1 OBJECTIFS DE CE DOCUMENT :

Déterminer et valider la configuration d'Isa Server pour publier un serveur SharePoint sur Internet avec utilisation de certificats clients (carte à puce) avec les contraintes suivantes :

- Le client doit s'authentifier à l'aide d'une carte à puce (certificat utilisateur).
- Le serveur Isa Server doit authentifier la demande de connexion tout comme le serveur web.
- Le serveur web doit être configuré avec de l'authentification intégré.
- Les utilisateurs ne doivent pas avoir besoin de s'authentifier (il insère uniquement leur carte à puce).

2 ACTIONS A EFFECTUER SUR ISA SERVER :

On va configurer Isa Server pour accepter l'authentification avec des certificats de type « *Utilisateur* ». Cela nécessite d'utiliser la « *Délégation Kerberos contrainte* ». Il n'est pas possible d'utiliser de la délégation NTLM avec les certificats client (certificat de type « Utilisateur ») comme le montre la capture ci-dessous :

Ρ	ropriétés de Pub	lication s	rvdfs5.a	rchidfs.l	ocal		? ×
	Chemins d'accès Général Action Délégation de <u>M</u> éthode utilisée publié :	Pontage De l'authentifi par ISA Se	Utilisate A cation rver pour	urs Plar Trafic P s'authenti	nification Port d'é 'aramètres fier auprès	Tradu coute : de l'ap s du se	nction de liens Nom public oplication rveur Web
	Délégation Kerberos contrainte Pas de délégation et le client ne peut pas s'authentifier directement Pas de délégation, mais le client peut s'authentifier directement Délégation Kerberos contrainte Tutilisateur via Kerberos. Active Directory doit etre configure pour raire				■ nent		

Les prérequis suivants doivent être respectés pour la mise en œuvre de la « *Délégation Kerberos contrainte* » :

- Le domaine doit être en mode natif 2003.
- Le serveur Isa Server 2006 et le serveur web doivent être dans le même domaine. Le correctif suivant (inclus dans le SP1) semble supprimer cette limitation mais en pratique cela ne marche pas : <u>http://support.microsoft.com/kb/942637/en-us</u>.
- Il faut autoriser la fragmentation IP dans Isa Server 2006.

Les articles ci-dessous expliquent comment configurer la délégation contrainte :

- http://technet.microsoft.com/en-us/library/bb794858.aspx
- http://technet.microsoft.com/fr-fr/library/bb794751.aspx (Exemple avec Publication OWA)
- http://technet.microsoft.com/fr-fr/library/cc786828(WS.10).aspx

Remarque :

- Il est préconisé d'installer le dernier pack de correctif Isa Server 2006 (POST SP1) : <u>http://support.microsoft.com/kb/960148/en-us</u>
- Pour contrôler le format de saisi du champ login / mot de passe : <u>http://support.microsoft.com/kb/960146/en-us</u>
- Autre problème avec la « délégation Kerberos contrainte » : <u>http://support.microsoft.com/kb/947124/en-us</u>

2.1 CONFIGURATION DU PORT D'ECOUTE :

Il faut configurer le port d'écoute Isa Server au niveau de la règle de publication WEB avec la méthode d'authentification « *Authentification de certificats de client SSL* ». Il faut ensuite autoriser le certificat de l'autorité de certification qui a émis les certificats clients (SRVDFS dans l'exemple).

Propriétés de HT	TPS		<u>?</u> ×	Options d'authentification ava	incées		?
Général Authentific Méthode d'auth Méthode d'auth	Réseaux ation hentification du clie hentification auprès	Connexions Formulaires ent s de ISA Server :	Certificats SSO	Restriction Préférences d'authentification C Agcepter tout certificat die Accepter yniquement les c	des certificats du client Liste des certificats de cor int approuvé par l'ordinateu ertificats client approuvés p une aller tionnées ci-desco	nfiance du r ISA Servi ar les	client er
Authentificatio	n des certificats de méthode d'authen urer	e client SSL tification de <u>s</u> ecours	<u> </u>	Émis pour SecureNet CA Roo SecureNet CA So SecureSign RootC SecureSign RootC SecureSign RootC SecureSign RootC SecureSign RootC SecureSign RootC	t Root A1 A2 A3 RTIFICACION - A.N.C.	Validité Valide Valide Valide Valide Valide Valide	•
Méthode de va ISA Server vali <u>W</u> indows (<i>)</i>	lidation de l'auther de les informations Active Directory)	ntification d'identification du cliei	nt via :	SIA Secure Client SIA Secure Server SIA Secure Server SIA Secure Server TO TrustCenter Cl	CA CA Meet CA	Valide Valide Valide	Ľ

2.2 CONFIGURATION DU PORT DE LA DELEGATION D'AUTHENTIFICATION :

Il faut ensuite configurer la délégation d'authentification sur « Délégation Kerberos contrainte ».

Il sera nécessaire de créer le SPN (Service Principal Name) au niveau du serveur web (même valeur que dans la capture ci-dessous).

2.3 CONFIGURER LE COMPTE ORDINATEUR DU SERVEUR ISA :

Il faut approuver la délégation au niveau du compte ordinateur du serveur ISA (SRVDF3-R3GPSSX dans l'exemple).

Propriétés de SRVDFS	3-R3GP55X			<u>? ×</u>
Géré par	Objet	Sécuri	té	Appel entrant
Général Systè	me d'exploitation	Membre de	Délégation	Emplacement
La délégation est une services d'agir à la pla <u>Ne</u> pas approuve A <u>p</u> prouver cet or N'app <u>r</u> ouver cet or <u>Utiliser unique</u> <u>Utiliser tout pr</u>	opération liée à la sér ace d'un utilisateur. r cet ordinateur pour la dinateur pour la déléga ordinateur que pour la ement <u>K</u> erberos otocole d'authentificat	curité de votre n a délégation ation à tous les s délégation aux s tion	éseau qui perme ervices (Kerberc services spécifié	t à des is uniquement) s
Ce compte peut p	présenter des informati	ons d'identificati	on déléguées à	ces services :
Type de ser http http www www	Utilisateur ou ordinat srvdfs5.archidfs.loca SRVDFS5 SRVDFS5 srvdfs5.archidfs.loca	Po Nor I	n du ser Do	
Affichage dév	reloppé	Ajouter	<u>S</u> upprimer	
		OK	Annul	er <u>A</u> ppliquer

2.4 AJOUTER LE SERVICE PRINCIPALNAME (SPN) AU NIVEAU DU COMPTE ORDINATEUR DU SERVEUR WEB :

Il faut ajouter le Service Principal Name (SPN) au niveau du serveur web. Cela peut être fait via ADSIEDIT ou via la commande SETSPN.

=SRVDFS5 Properties			<u>? ×</u>	Mu	lti-valued Etring Editor		Y
Attribute Editor Sécurité				۵ ۳ ۲۵	ttribute: servicePrincipalName		<u>~</u>
Show <u>m</u> andatory attrit	outes				alua ta add		
Show optional attribut	es			×	alue to add:		f
Show only attributes t	hat have values						Add
Attributes:				V	alues:		
Attri <u>b</u> ates.				F	HOST/SRVDFS5		Remove
Attribute	Syntax				HOST/srvdfs5.archidfs.local		
objectGUID	Uctet String	UXdD UX/C UX96 UX85 UX5			http/srvdfs5.archidfs.local		
	SID Unio de Osiere	VXUT UXUS UXUU UXUU UXU					
operating5ystem	Unicode String	Windows Server 2003					
operatingsystemservi	Unicode String	SERVICE FACK I					
primaruGroupID	Unicode String	5.2 (5750) 515					
primaryaroupid pwdLaetSet	I arge Integer/	129542575741769750					
replPropertuMetaData	Datet String						
somoccountName	Unicode String	SRVDES5¢					
sAMAccountTune	Integer	805306369					
«DBighteEffective	Integer	15					
servicePrincipalName	Unicode String	http://stydfs5.archidfs.loca					
structuralObjectClass	Object Identifier	top:person:organizational					
1		Þ					
						OK	Cancel
Edit							

Le SPN doit être identique à celui indiqué dans la règle Isa Server 2006.

Guillaume MATHIEU – MSREPORT (<u>http://msreport.free.fr</u>) La connaissance s'accroît quand on la partage

Chemins d'accès Pontage Utilisateurs Planification Traduction de liens Général Action De À Trafic Port d'écoute Nom public Délégation de l'authentification Paramètres de l'application Méthode utilisée par ISA Server pour s'authentifier auprès du serveur Web publié : Description ISA Serveur est autorisé à effectuer une authentification au nom de Iutilisateur via Kerberos. Active Directory doit être configuré pour faire confiance les ordinateurs ISA Server utilisés pour la délégation d'authentification, et le serveur Web est IIS, il doit alors être configuré pour accepter l'authentification intégrée. Entrez le nom principal de service (SPN) utilisé par ISA Server pour la délégation Kerberos contrainte :	Propriétés de Publication srvdfs5.arc	chidfs.local	×
	Chemins d'accès Pontage Utilisateur Général Action De À Délégation de l'authentification Méthode utilisée par ISA Server pour s'a publié : Image: Comparison of the server pour s'a publié : Délégation Kerberos contrainte Description ISA Serveur est autorisé à effectuer un l'utilisateur via Kerberos. Active Directu confiance les ordinateurs ISA Serveur d'authentification, et le serveur Web di l'authentification Kerberos. Si le serveu configuré pour accepter l'authentificat Entrez le nom principal de service (SPN délégation Kerberos contrainte :	rs Planification Traduction de lie Trafic Port d'écoute Nom put Paramètres de l'application authentifier auprès du serveur Web me authentification au nom de tory doit être configuré pour faire utilisés pour la délégation doit être configuré pour accepter ur Web est IIS, il doit alors être tion intégrée. I) utilisé par ISA Server pour la	ns lic
http/srvdfs5.archidfs.local	http/srvdfs5.archidfs.local		1

2.5 RESULTATS ET PROBLEMES RENCONTREES :

2.5.1 TESTS CONNEXION AVEC UN COMPTE UTILISATEUR SITUE DANS LE MEME DOMAINE QUE LE SERVEUR WEB ET ISA SERVER :

Si un utilisateur essaie de se connecter depuis Internet, il voit cette fenêtre :

省 Aucune page à afficher - Microsoft Internet Explo	orer
Fichier Edition Affichage Favoris Outils ?	
🕞 Précédente 👻 🕥 👻 📓 🏠 🔎 Reche	ercher 🤺 Favoris 🤣 🖂 - چ 💭 🕼 🗱
Adresse 🗃 https://srvdfs5.archidfs.local/	
Action annulée	uise. La page
n'est peut-être pas disponible temporairement.	Choisir un certificat numérique 🛛 🖓 🔀
 Essayez de la manière suivante : Cliquez sur le bouton Actualiser ou réessay ultérieurement. Si vous avez déjà visité cette page et souhait a été stocké sur votre ordinateur, cliquez sur sur Travailler hors connexion. Pour obtenir des informations sur la navigatio connexion avec Internet Explorer, cliquez sur puis sur Sommaire et index. 	Identification Le site Web que vous voulez visiter requiert une identification. Choisissez un certificat. Nom Émetteur Christelle Mathieu SRVDFS
Internet Explorer	Informations Afficher le certificat
	OK Annuler

Au niveau d'Isa Server 2006, on voit que la connexion est authentifiée et que c'est bien le module proxy qui est utilisé.

Tableau de b	ord Alertes See	ssions Service	s Configuration	Rapports Vérifi	cateurs de connectivité V	Journalisation Su
Définitio	n de filtre					
Pour définir un	filtre et créer une no	ouvelle requête, c	liquez sur Modifier	le filtre		
Activation	Nom du serveur	Type de ses	Adress 🔺	Réseau source	Nom d'utilisateur du	Nom de l'hôte cl
📥 7/4/2011	SRVDFS3-R3GPSSX	SecureNAT	192.168.1.80	Hôte local		192.168.1.80
🔩 7/4/2011	SRVDFS3-R3GPSSX	Proxy Web	192.168.32.95	Externe	anonymous	
Å 7/4/2011	SRVDFS3-R3GPSSX	SecureNAT	192.168.32.88	Hôte local		192.168.32.88
5/4/2011	SRVDFS3-R3GPSSX	Proxy Web	192.168.32.95	Externe	archidfs\administrateur	
Å 7/4/2011	SRVDFS3-R3GPSSX	SecureNAT	192.168.32.95	Externe		192.168.32.95

2.5.2 TEST CONNEXION AVEC UN COMPTE SITUE DANS UN AUTRE DOMAINE :

Cela échoue si utilisation d'un compte d'un autre domaine de la forêt (pas dans le même domaine que le serveur ISA et le serveur web). On a l'erreur ci-dessous.

Event Type: Error						
Event Source:	Microsoft ISA Server Web Proxy					
Event Category:	None					
Event ID: 2131	5					
Date:	7/5/2011					
Time: 2:58:30 PM						
User:	N/A					
Computer: SRVDFS3-R3GPSSX						
Description:						
ISA Server n'a pas pu déléguer d'informations d'identification au site Web publié par la règle						
Publication srvdfs5.archidfs.local à l'aide de la délégation Kerberos contrainte. Vérifiez que les						
noms principaux du service : http/srvdfs5.archidfs.local configurés dans ISA Server correspondent						
à ceux d'Active Directory.						

Le correctif suivant (inclus dans le SP1) semble supprimer cette limitation mais en pratique cela ne marche pas : <u>http://support.microsoft.com/kb/942637/en-us</u>.