



SAUVEGARDES AUTOMATIQUES

Produits concernés : SNS 1.x, SNS 2.x, SNS 3.x, SNS 4.x Date : 09 décembre 2019 Référence : sns-fr-sauvegardes_automatiques_note_technique





Table des matières

Avant de commencer	
Fonctionnement	
Stocker les sauvegardes sur l'espace client Mystormshield.eu	
Stocker les sauvegardes sur un serveur personnalisé	4
Configurer le firewall	
Activer les sauvegardes automatiques vers Stormshield Network Cloud Backup	5
Activer les sauvegardes automatiques vers un serveur HTTP/HTTPS personnalisé	
Vérifier le fonctionnement des sauvegardes automatiques	
Valider les paramètres	8
Consulter les fichiers de logs (traces)	8
Exemple de configuration serveur - Linux et Apache	
Installer Apache et ses composants	
Créer le certificat serveur et l'exporter	9
Importer le certificat sur le serveur Apache	
Paramétrer WebDAV	10
Exemple de configuration serveur - Windows 2008 Server et IIS	12
Créer le répertoire de stockage des sauvegardes	12
Créer le compte utilisateur pour les sauvegardes	12
Installer IIS et ses composants	
Dopper les droits d'explorer le répertoire	13 1/
Aiouter un tupe MIME pour les fichiers de sauvegardes	14
Activer WebDAV	
Ajouter une règle de création WebDAV	15
Paramétrer les mécanismes d'authentification	
Créer le certificat serveur	
Importer le certificat sur le serveur IIS	17
Autoriser uniquement le protocole 332	то



Avant de commencer

Il est essentiel de pouvoir compter sur une sauvegarde régulière de ses équipements. En effet, réaliser une sauvegarde de configuration à intervalle périodique (quotidien, hebdomadaire, mensuel) permet de reconfigurer rapidement un firewall en cas de sinistre (défaillance matérielle, erreur de configuration ayant provoqué des dysfonctionnements, etc.).

Depuis la version de firmware 1.0, les Firewalls Stormshield Network offrent la possibilité d'automatiser cette opération de sauvegarde afin de stocker les fichiers résultants, soit au sein de l'infrastructure proposée par le service **Stormshield Network Cloud Backup**, soit sur un serveur HTTP/HTTPS au sein de votre infrastructure.

Cette fonctionnalité permet de décharger l'administrateur de la planification des sauvegardes de configuration et supprime ainsi le risque d'oubli de cette opération.



Fonctionnement

Quelle que soit la méthode choisie (Cloud backup ou serveur personnalisé), une sauvegarde locale de la configuration du Firewall est réalisée lors de toute opération de sauvegarde automatique. Ce fichier, nommé backup.na.enc, est stocké dans le répertoire /data/Autobackup/ du Firewall.

Stocker les sauvegardes sur l'espace client Mystormshield.eu

Lorsque l'option Cloud backup est sélectionnée, les sauvegardes sont envoyées directement dans votre espace sécurisé (https://mystormshield.eu). Les 5 dernières sauvegardes (quotidiennes, hebdomadaires ou mensuelles) de votre équipement sont ainsi stockées et accessibles.

Stocker les sauvegardes sur un serveur personnalisé

Si vous choisissez de stocker les sauvegardes sur un serveur personnalisé, vous pouvez utiliser l'extension WebDAV (RFC 4918) du protocole HTTP pour l'envoi des fichiers. Les éléments nécessaires sont alors les suivants :

Serveur Microsoft Internet Information Services (IIS)

- Windows 2008 Server ou supérieur,
- WebDAV,
- SSL,
- Méthodes d'authentification Digest ou Basic.

Serveur Apache

- Système d'exploitation supportant Apache (Linux, FreBSD, ...),
- Modules Apache : WebDAV (dav et dav_fs), SSL, authentification Digest (auth_digest) ou Basic (auth_basic).



Configurer le firewall

Activer les sauvegardes automatiques vers Stormshield Network Cloud Backup

La fonctionnalité SN Cloud Backup est présente sur l'ensemble des Firewalls Stormshield Network. Le service nécessite cependant que le Firewall soit sous maintenance.

Les sauvegardes sont alors enregistrées dans votre espace sécurisé (https://mystormshield.eu) grâce à l'identification du numéro de série du Firewall.

- 1. Dans le menu **Configuration** > **Système** > **Maintenance**, positionnez-vous sur l'onglet *Sauvegarder*.
- 2. Dans l'écran Sauvegarde automatique de configuration, passez le bouton sur ON.
- 3. Sélectionnez la valeur Cloud backup.
- 4. Dans la partie Configuration avancée, sélectionnez la fréquence des sauvegardes automatiques (quotidienne, hebdomadaire ou mensuelle). La première sauvegarde réussie détermine le point de départ des sauvegardes à la fréquence choisie.
- 5. Si vous le souhaitez, indiquez un mot de passe destiné à protéger le fichier de sauvegarde. Ce mot de passe sera demandé lors de l'utilisation du fichier en vue d'une restauration de la configuration.
- 6. Appliquez les changements.

Configuration automatic backup	
ON	
Configuration:	Cloud backup Customized
Advanced properties	server
Advanced properties	

Activer les sauvegardes automatiques vers un serveur HTTP/HTTPS personnalisé

- 1. Dans le menu **Configuration** > **Système** > **Maintenance**, positionnez-vous sur l'onglet *Sauvegarder*.
- 2. Dans l'écran Sauvegarde automatique de configuration, passez le bouton sur ON.
- 3. Sélectionnez la valeur Serveur personnalisé.
- 4. Pour le champ Serveur de sauvegarde, sélectionnez ou créez directement un objet représentant le serveur vers lequel le Firewall enverra ses sauvegardes automatiques. Si le nom du serveur est de la forme server.mycompany.com (FQDN), assurez-vous que le firewall parvient à bien à résoudre ce nom DNS.

Le champ URL du serveur est complété automatiquement en fonction des valeurs données aux champs Serveur de sauvegarde, Port du serveur, Protocole de communication et Chemin d'accès.

- 5. Pour le champ **Port du serveur**, sélectionnez ou créez directement depuis ce champ un objet représentant le port d'écoute du serveur de sauvegarde (objet réseau de type port).
- 6. Pour le champ **Protocole de communication**, sélectionnez HTTP ou HTTPS (recommandé) selon le protocole utilisé sur le serveur.



- Pour le champ Certificat du serveur (uniquement si le protocole HTTPS est sélectionné), sélectionnez le certificat du serveur de sauvegardes, créé ou importé au préalable dans la PKI du Firewall.
- 8. Pour le champ **Chemin d'accès**, indiquez le répertoire du serveur dans lequel les sauvegardes seront stockées.

🚺 IMPORTANT

Pour les firewalls dont la version de firmware est inférieure à 1.2.0, ce chemin doit être précédé du caractère « / ». Exemple : /autobackup

- 9. Pour le champ **Méthode d'envoi**, sélectionnez la méthode d'accès ou d'authentification utilisée pour déposer les sauvegardes du Firewall sur le serveur (contrôle d'accès POST ou authentification Basic/Digest pour WebDAV).
 - La méthode POST ne présente aucune notion d'authentification. Côté serveur, elle nécessite un script pour traiter les données reçues (enregistrement des fichiers reçus dans un répertoire particulier, etc.). Ce script vérifie également la présence d'un « control name » dans le flux de données afin de traiter celles-ci.
 - La méthode d'identification Basic (RFC 2617) est par nature non sécurisée, car elle envoie le mot de passe encodé en Base64 mais en clair, donc facilement interprétable. Elle n'est donc conseillée qu'au travers d'une connexion chiffrée (HTTPS) pour le transfert des accréditations et des données.
 - La méthode d'identification Digest (RFC 2617) est plus sécurisée car basée sur un mécanisme de type « challenge/response » autour de l'empreinte MD5 du mot de passe client. Bien que pouvant être utilisée dans un flux HTTP, il est également fortement conseillé d'utiliser cette méthode au travers d'une connexion chiffrée (HTTPS) pour le transfert des données.
- 10. Pour le champ **Identifiant** (méthodes Basic ou Digest uniquement), indiquez le nom d'utilisateur requis pour se connecter au serveur.
- 11. Pour le champ **Mot de passe** (méthodes Basic ou Digest uniquement), indiquez le mot de passe de l'utilisateur renseigné précédemment.
- 12. Pour le champ **POST control name** (méthode POST uniquement), indiquez le nom de contrôle utilisé si la méthode d'accès choisie est POST.
- 13. Pour le champ **Fréquence des sauvegardes**, sélectionnez la fréquence des sauvegardes automatiques (quotidienne, hebdomadaire ou mensuelle). La première sauvegarde réussie détermine le point de départ des sauvegardes à la fréquence choisie.
- 14. Pour le champ **Mot de passe du fichier de sauvegarde** (recommandé), indiquez un mot de passe destiné à protéger le fichier de sauvegarde. Ce mot de passe sera demandé lors de l'utilisation du fichier en vue d'une restauration de la configuration.
- 15. Appliquez les changements.



Configuration automatic backup					
ON					
Configuration:	Cloud backup	۲	Customized server		
Customized server					
Server's URL:	https://10.2.50.2/auto	bacl	kup		
Backup server:	autobackup_server			•	9
Backup filename:					
Server port:	https			•	9 5
Communication protocol:	HTTPS				•
Server certificate:	Autobackup:Autoba	icku	р	•	×
Access path:	/autobackup				
Send method:	auth digest				•
ID:	admin				
Backup password:	•••••				Þ
POST - control name:					



Vérifier le fonctionnement des sauvegardes automatiques

Lors de la validation du formulaire de paramétrage, une sauvegarde automatique est systématiquement réalisée.

Valider les paramètres

Si les paramètres renseignés sont valides, la sauvegarde s'effectue avec succès : le fichier de sauvegarde est alors disponible sur le serveur de destination.

Notez que la première sauvegarde réussie détermine le point de départ des sauvegardes automatiques à la fréquence sélectionnée.

En revanche, si l'un des paramètres n'est pas valide :

• Un message d'avertissement indique que la sauvegarde a échoué :

BACKUP FAILURE		
The backup failed	because the bac	kup server is unreachable.
	ОК	

 Un message est également affiché dans le module Monitoring > Logs - Journaux d'audit > Alarmes :

LOG / ALARMS						
Last hour	-	🗎 📿 Refresh	Search		» Advanced	l search
SEARCH FROM - 09/30/2019 01:17:05 PM - TO - 09/30/2019 02:17:05 PM						
Saved at	Action	Priority	Message	So	Source Name	Source Port Na
02:14:12 PM		(1) Minor	Backup failed: server does not answer (sendfile)			

Corrigez le(s) paramètre(s) incorrect(s) et validez à nouveau.

Consulter les fichiers de logs (traces)

Lorsqu'une sauvegarde est réussie, une trace est enregistrée dans le fichier /log/l system :

```
id=firewall time="2014-11-05 11:07:17" fw="V50XXA3E0000011" tz=+0100
startime="2014-11-05 11:07:17" pri=5 msg="Backup successful (local, distant)"
service=sysevent alarmid=86
```

Lorsqu'une sauvegarde échoue, une trace est enregistrée dans le fichier : /log/l alarm :

```
id=firewall time="2014-11-05 11:12:23" fw="V50XXA3E00000011" tz=+0100
startime="2014-11-05 11:12:23" pri=4 msg="Backup failed: invalid server response
(sendfile)" class=system alarmid=87
```



Exemple de configuration serveur - Linux et Apache

Cet exemple précise les différentes étapes pour paramétrer un serveur Apache sur une plateforme Linux, autorisant une identification en mode Digest au travers d'une connexion SSL (certificat serveur généré via la PKI du firewall).

Installer Apache et ses composants

- 1. Installez les différents composants nécessaires :
 - Serveur Web Apache,
 - Module *ssl* pour Apache,
 - Module *dav* pour Apache,
 - Module *dav fs* pour Apache,
 - Module *auth_digest* pour Apache.
- 2. Créez le répertoire destiné à recevoir les sauvegardes automatiques (exemple : /var/www/html/autobackup).

Créer le certificat serveur et l'exporter

- Sur le firewall hébergeant la CA utilisée pour les sauvegardes automatiques, créez un certificat serveur relatif au serveur hébergeant les sauvegardes (module Configuration > Objets > Certificats et PKI).
- 2. Sélectionnez ensuite le certificat créé et exportez le au format PKCS12 (menu **Téléchargement > Certificat au format P12**).

Importer le certificat sur le serveur Apache

- 1. Déposez le fichier PKCS12 sur le serveur.
- 2. Pour extraire la clé privée, utilisez la commande :

openssl pkcs12 -in server_certificate.p12 -nocerts -nodes -out server_key.key

L'option *-nodes* est à supprimer de la ligne si vous souhaitez que la clé privée reste protégée par mot de passe. Attention, dans ce cas, ce mot de passe vous sera demandé à chaque démarrage du serveur Apache.

3. Pour extraire le certificat, utilisez la commande :

```
openssl pkcs12 -in server_certificate.p12 -clcerts -nokeys -out server_
certificate.crt
```

- 4. Déplacez le certificat et la clé privée dans leurs répertoires respectifs (exemple : /etc/pki/tls/certs et /etc/pki/tls/private).
- 5. Limitez les droits sur la clé privée au seul super-utilisateur (exemple : *chmod 400 /etc/pki/tls/private/server_key.key*).
- 6. Adaptez le fichier de configuration de SSL en conséquence (exemple : /etc/httpd/conf.d/ssl.conf) :





Paramétrer WebDAV

Après avoir installé les modules dav, dav fs et auth digest :

1. Créez un fichier de configuration WebDAV pour Apache (Exemple : /etc/httpd/conf.d/webdav.conf) contenant les directives suivantes:



Dans l'exemple présenté:

- Le serveur sera joignable à l'adresse https://serveur_name/autobackup (directive Alias pointant sur le répertoire physique /var/www/html/autobackup).
- Le domaine d'authentification (Realm) est « Autobackup » (directive AuthName).
- La méthode d'authentification utilisée est la méthode Digest (directive AuthType).
- Les couples utilisateurs / mots de passe autorisés à accéder à ce répertoire sont stockés dans le fichier /usr/local/www/user.passwd (directive AuthUserFile).
- Créez le fichier de mots de passe du mode Digest et le premier compte (domaine d'authentification Autobackup et utilisateur autobackup dans l'exemple) à l'aide de la commande:

htdigest -c /usr/local/www/user.passwd Autobackup autobackup



- 3. Renseignez le mot de passe de l'utilisateur à l'invite de commande.
- 4. Par la suite, si vous souhaitez ajouter un compte d'accès supplémentaire (new_account dans l'exemple), utilisez la commande :

htdigest /usr/local/www/user.passwd Autobackup new_account

5. Démarrez ou redémarrez le serveur Apache pour prendre en considération l'ensemble des modifications.



Exemple de configuration serveur - Windows 2008 Server et IIS

Cet exemple précise les différentes étapes pour paramétrer un serveur IIS sur Windows 2008 Server, autorisant une identification en mode Digest au travers d'une connexion SSL (certificat serveur généré via la PKI du firewall).

Notez que pour pouvoir activer SSL dans IIS, le serveur doit être membre d'un domaine Active Directory.

Créer le répertoire de stockage des sauvegardes

A l'aide de l'explorateur de fichiers Windows, créez dans l'arborescence Web le répertoire destiné à recevoir les sauvegardes automatiques (exemple : c:\inetpub\wwwroot\autobackup).

Créer le compte utilisateur pour les sauvegardes

Dans la console **Utilisateur et ordinateurs Active Directory**, créez un utilisateur dédié aux sauvegardes automatiques.

Dans cet exemple, le compte utilisé s'appelle *autobackup* et appartient au groupe *Autobackup Allowed Users* spécifiquement créé pour cet usage. Les droits d'écriture sur le répertoire dédié aux sauvegardes pourront être définis dans le paramétrage du site WebDAV.

autobackup Properties	?X autobackup Properties
Dial-in Environment Sessions Remote contro	trol Dial-in Environment Sessions Remote control
Remote Desktop Services Profile Personal Virtual Desktop COI	OM+ Remote Desktop Services Profile Personal Virtual Desktop COM+
General Address Account Profile Telephones Organization Memb	nber Of General Address Account Profile Telephones Organization Member Of
User logon name:	Member of:
autobackup @documentation.mycompany.cc	Name Active Directory Domain Services Folder
User logon name (pre-Windows 2000):	Domain Users documentation.mycompany.com/Users
	-
, <u> </u>	
Logon Hours Log On To	
Unlock account	
Account options:	
User must change password at next logon	1 '
Viser cannot change password	Add Remove
Password never expires	
Store password using reversible encryption	Primary group: Domain Users
Account expires	There is no need to change Primary group unless
• Never	you have Macintosh clients or POSIX-compliant
C End of: samedi 20 septembre 2014	applications.
,	
OK Cancel Apply Hel	elp OK Cancel Apply Help

Installer IIS et ses composants

1. S'il n'est pas déjà installé, ajoutez le rôle IIS depuis la console Server Manager (menu **Ajout de Rôles > Rôles de serveurs > Serveur Web (IIS)**) :





 Lors de l'installation du rôle IIS, ou en sélectionnant l'option Ajouter des services de rôles pour le rôle Serveur Web (IIS) dans la console Gestionnaire de serveur, cochez les options suivantes :

Serveur Web

----- Fonctionnalités HTTP communes

----- Publication WebDAV

----- Sécurité

----- Authentification de base

- ----- Authentification Digest
- ----- Outils de gestion

----- Service de gestion

Select Role Services Server Nola Web Server (t3): Confination Progress Results Wet Hard (table) Very Provide (table) Approx Results Wet Server (table) Progress Results Wet Server (table) Progress Wet Server (table) Progress After Extendibility After Extendibility Wet Server Sele Indides Wet Result Monthin Wet Server Sele Indides Wet Result Monthin Wet Server Sele Indides <	Add Roles Wizard		×
Before You Begin Select the role services to Install for Web Server (IIS): Role services Description: Web Server (IIS): Role services to Install for Web Server (IIS): Role services Description: Role Services Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Progress Comments Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Progress Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features Image: Common HTTP Features <	Select Role Servi	ices	
< Previous Next > Instal Cancel	Before You Begin Server Roles Web Server (IIS) Role Services Confirmation Progras Results	Select the role services to install for Web Server (IIS): Role services:	Description: <u>VideDAV Pablishing</u> (Web Distributed Athoring and Versione) enable: vance pablishing to torrefrozool. Because WebDAV uses HTTP, it works through most firewalls without modification. v

Créer un répertoire virtuel

Dans cet exemple, le site utilisé pour recevoir et stocker les sauvegardes n'est pas *Default Web Site*, mais un site dédié nommé *autobackup*, dont le répertoire de base est situé sous la racine de *Default Web Site* (c:\inetpub\wwwroot).

- 1. Lancez la console Gestionnaire des services Internet (IIS).
- 2. Faites un clic droit sur Default Web Site.
- 3. Choisissez l'option Ajouter un répertoire virtuel.



Add Virtual Directory	? ×
Site name: Default Web Site	
Path: /	
Alias:	
autobackup	
Example: images	
Physical path:	
C:\inetpub\wwwroot\autobackup	
Pass-through authentication	
Connect as Test Settings	
ОК Са	ncel

- 4. Dans le champ **Alias**, choisissez le nom donné à votre site (exemple : *autobackup*); l'adresse du site prendra la forme *https://nom server.company.com/alias*.
- 5. Dans le champ **Chemin d'accès physique**, sélectionnez (ou créez) le répertoire physique correspondant à votre site virtuel (exemple : *c:\inetpub\wwwroot\autobackup*).
- 6. Faites un clic droit sur votre site
- 7. Sélectionnez l'option **Modifer les autorisations** pour donner au groupe d'utilisateurs dédiés les droits d'écriture sur le répertoire physique de stockage des sauvegardes.
- 8. Dans l'onglet Sécurité, cliquez sur Modifier.
- 9. Sélectionnez le groupe d'utilisateurs (exemple : Autobackup Allowed Users).
- 10. Cochez les cases Modification et Ecriture.
- 11. Validez.

🔋 autobackup Properties 🛛 🗙	
General Sharing Security Previous Versions Customize	Permissions for autobackup
Object name: C:\inetpub\wwwroot\autobackup	Security
Group or user names:	Object name: C:\inetpub\wwwroot\autobackup
NETWORK SERVICE Autobackup Allowed Users (DOCUMENTATION) Autoback	Group or user names:
Administrators (DOCUMENTATION\Administrators)	& CREATOR OWNER
	SYSTEM .
	LOCAL SERVICE
To change permissions, click Edit. Edit	& NETWORK SERVICE
Permissions for Autobackup	Autobackup Allowed Users (DOCUMENTATION Autoback
Allowed Users Allow Deny	
Full control	Add Remove
Modify 🗸	Permissions for Autobackup
Read & execute 🗸	Allowed Users Allow Deny
List folder contents 🗸	Modify 🔽 🗖
Read 🗸 🚽	Read & execute
Write 🗸 🔽	List folder contents
For special permissions or advanced settings.	Read 🗹 🗖
click Advanced.	Write
Loom shout second control and normissions	
Learn about access control and permissions	Learn about access control and permissions
OK Cancel Apply	OK Cancel Apply

Donner les droits d'explorer le répertoire

1. Dans la console Gestionnaire des services Internet (IIS), sélectionnez votre site (autobackup



dans l'exemple).

- 2. Faites un double clic sur l'icône Exploration de répertoire.
- 3. Dans le panneau de droite (Actions), cliquez sur Activer.

Ajouter un type MIME pour les fichiers de sauvegardes

Les fichiers de sauvegarde sont cryptés et possèdent une extension « .enc ». Cette extension n'étant pas connue du serveur IIS, il est nécessaire de la définir afin que le serveur sache quelle action réaliser lorsque vous cliquez sur le lien correspondant à une sauvegarde (exécuter le fichier, proposer l'ouverture ou le téléchargement, etc.).

- 1. Dans la console **Gestionnaire des services Internet (IIS)**, sélectionnez votre site (*autobackup* dans l'exemple).
- 2. Faites un double clic sur l'icône Types MIME.
- 3. Dans le panneau de droite (Actions), cliquez sur Ajouter.
- 4. Dans le champ Extension du nom de fichier, indiquez ".enc."
- 5. Dans le champ **Type MIME**, précisez *application/octet-stream*.

Activer WebDAV

- 1. Dans la console Gestionnaire des services Internet (IIS), sélectionnez le site Default Web Site.
- 2. Faites un double clic sur l'icône Règles de création WebDAV :

Hinternet Information Services (IIS) Manager						
G S AUTOBACKUP2008 Sites Default Web Sit	te 🕨 autobackup	•				
File View Help						
Connections						
🔍 - 🔚 🖄 😥	auto	ораскир і	Home			
Giant Start Page ⊡ 9 AUTOBACKUP2008 (DOCUMENTATION\Administrator)	Filter:		• 🔐 Go 🔹 💆	Show All	Froup by: Area	
	IIS					
⊡ ⊕ Default Web Site	2	Ð	0	110	404	2
autobackup	Authentication	Compression	Default Document	Directory Browsing	Error Pages	Handler Mappings
		0	9			
	Output Caching	Request Filtering	SSL Settings	WebDAV Authoring Rules		

3. Dans le panneau de droite (Actions), cliquez sur Activer WebDAV :



Ajouter une règle de création WebDAV

- 1. Dans la console IIS, sélectionnez votre site (autobackup dans l'exemple).
- 2. Faites un double clic sur l'icône Règles de création WebDAV.
- 3. Dans le panneau de droite (Actions), cliquez sur Ajouter une règle de création.



4. Pour cette règle, cochez les options : **Tous les contenus**, **Tous les utilisateurs** et les autorisations : **Lecture**, **Source**, **Ecriture**.

Allow access to: All content Specified content: Example: *.bas, wsvc.axd Allow access to this content to: Allow access to this content to: Allow access to this content to: Allow access to this content to: Example: *.bas, wsvc.axd Allow access to this content to: Example: *.bas, wsvc.axd Specified roles or user groups: Example: Admin, Guest Specified users: Example: User1, User2 Permissions V Read Source V Write	? ×
All content Specified content: Example: *.bas, wsvc.axd Allow access to this content to: Specified users: Example: User 1, User 2 Permissions Visite Source Visite	
C Specified content: Example: *.bas, wsvc.axd Allow access to this content to: • C Specified roles or user groups: Example: Admin, Guest • C Specified users: Example: User1, User2 Permissions ✓ Read ✓ Source ✓ Write	
Example: *.bas, wsvc.axd Allow access to this content to: Example: Admin, Guest Example: Admin, Guest Example: User1, User2 Permissions Allow access Write	
Allow access to this content to: Allow access to this content to: Allow access to this content to: Allow access to this content to: Specified roles or user groups: Example: Admin, Guest Specified users: Example: User1, User2 Permissions V Read V Source V Write	
All users Specified roles or user groups: Example: Admin, Guest Specified users: Example: User 1, User 2 Permissions F Read Source V Write	
C Specified roles or user groups: Example: Admin, Guest C Specified users: Example: User 1, User 2 Permissions V Read V Source V Write	
Example: Admin, Guest C Specified users: Example: User 1, User 2 Permissions V Read Source V Write	
Example: Admin, Guest C Specified users: Example: User1, User2 Permissions V Read Source V Write	
C Specified users: Example: User1, User2 Permissions Read Source W Write	
Example: User1, User2 Permissions V Read V Source V Write	
Example: User1, User2 Permissions Read Source Write	
Permissions Image: Read Image: Source Image: Write	
I Read I Source I Write	
I Source I Write	
Vrite	
OK Cancel	

Paramétrer les mécanismes d'authentification

- 1. Dans la console Gestionnaire des services Internet (IIS), cliquez sur votre site.
- 2. Faites un double clic sur l'icône Authentification.



- 3. Activez Authentification de base et Authentification Digest.
- 4. Désactivez Authentification anonyme.



- 5. Sélectionnez Authentification Digest.
- 6. Dans le panneau de droite, cliquez sur **Modifier** pour préciser le domaine Active Directory du serveur (*documentation.mycompany.com* dans l'exemple).





7. Validez.

Créer le certificat serveur

Sur le firewall hébergeant la CA utilisée pour les sauvegardes automatiques :

- 1. Allez dans le module Configuration > Objets > Certificats et PKI.
- 2. Créez un certificat serveur pour le serveur hébergeant les sauvegardes (menu Ajouter > Ajouter un certificat serveur).
- 3. Sélectionnez ce certificat et exportez le au format PKCS12 (menu Téléchargement > Certificat au format P12).

Importer le certificat sur le serveur IIS

- 1. Dans la console Gestionnaire des services Internet (IIS), sélectionnez le nom du serveur.
- 2. Faites un double clic sur l'option Certificats de serveur.



- 3. Dans le panneau de droite (Actions), cliquez sur Import.
- 4. Sélectionnez le certificat serveur.
- 5. Renseignez le mot de passe associé. Le certificat apparaît alors dans le magasin de certificats IIS :

Hanager						
AJTOBACKUP2008 AUTOBACKUP2008 AUTOBACKUP2008						ĺ
File View Help						
Connections	Server Certificate	25 age certificates that the Web server can use with Web sites co	nfigured for SSL.			
Application Pools	Name 🔺	Issued To	Issued By	Expiration Date	Certificate Hash	l
E- Sites		documentation - AUTOBACKUP2008-CA	documentation-AUTOBACKUP20	28/08/2019 10:41:57	BEDF67EAF845ACDF2EBA07CF	Î
🖻 🌑 Default Web Site		WMSvc-AUTOBACKUP2008	WMSvc-AUTOBACKUP2008	18/08/2024 11:06:16	11B1E3E3364910D17730B4E83	
aspnet_clent autobackup	doc-2008-en.documentation.myc	doc-2008-en.documentation.mycompany.com	documentation.mycompany.com	20/10/2015 10:10:47	F9E1199674C5214E464B4DE55	



- 6. Dans la console Gestionnaire des services Internet (IIS), cliquez sur le site Default Web Site.
- 7. Sélectionnez l'option Liaisons dans le panneau de droite.
- 8. Ajoutez une liaison avec les valeurs suivantes :
 - Type : https,
 - Adresse IP : l'adresse IP sur laquelle le serveur doit être joint en HTTPS,
 - Port : 443,
 - Certificat SSL : le certificat serveur importé.

Add Site Binding		? ×
Type: https	IP address:	Port:
Host name:		
SSL certificate:		
doc-2008-en.do	cumentation.mycompany.com	View
	ОК	Cancel

Autoriser uniquement le protocole SSL

- 1. Dans la console Gestionnaire des services Internet (IIS), cliquez sur votre site.
- 2. Faites un double clic sur l'icône Paramètres SSL.
- 3. Cochez la case Exiger SSL.
- 4. Appliquez.





documentation@stormshield.eu

Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.

Copyright © Stormshield 2019. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.