
Table des matières

1	Généralités	3
1.1	Introduction	3
1.2	Structure du logiciel	3
1.3	Principe de fonctionnement	4
1.4	Configurations supportées	7
1.4.1	Serveur	7
1.4.2	Client	7
1.4.3	Incompatibilités connues	7
2	Installation	8
2.1	Installation sous Windows	8
2.1.1	Gestionnaire de serveur et filtre	8
2.1.2	Gestionnaire de cluster	16
2.2	Installation sous Linux	17
2.2.1	Gestionnaire de serveur	17
2.2.2	Filtre Apache	17
2.2.3	Gestionnaire de cluster	18
2.3	Installation sous FreeBSD	19
3	Configuration	20
3.0.1	Fichiers de configuration	20
3.1	Gestionnaire de serveur	22
3.1.1	Site indépendant	22
3.1.2	Site affilié à un cluster	23
3.2	Gestionnaire de cluster	24
3.2.1	Configuration	24
3.2.2	Production du fichier clustConf.txt	26
3.2.3	Sécurisation de la communication entre gestionnaire de serveur et de cluster	26

Table des matières	2
4 Fonctionnement	28
4.1 Gestion des permissions	28
4.2 Protection des pages Web	29
4.2.1 Voie descendante (du serveur vers le client)	29
4.2.2 Voie montante (du client vers le serveur)	30
4.3 Messages d'erreur	31
4.4 Cookie Validy	32
4.5 Variables Web Use	32
4.6 Personnalisation électrique des cartes à puce	33
4.7 Mise à jour du serveur	34
4.8 Action au retrait de la carte	34
4.9 Configuration en mode proxy	35
4.10 Problèmes liés au cryptage du cache	36
5 Exemple	38
5.1 Installation	39
5.2 Création du site	39
5.3 Création des cartes à puce	39
5.4 Mise à jour du serveur	40
5.5 Conclusion	40

1 Généralités

1.1 Introduction

Validy Web Business Server permet d'héberger des sites dont toutes ou partie des pages sont protégées par Validy, c'est-à-dire que l'accès à ces pages est conditionné par la présence côté client d'une carte à puce avec les droits requis. Validy Web Business Server doit donc être installé sur le serveur de tout hébergeur accueillant un site web protégé par Validy.

Validy Web Business Customizer permet au propriétaire d'un site protégé par Validy de personnaliser électriquement les cartes à puce Validy pour son site, afin de leur donner les droits nécessaires.

La version de Validy Web Business Server dont vous disposez fonctionne avec Internet Information Server (IIS 4 & 5) en environnement Windows, et Apache (1.3.x et 2.0.x) en environnement Linux ou FreeBSD.

La migration d'un site existant vers un site protégé par Validy s'effectue très simplement. Dans chaque page à protéger, il suffit d'insérer une ligne contenant une étiquette qui correspond à la catégorie de la page. Côté client, le navigateur utilise le schéma `vldy` au lieu de `http`¹. Il faut prévoir l'entrée dans la zone protégée en suivant un lien absolu vers une URL utilisant le schéma `vldy` :

```
vldy://www.example.com/
```

ou en stockant cette URL dans la carte en utilisant la fonction Web Portal. A l'intérieur de la zone protégée, l'utilisation de liens relatifs permet de rester dans le schéma `vldy`.

Il est également possible, pour contrôler l'accès au site en début d'exécution de la requête, d'utiliser des en-têtes ajoutés à la requête par Validy et qui fournissent une identification forte du client.

Afin de tirer le meilleur parti possible du logiciel, il est recommandé que la personne qui se charge de l'installation de Validy Web Business Server ait de bonnes connaissances en administration de serveur web IIS ou Apache et en création de pages internet.

1.2 Structure du logiciel

La version 2.0 du produit se composait uniquement d'un filtre ISAPI ou d'un module Apache chargé de réaliser la totalité des fonctions. Dans la version 3.0, les fonctions sont réparties sur deux ou trois entités :

1. le **filtre** est chargé de l'intégration dans le serveur Web. Il est spécialisé pour un type de serveur : filtre ISAPI pour IIS (Windows), module Apache 1.3.x (Linux

¹ Ce choix permet une meilleure intégration du logiciel Validy avec Internet Explorer en évitant les conflits avec d'autres logiciels qui interceptent le protocole standard http. Il se limite au navigateur et les requêtes et réponses échangées par le client et le serveur sont complètement conformes à la norme HTTP

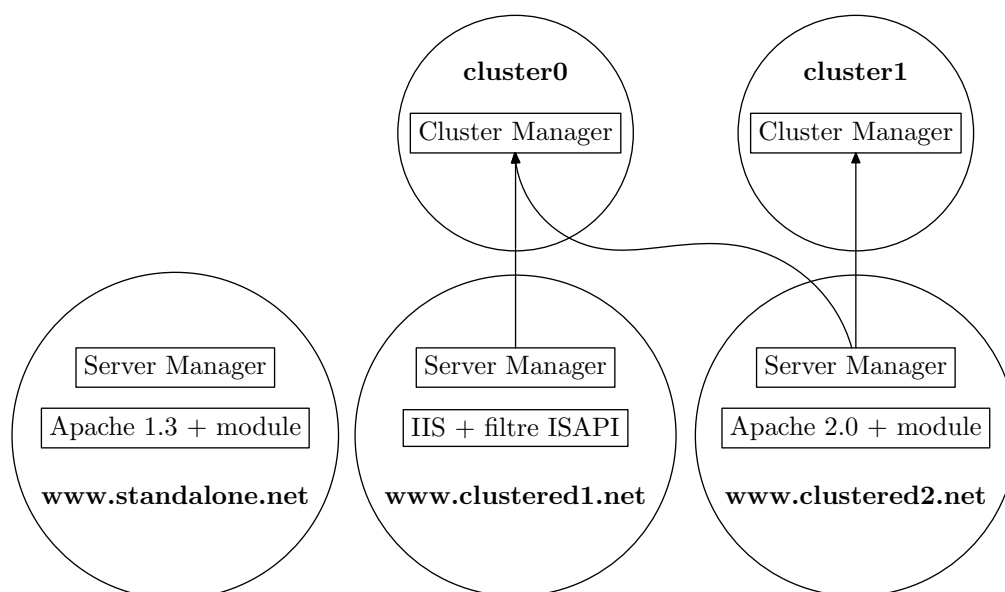


FIG. 1.1: Exemple de configuration avec trois serveurs et deux clusters.

ou FreeBSD) ou module Apache 2.0.x (Windows, Linux ou FreeBSD). Pour IIS 6, une extension ISAPI peut-être également nécessaire,

2. le **gestionnaire de serveur** (server manager) gère les protections des pages (permissions.txt), la définition de la zone protégée par cryptage en voie montante (cryptage des URL, des données de POST et des informations utilisateur) et la définition des pages d'erreurs (vdyerr*.*)). Si le site est indépendant (standalone), il gère aussi les utilisateurs. Le gestionnaire de serveur prend en charge un ou plusieurs sites d'un même serveur et s'exécute sur la même machine que le serveur Web associé.
3. en option, le **gestionnaire de cluster** (cluster manager) gère des utilisateurs qui peuvent accéder à plusieurs sites affiliés avec la même carte. Les sites sont connectés au gestionnaire de cluster par l'intermédiaire de leur gestionnaire de serveur. Le gestionnaire de cluster peut s'exécuter sur une machine indépendante ou bien sur la machine d'un des gestionnaires de serveur affiliés.

La Figure 1.1 donne un exemple de configuration avec :

- un site indépendant, www.standalone.net,
- un site affilié à un cluster, www.clustered1.net,
- un site affilié à deux clusters, www.clustered2.net.

1.3 Principe de fonctionnement

Création des cartes :

1. avec le logiciel Customizer, on personnalise électriquement des cartes,
2. cela produit un fichier update xxxxxx.upd, qui est utilisé ...
3. pour mettre à jour le serveur ou le cluster, avec le programme vwbUpdate.

Lors de la personnalisation, une clef de décryptage est introduite dans la carte. Pour une page protégée, le serveur renvoie des données sous forme cryptée. Celles-ci ne peuvent

être décryptées que par le client auquel elles sont destinées, avec l'aide de la clef contenue dans sa carte.

La protection des pages côté serveur est mise en place très simplement par le créateur du site. Il suffit d'ajouter à chaque page que l'on désire protéger un en-tête contenant une étiquette, ou label, qui est ensuite pris en compte par Validy Web Business Server. Avant d'envoyer la réponse, le serveur consulte le fichier permissions correspondant au site protégé. Ce fichier établit des correspondances entre les différents labels du site et les catégories de cartes en leur associant des périodes de validité. Un exemple de fichier permissions est installé avec Validy Web Business Server dans le répertoire suivant, pour Windows :

```
\Program Files\Validy\Web Business\sample_site
```

pour Linux :

```
/usr/share/doc/validy/sample_site
```

ou

```
/opt/validy/share/doc/validy/sample_site
```

et pour FreeBSD :

```
/usr/local/share/doc/validy/sample_site
```

et sa syntaxe est détaillée à la page [28](#).

Si la carte insérée dans le lecteur côté client donne effectivement le droit de consulter la page en cours, celle-ci est encryptée par Validy Web Business Server puis envoyée cryptée sur l'Internet. Elle est stockée cryptée dans le cache du navigateur puis décryptée par Validy Web Client au moment d'être présentée à l'utilisateur en utilisant la clef se trouvant dans la carte Validy côté client. Si le droit n'est pas accordé, Validy Web Business Server retourne un message d'erreur (pas de carte insérée, pas les droits requis, etc.).

Si un utilisateur illégitime essaie d'accéder à une page protégée en tentant de simuler la possession d'une carte Validy, des informations cryptées lui seront transmises par le serveur et il sera donc dans l'incapacité de les exploiter. Les méthodes de cryptage utilisées reposent sur les algorithmes triple DES pour la dérivation des clefs et AES pour le cryptage des données avec des clefs de 128 bits et sont donc extrêmement robustes.

Validy Web Business Server peut également être configuré pour utiliser le cryptage en voie montante. Cela permet :

- de transmettre en sûreté des informations sensibles dans l'URL ou le corps de la requête
- d'authentifier de manière infalsifiable le client qui a soumis la requête.

Les clefs utilisées pour le cryptage en voie montante combinent des nombres aléatoires tirés par le serveur et par le client avec la clef contenue dans la carte. Un mécanisme d'expiration et de vérification des clefs utilisées interdit de rejouer ou de modifier une requête qui aurait été interceptée.

Contenu du kit :

- 2 lecteurs de carte à puce
- 1 CD-Rom contenant les fichiers d'installation de Validy Web Business Customizer, Validy Web Server, Validy Web Cluster et Validy Web Client,
- 1 carte d'administration
- 3 cartes de démonstration personnalisables à volonté

Fichiers : Le CD-Rom contient des paquetages d'installation pour Windows, Linux et FreeBSD. Pour Windows :

1. VWB Cluster : gestionnaire de cluster
2. VWB Server for IIS : gestionnaire de serveur, filtre et extension ISAPI
3. VWB Server for Apache : gestionnaire de serveur et module apache 2.0
4. VWCustomizer : programme de personnalisation des cartes
5. VWB Client : logiciel client intégré au navigateur Internet Explorer et Web Portal.

Les installations 1 à 4 contiennent également le programme de mise à jour des fichiers udf (vwUpdate) et des fichiers d'exemple. Pour Linux (paquetages RPM) :

1. ValidyWebBusiness : gestionnaire de cluster et de serveur,
2. ValidyWebBusiness-apache : module apache 1.3,
3. ValidyWebBusiness-apache2 : module apache 2.0.

Les paquetages 2 et 3 dépendent du premier. Les paquetages suivants sont également nécessaires :

- libstdc++3.x qui contient la librairie standard C++,
- openssl-0.9.y pour sécuriser les communications entre gestionnaire de serveur et de cluster.

Pour FreeBSD (paquetages « ports ») :

1. vwb : gestionnaire de cluster et de serveur,
2. vwb-apache13 : module apache 1.3,
3. vwb-apache20 : module apache 2.0.

Configuration requise :

- Un PC sous Windows (95, 98, ME, NT, 2000 ou XP) avec 2 lecteurs de cartes à puce pour la machine de personnalisation
- Un PC sous Windows avec IIS, sous Linux ou FreeBSD avec Apache, et un lecteur de carte à puce pour la machine Validy Server si elle fonctionne sous Windows.

1.4 Configurations supportées

1.4.1 Serveur

Sur Windows, les serveurs Web supportés sont :

- IIS 4 (Windows NT 4.0)
- IIS 5 (Windows 2000)
- IIS 5.1 (Windows XP)
- IIS 6 (Windows 2003) En développement.
- Apache 2.0

Sur Linux, les combinaisons de distributions et de serveurs Web supportées sont :

- Red Hat 7.3 Apache 1.3.27
- Red Hat 7.3 Apache 1.3.28
- Red Hat 8.0 Apache 1.3.27
- Red Hat 8.0 Apache 1.3.28
- Red Hat Enterprise Linux 3 Apache 2.0.46
- Mandrake 8.2 Apache 1.3.26 (EAPI)
- Mandrake 8.2 Apache 1.3.27
- Mandrake 8.2 Apache 2.0.47
- Mandrake 9.0 Apache 1.3.26 (EAPI)
- Mandrake 9.1 Apache 1.3.27 (EAPI)
- Mandrake 9.1 Apache 2.0.47

EAPI indique une version compilée avec support pour mod-ssl.

Le support d'autres distributions Linux et de FreeBSD avec les serveurs Apache 1.3 et 2.0 est possible, nous consulter.

1.4.2 Client

Le client fonctionne sous Windows NT 4.0, 98 SE, 2000 ou XP avec Internet Explorer version 5.5 ou 6.0.

1.4.3 Incompatibilités connues

- Le module Validy pour Apache 2.0 ne fonctionne pas avec `mod_jk/mod_jk2` à cause d'une confusion entre les erreurs transmises par le module Validy au navigateur (pas de carte/droits insuffisants) et les erreurs renvoyées par le serveur Java (par exemple Tomcat) à `mod_jk/mod_jk2`.
- une applet Java ne peut pas charger des URL protégées par Validy car elle possède son propre module client du protocole HTTP.
- il ne semble pas possible d'avoir accès aux en-têtes `x-validy-info` ajoutées par le filtre Web Business dans une application WebDev.

2 Installation

! → Comme avant toute installation de logiciel, s'assurer qu'une sauvegarde des données sensibles de la machine a été effectuée récemment.

2.1 Installation sous Windows

2.1.1 Gestionnaire de serveur et filtre

Il suffit de lancer le programme d'installation souhaité (`Validy Web Business Server for IIS Setup.exe` pour IIS ou `Validy Web Business Server for Apache Setup.exe` pour Apache 2.0) et de suivre les instructions. Le gestionnaire de serveur est installé en tant que service. En dehors du répertoire d'installation de l'application, seule la racine de l'arborescence où seront placés les fichiers de configuration doit être saisie. Elle est stockée dans la base de registre sous la clef :

```
HKLM\CurrentControlSet\Service\vwbServerManager\Parameters
```

et peut être modifiée après l'installation.

Internet Information Server

Validy Web Server s'intègre dans IIS au moyen d'un filtre (IIS 4, 5 et 6) et d'une extension (IIS 6) ISAPI.

Deux copies du même filtre portant des noms différents sont fournies :

1. `vwbIsapiFilterDecryptPost.dll`.
2. `vwbIsapiFilter.dll`,

Les noms utilisés sont importants pour le bon fonctionnement du filtre. Ils ne doivent pas être changés.

L'extension existe en un seul exemplaire nommé `vwbIsapiExtension.dll`

L'inscription du filtre et de l'extension dépend à la fois de la version d'IIS utilisée (4/5 ou 6) et de l'utilisation ou non du cryptage en voie montante du corps des requêtes (POST ou PUT).¹

On distingue donc quatre cas :

1. **Utilisation du cryptage du corps des requêtes avec IIS 4 ou 5.**

Dans ce cas, il faut enregistrer le filtre `vwbIsapiFilterDecryptPost.dll` au niveau global du serveur².

¹ Le cryptage de l'URL ou des informations de personnalisation stockées dans la carte n'est pas concerné et est utilisable dans tous les cas.

² L'inscription au niveau global est plus coûteuse en ressources. Si vous n'utilisez que le cryptage des URL et des informations utilisateurs, enregistrez la DLL au niveau des sites.

2. Pas d'utilisation du cryptage du corps des requêtes avec IIS 4 ou 5.

Dans ce cas, il suffit d'enregistrer le filtre `vwbIsapiFilter.dll` au niveau de chaque site à protéger.

3. Utilisation du cryptage du corps des requêtes avec IIS 6.

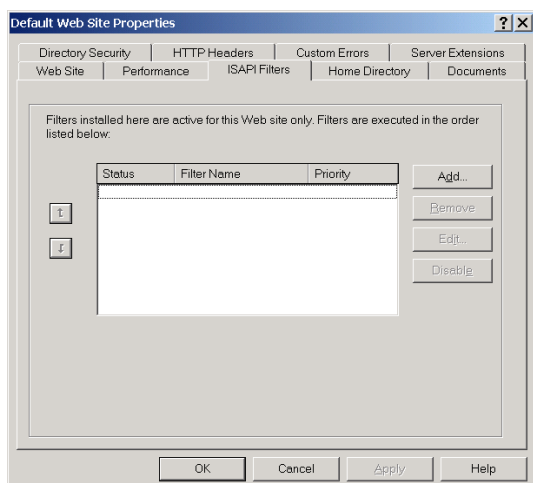
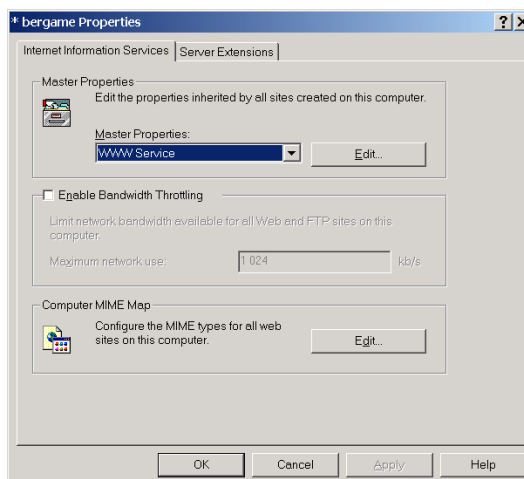
Dans ce cas, il faut enregistrer le filtre `vwbIsapiFilter.dll` et l'extension `vwbIsapiExtension.dll` en tant que «Mappage d'application générique» au niveau de chaque site à protéger.

4. Pas d'utilisation du cryptage du corps des requêtes avec IIS 6.

Dans ce cas, il suffit d'enregistrer le filtre `vwbIsapiFilter.dll` au niveau de chaque site à protéger.

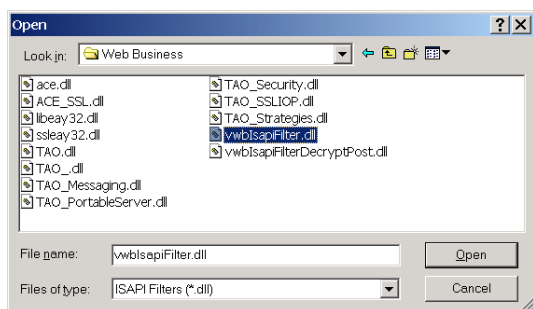
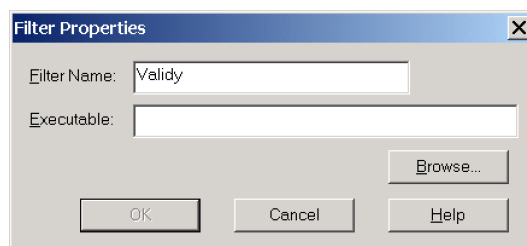
La procédure à suivre pour enregistrer le filtre est détaillée ci-après. Pour enregistrer `vwbIsapiFilterDecryptPost.dll`, commencez à l'étape [2.1](#), sinon commencez à l'étape [2.2](#)

2.1 Dans la console d'administration IIS, sélectionnez le serveur, appuyez sur le bouton droit de la souris et cliquez sur Propriétés. Dans l'onglet Internet Information Services, cadre Master Properties, vérifiez que WWW Services est bien sélectionné et cliquez sur Edit. La fenêtre Propriétés du serveur (2.2) apparaît, sélectionnez l'onglet Filtres ISAPI et passez à l'étape 2.3.



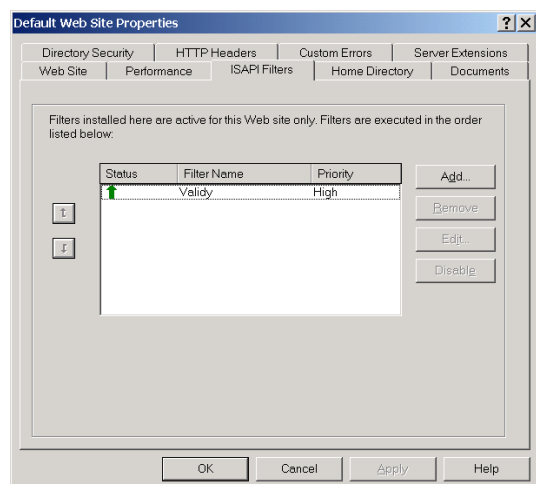
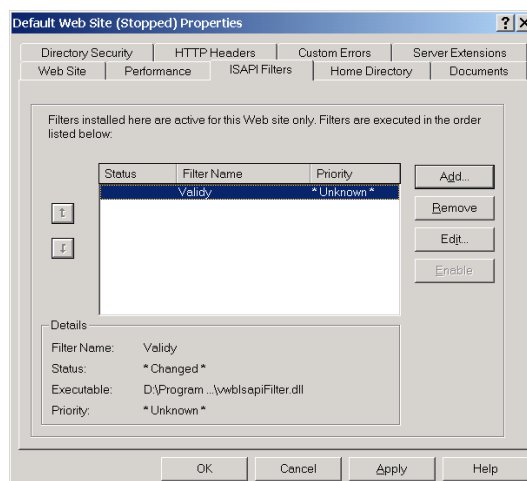
2.2 Dans la console d'administration IIS, sélectionnez le site web à protéger, appuyez sur le bouton droit de la souris et cliquez sur Propriétés. La fenêtre Propriétés du site apparaît, sélectionnez l'onglet Filtres ISAPI.

2.3 Créez un nouveau filtre ISAPI, pour cela, appuyez sur Ajouter, la fenêtre Propriétés du filtre apparaît, entrez Validy comme nom de filtre.



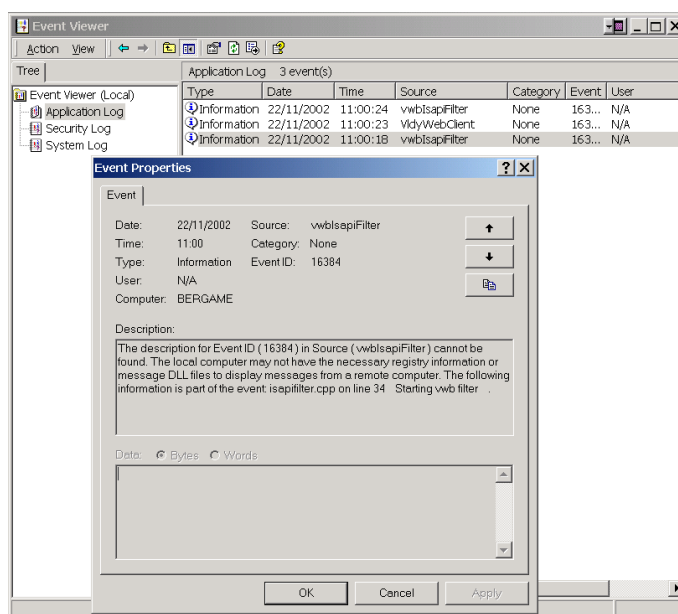
2.4 Cliquez sur Parcourir, puis sélectionnez la DLL vwbIsapiFilter.dll ou vwbIsapiFilterDecryptPost.dll qui se trouve dans le répertoire Program Files\Validy\Web Business. Cliquez sur Ouvrir.

2.5 Le filtre Vallyd créé apparaît dans la liste des filtres, il n'est pas encore actif. Appuyez sur Appliquer puis sur Ok pour fermer la fenêtre Propriétés.



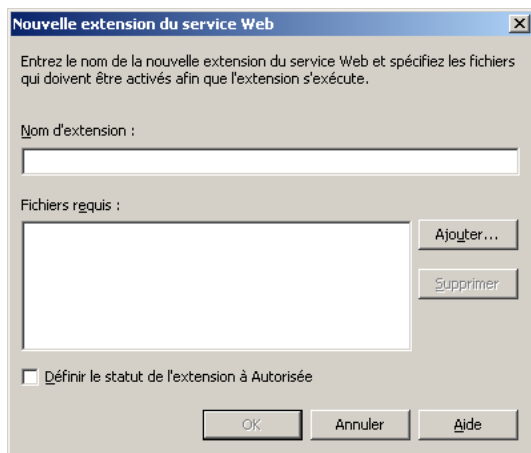
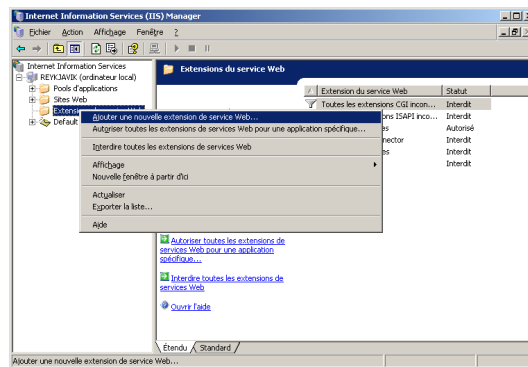
2.6 Pour que le filtre devienne actif il faut que le site que vous venez de protéger serve une page. Pour cela, lancez votre explorateur internet et connectez-vous au site pour lequel la DLL est active. Il n'est pas nécessaire de se connecter à une page protégée. Consultez à nouveau l'onglet Filtres ISAPI de la fenêtre Propriétés du site dans IIS afin de constater que le filtre est maintenant actif.

2.7 Vous pouvez également consulter le journal des applications à l'aide de l'observateur d'événements. Pour cela, dans le menu démarrer, lancez l'observateur d'événements qui se trouve dans le répertoire Outils d'administration. Dans l'onglet Journal sélectionnez le journal d'applications. Deux événements correspondent au lancement du filtre vwblsapiFilter, les descriptions des événements sont Starting vwbl filter et First request served.



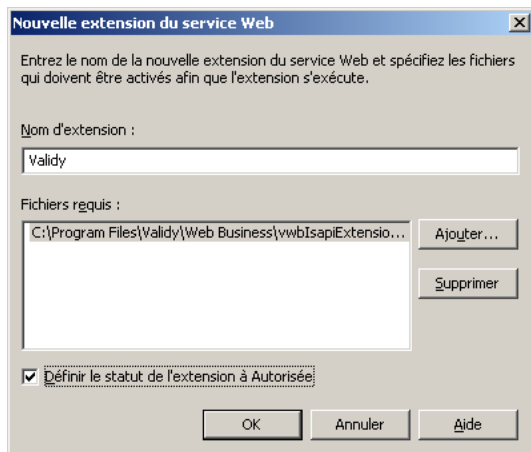
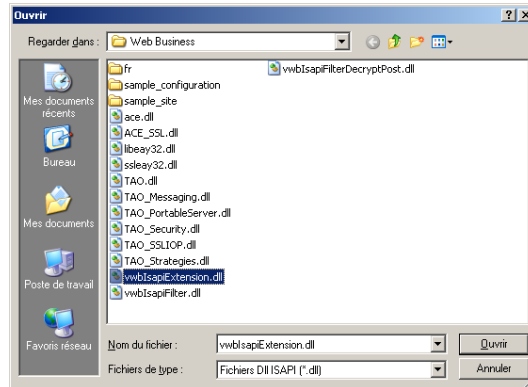
La procédure à suivre pour enregistrer l'extension est détaillée ci-après. Elle s'applique uniquement à IIS 6. Les cinq premières étapes (2.8 à 2.11) sont à effectuer une fois pour le serveur. Les deux dernières doivent être répétées avec chaque site pour lequel on souhaite utiliser le cryptage du corps des requêtes.

2.8 Dans la console d'administration IIS, sélectionnez le dossier Extensions du service Web, appuyez sur le bouton droit de la souris et cliquez sur Ajouter une nouvelle extension du service Web... La fenêtre Nouvelle extension du service Web (2.9) apparaît.



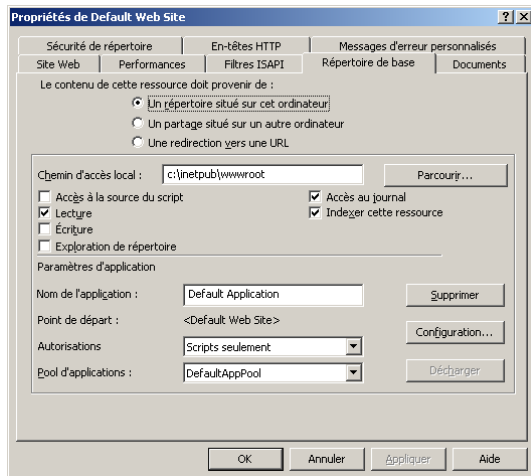
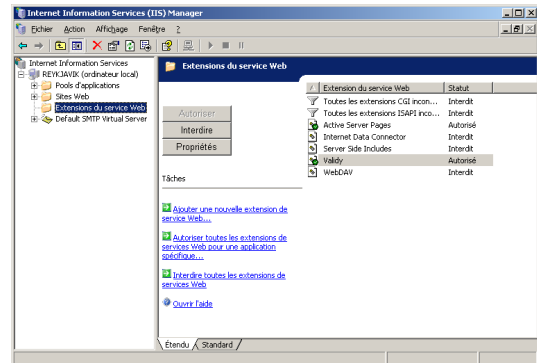
2.9 Entrez le nom Validy pour l'extension puis cliquez sur Ajouter à droite du cadre Fichiers requis.

2.10 Cliquez sur Parcourir, puis sélectionnez la DLL vwbIsapiExtension.dll qui se trouve dans le répertoire Program Files\Validy\Web Business. Cliquez sur Ouvrir.



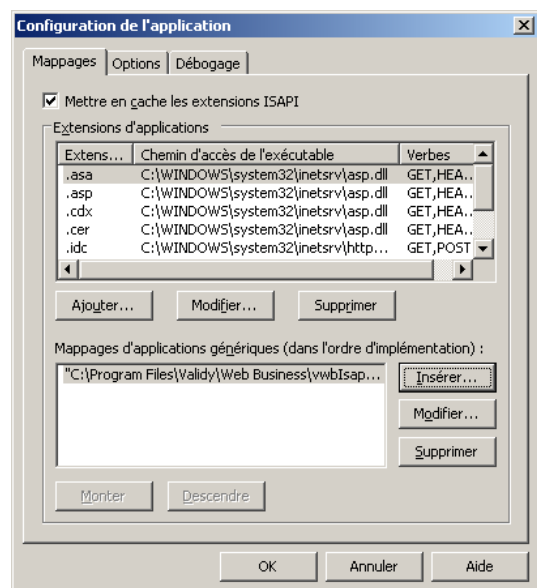
2.11 Cochez la case Définir le statut de l'extension à Autorisée et cliquez sur OK.

2.12 L'extension Validy créée apparaît dans la liste des extensions avec le statut Autorisé.



2.13 Dans la console d'administration IIS, sélectionnez un site, appuyez sur le bouton droit de la souris et cliquez sur Propriétés. Dans l'onglet Répertoire de base, cadre Paramètres d'application, cliquez sur Configuration.

2.14 A gauche du cadre Mappages d'applications génériques, cliquez sur Insérer et sélectionnez la DLL vwbIsapiExtension.dll comme en 2.10. Attention, il faut ensuite entourer le chemin sélectionné de guillemets car il contient un espace. Cliquez ensuite sur OK.



La version Serveur de Validy est maintenant installée, et active pour le site pour lequel vous avez ajouté le filtre (et si nécessaire l'extension) ISAPI. Vous pouvez protéger d'autres sites en répétant les mêmes opérations.

Attention, dans sa version 4, IIS comporte un bug qui n'a aucune incidence sur le fonctionnement de la DLL serveur Validy : Lorsqu'on fait pointer plusieurs filtres ISAPI sur le même fichier `vwbIsapiFilter.dll`, seul le premier créé apparaît comme ayant un statut actif (flèche verte vers le haut) dans la fenêtre Etat du filtre, les suivants apparaissent comme étant inactifs (flèche rouge vers le bas) bien qu'ils soient parfaitement opérationnels. De même, les messages relatifs au filtre au delà du premier n'apparaissent pas dans l'observateur d'événements. Ces problèmes concernent uniquement les informations affichées par IIS, et sont corrigés à partir de la version 5 de IIS. Ils n'interfèrent en aucune manière avec le bon fonctionnement de la DLL, que ce soit avec IIS 4, 5 ou 6.

- ! → Validy Web Business utilise les en-têtes standard d'authentification HTTP `WWW-Authenticate` et `Authorization`. Si l'authentification intégrée de Windows est active sur le site, Internet Explorer va intercepter les requêtes et présenter une fenêtre demandant au client de saisir un identifiant et un mot de passe.

Pour que le client Validy ait accès aux en-têtes et puisse authentifier automatiquement le client au moyen de la carte à puce, il faut désactiver l'authentification intégrée. Pour cela, dans les propriétés du serveur ou du site Web, sélectionnez l'onglet Sécurité de répertoire (Directory Security), puis dans le cadre Accès anonyme et contrôle d'authentification (Anonymous Access and Authentication Control), cliquez sur le bouton Modifier... (Edit...). Dans la fenêtre Accès authentifié (Authentication Methods) qui s'ouvre, assurez vous que la case Authentification intégrée de Windows (Integrated Windows Authentication) n'est pas cochée, puis cliquez sur OK.

- ! → Validy Web Business fait le lien entre une requête et la configuration d'un site au moyen du nom du site qui se trouve dans l'en-tête Host de la requête. Il ne faut pas que le serveur accepte de servir une requête en l'absence de cet en-tête, par exemple, quand le site est accédé par son adresse IP. Pour cela, il faut définir la valeur de l'en-tête de l'hôte en passant par l'onglet Site Web, cadre Identification de site Web, bouton Avancé dans la console d'administration IIS. La valeur utilisée doit être la même que le nom du répertoire situé sous `ValidyRootDir` et où se trouve les fichiers `siteConf.txt`, `permissions.txt` et `udf.txt` (voir 3.0.1).

Apache 2.0

Pour Apache 2.0, il faut ajouter la directive de chargement du module Validy dans le fichier `httpd.conf`, par exemple :

```
LoadModule validy_module "C:/Program Files/Validy/Web Business/mod_validy.so"
```

Comme dans la version 2.0 de Web Business, on peut activer ou désactiver le module pour un répertoire ou un hôte virtuel en utilisant les directives :

```
Validy On
```

ou :

```
Validy Off
```

Par défaut, le module n'est pas actif.

- ! → L'ajout du cryptage voie montante implique l'intervention du filtre Validy plus tôt dans le traitement de la requête par le serveur Apache. En particulier, les directives de niveau répertoire (<Directory> ou bien <Location>) ne sont pas connus avant le décryptage de l'URL. Pour cette raison, le module ne peut pas être activé pour un site au moyen des seules directives de niveau répertoire. Pour qu'un site soit protégé, il faut que la directive Validy On soit placée au niveau du serveur ou bien du site virtuel (<VirtualHost>) correspondant. On peut ensuite utiliser des directives au niveau répertoire pour désactiver ou réactiver le filtre localement.

La configuration suivante permet, par exemple, de protéger tous les sites à l'exception de `www.example2.com` et de ne pas traiter les fichiers du sous-répertoire `clear` pour le site `www.example1.com` :

```
Validy On

<VirtualHost *>

DocumentRoot /www/www.example1.com

ServerName www.example1.com

...

</VirtualHost>

<Directory "/www/www.example1.com/clear">

Validy Off

</Directory>

<VirtualHost *>

DocumentRoot /www/www.example2.com

ServerName www.example2.com

Validy Off

...

</VirtualHost>
```

2.1.2 Gestionnaire de cluster

L'installation du gestionnaire de cluster demande les informations suivantes :

- nom du cluster (c'est le nom qui sera donné dans la configuration d'un gestionnaire de serveur affilié, `siteConf.txt`, voir 3.1.2),
- nom de l'hôte sur lequel s'exécute le gestionnaire de cluster. Cela peut être un nom DNS ou une adresse IP. Il faut que la machine soit accessible par les gestionnaires de

- serveur sous ce nom,
 - numéro de port TCP pour la communication entre cluster et serveur,
 - numéro de port TCP SSL pour la communication sécurisée entre cluster et serveur,
 - racine de l'arborescence des fichiers de configuration décrite en 3.2.1.
- Les valeurs entrées sont stockées dans la base de registre sous la clef :

```
HKLM\CurrentControlSet\Service\vwbcClusterManager\Parameters
```

Elles peuvent être modifiées après l'installation.

2.2 Installation sous Linux

2.2.1 Gestionnaire de serveur

Pour un gestionnaire de serveur, il faut installer le paquetage ValidyWebBusiness :

```
rpm -ivh ValidyWebBusiness-3.0.x-1.i586.rpm
```

Les options de configuration qui sous Windows sont stockées dans la base de registres se trouvent dans le fichier de configuration `vwbusiness.conf` qui se trouve dans le répertoire `/etc` ou `/etc/opt/validy`. Ce fichier permet en plus de choisir de ne lancer que le gestionnaire de serveur ou de cluster. Ce fichier est inclus par le fichier de lancement `/etc/init.d/vwbusiness` qui ne doit pas lui être modifié.

2.2.2 Filtre Apache

Pour installer le filtre, il faut ajouter le paquetage correspondant à la version du serveur Apache utilisé. Ce paquetage ne comprend que le module Validy, qui peut donc être relogé avec les autres modules, en employant l'option `prefix`, par exemple :

```
rpm -ivh -prefix=/usr/local/apache2/modules  
ValidyWebBusiness-apache2-3.0.x-1.i586.rpm
```

L'emplacement des modules dépend de l'arrangement de votre installation Apache. L'installation Apache utilisée doit avoir été compilée avec le support pour le chargement dynamique de modules (DSO). Pour vous en assurer, exécutez la commande :

```
hhttpd -l
```

et vérifiez que `mod_so.c` fait partie des modules compilés. Vous devez ensuite ajouter la directive de chargement du module dans le fichier de configuration du serveur `httpd.conf`, dans la section `Dynamic Shared Support` :

```
LoadModule validy_module ../mod_validy.so
```

Le chemin vers le module dépend de votre installation Apache et doit être adapté.

Pour la version 1.3.x d'Apache, il peut exister en plus une section de reconstruction de la liste des modules qui commence par `ClearModuleList` et dans laquelle il faut ajouter en fin de liste la ligne :

```
AddModule mod_validy.c
```

Le module Validy peut être activé ou désactivé au niveau d'un serveur ou d'un répertoire en utilisant les directives :

```
Validy On
```

ou :

```
Validy Off
```

Par défaut, le module n'est pas actif.

- ! → Avec la version 1.3.x d'Apache, le filtre consomme des ressources pour capturer la réponse et y rechercher l'en-tête Validy, même pour les fichiers/URL qui ne sont pas protégés. Il est donc recommandé de ne l'activer que dans les répertoires contenant réellement des fichiers à protéger.

Avec la version 1.3.x uniquement, le filtre utilise des fichiers temporaires. Vous devez créer un répertoire pour ces fichiers. Ce répertoire doit être accessible en lecture, écriture et exécution à l'utilisateur désigné par la directive `User` du fichier `httpd.conf`, sous lequel Apache traite les requêtes (par défaut `nobody` ou `www`). On indiquera le chemin à utiliser au filtre avec la directive :

```
ValidyTmpDir /tmp/validy
```

Afin que les modifications de `httpd.conf` soient prises en compte, vous devez redémarrer le serveur Apache. Pour vous assurer que le module Validy a bien été chargé, vous pouvez consulter le fichier log d'erreur du serveur Apache. La ligne indiquant le démarrage du serveur doit comprendre la chaîne `Validy/3.0.x.y`

Pour aider à la mise au point, le module Validy ajoute 3 "notes" aux requêtes qu'il traite :

- `ValidyCookie` contient une reconstitution du cookie tel que l'aurait envoyé le client en version 2.0,
- `ValidyHeader` contient l'en-tête lu dans la réponse
- `ValidyDecision` contient 0 ou un code d'erreur si la requête est refusée (voir la section 4.3).

Il est possible d'exploiter ces notes en créant un fichier de log spécifique au moyen de la directive suivante (sur une seule ligne) :

```
CustomLog logs/validy "%T %t \"%r\"  
%{ValidyCookie}n %{ValidyHeader}n %{ValidyDecision}n"
```

2.2.3 Gestionnaire de cluster

Le gestionnaire de cluster se trouve dans le paquetage `ValidyWebBusiness`. Les options de configuration se trouvent dans `/etc/vwbusiness.conf` ou `/etc/opt/validy/vwbusiness.conf`. Pour une machine devant servir de gestionnaire de cluster seul, on activera seulement le démon `vwbcmd` :

```
RUN_CLUSTER_MANAGER=yes  
RUN_SERVER_MANAGER=no
```

2.3 Installation sous FreeBSD

L'installation est très proche de celle de Linux. Les paquetages s'installent avec la commande `pkg_add`. Pour un gestionnaire de serveur ou de cluster :

```
pkg_add vwb-3.0.x.0.tbz2
```

Les fichiers de configuration sont les mêmes mais pour respecter le placement standard sous FreeBSD, le fichier `vwbusiness.conf` se trouve sous `/usr/local/etc`. Le paquetage fournit un fichier avec des valeurs par défaut `vwbusiness.conf.sample` qu'il faut recopier sous le nom `vwbusiness.conf` et adapter.

Pour le filtre Apache, on ajoutera le paquetage correspondant à la version du serveur Apache utilisé, par exemple pour Apache 1.3 :

```
pkg_add vwb-apache13-3.0.x.0.tbz2
```

Les modifications de configuration du serveur Apache sont les mêmes que pour Linux (voir [2.2.2](#)).

3 Configuration

3.0.1 Fichiers de configuration

Les fichiers de configuration Web Business doivent être placés dans une arborescence dont la racine, `ValidyRootDir`, est choisie au moment de l'installation. Par défaut, `ValidyRootDir` est sur Windows :

```
%WINDIR%\validy
```

sur Linux :

```
/var/lib/validy
```

ou

```
/var/opt/validy
```

et sur FreeBSD :

```
/usr/local/var/lib/validy
```

Web Business utilise plusieurs fichiers de configuration :

1. `ValidyRootDir/siteName/siteConf.txt` décrit la configuration d'un site. Il est utilisé par le gestionnaire de serveur.
2. `ValidyRootDir/srvMgrClusters/clusterName/clustConf.txt` donne l'adresse d'un gestionnaire de cluster. Il est utilisé par le gestionnaire de serveur pour s'y connecter.
3. `ValidyRootDir/clustMgr/clusterName/sites.txt` donne la configuration d'un cluster. Il est utilisé par le gestionnaire de cluster.
4. `ValidyRootDir/siteName/permissions.txt` définit l'accès aux pages protégées en associant les catégories de carte aux labels utilisés. Il est décrit en détail à la section 4.1.
5. `ValidyRootDir/siteName/udf.txt` contient la base de données des cartes à puce pour un site indépendant. Ce fichier est créé par le programme de mise à jour de site ou de cluster `vwbUpdate` (voir la section 4.7) et utilisé par le gestionnaire de serveur.
6. `ValidyRootDir/clustMgr/clusterName/udf.txt` contient la base de données des cartes à puce pour un cluster. Il est utilisé par le gestionnaire de cluster.
7. `vwbsmd.conf` et `vwbsmd.conf` permettent de configurer la librairie de communication CORBA TAO qui est utilisée pour la communication entre gestionnaires de serveur et de cluster. Les fichiers `vwbsmd.conf` et `vwbscmd.conf` qui se trouvent dans le sous répertoire suivant, sur Windows :

```
\Program Files\Validy\Web Business\sample_configuration
```

sur Linux :

```
/usr/share/doc/validy/sample_configuration
```

ou

```
/opt/validy/share/doc/validy/sample_configuration
```

et sur FreeBSD :

```
/usr/local/share/doc/validy/sample_configuration
```

doivent être copiés dans le répertoire racine des fichiers de configuration (Validy-RootDir) si la fonction de gestion de cluster est utilisée. Ces fichiers doivent être modifiés quand SSL est utilisé pour sécuriser les communications entre cluster et server, voir la section 3.2.3.

Les fichiers `siteConf.txt`, `sites.txt` et `clustConf.txt` se composent de sections nommées (*scope*) qui peuvent être imbriquées. À l'intérieur de ces sections, on définit les clés de configuration qui peuvent prendre des valeurs de type booléen, entier, flottant, chaîne de caractère ou liste. Les commentaires sont à la mode C++. Un extrait de fichier est donné ci-dessous pour illustrer la syntaxe :

```
scope Site
{
    // une liste de chaînes de caractères
    Clusters = ("cluster0", "cluster1")
    scope Nonce
    {
        // une valeur entière
        Duration = 180
    };
    scope Capabilities
    {
        // une valeur booléenne
        crypt_upstream_url = true
    };
};
```

Dans la suite, on fera référence aux valeurs de configuration en utilisant une notation pointée : `Site.Nonce.Duration`.

Un exemple de chacun des fichiers de configuration décrits ci-dessous se trouve installé sous le répertoire `sample_configuration`.

Les fichiers de configuration contiennent des données sensibles. Il ne faut pas les placer dans la même arborescence que le contenu du site et il faut éviter de les placer dans l'arborescence où sont installés les fichiers de Validy Web Server (exécutables et bibliothèques partagées).

Il est important de distinguer :

1. le contenu du site qui se trouve par défaut sous `C:\Inetpub\wwwroot` pour IIS et sous `htdocs` pour Apache,
2. les fichiers exécutables de Validy Web Server qui se trouvent par défaut sous `C:\Program Files\Validy` pour Windows et sous `/usr` pour Linux,
3. les fichiers de configuration du site qui se trouvent sous `C:\Validy\nom.du.site` pour Windows et sous `/var/lib/validy/nom.du.site` pour Linux.

3.1 Gestionnaire de serveur

3.1.1 Site indépendant

La configuration d'un site indépendant (standalone) se compose des fichiers `udf.txt`, `siteConf.txt`, et `permissions.txt`. On retrouve une structure proche de celle de la version 2.0 (voir la Figure 3.1).

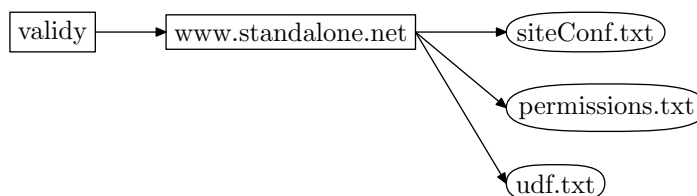


FIG. 3.1: Fichiers de configuration pour un site indépendant.

Les valeurs de configuration qui peuvent être définies pour un site indépendant dans le fichier `siteconf.txt` sont données dans le Tableau 3.1.

TAB. 3.1: Contenu de `siteConf.txt` pour un site indépendant

Clef	Type	Par défaut	Définition
Site.MaxBackupFiles	entier	5	nombre maximum de sauvegardes du fichier <code>udf.txt</code> maintenues lors des mises à jour ¹ .
Site.MaxCreditUsedBeforeSync	entier	1	nombre d'unités de crédit décomptées par le serveur pour l'ensemble des cartes Validy Web Use du site avant que l'information cachée en mémoire ne soit écrite sur le disque dur. ²
Site.MaxPageCoef	entier	100	le coût maximal d'une page Web Use ; si un label de page indique un coût supérieur, celui-ci est ramené à cette valeur par le serveur
Site.UrlPrefix	chaîne	""	le préfixe des URL qui doivent être protégées par un cryptage voie montante si celui-ci est actif
Site.ErrorPages.*	chaîne	-	Pages retournées au client en cas d'erreur
Site.ErrorPages.NoAccess	chaîne	<code>/err/vdyerr3.html</code>	Pas de carte insérée dans le lecteur
Site.ErrorPages.BadCard	chaîne	<code>/err/vdyerr4.html</code>	Mauvaise carte insérée dans le lecteur
Site.ErrorPages.MuteCard	chaîne	<code>/err/vdyerr5.html</code>	La carte insérée ne répond pas
Site.ErrorPages.InsuffRights	chaîne	<code>/err/vdyerr6.html</code>	Droits insuffisants pour accéder à cette page
Site.ErrorPages.InsuffCredits	chaîne	<code>/err/vdyerr7.html</code>	Crédits insuffisants pour accéder à cette page

¹ Lors d'une mise à jour du serveur (voir page 34), une sauvegarde de l'ancien fichier `udf.txt` est effectuée automatiquement afin de pouvoir restaurer la version précédente en cas d'erreur ou de problème.

² Pour des sites gérant des cartes Validy Web Use et ayant un trafic important, il est possible d'augmenter la valeur de ce paramètre pour éviter des accès disques répétés au niveau du serveur. Par exemple en réglant le paramètre à 1000, les informations stockées sur le disque dur sont resynchronisées avec la version cachée en mémoire lorsque 1000 unités ont été débitées par le serveur pour l'ensemble des cartes Validy Web Use ayant accédé au site.

TAB. 3.1: Contenu de siteConf.txt pour un site indépendant

Clef	Type	Par défaut	Définition
Site.ErrorPages.WrongCluster	chaîne	/err/vdyerr9.html	La carte ne correspond pas au site/cluster
Site.Capabilities.*	booléen	true	
Site.Capabilities.units	booléen	true	Web Units
Site.Capabilities.loyalty	booléen	true	Web Loyalty
Site.Capabilities.user_access	booléen	true	Web Site avec accès individuel
Site.Capabilities.group_access	booléen	true	Web Site avec accès de groupe
Site.Capabilities.use	booléen	true	Web Use
Site.Capabilities.cluster	booléen	true	support des clusters
Site.Capabilities.send_user_info	booléen	true	envoi d'en-têtes contenant les informations utilisateurs stockées sur la carte
Site.Capabilities.crypt_upstream_header	booléen	true	cryptage des informations utilisateurs
Site.Capabilities.crypt_upstream_url	booléen	true	cryptage des URL en voie montante
Site.Capabilities.crypt_upstream_body	booléen	true	cryptage des données de post
Site.Capabilities.crypt_redirect_location	booléen	true	cryptage des URL de redirection (voie descendante)
Site.Capabilities.crypt_downstream_text	booléen	true	cryptage descendant des réponses de type MIME text/*
Site.Capabilities.crypt_downstream_image	booléen	true	cryptage descendant des réponses de type MIME image/*
Site.Capabilities.crypt_downstream_other	booléen	true	cryptage descendant des réponses d'autres types
Site.Nonce.Duration	entier	120	Intervalle entre deux tirages de nonce ³ par le serveur (en secondes)
Site.Nonce.NbKept	entier	2	Nombre de nonces conservés et considérés comme valides par le serveur

3.1.2 Site affilié à un cluster

La configuration d'un site affilié à un ou plusieurs clusters (clustered) se compose des fichiers `siteConf.txt` et `permissions.txt`. Il n'y a pas de fichier `udf.txt` puisque la base de données des cartes autorisées à utiliser le site est gérée par les clusters auxquels il est affilié (voir Figure 3.2).

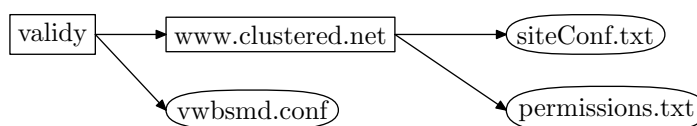


FIG. 3.2: Fichiers de configuration pour un site affilié à un cluster.

Les valeurs de configuration pour un site affilié sont celles d'un site isolé avec deux exceptions :

³ Un nonce est un nombre aléatoire tiré par le serveur et qui intervient dans le calcul de la clef utilisée par le client pour le cryptage en voie montante. En conservant les dernières valeurs choisies et une trace des requêtes qui les ont utilisées, le serveur peut vérifier qu'une requête n'est jamais rejouée. Un nonce tiré par le client est aussi utilisé pour empêcher un serveur malveillant d'obtenir le calcul par la carte du client de clefs choisies par lui seul.

1. la liste `Site.Clusters` doit contenir la liste des noms des clusters auxquels le site est affilié (voir Tableau 3.2),
2. `Site.MaxCreditUsedBeforeSync` et `Site.MaxBackupFiles` n'ont pas de sens.

TAB. 3.2: Contenu supplémentaire de `siteConf.txt` pour un site affilié

Clef	Type	Par défaut	Définition
<code>Site.Clusters</code>	liste de chaînes	()	liste des noms des clusters auxquels le site est affilié.

Pour chaque cluster auquel un des sites gérés par le serveur doit se connecter, un répertoire portant le nom du cluster doit être créé dans le sous-répertoire

`ValidyRootDir/srvMgrClusters`.

Ce répertoire contient le fichier `clustConf.txt` qui permet au gestionnaire de serveur de se connecter au gestionnaire de cluster. On aboutit à l'arborescence de la Figure 3.3.

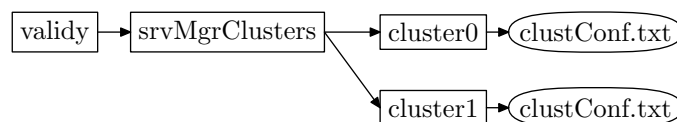


FIG. 3.3: Fichiers de configuration pour un site appartenant à un cluster (suite).

Les fichiers `clustConf.txt` sont produits automatiquement en fonction de la configuration du gestionnaire de cluster (voir 3.2.2). Ils peuvent être complétés par l'administrateur du serveur pour ajuster la taille du cache associé au cluster et le timeout sur les communications (voir Tableau 3.3).

TAB. 3.3: Contenu de `clustConf.txt` pour un cluster référencé

Clef	Type	Par défaut	Définition
<code>Cluster.CorbaRef</code>	chaîne	-	adresse CORBA du gestionnaire de cluster (produite automatiquement)
<code>Cluster.CacheSize</code>	entier	64	taille du cache de cartes maintenu par le serveur pour ce cluster
<code>Cluster.Timeout</code>	entier	10	timeout pour les requêtes vers ce cluster (en secondes)

3.2 Gestionnaire de cluster

3.2.1 Configuration

La configuration d'un cluster se compose des fichiers `udf.txt` et `sites.txt` (voir la Figure 3.4).

Le fichier `sites.txt` décrit les sites pouvant se connecter au cluster manager et pour chacun, les capacités actives. A chaque site est associée une section du fichier de configuration `Cluster.SiteI`, où $I = 0 \dots N$. Les valeurs de configuration pour un cluster sont

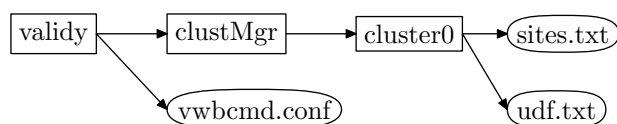


FIG. 3.4: Fichiers de configuration pour un cluster.

décrites dans le Tableau 3.4.

TAB. 3.4: Contenu de sites.txt pour un cluster

Clef	Type	Par défaut	Définition
Cluster.MaxBackupFiles	entier	5	même définition que pour un site indépendant (3.1)
Cluster.MaxCreditUsedBeforeSync	entier	1	même définition que pour un site indépendant (3.1)
Cluster.Site I .Name	string	-	nom du site I , par exemple www.clustered.net
Cluster.Site I .Capabilities.*	booléen	true	même définition pour le site I que pour un site indépendant

Pour qu'une fonction soit réellement active sur un site appartenant à un cluster, il faut qu'elle soit active dans la configuration du gestionnaire de serveur (`siteConf.txt`) et dans celle du gestionnaire de cluster (`sites.txt`).

3.2.2 Production du fichier `clustConf.txt`

L'administrateur du cluster doit produire le fichier `clustConf.txt` pour son cluster et le transmettre aux administrateurs des gestionnaires de serveurs affiliés. Pour cela, il suffit d'exécuter l'une des commandes suivantes. Pour Windows :

```
"%ProgramFiles%\Validy\Web Business\vwbcmd.exe" /conf > clustConf.txt
```

pour Linux :

```
/etc/init.d/vwbusiness conf > clustConf.txt
```

et pour FreeBSD :

```
/usr/local/etc/rc.d/vwbusiness conf > clustConf.txt
```

! → Le contenu du fichier `clustConf.txt` dépend du nom du cluster, du nom de sa machine hôte, des ports TCP choisis et de l'utilisation ou non de la sécurisation SSL (mais pas des certificats employés). Si l'un de ces éléments change, il faut produire un fichier mis à jour et le transmettre. Ce fichier doit être placé dans le répertoire

```
ValidyRootDir/srvMgrClusters/ClusterName
```

sur les serveurs.

3.2.3 Sécurisation de la communication entre gestionnaire de serveur et de cluster

SSL peut être utilisé pour sécuriser la communication entre gestionnaire de serveur et de cluster (en utilisant le protocole SSLIOP). Il est possible d'authentifier le gestionnaire de cluster auprès du gestionnaire de serveur et le gestionnaire de serveur auprès du gestionnaire de cluster. Les étapes pour la configuration du gestionnaire de cluster sont les suivantes :

1. produire un certificat pour le gestionnaire de cluster (et éventuellement un pour le gestionnaire de serveur). Le certificat du gestionnaire de cluster sera fourni à l'administrateur du serveur en même temps que le fichier `clustConf.txt`. Pour permettre le démarrage automatique du gestionnaire de cluster, il faut produire une clef privée non protégée par une phrase de passe et sécuriser le fichier correspondant,
2. dans le fichier `vwbcmd.conf`, décommenter les deux lignes indiquées et fournir les chemins vers le certificat (option `-SSLCertificate`) et vers la clef privée (option `-SSLPrivateKey`). Attention, sous Windows, l'interprétation du caractère « : » par TAO ne permet pas d'utiliser la lettre du disque dans le nom du fichier. La solution la plus simple consiste à placer les certificats sur le même disque que le répertoire de travail des services (`%SYSTEMDRIVE%`) et à utiliser un chemin absolu pour le nom du fichier, par exemple `\winnt\certs\clustercert.pem`.

Les étapes pour la configuration du server manager sont :

1. dans le fichier `vwbsmd.conf`, décommenter les deux lignes indiquées,

2. placer dans l'environnement les variables `SSL_CERT_FILE` et `SSL_CERT_DIR` (voir la définition de ces variables dans la documentation d'OpenSSL).
Sous Windows, ces variables doivent être placées dans l'environnement « System » et non dans celui de l'administrateur.
Sous Linux (resp. FreeBSD), il suffit d'éditer le fichier `/etc/vwbusiness.conf` ou `/etc/opt/validy/vwbusiness.conf` (resp. `/usr/local/etc/vwbusiness.conf`).
3. copier le certificat fourni par l'administrateur du cluster manager dans le répertoire `SSL_CERT_DIR` et l'indexer (voir la documentation SSL).

Cette procédure ne correspond qu'au cas de l'authentification du cluster auprès du server. Pour authentifier le server auprès du cluster, il faut effectuer les procédures symétriques puis remplacer l'option :

```
-SSLAuthenticate SERVER
```

par

```
-SSLAuthenticate SERVER_AND_CLIENT
```

dans les fichiers `vwbcmd.conf` et `vwbsmd.conf`. Enfin, il faut ajouter les options `-SSLCertificate` et `-SSLPrivateKey` dans le fichier `vwbsmd.conf`.

4 Fonctionnement

4.1 Gestion des permissions

Pour chaque site protégé, Vality Web Business Server va lire les informations concernant la protection des pages dans le fichier `permissions.txt` qui se trouve dans un répertoire du type `www.nom-du-site.com`. En fonction du système d'exploitation du serveur, ce fichier peut être dans notre exemple, pour Windows :

```
c:\validy\www.example.com\permissions.txt
```

pour Linux :

```
/var/lib/validy/www.example.com/permissions.txt
```

ou

```
/var/opt/validy/www.example.com/permissions.txt
```

et pour FreeBSD :

```
/usr/local/var/lib/validy/www.example.com/permissions.txt
```

Chaque fichier `permissions` est une suite de lignes de la forme suivante :

```
LABEL CATEGORIE PERIODE_DE_VALIDITE
```

Où :

- LABEL est le label inséré dans la page protégée du site,
 - CATEGORIE est la catégorie d'utilisateur à laquelle correspond la carte,
 - PERIODE_DE_VALIDITE est la période durant laquelle cet accès est valide.
- PERIODE_DE_VALIDITE peut prendre les valeurs suivantes :

```
always
before time_andor_date
after time_andor_date
between time_andor_date1 and time_andor_date2
```

où `time_andor_date` (en heure locale du serveur) peut avoir l'une des 3 formes suivantes :

1. `yyyy/mm/dd hh :mm`
2. `yyyy/mm/dd` l'heure est implicitement fixée à `00 :00`
3. `hh :mm` implicitement, pour chaque jour

Les lignes ayant une mauvaise syntaxe, les lignes blanches ou commençant par `//` sont ignorées.

Pour toute requête sur une page possédant un label, le serveur parcourt la liste des permissions. S'il trouve une ligne pour laquelle label et catégorie correspondent et pour laquelle l'accès est dans la période valide, il accepte d'envoyer la page au client. S'il arrive en fin de liste, l'accès est refusé avec l'erreur `InsufficientRights`.

Quand le fichier `permissions.txt` est mis à jour le serveur prend en compte la nouvelle version au bout de 20 secondes environ.

Le fichier `permissions.txt` dans le sous répertoire `sample_site` contient des exemples.

4.2 Protection des pages Web

4.2.1 Voie descendante (du serveur vers le client)

Validy Web Business Server reconnaît les pages à protéger lorsqu'elles ont un en-tête particulier, qui a pour nom `Validy` et pour valeur le label de la page en question. Plusieurs techniques sont disponibles pour ajouter ce label à la page en fonction du serveur Web ou de l'application qui produit le contenu de la page.

IIS

Pour une page ASP, le fragment de code VBScript suivant ajoute le label `Validy` dans la page :

```
<%@ Language=VBScript %>
<% response.AddHeader "validy", "label" %> pour Web Site
<% response.addheader "validy", "label#N"%> pour Web Use,
```

où `N` est le nombre d'unités débitées pour visualiser cette page. `N` peut avoir toute valeur entre 0 et 100 inclus.

Pour une page Cold Fusion, le fragment de code suivant ajoute le label `Validy` dans la page :

```
<cfheader name="validy" value="label"> pour Web Site
<cfheader name="validy" value="label#N"> pour Web Use
```

Il est également possible d'ajouter le label à toutes les pages du site ou d'un répertoire en éditant ses propriétés avec la console Internet Information Services. Dans l'onglet HTTP Headers, cadre Custom HTTP Headers, cliquez sur Add puis saisir `Validy` comme Custom Header Name et le label comme Custom Header Value.

La méthode de marquage des pages par un label `Validy` s'étend au cryptage de l'en-tête `Location` pour la redirection vers une autre page. Par exemple, on peut réaliser une redirection vers une URL cryptée en ASP avec la page suivante :

```
<%@ LANGUAGE = VBScript %>
<% Option Explicit %>
<% Response.AddHeader "validy", "MonLabel" %>
<% Response.Redirect("http://" &
Request.ServerVariables("SERVER_NAME") & "/redirected.asp") %>
```

! → L'URL de redirection qui va être renvoyée cryptée au client doit être absolue. Le client `Validy Web Business` ne sait pas traiter une URL relative cryptée.

Apache

Pour une page PHP, le fragment de code suivant ajoute le label `Validy` dans la page :

```
<?php header("Validy: label")?>
```

Il est également possible d'utiliser le module headers (livré en standard mais qu'il faut activer au moment de la configuration) pour l'ensemble des fichiers d'un répertoire donné. Il faut alors ajouter une directive dans le fichier de configuration. Par exemple :

```
<Directory "/usr/local/apache/htdocs/x/y">
    Validy On
    Header set Validy label
</Directory>
```

On peut réaliser une redirection vers une URL cryptée en PHP avec le code suivant :

```
<?php
$headers = getallheaders();
$host = $headers["Host"];
header ("validy: MonLabel");
header ("Location: http://$host/redirected.php");
exit;
?>
```

4.2.2 Voie montante (du client vers le serveur)

Avec le cryptage en voie descendante, un client ne possédant pas de carte peut tout de même provoquer l'exécution d'une requête sur le serveur. La vérification d'accès se fait en cherchant le label Validy une fois la page produite par le serveur. Un client peut contrefaire la possession d'une carte en utilisant un identifiant valide. Il lui sera par contre impossible de décrypter la réponse.

Outre la protection des données circulant entre le client et le serveur, le cryptage en voie montante permet d'implanter un contrôle d'accès en amont de l'exécution de la requête. On peut ainsi protéger des sites pour lesquels, l'exécution de la requête elle-même doit être interdite parce qu'elle provoque des effets de bord sur le serveur, par exemple la mise à jour d'une base de données.

Les URL pour lesquelles le cryptage montant est nécessaire sont définies par le champ `UrlPrefix` dans le fichier de configuration `siteConf.txt` (voir 3.1). Toutes les URL commençant par ce préfixe seront interdites d'accès par le serveur si elles sont réclamées en clair.

Le cryptage en voie montante du corps de la requête (POST ou PUT) ne peut se faire que vers des URL commençant par ce préfixe. Si les fonctions `send_user_info` et `crypt_upstream_header` sont actives, les informations utilisateurs seront envoyées cryptées avec les requêtes vers des URL commençant par ce préfixe et pas envoyées du tout sinon.

Pour permettre le contrôle d'accès, le filtre Validy Web Business met à la disposition de l'application deux en-têtes :

- `x-validy-info0` contient l'identifiant de la carte,
- `x-validy-info3` contient la catégorie à laquelle elle appartient.

Ces deux en-têtes constitue une identification forte du client. Elles sont disponibles uniquement si le cryptage voie montante a été utilisé et si le client a fourni une autorisation valide. L'autorisation protège contre la répétition (*replay*) des requêtes et la modification de l'URL ou des informations utilisateurs pendant le transfert entre le client et le serveur.

Deux autres en-têtes sont également disponibles :

- x-validy-info1 contient le nom de l'utilisateur,
- x-validy-info2 contient l'information supplémentaire stockée dans la carte.

Ces en-têtes peuvent être transmis en clair entre le client et le serveur si le cryptage voie montante n'est pas utilisé et ne peuvent donc pas être utilisés pour réaliser le contrôle d'accès. Par contre, si l'en-tête x-validy-info0 est présent, alors le contenu de x-validy-info1 et x-validy-info2 est lui aussi authentifié.

Les en-têtes x-validy-info remplacent les données fournies par le cookie Validy dans la version 2. Ils ne font pas partie tels quels de la requête envoyée par le client au serveur mais sont reconstruits par le filtre à partir du contenu de l'en-tête standard Authorization pour le schéma d'authentification Validy.

4.3 Messages d'erreur

Validy Web Business Server peut produire des messages d'erreurs suite à une requête venant d'un navigateur client. 9 types d'erreur différents peuvent se présenter :

1. Version du navigateur non supportée,
2. Pas d'en-tête d'autorisation alors que la page est protégée (client non installé sur le navigateur),
3. Pas de carte insérée dans le lecteur,
4. Mauvaise carte insérée dans le lecteur,
5. Carte muette,
6. Pas les droits requis,
7. Carte Web Use n'ayant pas le crédit suffisant pour cette page,
8. Fonction non supportée par le serveur,
9. La carte dans le lecteur correspond à un autre site/cluster

Lorsqu'une erreur est rencontrée, une redirection est faite vers la page configurée dans le fichier `siteConf.txt` (voir le Tableau 3.1). Dans le cas de l'erreur 3, la code de la réponse est 401 Authorization required mais le traitement de ce code de retour est fait automatiquement par le logiciel client et l'erreur est présentée l'utilisateur uniquement si aucune carte n'est trouvée. Des exemples de messages d'erreurs se trouvent installés dans le répertoire suivant, pour Windows :

```
\Program Files\Validy\Web Business\sample_site\www.example.com\err
```

pour Linux :

```
/usr/share/doc/validy/sample_site/www.example.com/err
```

ou

```
/opt/validy/share/doc/validy/sample_site/www.example.com/err
```

et pour FreeBSD :

```
/usr/local/share/doc/validy/sample_site/www.example.com/err
```

4.4 Cookie Validy

Dans la version 2 de Validy Web Business, le logiciel client s'identifiait auprès du serveur en envoyant un cookie produit à partir du contenu de la carte. **Ce cookie n'existe plus.** Dans la version 3, les informations client sont contenues dans l'en-tête HTTP standard `Authorization` pour le schéma d'authentification Validy. Elles peuvent être cryptées en fonction de la configuration du serveur.

L'application doit utiliser les en-têtes `x-validy-info` à la place du cookie Validy pour contrôler l'accès aux pages ou en personnaliser le contenu en fonction du client. Le Tableau 4.1 rappelle la définition de ces en-têtes et donne la correspondance avec les champs du cookie de la version 2.

TAB. 4.1: En-têtes d'information Validy

En-tête	Contenu	Authenticité	Equiv. cookie
x-validy-info0	identifiant de la carte	oui	champ 2 (ident)
x-validy-info1	nom de l'utilisateur	si x-validy-info0 est présent	champ 3 (name)
x-validy-info2	info supplémentaire	si x-validy-info0 est présent	champ 4 (company)
x-validy-info3	catégorie de la carte	oui	-

Le code suivant montre comment récupérer la valeur des en-têtes Validy en ASP :

```
<%@ LANGUAGE = VBScript %>
<% Option Explicit %>
<%
    Dim sId, sName, sExtra, sCategory
    Set sId = Request.ServerVariables("HTTP_X_VALIDY_INFO0")
    Set sName = Request.ServerVariables("HTTP_X_VALIDY_INFO1")
    Set sExtra = Request.ServerVariables("HTTP_X_VALIDY_INFO2")
    Set sCategory = Request.ServerVariables("HTTP_X_VALIDY_INFO3")
%>
```

et en PHP :

```
<?php
$headers = getallheaders();
$id = $headers["x-validy-info0"];
$name = $headers["x-validy-info1"];
$extra = $headers["x-validy-info2"];
$category = $headers["x-validy-info3"];
?>
```

4.5 Variables Web Use

Deux variables relatives à Validy Web Use sont gérées par le serveur. Il s'agit de :

- `vdyvar_cost` qui correspond au coût de la page courante,
- `vdyvar_balance` qui correspond au nombre d'unités restant sur la carte de l'utilisateur.

Pour les afficher il suffit d'insérer leur nom en commentaire à l'intérieur du code HTML. Le serveur Validy les remplace alors par leurs valeurs respectives. Par exemple :

```
<html>
Cette page coûte <!--vdyvar_cost--> unités.
Il reste <!--vdyvar_balance--> unités sur votre carte.
</html>
```

4.6 Personnalisation électrique des cartes à puce

Le kit contient une carte administrateur vous permettant de personnaliser des cartes Validy et 3 cartes Validy pouvant être personnalisées à volonté, un nombre illimité de fois. Vous devez au préalable installer Validy Web Customizer sur la machine de personnalisation afin que les lecteurs de cartes à puce soient reconnus. Pour cela vous pouvez utiliser le program d'installation `\win32\WVCustomizer w.x.y.z Setup.exe` qui se trouve sur le CD-Rom. Le programme de personnalisation est ensuite accessible dans le menu Démarrer, Validy, Customizer.

Le programme présente une première page qui permet de sélectionner les lecteurs à utiliser pour la carte d'administration et la carte à personnaliser puis une deuxième page pour les applications à personnaliser et l'utilisation ou non d'un code PIN.

- ! → Toutes les applications ne peuvent pas être utilisées avec toutes les cartes. Pour des cartes Web Business, vous pouvez sélectionner les applications Web Business et Web Portal. Pour les autres applications, cochez la case Ignorer. Le programme propose ensuite de saisir les différents champs en fonction de la ou des applications et modes (Web Loyalty, Web Site, Web Use) retenus.

Sélectionner un PIN code pré-expiré va forcer l'utilisateur à choisir son PIN code à la première utilisation de la carte. La valeur par défaut du PIN code doit être donné à l'utilisateur pour lui permettre de le changer.

Le dernier écran de saisie permet de fournir les informations utilisateurs : nom et information supplémentaire stockée sur la carte. Dans ces deux champs, les espaces sont remplacés par des "_". L'identifiant de carte peut être saisi explicitement ou calculé automatiquement.

Le programme demande ensuite l'insertion de la carte d'administrateur, nécessaire pour créer des cartes Validy. Lorsque la carte est détectée dans le lecteur d'administration, il faut saisir son PIN. On peut ensuite vérifier sur la page suivante les éléments qui vont être inscrits dans la carte à personnaliser puis l'insérer dans le second lecteur. La carte est ensuite personnalisée.

Une fois la personnalisation terminée et la carte personnalisée retirée, on revient à l'écran de saisie des informations utilisateurs. On peut ainsi répéter l'opération plusieurs fois pour des cartes ayant les mêmes droits mais des noms d'utilisateur différents. Pour changer les autres champs (nom du site, catégorie, URL pour Web Portal, etc.) il suffit d'utiliser le bouton Retour pour revenir à la page correspondante.

4.7 Mise à jour du serveur

Lors de la personnalisation des cartes, un fichier update est produit dans le répertoire %temp% (par exemple c:\temp) de la machine de personnalisation. Ce fichier a pour nom nom_du_site.upd ou nom_du_cluster.upd (par exemple www.example.com.upd). Si la machine de personnalisation n'est pas la même que la machine serveur, il faut transférer le fichier upd sur le serveur pour pouvoir effectuer la mise à jour.

Pour mettre à jour le serveur avec les informations contenues dans le fichier update, il faut utiliser le programme vwbUpdate.exe, sur la machine serveur. Ce programme est accessible par le menu Démarrer, Validy Web Business, Updater.

vwbUpdate demande les paramètres suivants :

- Chemin d'accès aux fichiers de configuration Web Business (c:\Validy) :
- Nom du site à mettre à jour : www.example.com
- Fichier de mise à jour : chemin d'accès au fichier update produit par le customizer (c:\temp\www.example.com.upd).
- Mettez-vous à jour un serveur ou bien un cluster (serveur) : server

Le programme demande ensuite l'insertion de la carte d'administrateur dans le lecteur 0, la saisie de son PIN, et met à jour le fichier udf.txt, se trouvant dans le répertoire c:\Validy\www.example.com\ et contenant les informations sur les cartes valides pour le site www.example.com. La procédure à suivre est reprise dans l'exemple de la section 5.

- ! → Le programme de mise à jour fonctionne pour l'instant uniquement sur machine Windows. Pour un serveur Linux ou FreeBSD, il faut donc faire tourner le programme de mise à jour sur la machine de personnalisation puis transférer le fichier udf.txt sur le serveur. Comme le contenu du fichier udf.txt est sensible, on aura intérêt à utiliser une disquette en procédant comme suit :

1. placer une disquette formatée dans le lecteur de la machine de personnalisation,
2. lancer le programme de mise à jour et donner la racine du lecteur de disquette (a:\) comme chemin d'accès aux fichiers de configuration Web Business,
3. placer la disquette dans le lecteur du serveur et copier le fichier udf.txt à son emplacement dans l'arborescence ValidyRootDir du serveur,
4. formater la disquette.

4.8 Action au retrait de la carte

La fonction Validy Web Portal permet de lancer le navigateur Internet vers une page après l'insertion de la carte dans le lecteur. L'URL de cette page est fixée au moment de la personnalisation électrique de la carte à puce et stockée dans celle-ci.

Portal permet également de réagir au retrait de la carte. Deux actions sont possibles :

1. fermer la fenêtre du navigateur,
2. diriger le navigateur vers une nouvelle URL (non protégée).

L'action à effectuer n'est pas définie au moment de la personnalisation de la carte mais au niveau du serveur au moyen d'un cookie persistant nommé OnRemoveValidyCard. La valeur de ce cookie doit être close pour provoquer la fermeture du navigateur et une

URL pour provoquer une redirection. L'action de fermeture ou de redirection s'applique à toutes les fenêtres du navigateur qui affichent une URL sur le même serveur que l'URL Portal de départ.

Avec ASP, on peut placer un cookie pour provoquer la fermeture du navigateur au moyen du code suivant :

```
<%  
Response.Cookies("OnRemoveValidyCard").Expires = DateAdd("d", 1, Now())  
Response.Cookies("OnRemoveValidyCard") = "close"  
' ou bien  
Response.Cookies("OnRemoveValidyCard") = "http://www.example.com/bye.html"  
%>  
<html>  
...
```

Ce code doit être placé en début de page. Pour être sûr que le client visite cette page, on a intérêt à utiliser celle qui correspond à l'URL stockée dans la carte. Le délai d'expiration (un jour dans l'exemple) doit être suffisamment long pour que le cookie soit toujours valide au moment où l'utilisateur retire sa carte du lecteur.

Avec PHP, on peut placer un cookie pour provoquer la redirection du navigateur au moyen du code suivant :

```
<?php  
setcookie("OnRemoveValidyCard", "close", time()+24*3600, "/");  
// ou bien  
setcookie("OnRemoveValidyCard", "about:blank", time()+24*3600, "/");  
?>  
<html>  
...
```

4.9 Configuration en mode proxy

En utilisant un serveur Apache et le module `mod_proxy`, il est possible de protéger l'accès à un serveur Web qui n'est pas supporté directement par Validy Web Business, par exemple un serveur Tomcat. Les requêtes adressées au serveur original sont dirigées vers le serveur Apache où le module Validy peut réaliser les opérations de validation, de cryptage ou de décryptage nécessaires avant éventuellement de les faire suivre. Dans ce mode, les requêtes sont protégées entre le client et le serveur proxy et celles qui reçoivent l'autorisation circulent en clair entre le serveur proxy et le serveur original.

La configuration du serveur Apache est la même que dans le cas normal et elle s'applique à un hôte virtuel. Les requêtes vers cet hôte sont dirigées vers le serveur original par le

module `mod_proxy`. La configuration suivante illustre cette utilisation :

```
LoadModule proxy_module ../mod_proxy.so
LoadModule validy_module ../mod_validy.so
LoadModule headers_module ../mod_headers.so

<VirtualHost aaa.bbb.ccc.ddd>
ServerName www.example.com
DocumentRoot "...

<IfModule mod_proxy.c>
ProxyRequests Off

<Proxy *>
    Order deny,allow
    Allow from all
</Proxy>

ProxyPass /err !
ProxyPass / http://www.example.com:8080/
ProxyPassReverse / http://www.example.com:8080/
</IfModule>
</VirtualHost>
```

où `aaa.bbb.ccc.ddd` est l'adresse IP du serveur et `www.example.com` est le nom du site protégé accessible par les clients. La configuration du serveur Web original est changée pour qu'il reçoive les requêtes sur un port différent, ici 8080. On peut aussi placer le serveur Apache sur un serveur différent. Il faut alors changer le DNS pour que `www.example.com` pointe sur le serveur Apache et changer les directives `ProxyPass` et `ProxyPassReverse` pour y mettre le nouveau nom ou l'adresse IP du serveur d'origine. Des règles de pare-feu doivent aussi être mises en place pour que le serveur d'origine ne soit pas accessible directement par les clients en utilisant son nouveau port ou son nouveau nom.

Dans la configuration ci-dessus, le serveur Apache ne fournit directement que les messages d'erreur situés sous `/err`. Ce sont *a priori* les seuls fichiers que l'on trouvera sous le répertoire indiqué par la directive `DocumentRoot` mais il est possible de servir d'autres contenus statiques ou non à partir du serveur Apache. On se référera pour cela à la documentation de `mod_proxy`.

Le serveur original peut examiner les en-têtes `x-validy` (voir 4.1) pour avoir des informations sur le client dont provient la requête et ajouter un en-tête `Validy` (voir 4.2.1) à la réponse pour demander au proxy de crypter son contenu avant de la renvoyer vers le client. Les requêtes qui ne sont pas autorisées par le module `mod_validy` ne parviennent pas jusqu'au serveur original. Il est possible de conserver un accès libre à une partie du site original en jouant sur la configuration du préfixe d'URL (voir 3.1) et sur le placement des en-têtes `Validy`.

4.10 Problèmes liés au cryptage du cache

En utilisation normale, les pages protégées transmises par le serveur peuvent être cachées par Internet Explorer sur le disque dur. Elles sont alors sauvées avant leur décryptage ce qui protège contre les accès non autorisés *a posteriori*. Quand une carte à puce valide est présente, le filtre `Validy Web Business` décrypte les données à la volée pour permettre leur affichage. Pour certains types de contenu, cette façon de procéder ne fonctionne pas. En effet, le composant chargé de la présentation du contenu ignore le flux de données

décryptées et essaye d'utiliser directement le fichier du cache. Comme celui-ci est crypté, il n'arrive pas à l'afficher. C'est le cas par exemple :

- des animations Macromedia Flash,
- des videos,
- de certains types de fichier que l'on télécharge sur le disque dur en utilisant le menu `Enregistrer sous` (fichiers Zip).

Pour ces contenus, il faut que le filtre crée une copie en clair du fichier caché en plus de l'original crypté. Comme cette copie représente un risque de sécurité, le choix des pages qui doivent être sauvées en clair dans le cache est effectué côté serveur au moyen d'un deuxième en-tête qui a pour nom `ValidyFlags` et pour valeur `clearcache`. Cette information est transmise au client de manière sécurisée pour qu'un tiers ne puisse pas provoquer le stockage en clair d'une page en altérant la réponse du serveur.

Les techniques permettant d'ajouter l'en-tête `ValidyFlags` à une page sont les mêmes que pour l'en-tête `Validy` (voir [4.2.1](#)).

5 Exemple

Un site exemple se trouve dans le répertoire suivant, pour Windows :

```
\Program Files\Validy\Web Business\sample_site\www.example.com
```

pour Linux :

```
/usr/share/doc/validy/sample_site/www.example.com
```

ou

```
/opt/validy/share/doc/validy/sample_site/www.example.com
```

et pour FreeBSD :

```
/usr/local/share/doc/validy/sample_site/www.example.com
```

Il contient 4 pages : une page html de sommaire pointant vers 3 pages ASP ou PHP protégées. Une de ces pages est accessible uniquement aux fournisseurs, une autre uniquement aux distributeurs, et la troisième est accessible aux fournisseurs ET aux distributeurs. La page distributeurs est de la forme :

```
<% response.AddHeader "validy", "LabResellers" %>
<html>
... Ceci est une page visible uniquement par les distributeurs...
</html>
```

La page fournisseurs est de la forme :

```
<% response.AddHeader "validy", "LabSuppliers" %>
<html>
... Ceci est une page visible uniquement par les fournisseurs...
</html>
```

La page pour les distributeurs et les fournisseurs est de la forme :

```
<% response.AddHeader "validy", "LabResellersSuppliers" %>
<html>
... Ceci est une page visible
    par les distributeurs et par les fournisseurs...
</html>
```

Un fichier `permissions.txt` correspondant à ces droits se trouve après l'installation du serveur dans le répertoire `sample_site` du serveur.

Il faut ensuite créer deux cartes de démonstration avec les droits appropriés. Dans cet exemple sont détaillées pas à pas les différentes étapes permettant de créer deux cartes client+portal amenant directement sur la page d'accueil du site d'exemple.

! → Dans l'exemple suivant, on considère que le site se nomme `www.example.com`. Pour vos essais, vous pouvez utiliser ce nom de site mais vous devez pour cela disposer d'un

serveur DNS en local afin de faire pointer le nom `www.example.com` vers votre machine d'essai. Vous pouvez également ajouter la ligne suivante dans le fichier `hosts` de votre poste client se trouvant dans `\WinRoot\system32\drivers\etc` :

```
127.0.0.1 www.example.com
```

Cela redirigera toutes les requêtes pour `www.example.com` vers votre machine locale. N'oubliez de retirer cette ligne lorsque vos tests seront terminés.

5.1 Installation

Installez Validy Web Business pour un site indépendant en suivant les instructions de la section 2.1.1.

5.2 Création du site

Les 4 pages du site ainsi que les fichiers correspondant aux messages d'erreur envoyés par le serveur Validy sont installées en même temps que Validy Web Server. Attention à ne pas confondre le répertoire qui contient les pages web du site avec le répertoire de même nom qui contient le fichier `permissions.txt` et qui se trouve dans l'arborescence des fichiers de configuration.

Copiez le répertoire `www.example.com` contenant le site d'exemple dans le répertoire contenant les sites Web sur votre disque dur, et créez un site web pointant dessus à l'aide d'Internet Information Server ou de Apache.

5.3 Création des cartes à puce

1. Première carte
 - lancez `vwbCustomizer` et sélectionnez les applications Web Business et Web Portal, pas de PIN,
 - dans la page des paramètres Web Business, sélectionnez le mode Web Site, entrez le nom du site `www.example.com` et la catégorie `CatResellers`. Cochez la case Utilisateur dans le cadre Web Site.
 - dans la page des paramètres Web Portal, cochez la case Standard et entrez l'URL `vldy://www.example.com/default.htm`
 - dans l'écran de saisie des informations utilisateur, entrez :
Nom : Ross Sailor
Extra information : Reseller Inc.
Identifiant : laissez la valeur calculée automatiquement
 - Cliquez sur Suivant et introduisez la carte d'admin dans le lecteur 0 puis saisissez son PIN.
 - Introduisez la carte Revendeur dans le lecteur 1.
 - Attendez quelques secondes que la carte soit personnalisée.
 - Retirez la carte.
2. Deuxième carte
 - Revenez en arrière pour retourner à la saisie des paramètres Web Business. Remplacez la catégorie `CatResellers` par `CatSuppliers`.
 - Avancez jusqu'à la page de saisie des informations utilisateur et entrez :
Nom : Sue Plyer
Extra information : Supplier Corp
Identifiant : laissez la valeur calculée automatiquement
 - Cliquez sur Suivant et introduisez la carte Fournisseur dans le lecteur 1.
 - Attendez quelques secondes que la carte soit personnalisée.
 - Retirez les cartes.

- Quittez le programme.

5.4 Mise à jour du serveur

- Lancez le programme de mise à jour du serveur vwbUpdate
Paramètres à saisir :
Chemin d'accès aux fichiers de configuration Web Business : c:\validy
Site à mettre à jour : www.example.com
Mise à jour d'un serveur ou d'un cluster (server) : server
Fichier de mise à jour : C:\TEMP\www.example.com.upd
- Introduisez alors la carte d'administration dans le lecteur 0,
- Saisissez le PIN Code de la carte d'administration.

5.5 Conclusion

Vous avez maintenant en votre possession 2 cartes à puce Web Business + Web Portal donnant accès directement à la page [default.htm](#) du site [www.example.com](#).

La carte à puce Revendeur de Ross Sailor vous donne accès à la page revendeurs et à la page commune aux revendeurs et aux fournisseurs.

La carte à puce Fournisseur de Sue Plyer vous donne accès à la page fournisseurs et à la page commune aux fournisseurs et aux revendeurs.

La page d'accueil default.htm n'est pas protégée et est accessible à tout internaute. Les autres pages sont uniquement accessibles à des utilisateurs munis de la carte Validy ayant les droits appropriés.