Sage FRP 1000

Guide de déploiement

Azure

Sage

Mai 2016

Table des matières

Table des matières

[Table des matières 2](#_Toc454357091)

[1.0 Introduction 4](#_Toc454357092)

[1.1 Introduction 4](#_Toc454357093)

[1.2 Prérequis 4](#_Toc454357094)

[1.3 Fonctionnalités supportées 4](#_Toc454357095)

[1.4 Architectures type 6](#_Toc454357096)

[1.4.1 Architecture Single VM 6](#_Toc454357097)

[1.4.2 Architecture Cluster multi-VM (Application Gateway) 7](#_Toc454357098)

[1.4.3 Architecture Cluster multi-VM (Load balancer) 8](#_Toc454357099)

[2.0 Sélection des composants 9](#_Toc454357100)

[2.1 Sélection du type de machine virtuelle. 9](#_Toc454357101)

[2.2 Système d’exploitation. 9](#_Toc454357102)

[2.3 Sélection du moteur de base de données 9](#_Toc454357103)

[2.3.1 Utilisation de Azure SQL Database 9](#_Toc454357104)

[2.3.2 Utilisation de Microsoft SQL Server 9](#_Toc454357105)

[3.0 Installation et configuration 11](#_Toc454357106)

[3.1 Installation de Sage FRP 1000 11](#_Toc454357107)

[3.1.1 Création de la machine virtuelle 11](#_Toc454357108)

[3.1.2 Création du serveur SQL 12](#_Toc454357109)

[3.1.3 Installation de Sage FRP 1000 12](#_Toc454357110)

[3.2 Configuration du service Sage FRP 1000 13](#_Toc454357111)

[3.3 Configuration du Firewall de la machine virtuelle. 13](#_Toc454357112)

[3.4 Configuration du Firewall de Azure SQL Server. 13](#_Toc454357113)

[3.5 Configuration de la sauvegarde des données. 14](#_Toc454357114)

[3.5.1 Point in time 14](#_Toc454357115)

[3.5.2 Fonctionnalités base de données du portail Azure 14](#_Toc454357116)

[3.5.3 Exportation automatisée. 14](#_Toc454357117)

[3.6 Configuration du Service de messagerie (SMTP) 15](#_Toc454357118)

[3.7 Configuration d’un fournisseur de SMS 15](#_Toc454357119)

[4.0 Configuration Cluster 17](#_Toc454357120)

[4.1 Mise en œuvre de Microsoft Azure Load Balancer 17](#_Toc454357121)

[4.1.1 Configuration Sage 1000 20](#_Toc454357122)

[4.2 Mise en œuvre de Microsoft Azure Application Gateway 22](#_Toc454357123)

[4.2.1 Configuration des machines virtuelles 22](#_Toc454357124)

[4.2.2 Configuration des services Sage FRP 1000 22](#_Toc454357125)

[4.2.3 Création de l’Application Gateway 23](#_Toc454357126)

[4.2.4 Configuration de votre DNS 25](#_Toc454357127)

[5.0 Annuaire de gestion des identités 26](#_Toc454357128)

[5.1 Configurez le compte Administrateur 26](#_Toc454357129)

[5.2 Configurer l’utilisation de Recaptcha 26](#_Toc454357130)

[5.3 Mise en œuvre de l’Annuaire Sage FRP 1000 Entreprise 27](#_Toc454357131)

[5.3.1 Comptes utilisateurs 27](#_Toc454357132)

[5.3.2 Comptes de service 30](#_Toc454357133)

[5.4 Mise en œuvre de Microsoft Azure Directory 31](#_Toc454357134)

[5.4.1 Annuaire Azure Directory 32](#_Toc454357135)

[5.4.2 Annuaire Sage FRP 1000 33](#_Toc454357136)

[5.4.3 Enregistrement des utilisateurs. 35](#_Toc454357137)

[6.0 Sécurité 41](#_Toc454357138)

[6.1 Mise en place d’un certificat SSL. 41](#_Toc454357139)

[6.1.1 Mise en place au niveau des services Sage FRP 1000 41](#_Toc454357140)

[6.1.2 Configuration DNS 41](#_Toc454357141)

[6.1.3 Mise en place au niveau de Microsoft Application Gateway 42](#_Toc454357142)

[7.0 Intégration avec le Système d’information 43](#_Toc454357143)

[7.1 Architecture 43](#_Toc454357144)

[7.2 Paramétrage des tâches d’exportation. 43](#_Toc454357145)

[7.2.1 Configuration des files d’attente 44](#_Toc454357146)

[7.2.2 Configurer un compte de service 46](#_Toc454357147)

[7.2.3 Installation et configuration de Sage Sync Agent. 47](#_Toc454357148)

[7.2.4 Tester la communication 50](#_Toc454357149)

[7.2.5 Paramétrage des automates 51](#_Toc454357150)

[7.3 Paramétrage des tâches d’exportation. 52](#_Toc454357151)

[7.3.1 Créer une file d’attente d’exportation. 52](#_Toc454357152)

[7.3.2 Configurer le Sync Agent. 53](#_Toc454357153)

[7.3.3 Créer une tâche d’automate d’exportation. 55](#_Toc454357154)

1. Introduction
   1. Introduction

Ce document décrit les recommandations pour le déploiement de Sage FRP 1000 sur Microsoft Azure.

Note :

Ce document fait référence au mode de déploiement « classique » de Microsoft Azure.

* 1. Prérequis

Le déploiement d’une solution Sage FRP 1000 nécessite :

* Une souscription Microsoft Azure.
* Une clé d’installation plateforme Sage FRP 1000 avec l’option « Cloud publique »
* Une clé d’installation plateforme Sage FRP 1000 Cluster si vous installez une configuration multi-machines.
  1. Fonctionnalités supportées

Toutes les fonctionnalités Sage FRP 1000 sont supportées à l’exception des fonctionnalités suivantes :

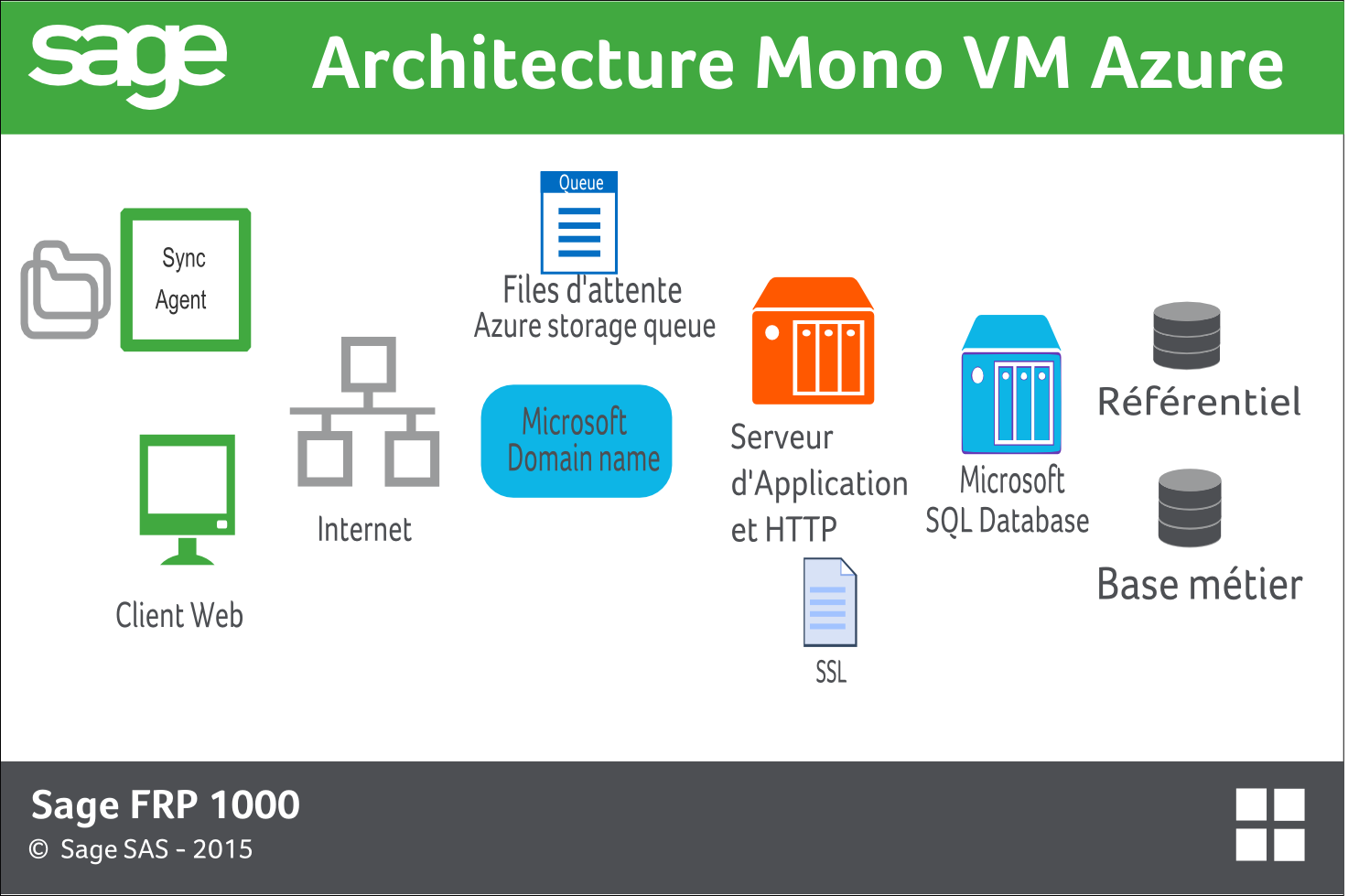
|  |  |  |
| --- | --- | --- |
| Fonctionnalité | Supporté |  |
| Oracle | Non |  |
| SQL Server version antérieur à 2014 | Non | Utilisez une version supérieure |
| Windows Server version antérieur à 2012 | Non | Utilisez une version supérieure |
| Edition piloté (Business Object) | Non |  |
| Sage FRP Reporting | Non |  |
| Processus Métiers | Non |  |
| Client Outlook | Non | (\*) |
| Serveurs HTTP externes (IIS, Apache) | Non | Utilisez le serveur embarqué |
| Sage Communication bancaire | Non |  |
| Sage FRP 1000 Service 32 bits | Non | Utilisez la version 64 bits |
| Active Directory | Non | Utiliser Azure Directory en mode OAUTH 2.0 |

(\*) Non testé actuellement dans l’environnement Azure

Les fonctionnalités Azure suivantes sont supportées :

|  |  |  |
| --- | --- | --- |
| Fonctionnalité | Supporté |  |
| SQL Database | Oui |  |
| Azure Storage Queue | Oui |  |
| Azure load balancer | Oui | Load balancer state less |
| Azure Application Gateway | Oui | Load balancer state full et frontal SSL |
| Azure Active Directory (OAUTH 2.0) | Oui | OAuth 2.0 uniquement |
|  |  |  |

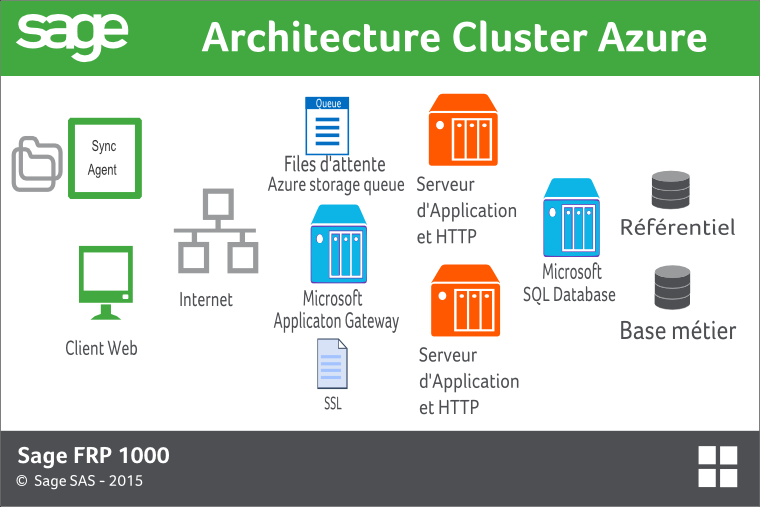
* 1. Architectures type
     1. Architecture Single VM



|  |  |  |
| --- | --- | --- |
| Composant | Fournisseur | Rôle |
| Serveur d’Application | Sage | Serveur frontal Web HTTPS et serveur de traitement |
| Sync Agent | Sage | Agent de synchronisation entre les fichiers d’import / export et les files d’attente de traitement. |
| SQL Database | Microsoft |  |
| Azure Storage Queue | Microsoft | File d’attente de traitement des imports / exports de fichier |
| Domain Name | Microsoft | Point d’accès HTTPs |
|  |  |  |

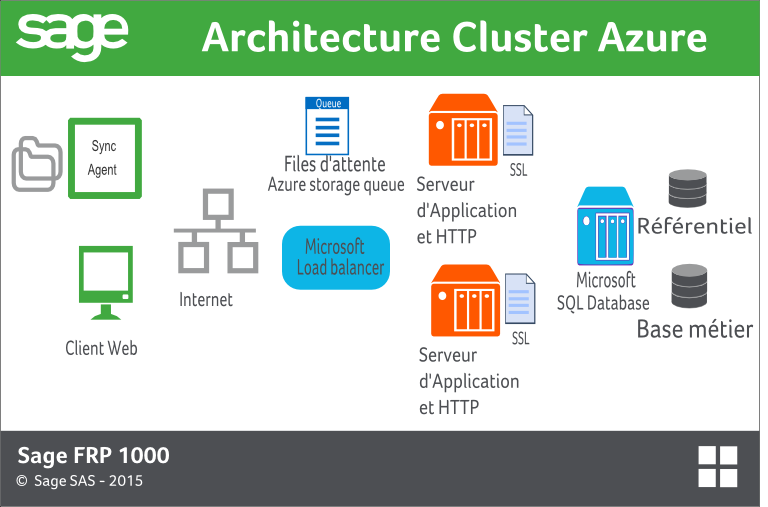
* + 1. Architecture Cluster multi-VM (Application Gateway)

L’architecture typique recommandée, utilisant Application Gateway, est la suivante :



|  |  |  |
| --- | --- | --- |
| Composant | Fournisseur | Rôle |
| Serveur d’Application | Sage | Serveur frontal Web et serveur de traitement |
| Sync Agent | Sage | Agent de synchronisation entre les fichiers d’import / export et les files d’attente de traitement. |
| SQL Database | Microsoft |  |
| Azure Storage Queue | Microsoft | File d’attente de traitement des imports / exports de fichier |
| Azure Application Gateway | Microsoft | Load balancer state full et frontal SSL |
|  |  |  |

* + 1. Architecture Cluster multi-VM (Load balancer)



|  |  |  |
| --- | --- | --- |
| Composant | Fournisseur | Rôle |
| Serveur d’Application | Sage | Serveur frontal Web HTTPS et serveur de traitement ; load balancing |
| Sync Agent | Sage | Agent de synchronisation entre les fichiers d’import / export et les files d’attente de traitement. |
| SQL Database | Microsoft |  |
| Azure Storage Queue | Microsoft | File d’attente de traitement des imports / exports de fichier |
| Azure Load balancer | Microsoft | Load balancer state less |
|  |  |  |

Note :

Dans cette architecture la fonctionnalité d’équilibrage de charge est prise en compte à la fois par le Azure Load balancer (sans état) et par sage FRP 1000 (avec état).

Chaque Service Sage FRP 1000 doit détenir le certificat SSL

1. Sélection des composants
   1. Sélection du type de machine virtuelle.

Les recommandations sont les suivantes :

* Utilisez une machine virtuelle par Service Sage FRP 1000
* Sélectionnez une machine 2 cores minimum
* Sélectionnez le niveau Standard.

Compte tenu de ces recommandations le type de machine minimum recommandé est A2

Note :

Sage FRP 1000 ne fait pas un usage intensif du disque dur, les types de machines avec disques SSD ne sont pas nécessaires.

* 1. Système d’exploitation.

Le système d’exploitation recommandé est la dernière version de Windows Server supportée et disponible en tant qu’image Azure, actuellement Windows Server 2012 R2 Datacenter.

* 1. Sélection du moteur de base de données
     1. Utilisation de Azure SQL Database

SQL Database peut être utilisé comme service de base de données.

Le niveau minimum requis est S2.

Le niveau de la base de données impacte certaine fonctionnalités d’Azure, en particulier la fonction « Point in time » qui permet de restaurer l’état d’une base de données à un certain point dans le passé. Ceci peut être un critère de choix entre Standard et Premium. Reportez-vous à la documentation.

Suivant le nombre d’utilisateurs et le volume de données traité, vous pouvez être amené à utiliser des niveaux de base de données supérieurs.

Note :

Les bases de données sont créées au niveau S0, pensez à modifier le niveau avant d’utiliser les bases.

* + 1. Utilisation de Microsoft SQL Server

Vous pouvez utiliser une instance de SQL Serveur comme serveur de données. Dans ce cas, l’installation et les préconisations sont identiques à une version On Premise.

La version de SQL Serveur recommandée est la dernière version de SQL Server supportée, actuellement SQL Server 2016.

Reportez-vous à la documentation Azure, notamment si vous utilisez la fonctionnalité « bring your own licences », et au Guide de préconisation de Sage FRP 1000.

Note :

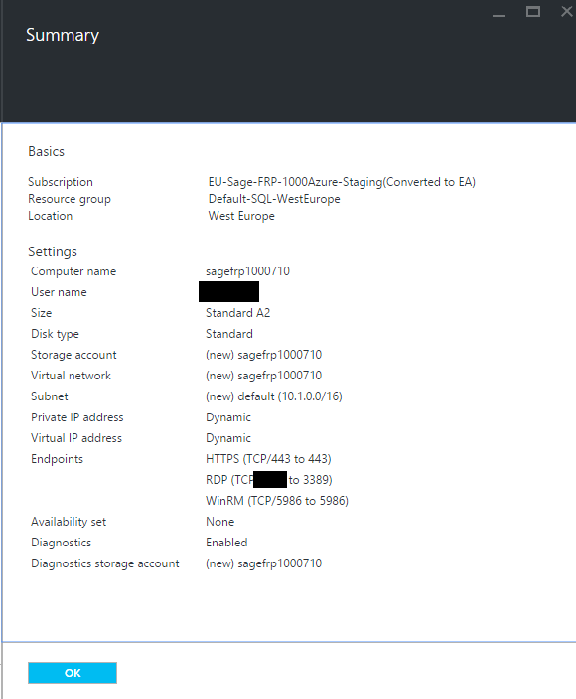
Microsoft Azure propose des VM préconfigurées pour SQL Serveur.

1. Installation et configuration
   1. Installation de Sage FRP 1000

Cette section décrit l’installation d’une configuration basique (Mono machine, SQL Database). On suppose que l’utilisateur est connecté sur le portail de Microsoft Azure.

* + 1. Création de la machine virtuelle

La première étape consiste à créer la machine virtuelle.



Lors de la création de la machine :

* Définissez le réseau virtuel
* Définissez le compte de stockage
* Configurez les ends points RDP et WinRM si nécessaire, vous aurez besoin de vous connecter en RDP pour l’installation de sage FRP 1000 et pour les opérations de maintenance. Une fois l’installation terminée sécurisez l’accès à cet end point (Voir …)
* Ajoutez un end point HTTPs pour l’accès HTTPs

Note : Votre service sera accessible en Internet, n’utilisez pas http mais https

* + 1. Création du serveur SQL

La seconde étape consiste à créer un serveur SQL virtuel.

Il ni a pas de configuration particulière au moment de la création.

Note :

Suivant la configuration il peut être plus intéressant d’utiliser un pool de base de données, reportez-vous à la documentation Azure.

* + 1. Installation de Sage FRP 1000

La troisième étape consiste à installer Sage FRP 1000, pour cela :

* Connectez-vous sur en RDP sur la machine virtuelle.
* Récupérez l’ISO de l’installation de Sage FRP 1000. Vous pouvez obtenir un lien de téléchargement de l’ISO de Sage FRP 1000 dans l’espace partenaire de Sage.
* Montez l’ISO en tant que disque virtuel. (Clique droit, Mount)
* Installez le Client odbc SQL Server Native Client 11.0
* Installez Sage FRP 1000 à partir du CD d’installation

Vous devez installer le poste client avec la console d’administration et le Service Sage FRP 1000 64 bits

Lancez Sage FRP 1000, sélectionnez créer la base master.

Note :

* Le nom du serveur doit être le nom DNS du serveur SQL, par exemple sagefrp1000.database.windows.net
* les noms d’utilisateur doivent être complétés par le nom du Serveur SQL, par exemple pour un utilisateur sqlAdmin sur sagefrp1000 le nom d’utilisateur est sqlAdmin@sagefrp1000

Par défaut, SQL Database crée la base de données au niveau S0. Les performances à ce niveau sont limitées ce qui peut provoquer un temps d’installation très long.

Une fois la base master créée, sortez de Sage FRP 1000 et modifiez le niveau de DTU de la base master.

Relancer Sage FRP 1000 et installez les Applications.

La suite de l’installation est identique à une installation On Premise.

Note :

Ne pas confondre avec « ODBC SQL Driver 11.0 pour SQL Server » qui est un driver différent ; SQL Native Client pour SQL 2012 peut être trouvé sur le master de Sage FRP 1000 ou bien téléchargé à partir de ce lien :

<http://go.microsoft.com/fwlink/?LinkID=239648&clcid=0x409>

* 1. Configuration du service Sage FRP 1000

Dans la console d’administration :

* Créez un utilisateur pour démarrer le service et associez le au dossier.

Dans la console d’administration, configurez le service Sage FRP 1000 :

* Configurez l’application, le dossier et l’utilisateur du service.
* Activez le mode Internet
* Désactivez le moteur de wrkflow
* Démarrez le serveur http intégré
* Démarrez le serveur en HTTPs

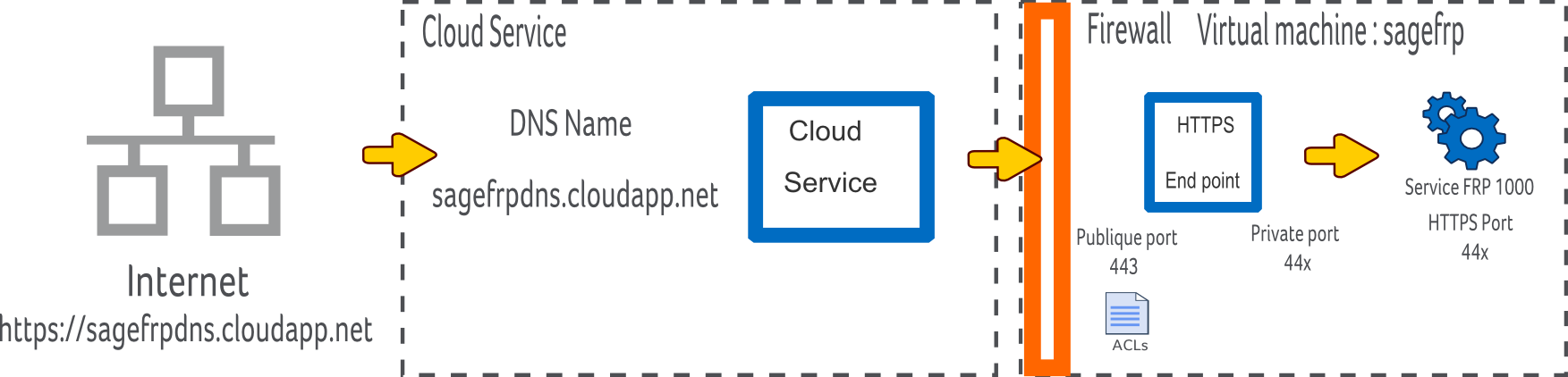
Dans la console des services Windows (services.msc) :

* Modifiez la configuration du service pour le passer de « Automatic » à « Automatic delayed ».

A défaut il est probable que le service démarre trop tôt et ne soit pas opérationnel après un reboot.

* 1. Configuration du Firewall de la machine virtuelle.

Dans une configuration basique la vue des flux réseau est celle-ci :



Pour que la configuration soit complète vous devez configurer le firewall de la machine virtuelle pour autoriser les flux entrant sur le port publique du end-point (ici 443)

Sur la machine virtuelle exécutez firewall.cpl :

* Ajoutez une « Inbound rule »
* De type port sur le port publique du end point.
* Pour tous les réseaux.

A ce stade vous devez vous pouvoir vous connecter sur le service à l’adresse du Cloud Service, dans cet exemple sur https://sagefrpdns.cloudapp.net

* 1. Configuration du Firewall de Azure SQL Server.

Par défaut la connexion au Server SQL virtuelle à l’extérieur de la souscription n’est pas autorisée.

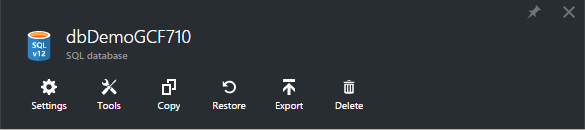
Sage FRP 1000 ne nécessite pas l’accès au serveur de données de l’extérieur et ne recommande pas d’ouvrir ces accès.

Néanmoins si vous avez besoin d’accéder à ces serveurs, par exemple pour SQL Management Studio, vous pouvez configurer le Firewall du serveur SQL en définissant les plages d’ip autorisées.

* 1. Configuration de la sauvegarde des données.
     1. Point in time

Par défaut, les bases de données SQL Database incluent la fonctionnalité de restauration « Point in time ».

Cette fonctionnalité vous permet de restaurer l’état de la base de données à un certain point de le passé (en fonction du niveau de la base de données). Il ni a pas de configuration particulière pour disposer de cette fonctionnalité. Pour restaurer la base de données utilisez la fonction « Restore » dans le portail Azure :



* + 1. Fonctionnalités base de données du portail Azure

Copy

Réalise une copie de la base de données sur un serveur SQL.

Restore

Restaure la base de données en utilisant la fonction « Point in time ». Notez que la restauration crée une nouvelle base qui doit être ensuite renommée.

Export

Réalise un export de la base de données au format bacpac dans un blob de l’espace de stockage.

* + 1. Exportation automatisée.

Azure propose une fonction d’export automatique.

Toutefois cette fonction n’est pas actuellement disponible dans le nouveau Portail Azure.

Vous pouvez y accéder en basculant sur le « Azure classic portal » puis dans Base de données / Configurer / Exportation automatisée.

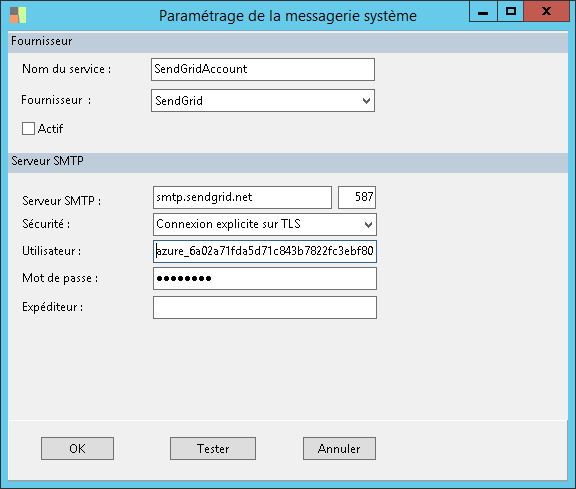
* 1. Configuration du Service de messagerie (SMTP)

Azure supporte l’envoi de email par l’intermédiaire d’un Service associé, SendGrid

La première étape consiste à créer un compte SendGrid, via le portail Azure.

La seconde à paramétrer Sage FRP 1000 :

Dans la console d’administration, Fournisseur de Service / Serveur de messagerie système (SMTP) ; renseigné les informations de votre compte :



* 1. Configuration d’un fournisseur de SMS

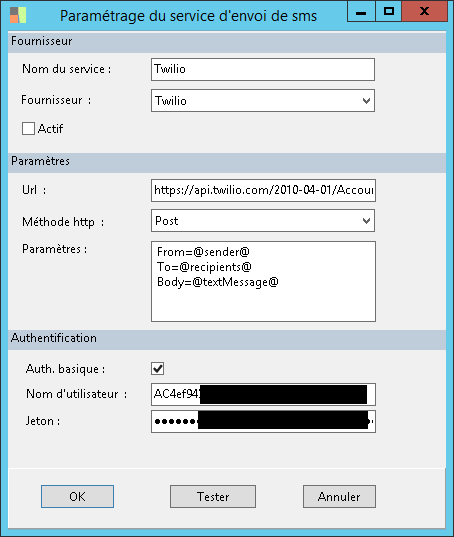
Le service SMS permet de mettre en œuvre la double authentification et la récupération de mot de passe.

Actuellement seul le service en ligne <https://www.twilio.com/> est supporté en standard.

La première étape consiste à créer un compte Twilio sur le site de Twilio.

La seconde à paramétrer Sage FRP 1000 :

Dans la console d’administration, Fournisseur de Service / Service d’envoi de sms ; renseigné les informations de votre compte :



Vous devez renseigner le sid fournit par Twilio comme utilisateur.

1. Configuration Cluster

Cette section décrit l’installation d’une configuration Cluster multi-machines avec équilibrage de charge.

Cette architecture nécessite une clé sage FRP 1000 Cluster.

Deux architectures sont possibles :

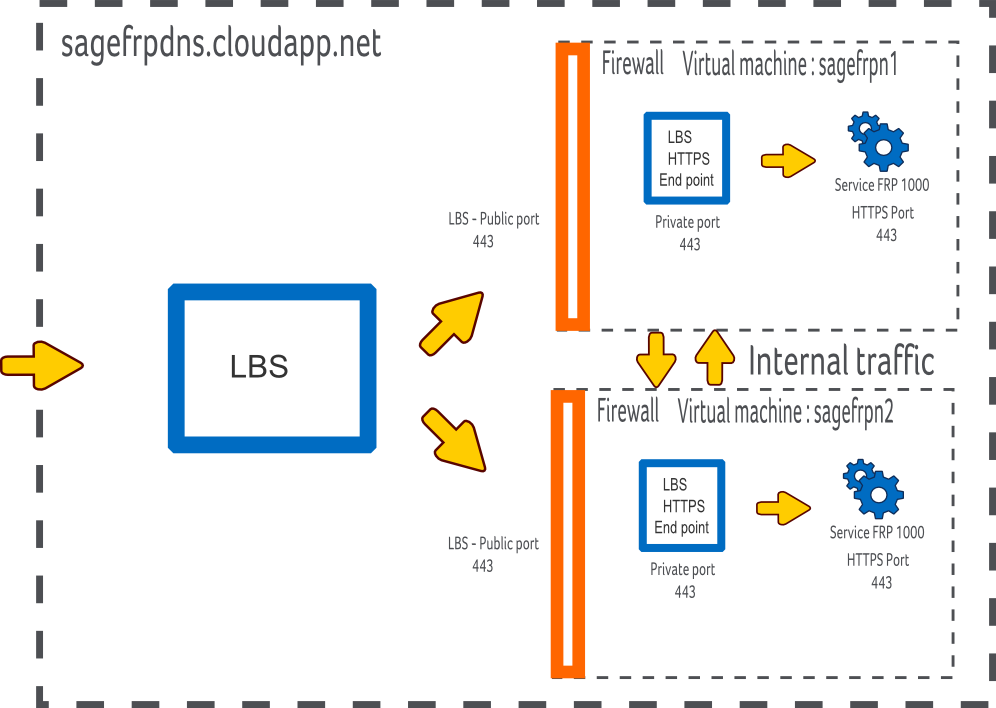
* Utilisation de Azure load balancer
* Utilisation de Azure Application Gateway

Les différences entre les deux architectures sont les suivantes :

|  |  |
| --- | --- |
| Architecture |  |
| Azure load balancer | * Equilibrage de charge state less au niveau du point d’accès * Routage des requêtes entre services Sage FRP 1000 * Prise en charge de SSL au part les services Sage FRP 1000. |
| Azure Application Gateway | * Equilibrage de charge state full au niveau de la gateway * Prise en charge de SSL par la Gateway |

Il est recommandé de mettre en œuvre Azure Application Gateway car :

* Vous pouvez centraliser l’installation du certificat SSL à un seul endroit
* Vous bénéficiez de la prise en charge complète de l’équilibrage de charge par un composant Microsoft Azure.
  1. Mise en œuvre de Microsoft Azure Load Balancer



La première étape consiste à installer deux machines virtuelles identiques configurées de la même manière.

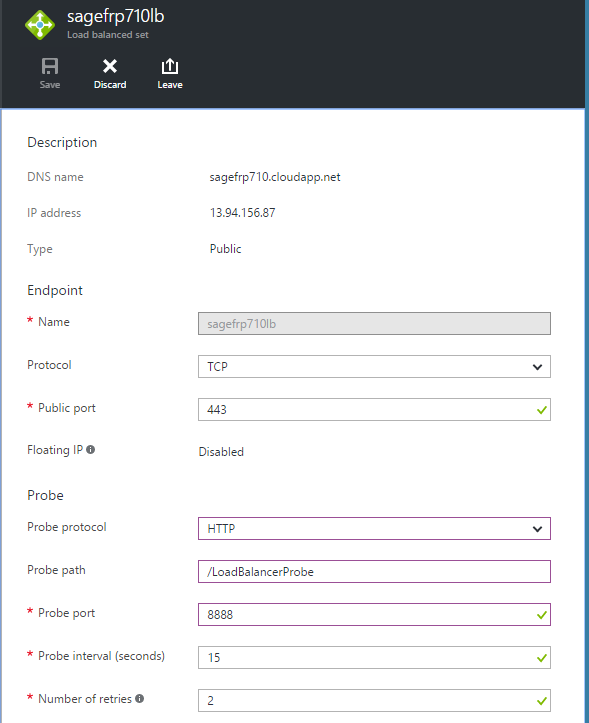
Sur la seconde machine vous pouvez n’installer que le service sage FRP 1000 et recopier le fichier de configuration servicel1000.ini

La configuration supplémentaire pour les nœuds est la suivante :

* Ajouter une règle de FireWall pour le port d’équilibrage HTTP des services Sage FRP ; par exemple sur le port 8888
* Ne définissez pas de end-point pour le port d’équilibrage, ce port ne sera accessible qu’à l’intérieur du réseau virtuel.

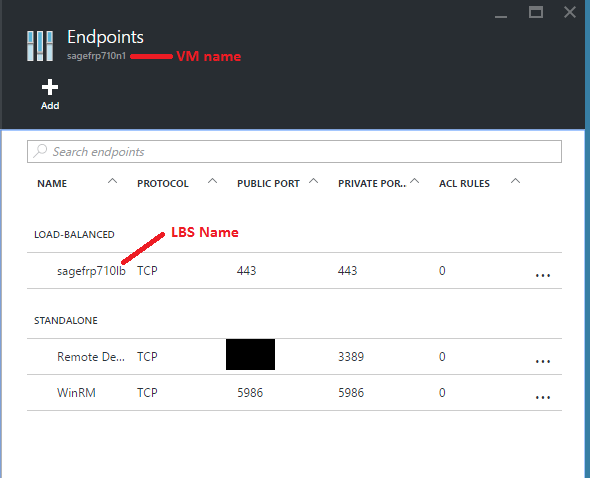
La seconde étape consiste à rattacher les machines à un « load balancing set ». Cette fonction est accessible dans les propriétés de la machine virtuelle.

Au moment du rattachement de la première machine vous créez le « load balancing set » :



La sonde doit être configurée sur le port d’équilibrage HTTP du service en sélectionnant les informations comme ci-dessus.

Une fois l’opération terminée vous devez avoir :



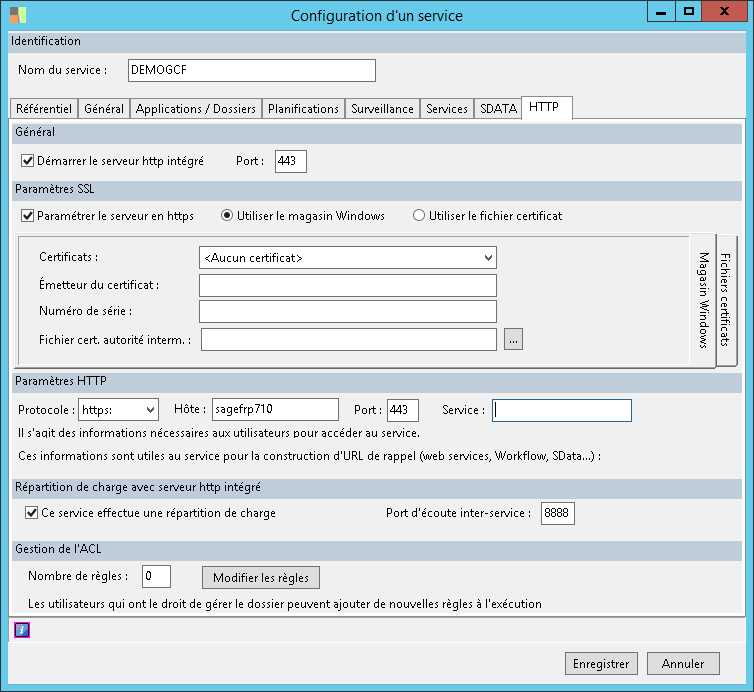
* + 1. Configuration Sage 1000

Le service Sage FRP 1000 doit être configuré pour supporter l’équilibrage de charge.

* Installer la clé Sage FRP 1000 Cluster
* Créer un cluster défini sur les nœuds ; dans cet exemple: sagefrpn1 et sagefrpn2

Modifier la configuration du service :

* Nom public du service = Nom du domain = Nom du cloud service (sagefrp710)
* Port d’équilibrage en 8888



Une fois les services redémarrés vous pouvez tester le fonctionnement du port d’équilibrage en vous connectant d’une machine sur l’autre en http sur ce port (Par exemple, sur la machine sagefrp710n1 connectez-vous sur l’url http://sagefrp710n2:8888)

Notes :

Si votre machine a déjà un end-point sur le port public vous devez le supprimer au préalable.

Dans cette configuration le routage des flux https vers les serveurs concernés est réalisé par les services Sage FRP 1000.

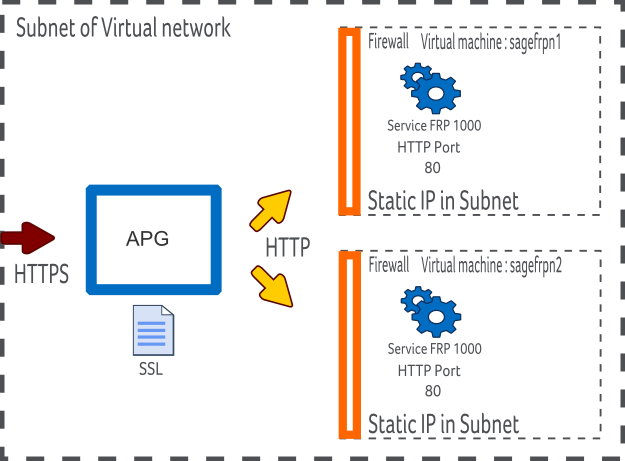
Les fichiers servicel1000.ini de chaque nœud doivent être identiques, vous pouvez modifier la configuration d’un nœud et recopier cette configuration sur les autres nœuds.

L’ensemble des machines sont hébergées dans le même domaine, les ports publics des end-points doivent être distincts.

Une méthode plus efficace consiste à installer une première machine, puis une fois la configuration satisfaisante, la capturer pour créer une image. Vous pouvez alors créer les machines à partir de cette image. Lorsque vous créez les machines assurez-vous de configurer correctement la partie network pour les placer dans le même domaine (ie Cloud Service)/ Reportez-vous à la documentation Azure sur « Comment créer une image à partir d’une machine virtuelle ».

* 1. Mise en œuvre de Microsoft Azure Application Gateway

Application Gateway est un service d’équilibrage de charge et de routage pouvant faire office de frontal Web.

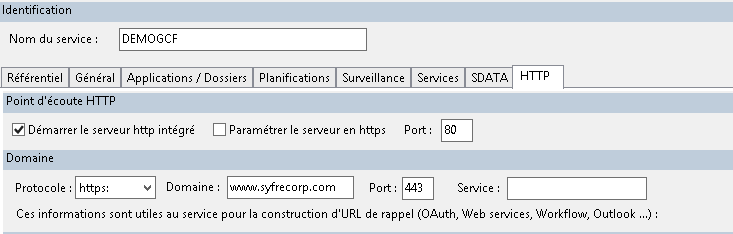


Les avantages d’Application Gateway sont :

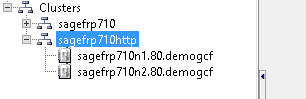
* Prise en charge de SSL
* Gestion des sessions

Au moment de la rédaction de ce document Application Gateway n’est pas encore gérée dans les consoles d’administration d’Azure et vous devez la déployer en utilisant des commandes Power Shell.

* + 1. Configuration des machines virtuelles
* Les IP des machines doivent être statiques
* Vous devez les retirez des « Load Balancer Set » si nécessaire
* Définissez une règle de Firewall pour ouvrir le port 80
  + 1. Configuration des services Sage FRP 1000
* Modifiez la configuration http pour que le port d’écoute soit http.



* Créez un Cluster pour les nœuds



* + 1. Création de l’Application Gateway

La première étape consiste à installer Power Shell et les composants Azure Power Shell.

<https://azure.microsoft.com/fr-fr/documentation/articles/powershell-install-configure/>

Une fois Power Shell installé, lancez une console Power Shell et récupérez les informations de votre souscription :

Get-AzurePublishSettingsFile

Import-AzurePublishSettingsFile "c:\temp\<my setting file>.publishsettings"

select-AzureSubscription "<my subscription name>"

Une Application Gateway se configure sur le réseau virtuel hébergeant les nœuds de votre cluster, vous devez récupérer le nom complet du réseau :

Get-AzureVNetConfig -ExportToFile "c:\temp\MyAzureVirtNets.netcfg"

Le fichier créé par cette commande contient le nom complet du réseau :

<?xml version="1.0" encoding="utf-8"?>

<NetworkConfiguration xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.microsoft.com/ServiceHosting/2011/07/NetworkConfiguration">

<VirtualNetworkConfiguration>

<Dns>

<DnsServers>

<DnsServer name="AZURE" IPAddress="100.91.250.140" />

</DnsServers>

</Dns>

<VirtualNetworkSites>

<VirtualNetworkSite name="Group Default-SQL-WestEurope sagefrp1000710" Location="West Europe">

<AddressSpace>

<AddressPrefix>10.1.0.0/16</AddressPrefix>

</AddressSpace>

<Subnets>

<Subnet name="default">

<AddressPrefix>10.1.0.0/24</AddressPrefix>

</Subnet>

</Subnets>

</VirtualNetworkSite>

Vous devez ensuite créer le fichier de configuration de la gateway, ce fichier est un xml, dans ce fichier renseignez les adresses ip (statique) des nœuds de vos services :

<?xml version="1.0" encoding="utf-8"?>

<ApplicationGatewayConfiguration xmlns:i="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.microsoft.com/windowsazure">

<FrontendPorts>

<FrontendPort>

<Name>FrontEndPort</Name>

<Port>443</Port>

</FrontendPort>

</FrontendPorts>

<BackendAddressPools>

<BackendAddressPool>

<Name>BackEndPool1</Name>

<IPAddresses>

<IPAddress>10.1.0.4</IPAddress>

<IPAddress>10.1.0.5</IPAddress>

</IPAddresses>

</BackendAddressPool>

</BackendAddressPools>

<BackendHttpSettingsList>

<BackendHttpSettings>

<Name>BackEndSetting1</Name>

<Port>80</Port>

<Protocol>Http</Protocol>

<CookieBasedAffinity>Enabled</CookieBasedAffinity>

</BackendHttpSettings>

</BackendHttpSettingsList>

<HttpListeners>

<HttpListener>

<Name>HTTPListener</Name>

<FrontendPort>FrontEndPort</FrontendPort>

<Protocol>Https</Protocol>

<SslCert>sagefrp710APGCert</SslCert>

</HttpListener>

</HttpListeners>

<HttpLoadBalancingRules>

<HttpLoadBalancingRule>

<Name>HttpLBRule1</Name>

<Type>basic</Type>

<BackendHttpSettings>BackendSetting1</BackendHttpSettings>

<Listener>HTTPListener</Listener>

<BackendAddressPool>BackEndPool1</BackendAddressPool>

</HttpLoadBalancingRule>

</HttpLoadBalancingRules>

</ApplicationGatewayConfiguration>

Vous pouvez ensuite enchaîner les commandes :

* Création de l’APG
* Installation du certificat SSL
* Configuration de l’APG
* Démarrage de l’APG
* Récupération de l’adresse DNS de l’APG

New-AzureApplicationGateway -Name sagefrp710APG -VnetName "Group Default-SQL-WestEurope sagefrp1000710" -Subnets "default"

Add-AzureApplicationGatewaySslCertificate -Name sagefrp710APG -CertificateName sagefrp710APGCert -Password "xxxxxx" -CertificateFile "c:\temp\xxxx\private\_key.pfx"

Set-AzureApplicationGatewayConfig -Name sagefrp710APG -ConfigFile "c:\temp\apg.xml"

Start-AzureApplicationGateway -Name sagefrp710APG

Get-AzureApplicationGateway sagefrp710APG

* + 1. Configuration de votre DNS

Get-AzureApplicationGateway sagefrp710APG

Name : sagefrp710APG

Description :

VnetName : Group Default-SQL-WestEurope sagefrp1000710

Subnets : {default}

InstanceCount : 2

GatewaySize : Medium

State : Running

VirtualIPs : {40.118.97.98}

DnsName : a8afd746-8665-4e8c-8003-0f4c61024b64.cloudapp.net

La dernière étape vous a fourni l’adresse DNS de la Gateway, c’est cette adresse qui doit être renseignée dans le CName de votre configuration DNS.

1. Annuaire de gestion des identités

Les annuaires supportés sur un déploiement Azure sont :

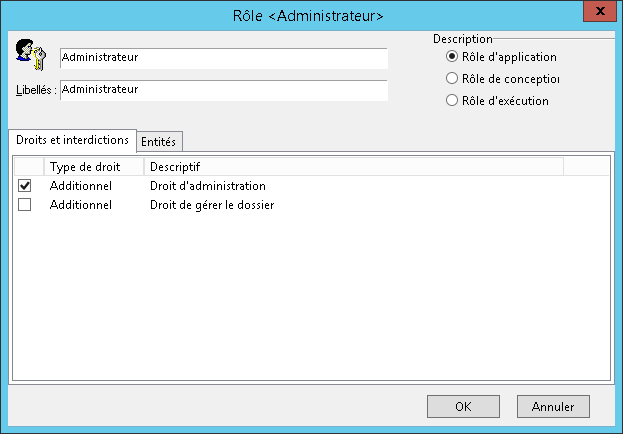
* Annuaire d’Entreprise
* Annuaire Azure Directory en mode OAUTH 2.0
* Annuaire OAUT 2.0

Les annuaires Active Directory « On Premise » ne sont pas directement supportés. Vous devez configurer un annuaire Azure Directory et synchroniser cet annuaire avec l’annuaire On Premise. Reportez-vous à la documentation Azure.

* 1. Configurez le compte Administrateur

Il est indispensable de renseigner l’adresse de messagerie d’au moins un compte administrateur. Cette adresse est utilisée pour toutes les alertes d’administration.

Créer un rôle d’application « Administrateur »



Associé le compte administrateur au rôle.

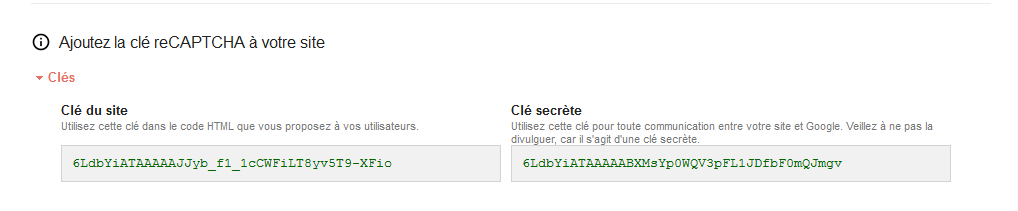
* 1. Configurer l’utilisation de Recaptcha

Recaptcha vous permet de vous protéger contre les robots.

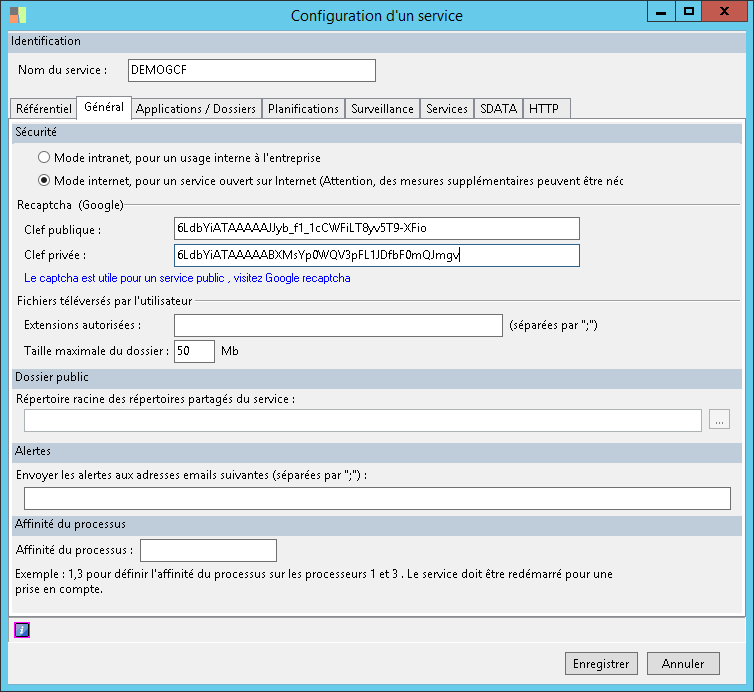
Pour activer Recaptcha :

* Visitez le lien Recaptcha de Google
* Cliquez sur Get Recaptcha
* Renseigner le domaine du site

Google vous génère deux clés :



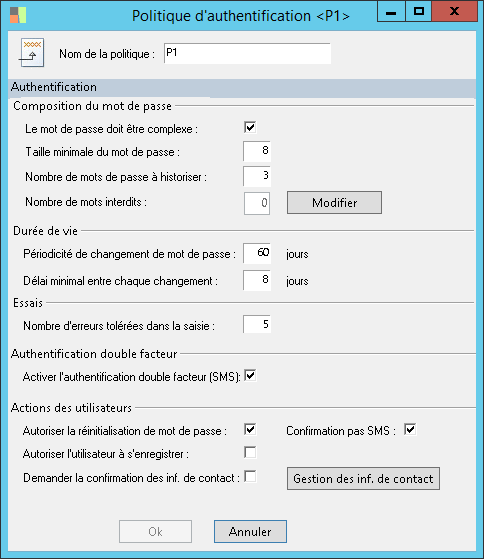
Dans la console d’administration des services :



* 1. Mise en œuvre de l’Annuaire Sage FRP 1000 Entreprise
     1. Comptes utilisateurs

Les recommandations pour l’utilisation de l’annuaire d’Entreprise sont les suivantes :

* Définissez une politique de d’authentification forte.
* Définissez une politique d’accès forte.

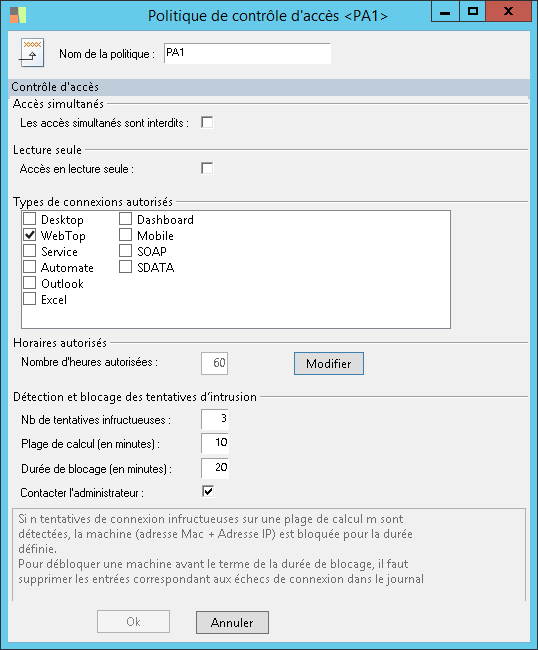


L’activation de l’authentification double facteur et la confirmation par SMS de la récupération de mot de passe, imposent le numéro de téléphone mobile renseigné dans les informations de compte de l’utilisateur.

Autoriser l’utilisateur à s’enregistrer peut être utilisé si besoin.

Note :

La fonction Gestion des informations de contact vous permet de gérer des campagnes de requalification de ces informations.

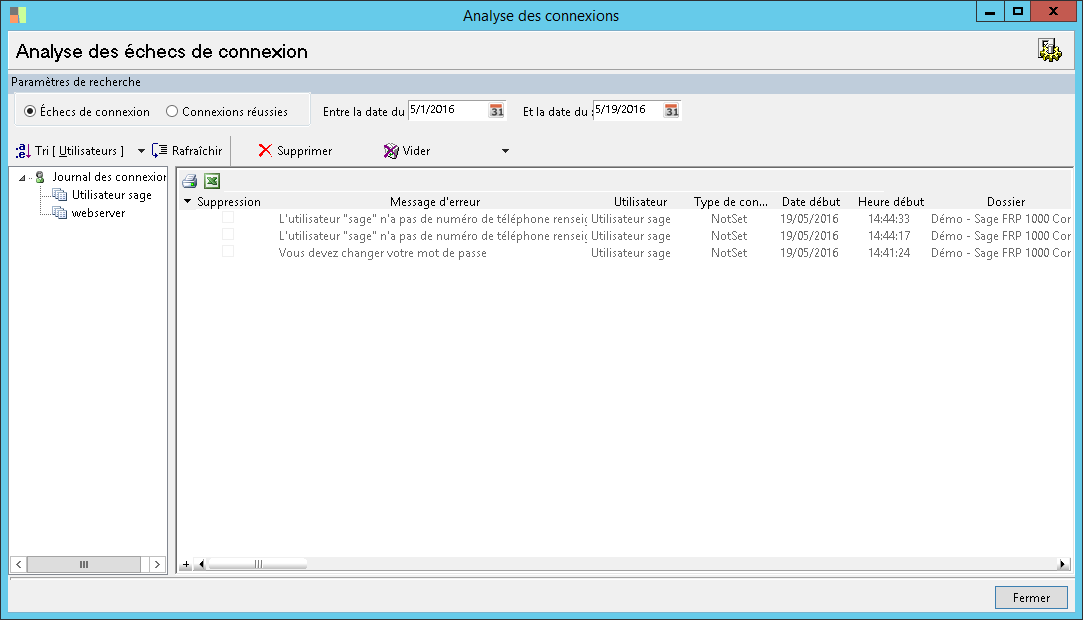


Note :

* Les restrictions de connexion ne s’appliquent pas à l’utilisateur « admin » mais celui-ci ne peut pas se connecter sur une Application Métier autre que la Console d’Administration
* Les comptes de services utilisés pour interfaces de programmation et les interfaces de traitements doivent être associés à une politique de contrôle d’accès adaptée.
* La détection et le blocage des tentatives d’intrusion n’est pas une mesure contre les attaques DOS, le blocage des IP se faisant après identification.

Note :

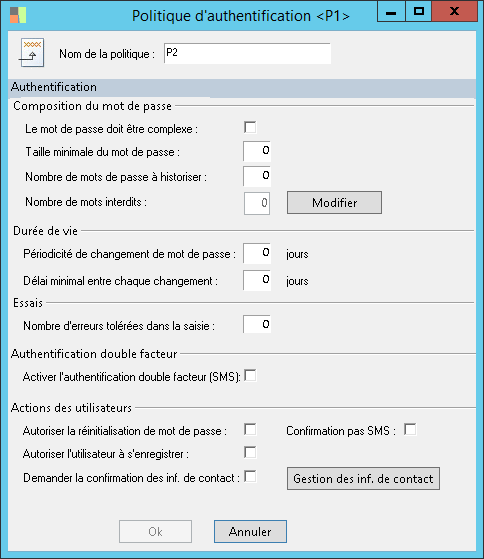
En cas d’erreur d’authentification des utilisateurs, vous pouvez consulter le journal des échecs de connexion :



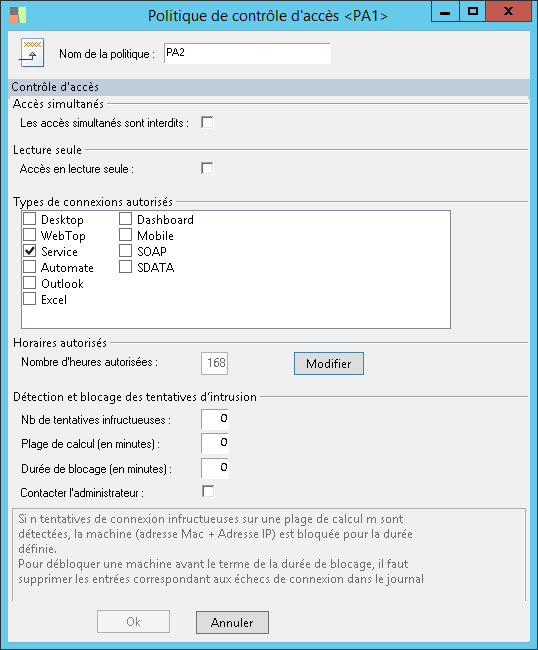
* + 1. Comptes de service

Les comptes de service, incluant le compte qui démarre le service, doivent être configurés sur un jeu de politique spécifique.

Définissez un jeu de politique pour les comptes de service :

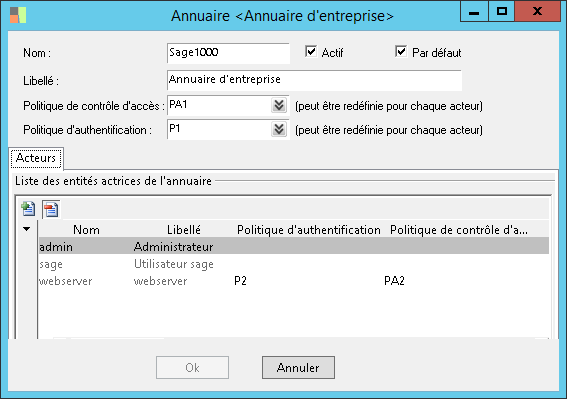


Cette politique n’impose pas un renouvellement des mots de passe



Cette politique autorise les accès services.

Associez ces politiques aux utilisateurs de service :



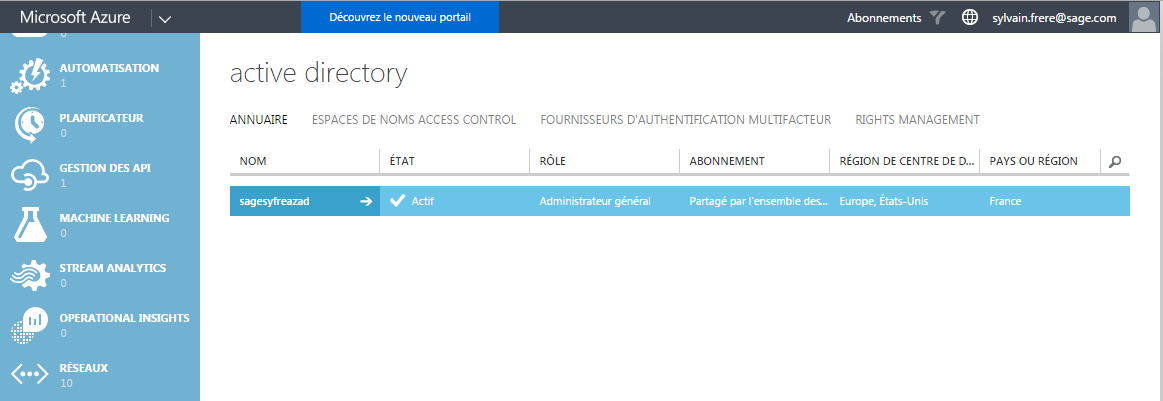
* 1. Mise en œuvre de Microsoft Azure Directory

Azure Directory peut être utilisé à travers le protocole OAUTH 2.0

Pour mettre en œuvre Azure Directory vous devez :

* Créer un annuaire dans Azure
* Ajouter votre application à l’annuaire
* Configurer votre application
* Configurer l’annuaire dans Sage FRP 1000
* Activer cet annuaire.
  + 1. Annuaire Azure Directory

Créer un annuaire AZD (Ancien portail) :



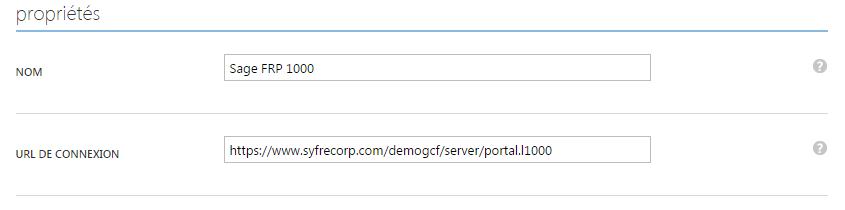
Ajouter une application :

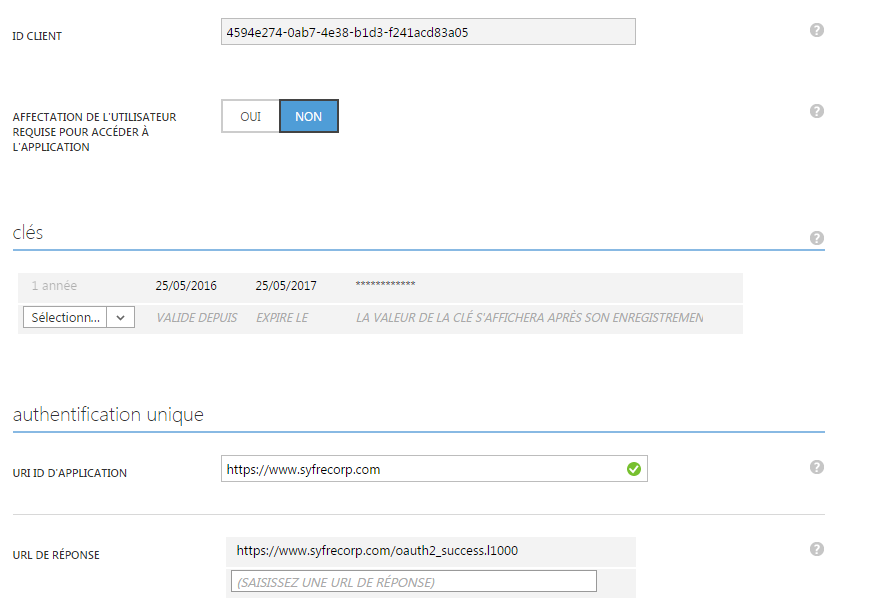
* Ajouter une application développée par mon organisation
* Application Web
* Url de connexion : Saisissez l’url de la home page de Sage FRP 1000
* Uri ID de l’application : Saisissez l’url du domaine de Sage FRP 1000

Configurez l’application :

* Ajoutez une clé
* Renseignez l’url de réponse

Vous devez obtenir une configuration de ce type ([www.syfrecorp.com](http://www.syfrecorp.com) est le domaine de l’Application dans cet exemple), notez l’url de réponse :



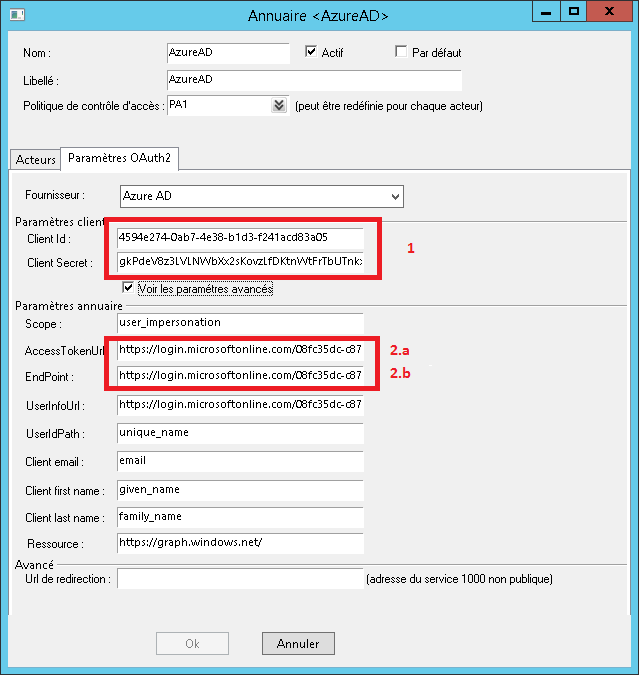


Notez la clé secrète affichée lors de la validation

Attention : C’est le seul moment où cette clé est affichée.

* + 1. Annuaire Sage FRP 1000

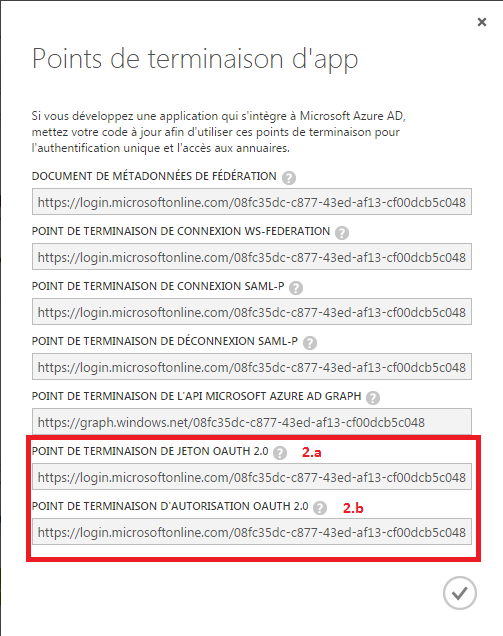
Créez un annuaire OAuth2 dans Sage FRP 1000 de type Azure AD :



1 : Renseignez le client Id et la clé secrète, ces informations sont celles obtenues à l’étape précédente.

2 : Renseignez les informations du point de terminaison, c’est informations sont accessible sur





Vous devez redémarrer les services après cette configuration.

Note

Cet annuaire doit s’appeler AzureAD pour que le logo correct apparaisse sur la page Web de connexion

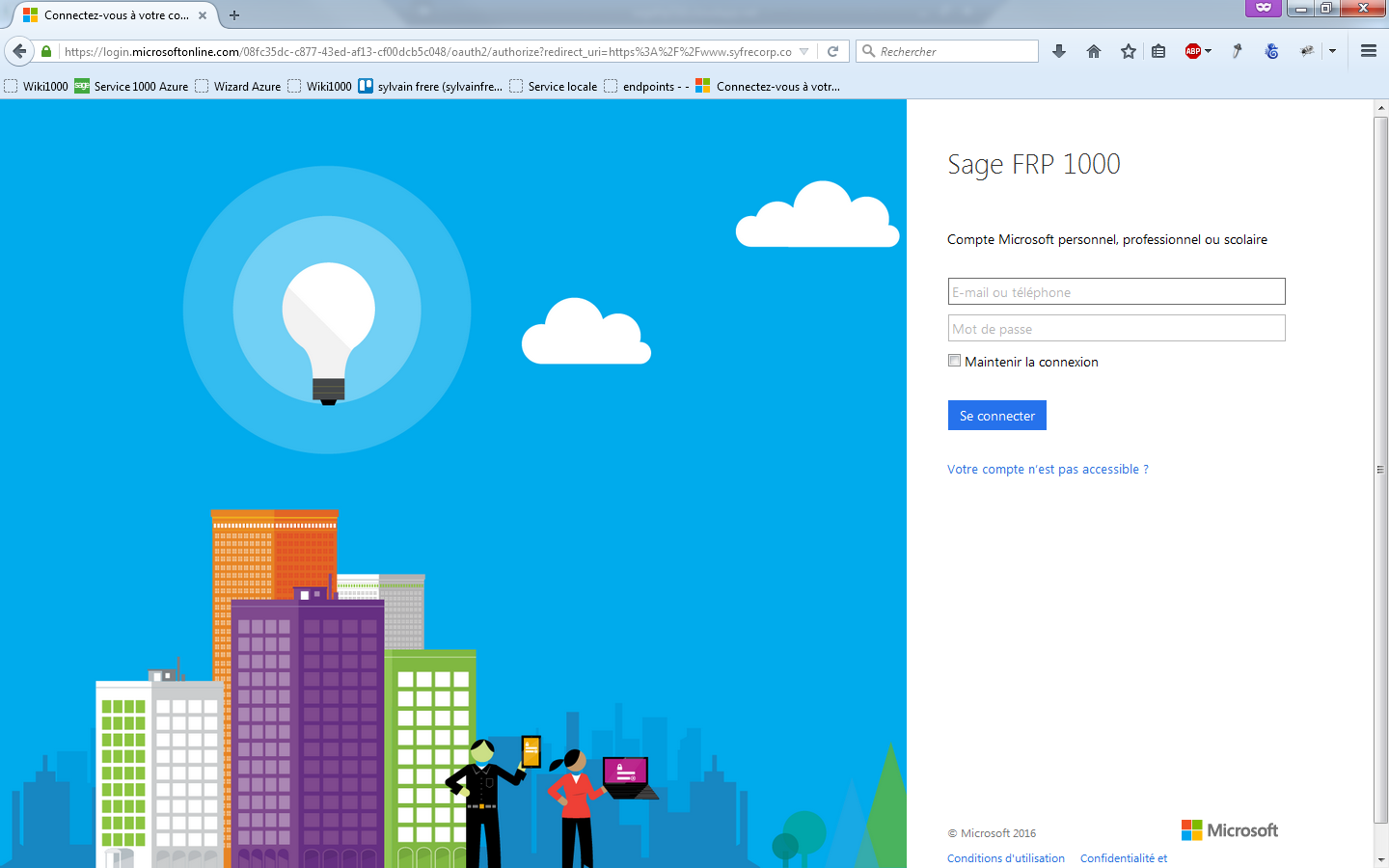
* + 1. Enregistrement des utilisateurs.

En mode OAuth le processus d’enregistrement d’un utilisateur est le suivant :

L’utilisateur se connecte une première fois en cliquant sur l’icône.

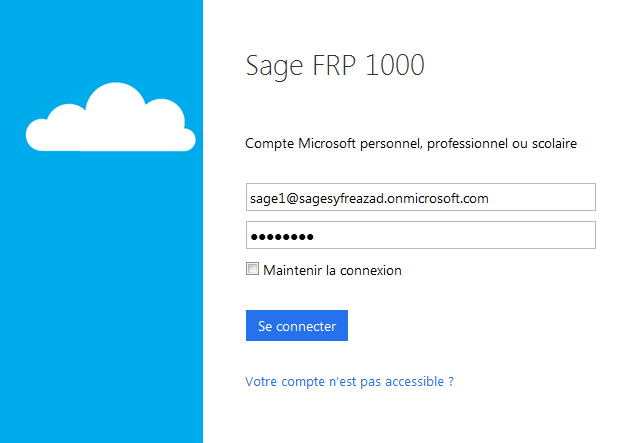


Si l’utilisateur n’est pas connecté sur azure une fenêtre de connexion apparait :

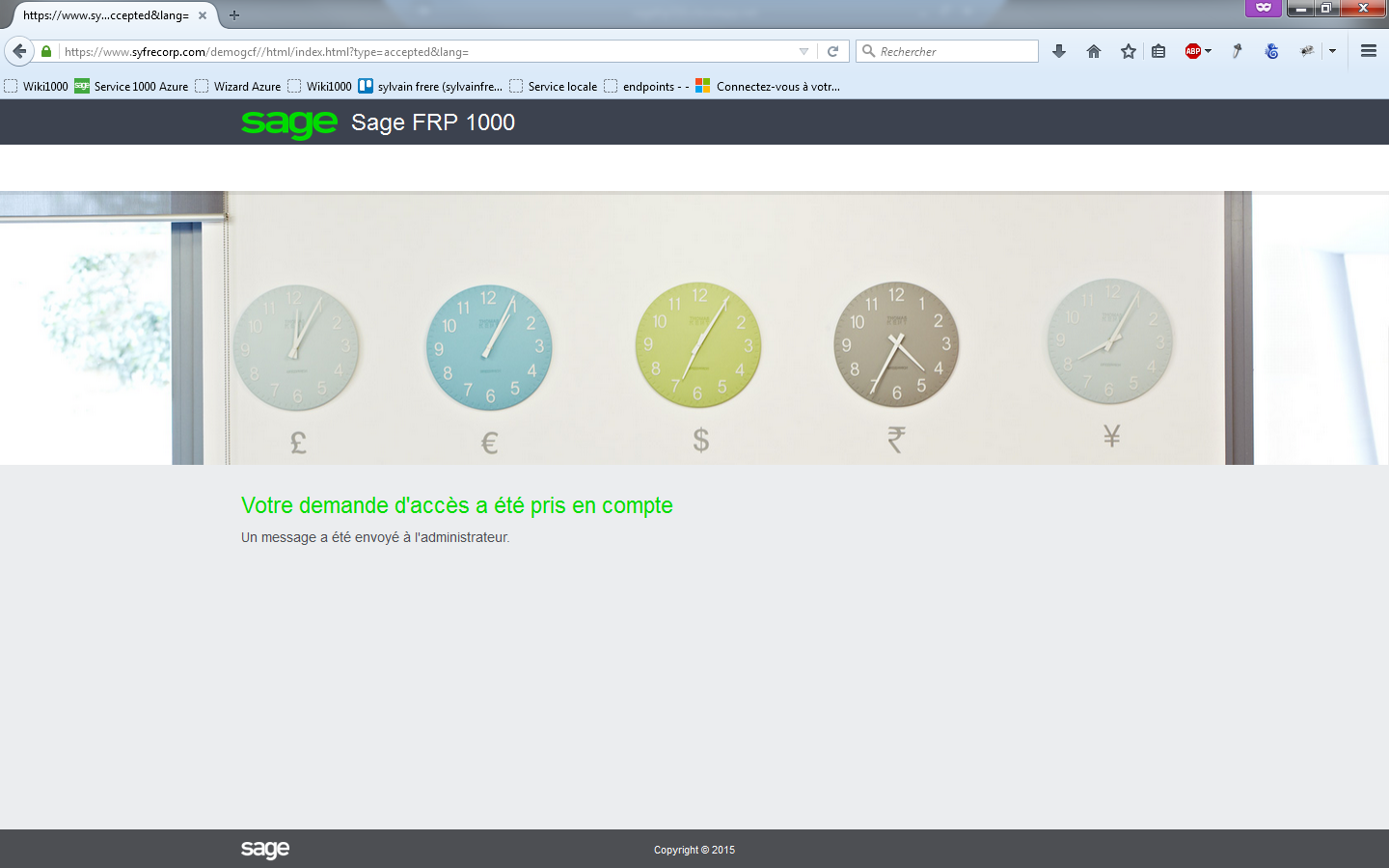


Cette fenêtre est géré par Azure

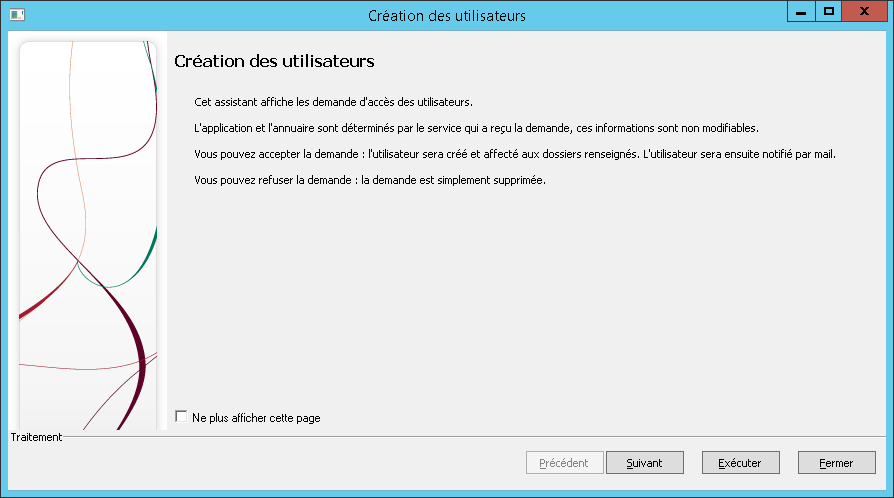
L’utilisateur se connecte en utilisant son compte de l’annuaire Azure.

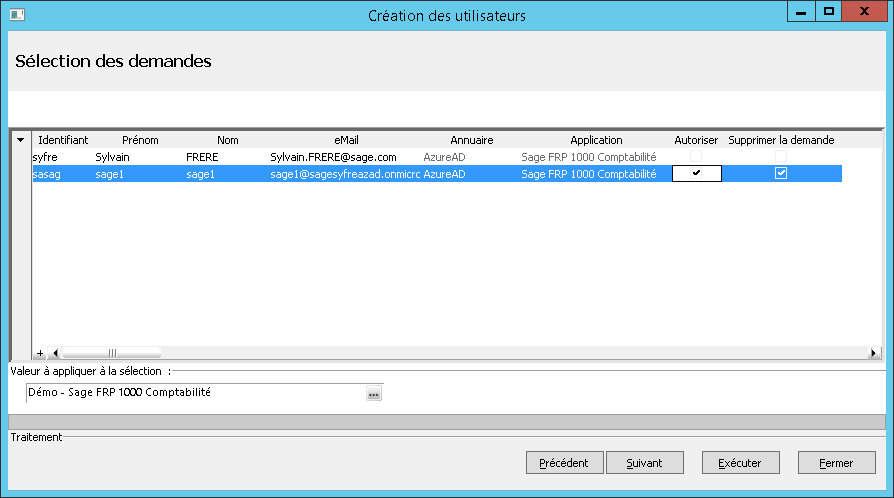
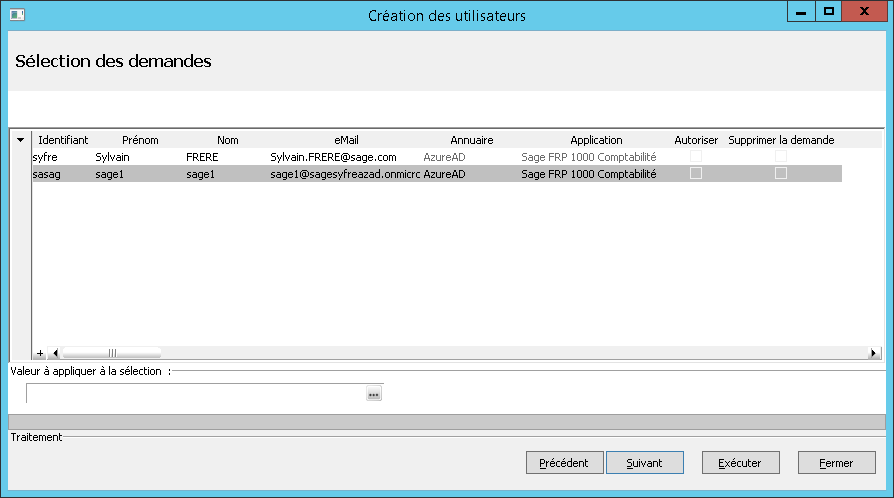


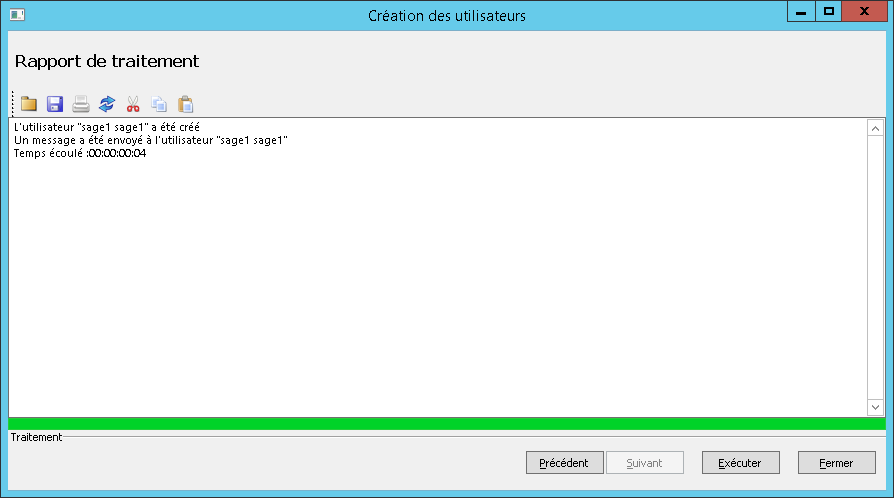
Du fait que l’utilisateur n’est pas renseigné dans Sage FRP 1000 une demande d’accès est enregistrée et un message est envoyé aux administrateurs.



Pour autoriser l’utilisateur, un administrateur doit utilisez « Gérer les utilisateurs » :







Note

Les comptes utilisateurs doivent être renseignés dans l’annuaire AZD, si ce compte est synchronisé avec l’AD de l’entreprise ce sont les comptes d’entreprise.

1. Sécurité
   1. Mise en place d’un certificat SSL.

La mise en place d’un certificat SSL est nécessaire sur un site de production.

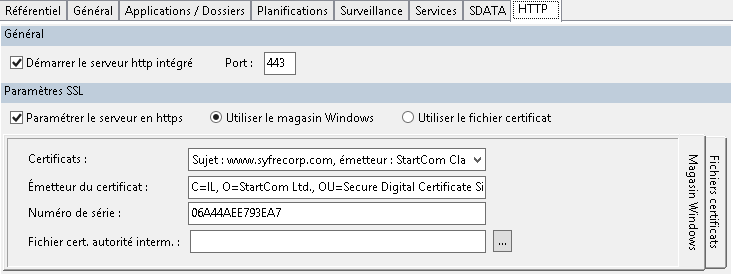
Vous devez disposer :

* D’un certificat SSL valide sur le domaine de votre service
* D’un fournisseur de nom de domaine.
  + 1. Mise en place au niveau des services Sage FRP 1000

Si vous utilisez Azure Load Balancer et un LBS vous devez installer le certificat SSL au niveau de chaque nœud Sage FRP 1000.

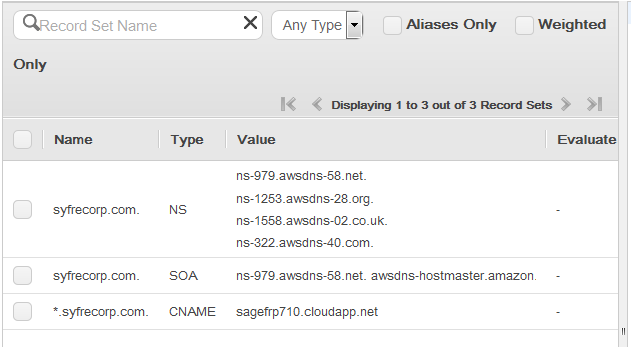
Pour configurer SSL :

* Installer le certificat dans le magasin de Windows (sur chaque nœud)
* Dans la Console des services sélectionner le certificat



* + 1. Configuration DNS

Vous devez configurer votre fournisseur DNS pour router le trafic sur votre domaine :



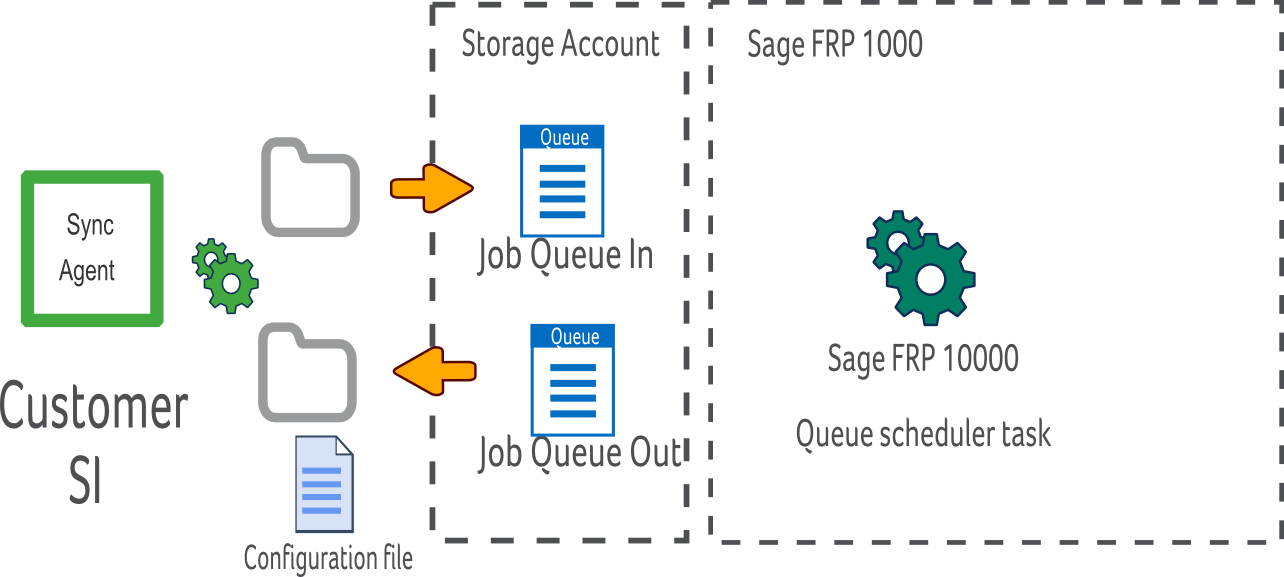
Cet exemple utilise Route 53 d’Amazon et route le trafic de syfrecorp.com vers sagefrp710.cloudapp.net

* + 1. Mise en place au niveau de Microsoft Application Gateway

L’installation du certificat est réalisée au niveau de l’Application Gateway, reportez-vous à cette section.

1. Intégration avec le Système d’information
   1. Architecture

Le principe d’interface entre la solution déployée dans Microsoft Azure et le système d’information du Client est celui-ci :



Des files d’attente Azure sont utilisées en interface, une entrée et une en sortie.

Un agent de synchronisation est installé sur le système du client.

Cet agent surveille un jeu de répertoires et transfère les fichiers déposés dans la file d’attente de traitement de la solution. La tâche de traitement est déterminée par la configuration de l’agent.

Un automate est configuré pour consommer les messages de la file d’attente et exécuter les traitements.

Les exportations sont configurées pour alimenter la file d’attente de sortie.

Note :

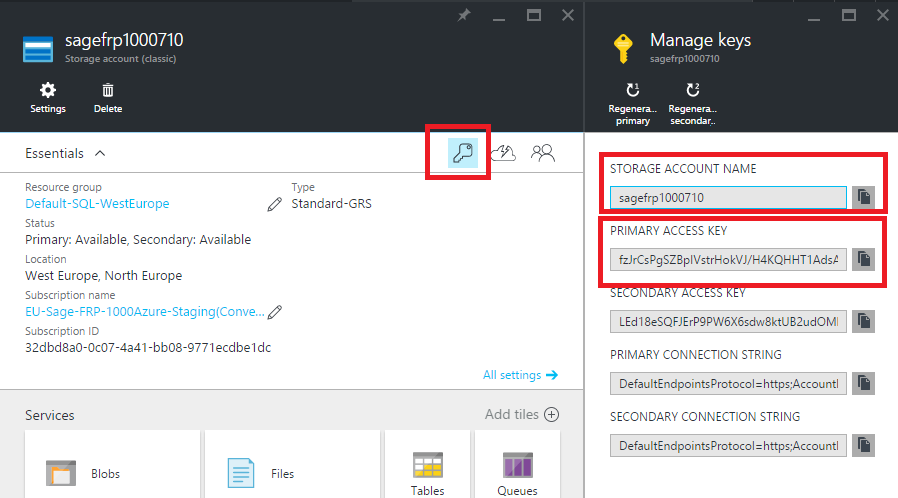
N’utiliser pas des files d’attente gérées par la base de données, utiliser des files d’attentes Azure.

* 1. Paramétrage des tâches d’exportation.

Par la suite nous allons réaliser la configuration d’un import d’écriture comptable, les étapes sont :

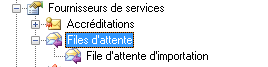
* Configurer les files d’attente
* Configurer un compte de service et obtenir un jeton d’authentification
* Installer et configurer le Sync Agent
* Paramétrer les automates Sage FRP 1000
  + 1. Configuration des files d’attente

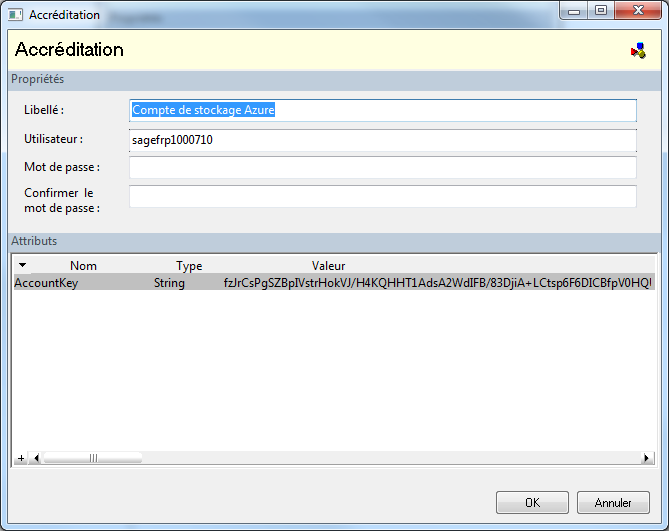
La première étape consiste à récupérer la clé publique d’accès du compte de stockage :

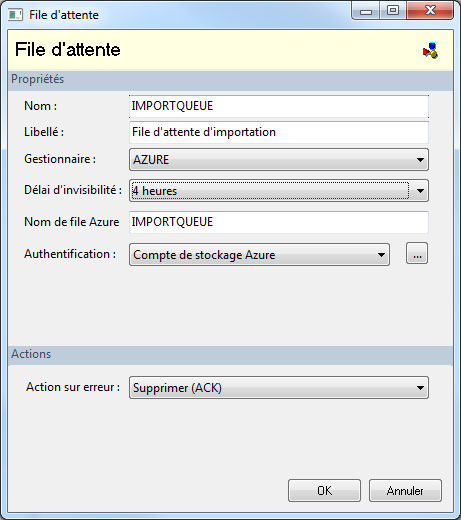


Configurez en suite une file d’attente :

Dans la console d’administration :



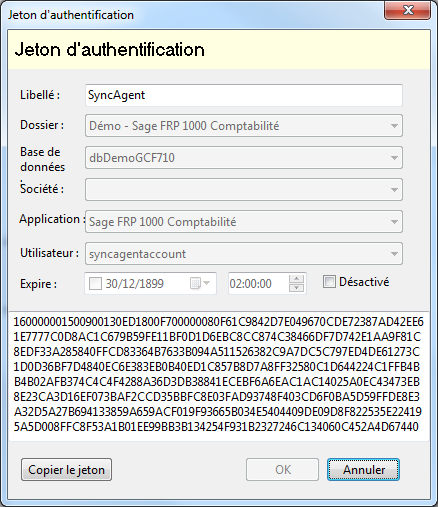




* + 1. Configurer un compte de service

Les messages de traitement sont authentifiés par un jeton d’authentification, pour créer un jeton :

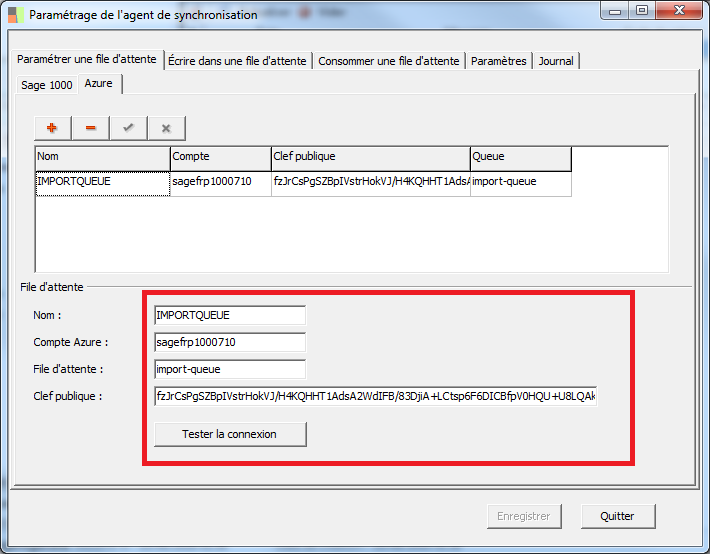
* Créez un compte de service
* Associez-le à votre dossier
* Sur l’association créé un jeton d’authentification.



* + 1. Installation et configuration de Sage Sync Agent.

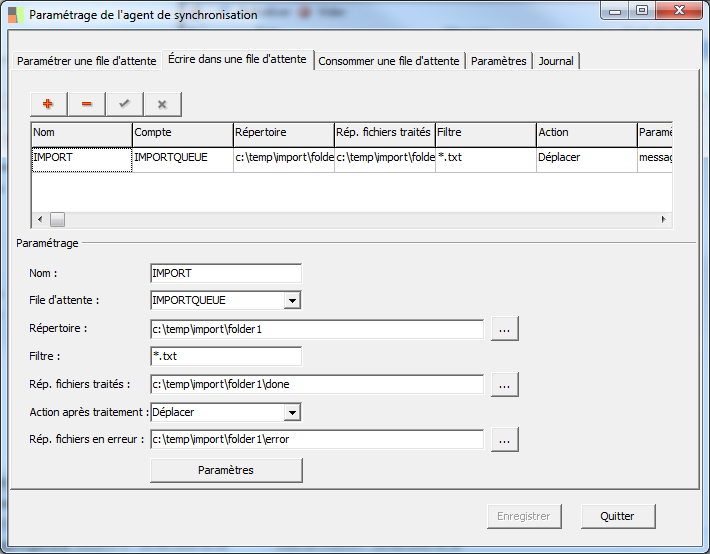
Le « Sync Agent » est un service Windows s’installant sur un poste du système du réseau du Client et permettant de faire le lien entre des fichiers déposés sur le système de fichiers du Client et les files d’attente Azure.

Dans l’assistant de configuration du Sync Agent configurez la file d’attente Azure :



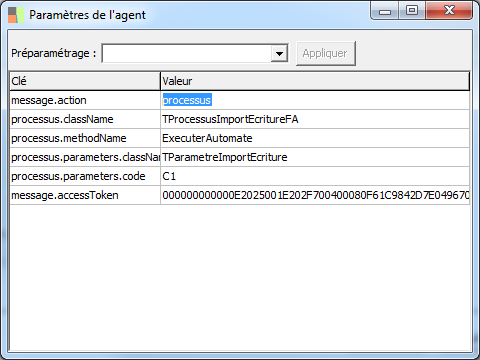
* Compte Azure : Le nom du compte de stockage Azure
* File d’attente : Le nom de la file d’attente Azure
* Clé publique : La clé publique du compte de stockage.

Configurez ensuite un répertoire d’envoi de message :



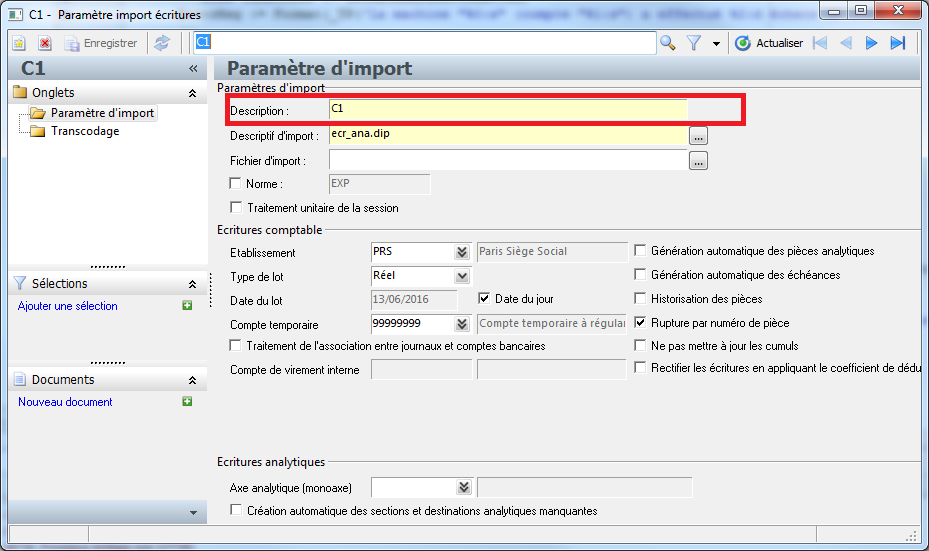
* File d’attente : Le nom de la file d’attente précédemment configurée.

Dans les paramètres de la tâche sélectionner le type d’importation souhaité et renseignez les paramètres complémentaires :



* Le code de paramétrage de la tâche
* Le jeton d’authentification

Le code de paramétrage correspond au paramétrage de la tâche dans Sage FRP 1000, dans cet exemple pour un import d’écriture comptable :



Le jeton d’authentification correspond au jeton précédemment créé sur le compte de service sage FRP 1000.

Note :

Vous pouvez configurer manuellement le Sync Agent en modifiant le fichier de configuration.

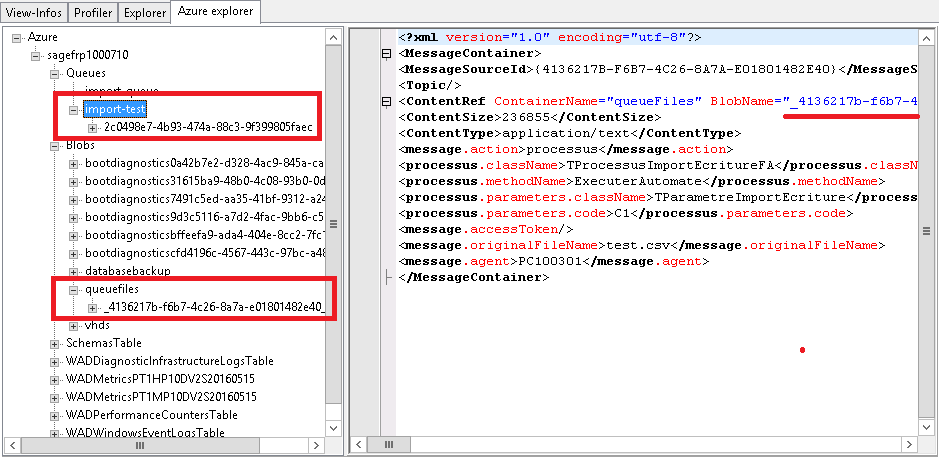
* + 1. Tester la communication

Avant de procéder à l’étape suivante il peut être utile de vérifier la communication entre le Sync Agent et Azure.

Pour ceci vous pouvez :

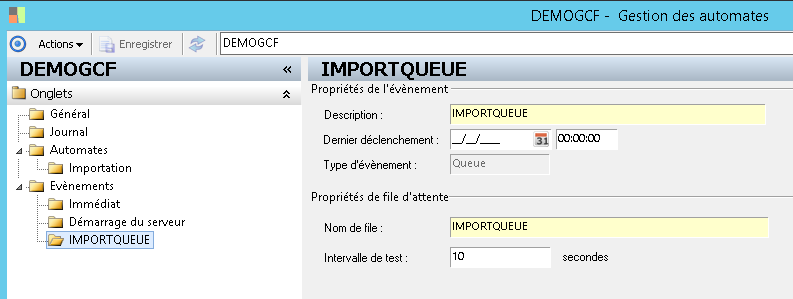
* Paramétrer un nom de file d’attente Azure de test
* Copier un fichier dans le répertoire surveillé
* Vérifier que le fichier et le message ont bien été créés.

Il existe de nombreux outils pour explorer un compte de stockage Azure, un outil rudimentaire est fourni dans le concepteur de modèle de Sage FRP 1000 :

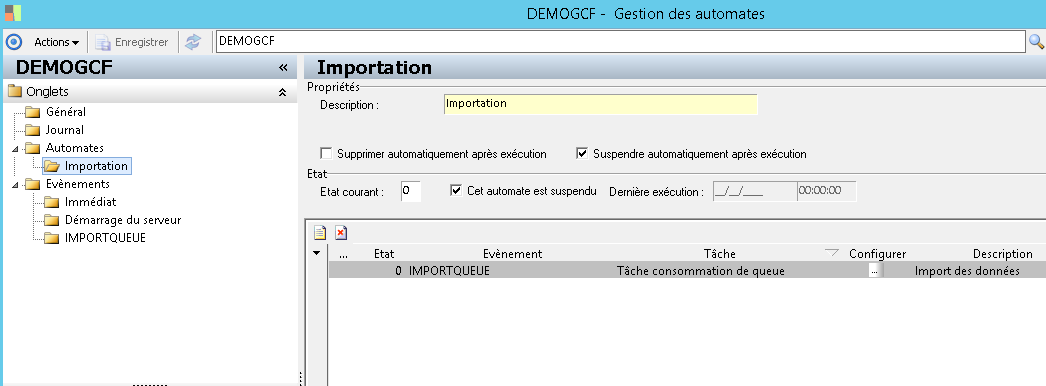


* + 1. Paramétrage des automates

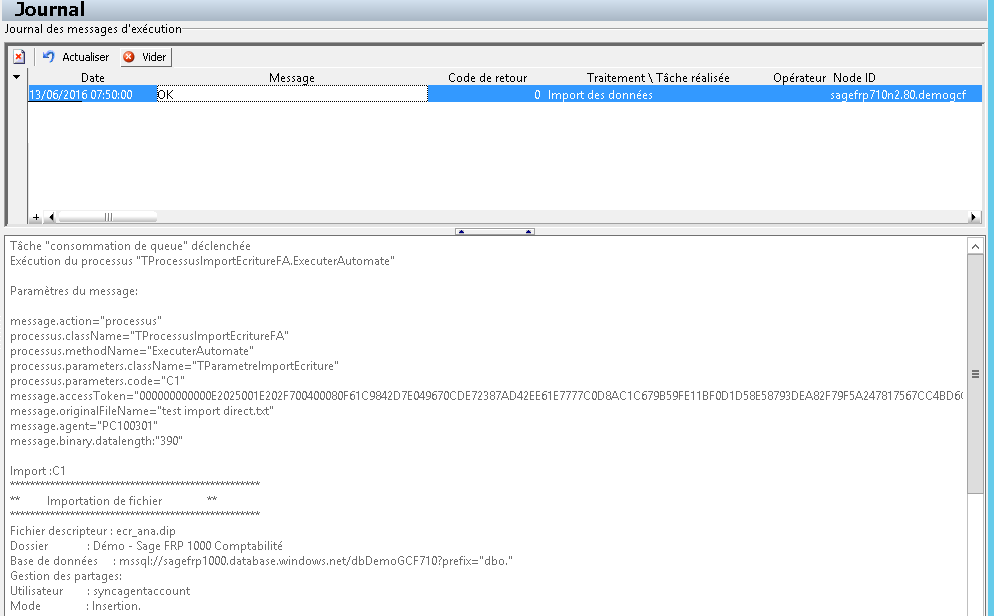
Créez un évènement file d’attente associé à la file d’attente Azure :



Puis un automate déclenché par cet évènement et exécutant la tâche « Tache consommation de queue » :



Cette épate termine la configuration, si vous déposer un fichier dans le répertoire d’envoi celui-ci est envoyé dans la file Azure et consommé par la tâche de l’automate :

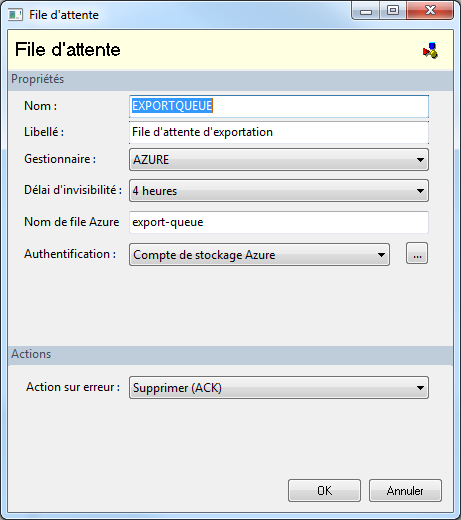


* 1. Paramétrage des tâches d’exportation.

Les étapes pour configurer une tâche d’exportation sont :

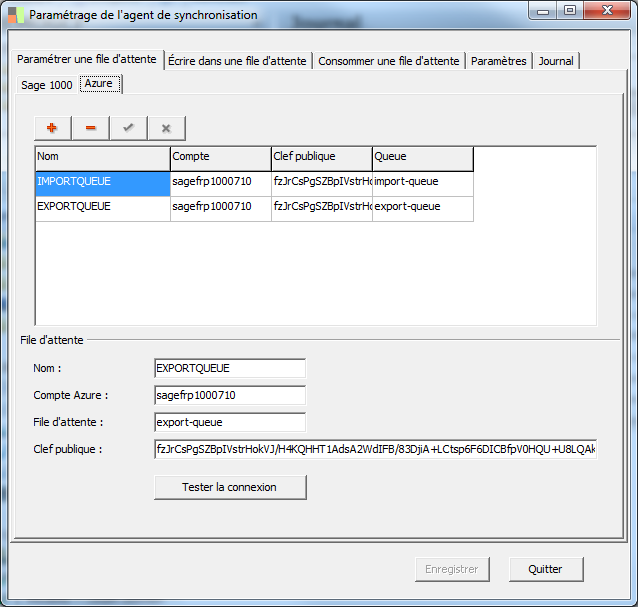
* Créer une file d’attente d’exportation.
* Configurer le Sync Agent.
* Créer une tâche d’automate d’exportation.
  + 1. Créer une file d’attente d’exportation.

Ces files d’attente sont identiques aux files d’attente d’exportation, utiliser simplement un nom de file Azure différent :

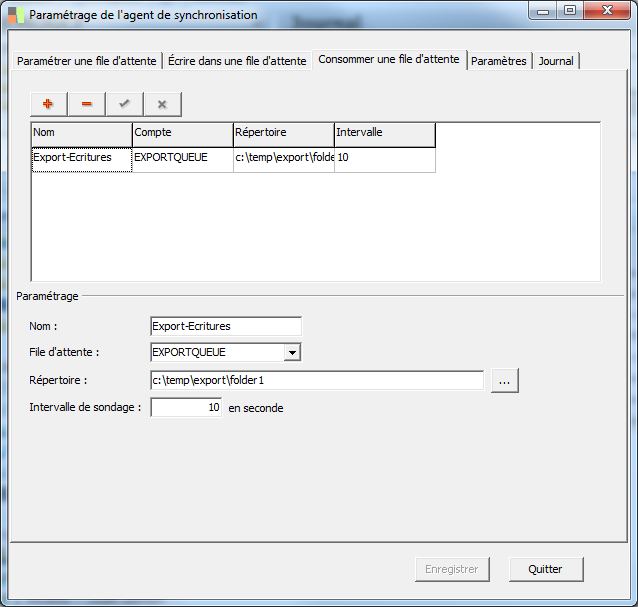


* + 1. Configurer le Sync Agent.

Vous devez ajouter la file d’attente dans la configuration du Sync Agent :

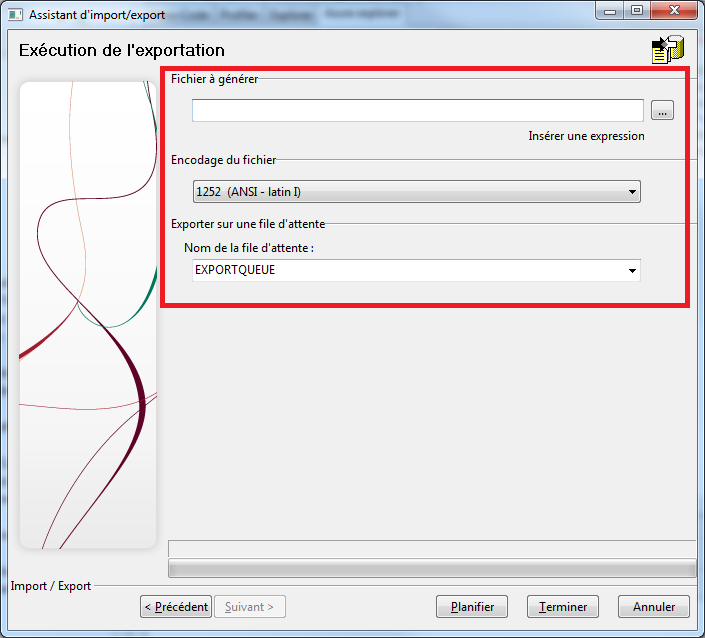


Et ajouter un répertoire pour recevoir les fichiers de cette file :



* + 1. Créer une tâche d’automate d’exportation.

Lorsque vous planifiez la tâche d’automate sélectionnez la file d’attente d’exportation :



* Ne pas renseigner de fichier de sortie (un fichier temporaire sera créé)
* Définir le format du fichier
* Sélectionner la file d’attente.

|  |  |  |
| --- | --- | --- |
| Table subtitle | Table subtitle | Table subtitle |
| Table text | Table text | Table text |
| Table text | Table text | Table text |
| Table text | Table text | Table text |
| Table text | Table text | Table text |