NOTE TECHNIQUE

Firewall Stormshield Network

SAUVEGARDES AUTOMATIQUES

Version du document : 1.0

Référence : snfrtno_autobackup

SOMMAIRE

INTRODUCTION

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.

Stockage 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.

Stockage 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 :

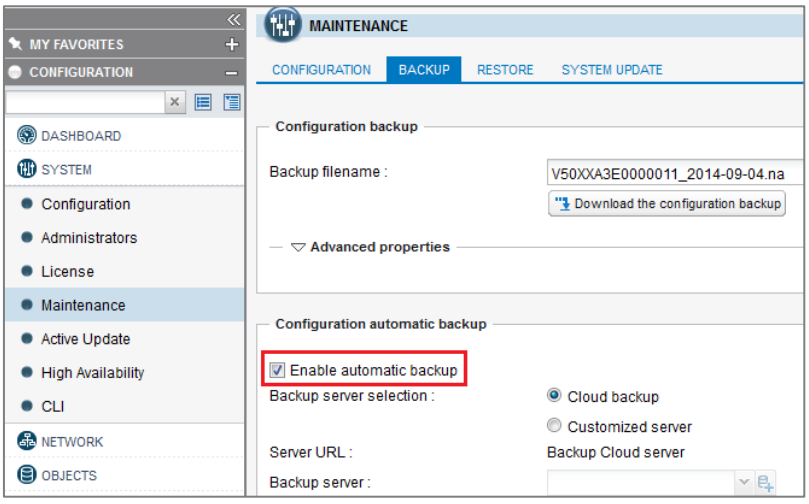
- Système d'exploitation supportant Apache (Linux, FreBSD, …),
- Modules Apache : WebDAV (dav et dav_fs), SSL, authentification Digest (auth_digest) ou Basic (auth_basic).

CONFIGURATION DU FIREWALL

Activation des sauvegardes automatiques

Sélectionnez l'onglet *Sauvegarder* du module **Configuration** > **Système** > **Maintenance**.

Dans l'écran *Sauvegarde automatique de configuration*, cochez la case **Activer la sauvegarde automatique**.

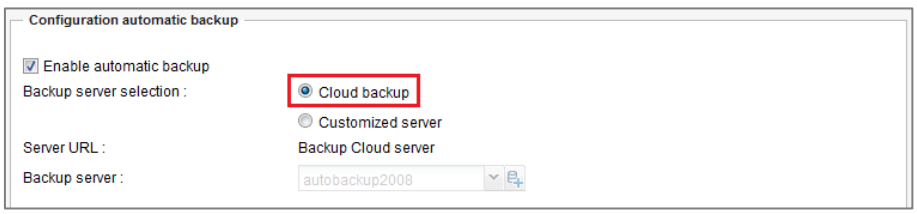


Stormshield Network Cloud Backup

Pour activer les sauvegardes automatiques vers le service **Stormshield Network Cloud backup**, sélectionnez la valeur « Cloud backup » pour le champ **Choix du serveur de sauvegarde**. Les sauvegardes sont alors enregistrées dans votre espace sécurisé (https://mystormshield.eu) grâce à l'identification du numéro de série du Firewall. Il n'est donc pas nécessaire, pour cette fonctionnalité, de renseigner un identifiant et un mot de passe dans le module **Préférences**.

NOTE

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



Seuls deux champs complémentaires sont à renseigner :

- **Fréquence des sauvegardes** : sélectionnez l'une des 3 fréquences proposées (chaque jour, chaque semaine ou chaque mois).

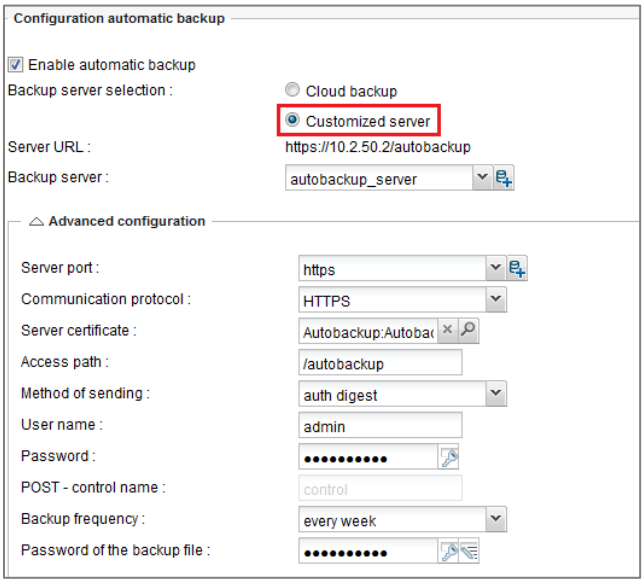
- **Mot de passe du fichier de sauvegarde** (optionnel): Indiquez un mot de passe destiné à protéger le fichier de sauvegarde. Ce mot de passe sera demandé lors de l'utilisation du fichier en vue d'une restauration de la configuration.

Sauvegardes sur un serveur HTTP/HTTPS personnalisé

Dans le champ **Choix du serveur de sauvegarde**, sélectionnez la valeur « Serveur personnalisé ». Complétez ensuite les différents champs du module **Configuration avancée.**

REMARQUE

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.**



Serveur de sauvegarde

Sélectionnez ou créez directement depuis ce champ un objet représentant le serveur vers lequel le Firewall envoie 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.

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).

Protocole de communication

Sélectionnez **HTTP** ou **HTTPS** (recommandé) selon le protocole utilisé sur le serveur.

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.

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*

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.

Identifiant (méthodes Basic ou Digest uniquement)

Indiquez le nom d'utilisateur requis pour se connecter au serveur.

Mot de passe (méthodes Basic ou Digest uniquement)

Indiquez le mot de passe de l'utilisateur renseigné précédemment.

POST – control name (méthode POST uniquement)

Indiquez le nom de contrôle utilisé si la méthode d'accès choisie est POST.

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.

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.

Vérification du fonctionnement des sauvegardes automatiques

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

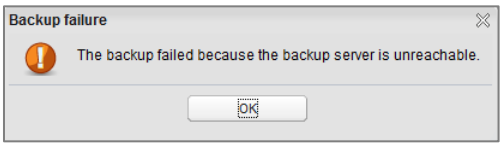
Validation du paramétrage

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

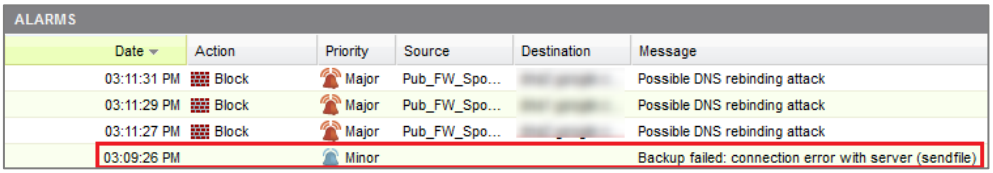
NOTE

Cette 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 :



Un message est également affiché dans la fenêtre *Alarmes* du module **Tableau de bord** :



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

Fichiers de 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="V50XXA3E0000011"
tz=+0100 startime="2014-11-05 11:12:23" pri=4 msg="Backup failed:
invalid server response (sendfile)" class=system alarmid=87
```

EXEMPLES DE CONFIGURATIONS SERVEURS

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).

Installation d'Apache et de ses composants

Installez les différents composants nécessaires :

- Apache,
- Module ssl pour Apache,
- Modul dav pour Apache,
- Module dav_fs pour Apache,
- Module _auth_digest pour Apache.

Créez le répertoire destiné à recevoir les sauvegardes automatiques (exemple : */var/www/html/autobackup*).

Paramétrage SSL

Création du certificat serveur

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**).

Sélectionnez ensuite le certificat créé et exportez le au format PKCS12 (menu **Téléchargement** > **Certificat au format P12**).

Import du certificat sur le serveur Apache

Déposez le fichier PKCS12 sur le serveur et procédez à l'extraction de la clé privée et du certificat.

Pour extraire la clé privée, utilisez la commande suivante:

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

REMARQUE

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.

Pour extraire le certificat, utilisez la commande suivante :

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

Déplacez ensuite le certificat et la clé privée dans leurs répertoires respectifs (exemple : */etc/pki/tls/certs* et */etc/pki/tls/private*). Limitez les droits sur la clé privée au seul superutilisateur (exemple : `chmod 400 /etc/pki/tls/private/server_key.key`).

Adaptez le fichier de configuration de SSL en conséquence (exemple : */etc/httpd/conf.d/ssl.conf*):

```
#   Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate.  If
# the certificate is encrypted, then you will be prompted for a
# pass phrase.  Note that a kill -HUP will prompt again.  A new
# certificate can be generated using the genkey(1) command.
SSLCertificateFile /etc/pki/tls/certs/server_certificate.cert

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile /etc/pki/tls/private/server_key.key

#   Server Certificate Chain:
#   Point SSLCertificateChainFile at a file containing the
#   concatenation of PEM encoded CA certificates which form the
#   certificate chain for the server certificate. Alternatively
#   the referenced file can be the same as SSLCertificateFile
#   when the CA certificates are directly appended to the server
#   certificate for convinience.
#SSLCertificateChainFile /etc/pki/tls/certs/server-chain.crt
```

Paramétrage de WebDAV

Après avoir installé les modules dav, dav_fs et auth_digest, créez un fichier de configuration WebDAV pour Apache (Exemple : /etc/httpd/conf.d/webdav.conf) contenant les directives suivantes:

```
# DIGEST method
Alias /autobackup /var/www/html/autobackup
<Directory "/var/www/html/autobackup">
                Dav On
                Order Allow,Deny
                Allow from all

                AuthType Digest
                AuthName "Autobackup"
                AuthUserFile "/etc/httpd/user.passwd"
                AuthDigestProvider file

                Require valid-user
</Directory>
```

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 ensuite 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
```

Renseignez le mot de passe de l'utilisateur à l'invite de commande.

Par la suite, si vous souhaitez ajouter un compte d'accès supplémentaire (new_account dans l'exemple), utilisez la commande suivante:

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

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

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).

NOTE

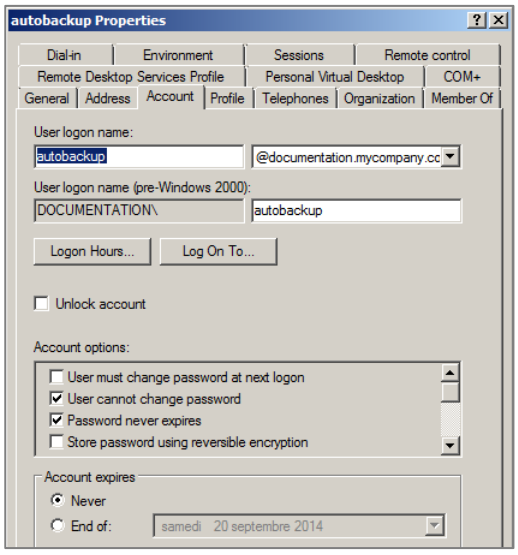
Pour pouvoir activer SSL dans IIS, le serveur doit être membre d'un domaine Active Directory.

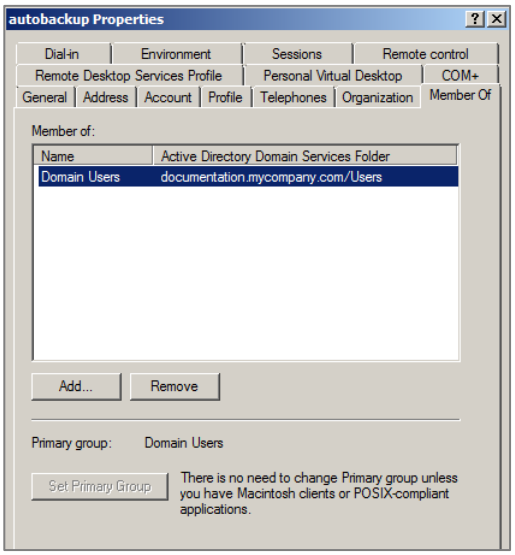
A l'aide de l'explorateur de fichiers Windows, créez le répertoire destiné à recevoir les sauvegardes automatiques (exemple : c:\inetpub\wwwroot\autobackup).

Compte utilisateur pour les sauvegardes

Créez un utilisateur dédié aux sauvegardes automatiques dans la console Utilisateur et ordinateurs Active Directory.

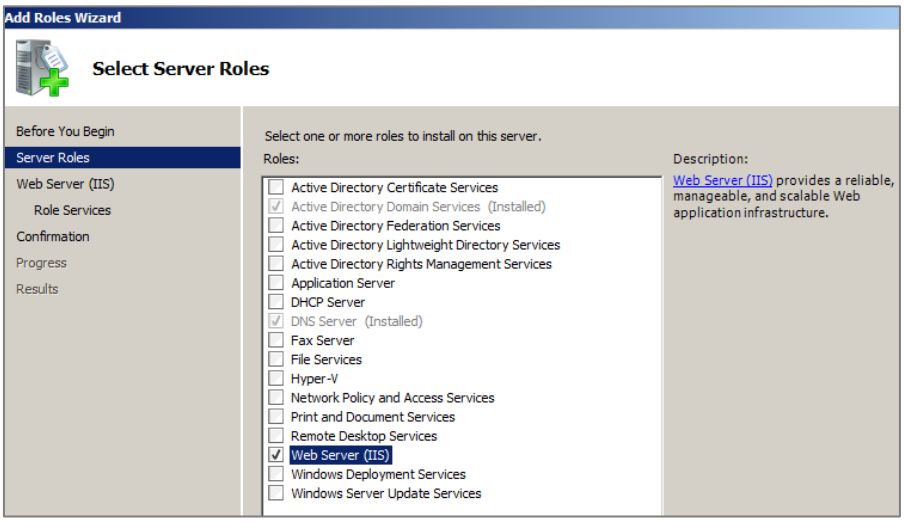
Dans cet exemple, le compte utilisé s'appelle *autobackup* et appartient au groupe *Autobackup Allowed Users* spécifiquement créé pour cet usage. Les droits d'écriture sur le répertoire dédié aux sauvegardes pourront être définis dans le paramétrage du site Webdav.





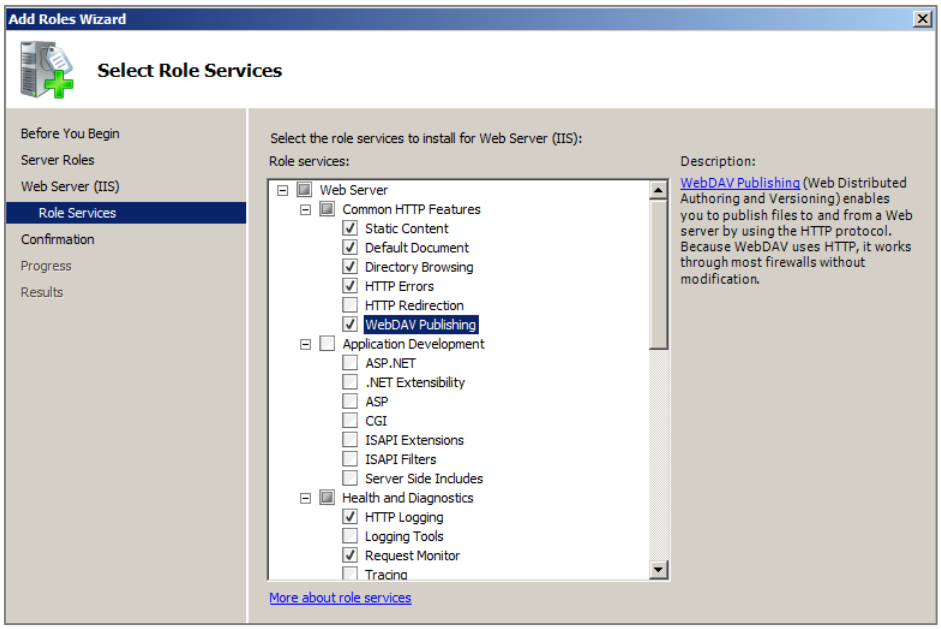
Installation de IIS et de ses composants

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 :

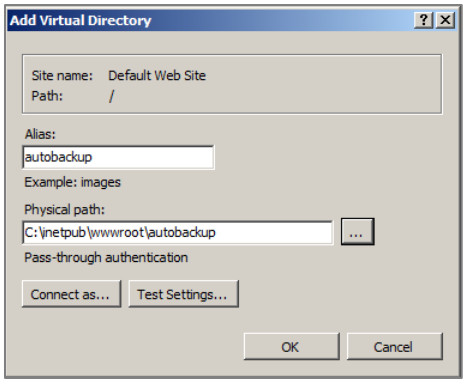
Serveur Web
- Fonctionnalités HTTP communes
  - Publication WebDAV
- Sécurité
  - Authentification de base
  - Authentification Digest
- Outils de gestion
  - Service de gestion



Création d'un répertoire virtuel

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

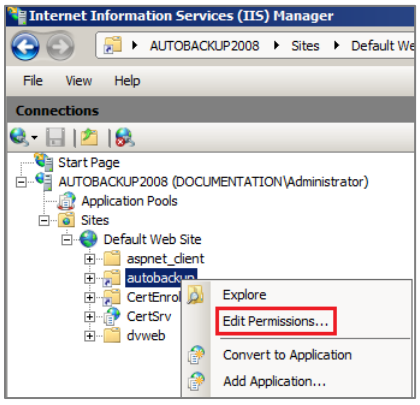
Lancez la console Gestionnaire des services Internet (IIS). Faites un clic droit sur **Default Web Site** et choisissez l'option **Ajouter un répertoire virtuel**.



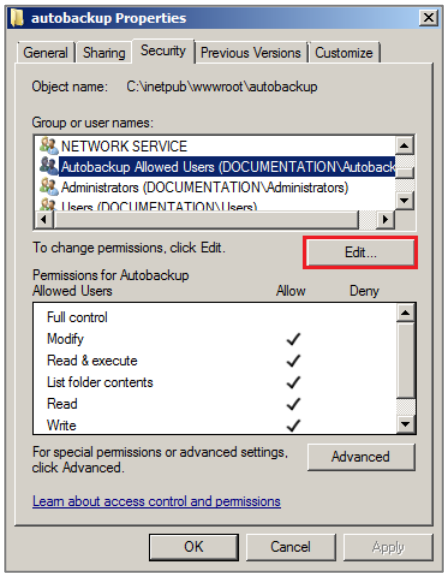
Dans le champ **Alias**, choisissez le nom donné à votre site (exemple : *autobackup*); l'adresse du site prendra la forme *https://nom_server.company.com/alias*.

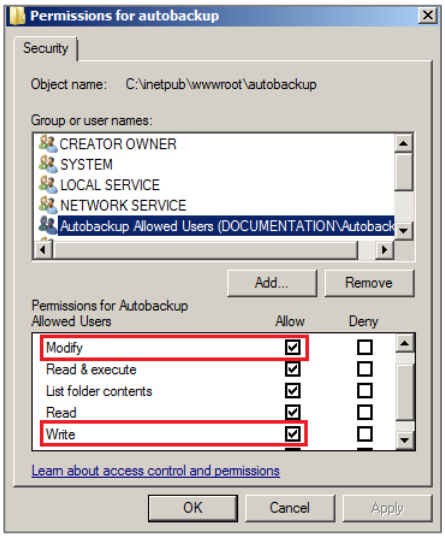
Dans le champ **Chemin d'accès physique**, sélectionnez (ou créez) le répertoire physique correspondant à votre site virtuel (exemple : *c:\inetpub\wwwroot\autobackup*).

Donnez ensuite les droits d'écriture *sur le répertoire* physique de stockage des sauvegardes au groupe d'utilisateurs dédiés. Pour cela, faites un clic droit sur votre site et sélectionnez l'option **Modifer les autorisations** du menu contextuel.



Dans l'onglet *Sécurité*, cliquez sur **Modifier**. Sélectionnez le groupe d'utilisateurs (exemple : *Autobackup Allowed Users*) et cochez les cases **Modification** et **Ecriture**, puis validez.





Droits d'exploration du répertoire

Dans la console *Gestionnaire des services Internet (IIS)*, sélectionnez votre site (*autobackup* dans l'exemple) et faites un double clic sur l'icône **Exploration de répertoire**.

Dans le panneau de droite (*Actions*), cliquez sur **Activer**.

Ajout d'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.).

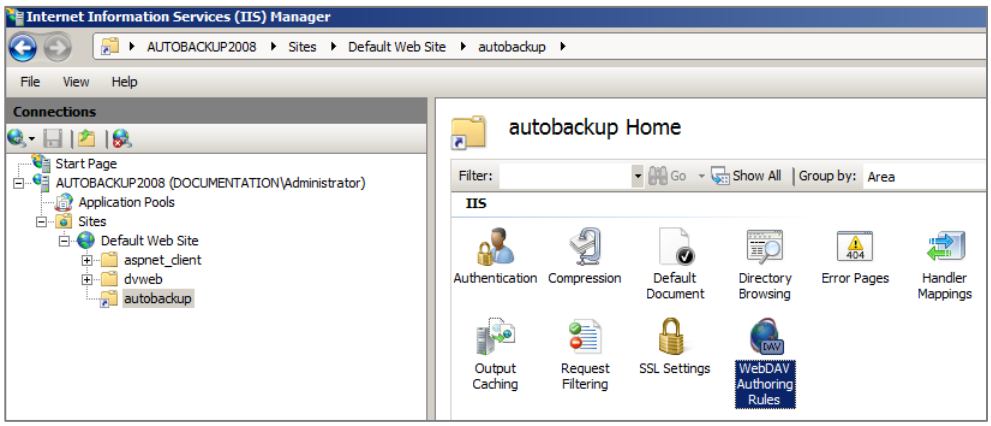
Dans la console *Gestionnaire des services Internet (IIS)*, sélectionnez votre site (*autobackup* dans l'exemple) et faites un double clic sur l'icône **Types MIME**.

Dans le panneau de droite (*Actions*), cliquez sur **Ajouter**. Dans le champ **Extension du nom de fichier**, indiquez *.enc*. Dans le champ **Type MIME**, précisez *application/octet-stream*.

Paramétrage de WebDAV

Activation de WebDAV

Dans la console *Gestionnaire des services Internet (IIS)*, sélectionnez le site *Default Web Site* et faites un double clic sur l'icône **Règles de création WebDAV**.

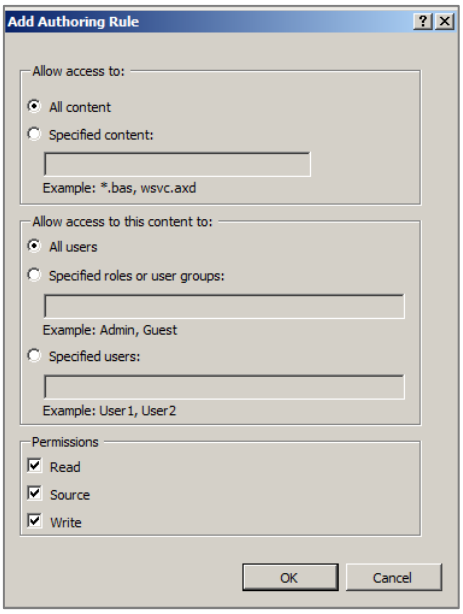


Dans le panneau de droite (*Actions*), cliquez sur **Activer WebDAV** :

Règles de création WebDAV

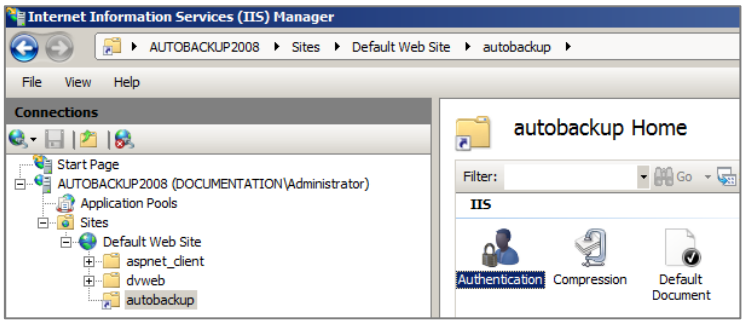
Dans la console IIS, sélectionnez votre site (*autobackup* dans l'exemple) et faites un double clic sur l'icône **Règles de création WebDAV**.

Dans le panneau de droite (*Actions*), cliquez sur **Ajouter une règle de création**. Pour cette règle, choisissez les options **Tous les contenus**, **Tous les utilisateurs** et **Autorisations : Lecture, Source, Ecriture**.

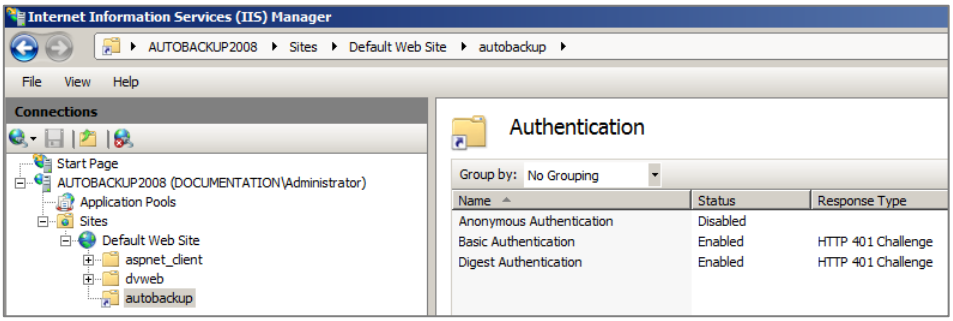


Authentification

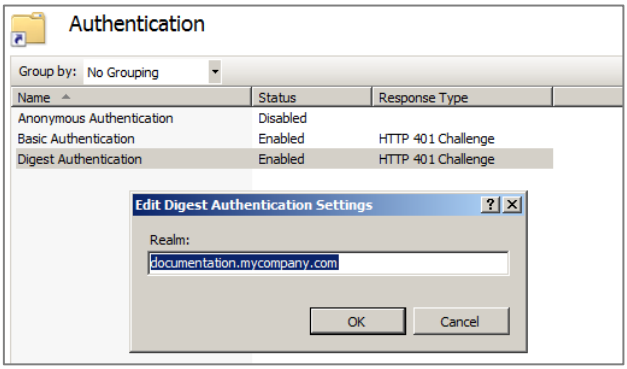
Dans la console *Gestionnaire des services Internet (IIS)*, cliquez de nouveau sur votre site et faites un double clic sur l'icône **Authentification**.



Activez **Authentification de base**, **Authentification Digest**, et désactivez **Authentification anonyme**.



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



Paramétrage SSL

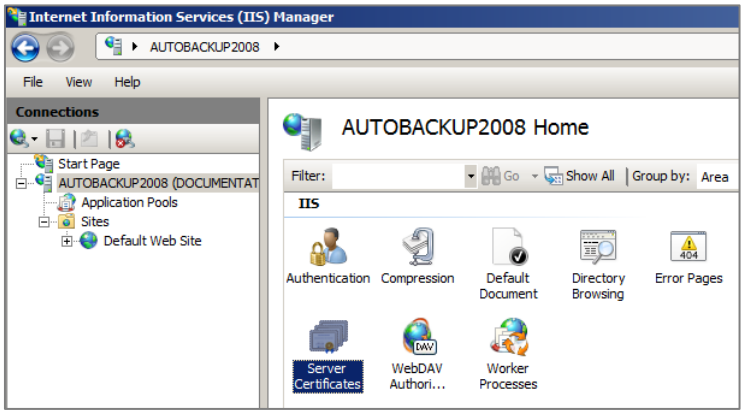
Création du certificat serveur

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**).

Sélectionnez ensuite le certificat créé et exportez le au format PKCS12 (menu **Téléchargement** > **Certificat au format P12**).

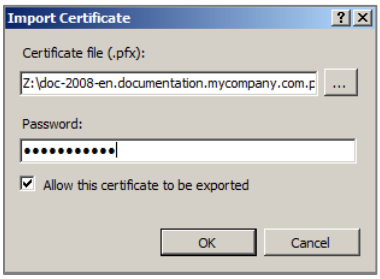
Import du certificat sur le serveur IIS

Dans la console *Gestionnaire des services Internet (IIS)*, sélectionnez le nom du serveur et double cliquez sur l'option **Certificats de serveur**.

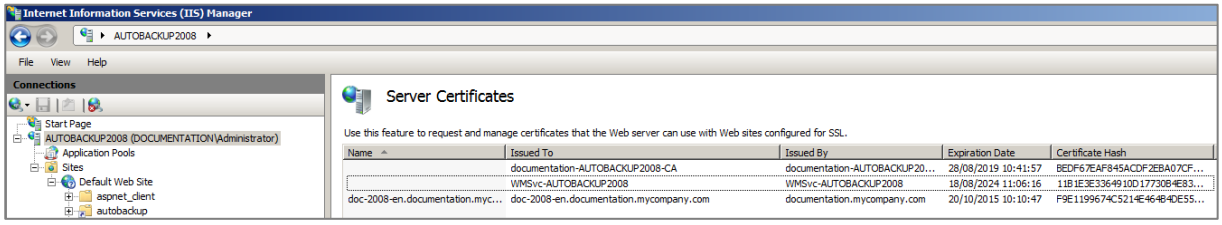


Dans le panneau de droite (*Actions*), cliquez sur **Import**.

Sélectionnez le certificat précédemment exporté et renseignez le mot de passe associé.



Le certificat apparaît alors dans le magasin de certificats IIS :



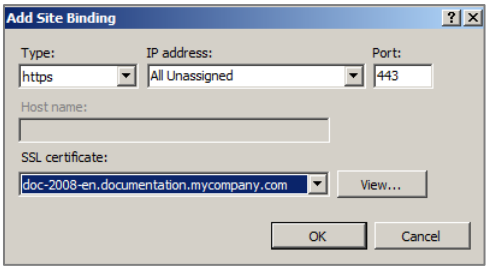
Dans la console *Gestionnaire des services Internet (IIS)*, cliquez de nouveau sur le site *Default Web Site* puis sélectionnez l'option **Liaisons** dans le panneau de droite. Ajoutez une liaison avec les valeurs suivantes :

Type : https

Adresse IP : l'adresse IP sur laquelle le serveur doit être joint en HTTPS

Port : 443

Certificat SSL : le certificat précédemment importé.



Accès exclusif en SSL

Il s'agit ici d'autoriser exclusivement l'accès en SSL au serveur de stockage des sauvegardes.

Dans la console *Gestionnaire des services Internet (IIS)*, cliquez sur votre site et faites un double clic sur l'icône **Paramètres SSL**. Cochez la case **Exiger SSL** et appliquez.