprès de boîtiers d'équilibrage de charge réseau (Global Server Local Balancing).

Un exemple de [mise en œuvre d'une ferme de deux serveurs UAG pour DirectAccess](#) est disponible sur mon blog. Les prérequis nécessaires à la mise en œuvre de DirectAccess changent quelque peu. Chaque serveur UAG de la ferme doit disposer d'une adresse IPv4 publique. A cela, on n'oublie pas d'ajouter les deux adresses IPv4 publiques consécutives pour DirectAccess. Ces adresses IP seront portées par le module Network Load Balancing.



La principale conséquence d'un déploiement de DirectAccess dans un ferme de deux serveurs UAG en NLB est qu'il sera nécessaire de disposer d'un bloc d'adresses IPv4 avec un masque de sous-réseau /29.

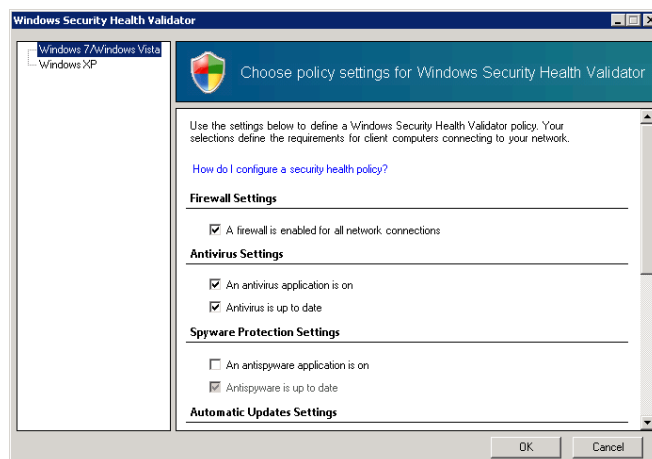
10.7 Gérer la défaillance

La défaillance d'UAG peut être adressée au travers de la notion de ferme d'UAG. Dans une configuration en Network Load Balancing, on sera limité par le fait que nos deux serveurs seront nécessairement localisés sur le même site. Cette contrainte peut être levée en déportant la gestion de l'équilibrage de charge et de la disponibilité sur des boîtiers d'équilibrage de charge réseau GSLB (Global Server Local Balancing). Dans ce mode de fonctionnement, chaque serveur UAG doit disposer non plus d'une adresse IPv4 publique mais bien de deux.

La défaillance peut aussi être adressée plus simplement avec deux serveurs UAG configurés en mode autonome. Le premier serveur sera dédié aux accès DirectAccess. Le second sera quant à lui dédié aux accès en SSTP. En cas de défaillance du premier serveur, le DirectAccess Connectivity Wizard informera l'utilisateur de la situation et le redirigera vers le portail d'authentification UAG sur le second serveur. La bascule est certes manuelle mais bien plus simple à mettre en œuvre que la haute disponibilité.

10.8 Le NAP avancé

Avec le Service Pack 1 d'UAG, Network Access Protection est intégralement pris en charge. Cette implémentation n'utilise que le couple SHA/SHV (System Health Agent / System Health Validator) livré en standard avec le système d'exploitation. On ne dispose donc que des critères issus du centre de sécurité :



Si on désire aller plus loin, il nous faut d'autres couples de SHA/SHV. Des partenaires tels que [UNET](#) proposent un couple de « SHA/SHV » pour étendre les possibilités de Network Access Protection. Un produit tel que System Center Configuration Manager propose aussi son propre [System Health Validator](#) qui va lui-même exploiter le module [Desired Configuration Manager](#). Par extension, on pourra exploiter les fonctionnalités de reporting de SCCM pour générer des rapports de conformité.

Enfin, pour finir, on peut aussi différencier les exigences de conformité selon que le poste de travail est localisé sur le réseau interne de l'entreprise ou non. Pour cela, depuis Windows Server 2008 R2, le Network Policy Server supporte plusieurs stratégies de conformité. Bien entendu on appliquera une stratégie plus restrictive lorsque le poste de travail sera localisé sur Internet.

11 CONCLUSION

Merci à tous ceux qui ont pris le temps de lire cet article. Je vous invite à me faire des remarques, qui me permettront d'améliorer mes prochains dossiers sous le même format (moins long ?). Chez Microsoft, je recommande la consultation des sites web ci-dessous :

- [Le blog de l'équipe UAG](#)
- [The Edge Man \(Microsoft\)](#)
- [Le blog de Frederic ESNOUF \(Microsoft\)](#)
- [Le blog de Stanislas Quastana \(Microsoft\)](#)
- [Forefront UAG DirectAccess with SP1 planning guide](#)
- [Forefront UAG DirectAccess design guide](#)
- [Forefront UAG DirectAccess deployment guide](#)
- [DirectAccess Troubleshooting Guide](#)
- [Les Tests Lab Guides autour de DirectAccess](#)

A l'extérieur, la liste est plus courte mais toute aussi intéressante :

- [Mon blog : Simple and Secure by Design](#)
- [Le blog de Jason Jones \(MVP ForeFront\)](#)
- [Le blog d'Alexandre GIRAUD \(MVP ForeFront\)](#)

Sur ce bon puzzle et intégrez d'autres briques tel que Forefront Endpoint Protection, ...