

sage FRP 1000

Guide de déploiement Azure

Version 7.10

Juin 2016



Ce document décrit les recommandations pour le déploiement de Sage FRP 1000 sur Microsoft Azure. Ce document fait référence au mode de déploiement « Classique » sur Microsoft Azure.

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.

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 pilotée (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

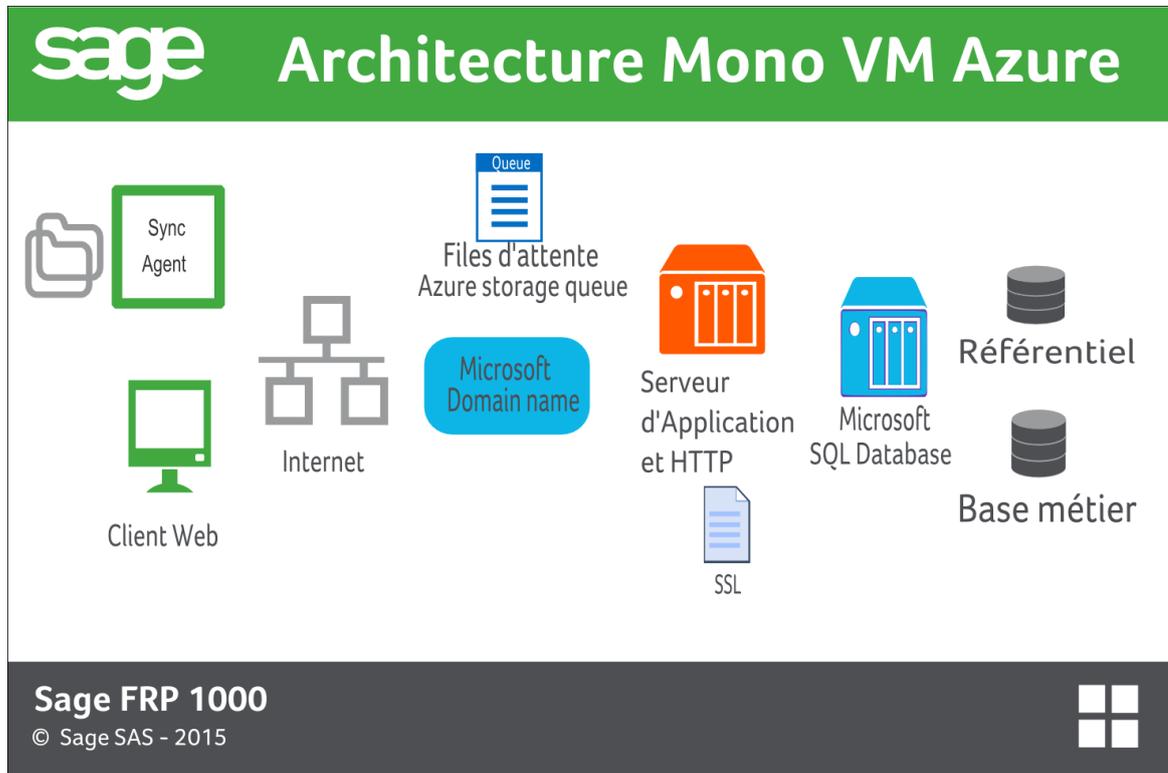
Contenu

Architecture types	6
Architecture Single VM	6
Architecture Cluster multi-VM (Application Gateway)	7
Architecture Cluster multi-VM (Load balancer)	8
SELECTION DES COMPOSANTS	9
Sélection du type de machine virtuelle.	9
Système d'exploitation.	9
Sélection du moteur de base de données	9
Utilisation de Azure SQL Database	9
Utilisation de Microsoft SQL Server	10
INSTALLATION ET CONFIGURATION	11
Installation de Sage FRP 1000	11
Création de la machine virtuelle	11
Création du serveur SQL	12
Installation de Sage FRP 1000	12
Configuration du service Sage FRP 1000	13
Configuration du Firewall de la machine virtuelle.	13
Configuration du Firewall de Azure SQL Server.	14
Configuration de la sauvegarde des données.	14
Point in time	14
Fonctionnalités base de données du portail Azure	14
Exportation automatisée.	15
Configuration du Service de messagerie (SMTP)	15
Configuration d'un fournisseur de SMS	16
CONFIGURATION CLUSTER	18
Mise en œuvre de Microsoft Azure Load Balancer	19
Configuration Sage 1000	21

Mise en œuvre de Microsoft Azure Application Gateway	23
Configuration des machines virtuelles	23
Configuration des services Sage FRP 1000	23
Création de l'Application Gateway	24
Configuration de votre DNS	26
ANNUAIRE DE GESTION DES IDENTITES	28
Configurez le compte Administrateur	28
Configurer l'utilisation de Recaptcha	28
Mise en œuvre de l'Annuaire Sage FRP 1000 Entreprise	30
Comptes utilisateurs	30
Comptes de service	32
Mise en œuvre de Microsoft Azure Directory	34
Annuaire Azure Directory	34
Annuaire Sage FRP 1000	35
Enregistrement des utilisateurs.	37
SECURITE	42
Mise en place d'un certificat SSL.	42
Mise en place au niveau des services Sage FRP 1000	42
Configuration DNS	42
Mise en place au niveau de Microsoft Application Gateway	43
INTEGRATION AVEC LE SYSTEME D'INFORMATION	44
Architecture	44
Paramétrage des tâches d'exportation.	44
Configuration des files d'attente	45
Configuration d'un compte de service	47
Installation et configuration de Sage Sync Agent.	47
Tester la communication	50
Paramétrage des automates	51
Paramétrage des tâches d'exportation.	52
Création d'une file d'attente d'exportation.	53
Configuration du Sync Agent.	54
Création d'une tâche d'automate d'exportation	56

Architecture types

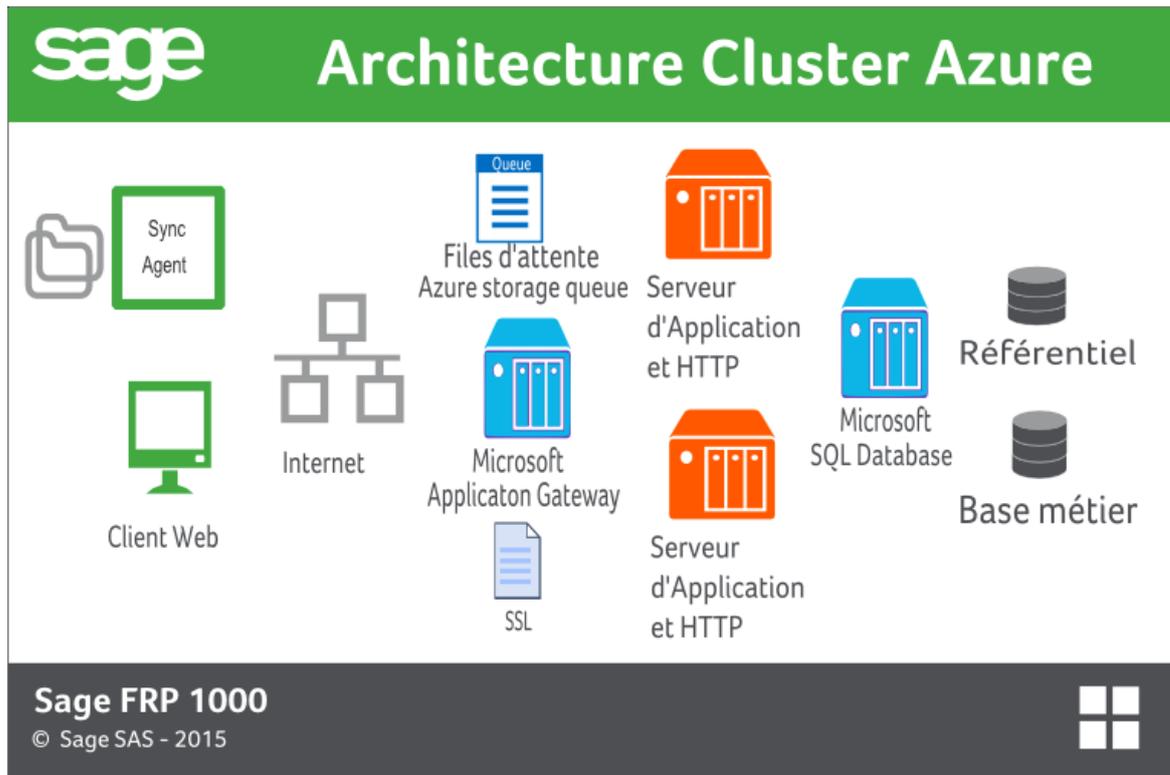
Architecture Single VM



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

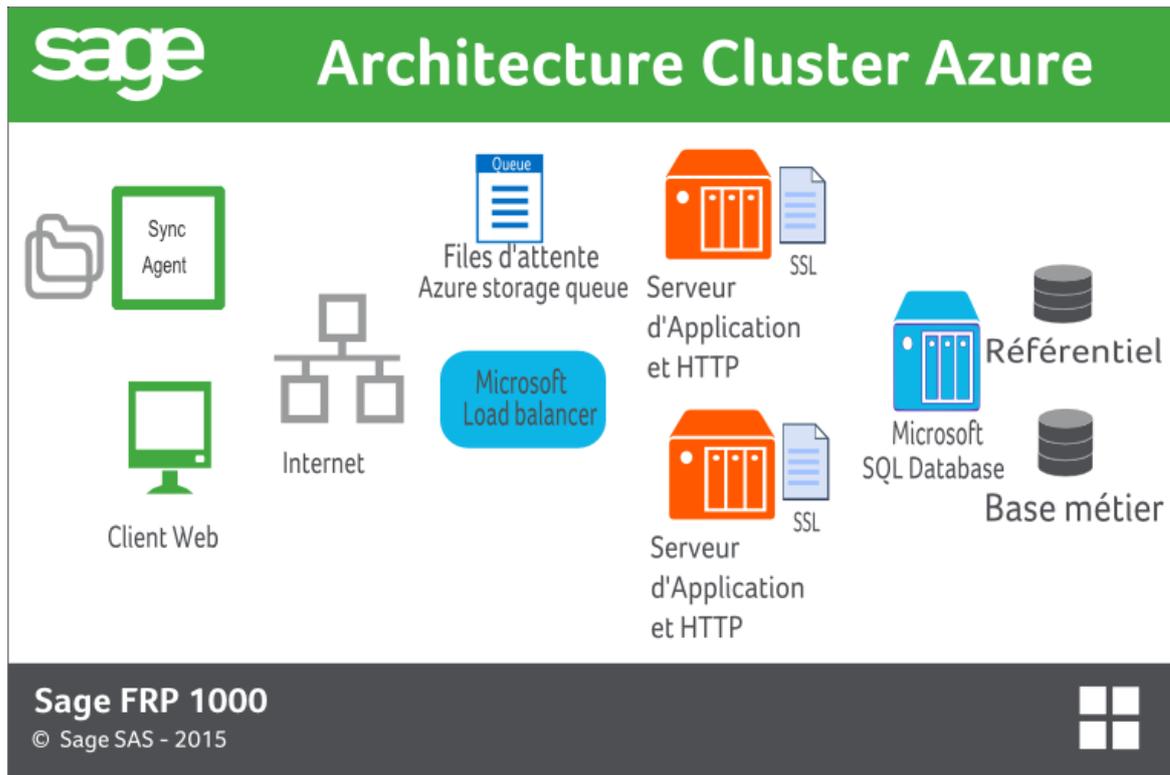
Architecture Cluster multi-VM (Application Gateway)

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
Domain Name	Microsoft	Load balancer state full et frontal SSL

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
Domain Name	Microsoft	Load balancer state less

Note: Dans cette architecture, la fonctionnalité d'équilibrage de charge est prise en compte à la fois par l'Azure Load balancer (sans état) et par Sage FRP 1000 (avec état).
Chaque Service Sage FRP 1000 doit détenir le certificat SSL

Sélection des composants

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.

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.

Sélection du moteur de base de données

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 certaines 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.

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

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.

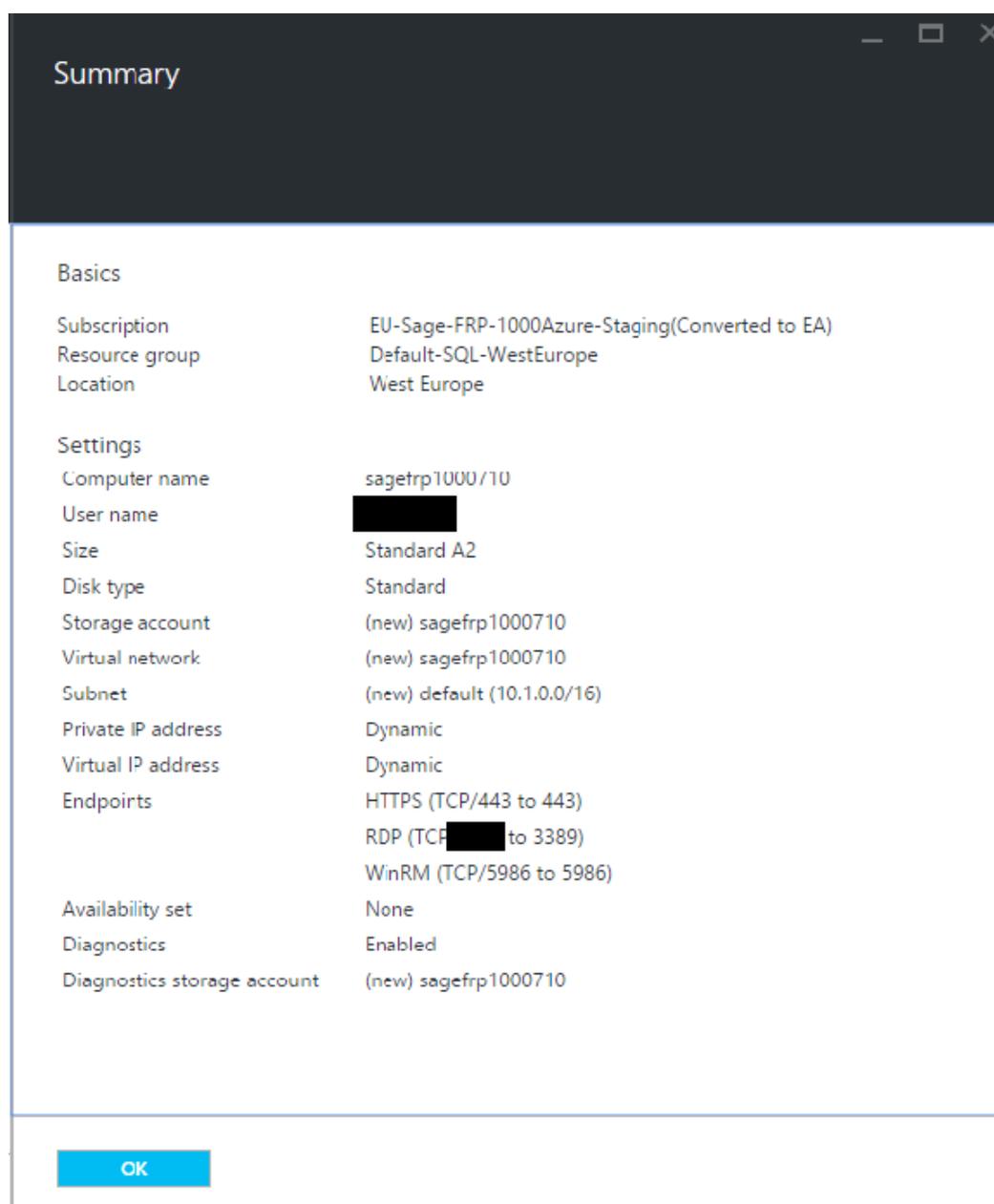
Installation et configuration

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.

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 HTTPsApply to indented text like this.

Important! Votre service sera accessible en Internet, n'utilisez pas http mais https

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.

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>

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 workflow
- Démarrez le serveur http intégré
- Démarrez le serveur en Https

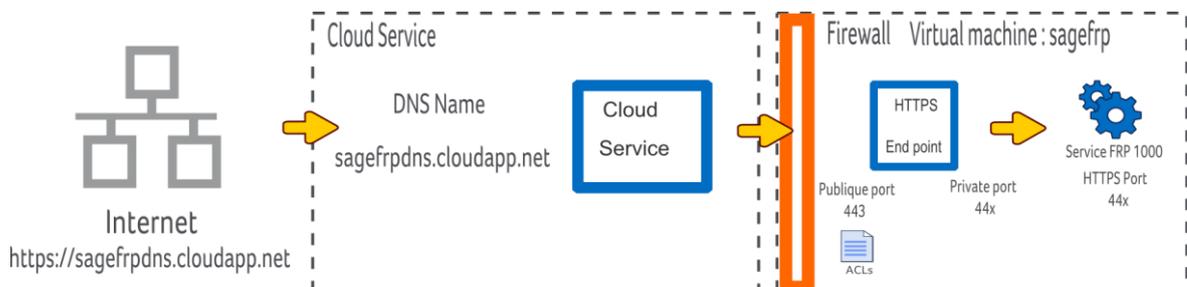
Dans la console des services Windows (services.msc) :

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

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

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>

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.

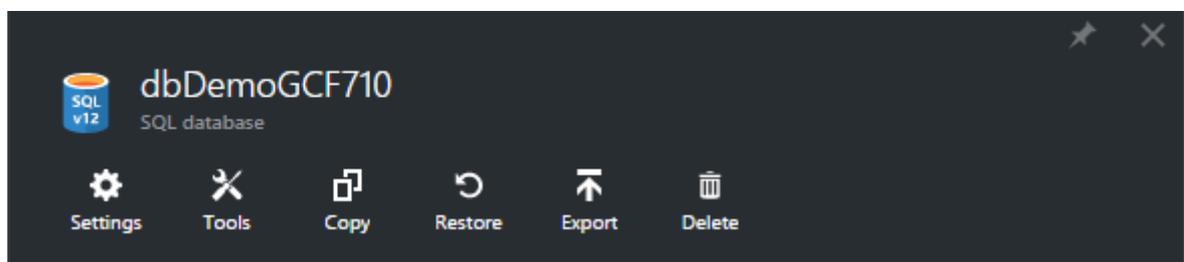
Néanmoins si vous avez besoin d'accéder à ces serveurs, par exemple pour SQL Management Studio, vous pouvez configurer le Firewall du serveur SQL en définissant les plages d'IP autorisées.

Configuration de la sauvegarde des données.

Point in time

Par défaut, les bases de données SQL Data base 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 dans 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 :



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.

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.

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 :

Paramétrage de la messagerie système

Fournisseur

Nom du service :

Fournisseur :

Actif

Serveur SMTP

Serveur SMTP :

Sécurité :

Utilisateur :

Mot de passe :

Expéditeur :

OK Tester Annuler

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 :

Paramétrage du service d'envoi de sms

Fournisseur

Nom du service : Twilio

Fournisseur : Twilio

Actif

Paramètres

Url : https://api.twilio.com/2010-04-01/Account...

Méthode http : Post

Paramètres :
From=@sender@
To=@recipients@
Body=@textMessage@

Authentification

Auth. basique :

Nom d'utilisateur : AC4ef94...

Jeton :

OK Tester Annuler

Vous devez renseigner le sid fournit par Twilio comme utilisateur.

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

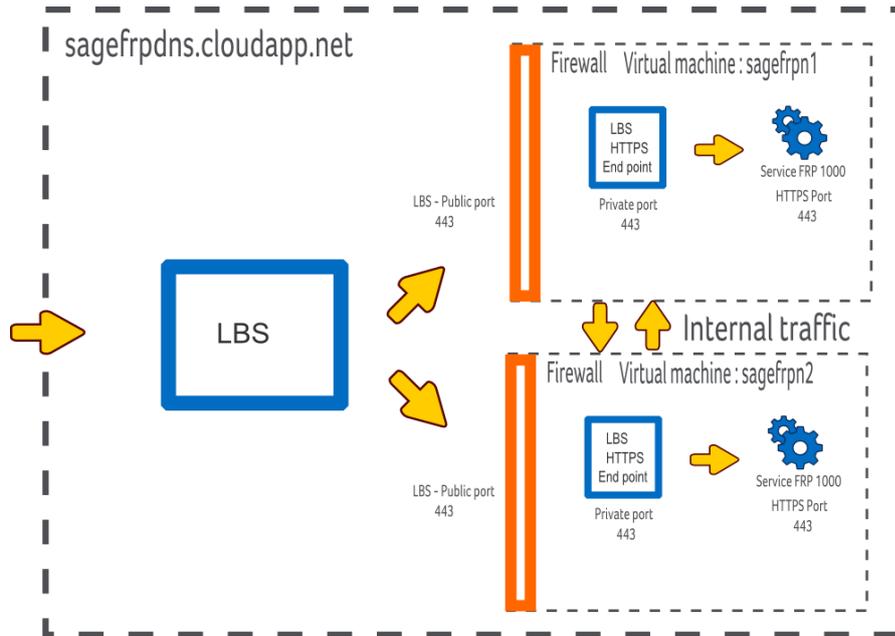
Les différences entre les deux architectures sont les suivantes :

Architecture	
Azure load balancer	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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.

Mise en œuvre de Microsoft Azure Load Balancer



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

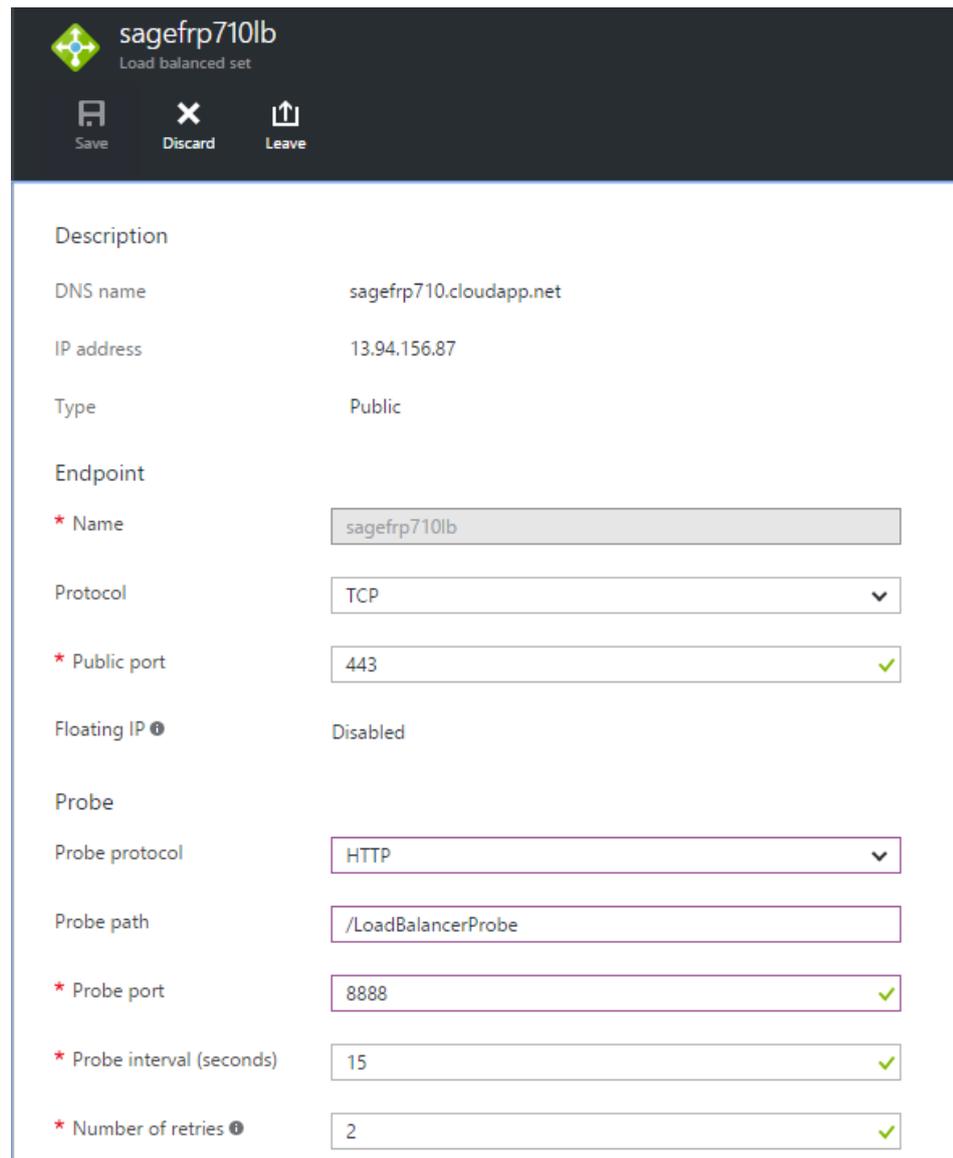
Sur la seconde machine vous pouvez n'installer que le service sage FRP 1000 et recopier le fichier de configuration servicel1000.ini

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 » :



The screenshot shows the configuration page for a Load Balanced Set in the Azure portal. The page title is 'sagefrp710lb Load balanced set'. At the top, there are three buttons: 'Save', 'Discard', and 'Leave'. The configuration is organized into sections: 'Description', 'Endpoint', and 'Probe'. The 'Description' section includes fields for 'DNS name' (sagefrp710.cloudapp.net), 'IP address' (13.94.156.87), and 'Type' (Public). The 'Endpoint' section includes 'Name' (sagefrp710lb), 'Protocol' (TCP), 'Public port' (443), and 'Floating IP' (Disabled). The 'Probe' section includes 'Probe protocol' (HTTP), 'Probe path' (/LoadBalancerProbe), 'Probe port' (8888), 'Probe interval (seconds)' (15), and 'Number of retries' (2). Green checkmarks are visible next to the 'Public port', 'Probe port', 'Probe interval', and 'Number of retries' fields, indicating they are valid.

Description	
DNS name	sagefrp710.cloudapp.net
IP address	13.94.156.87
Type	Public

Endpoint	
* Name	sagefrp710lb
Protocol	TCP
* Public port	443
Floating IP	Disabled

Probe	
Probe protocol	HTTP
Probe path	/LoadBalancerProbe
* Probe port	8888
* Probe interval (seconds)	15
* Number of retries	2

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 :

NAME	PROTOCOL	PUBLIC PORT	PRIVATE POR..	ACL RULES
LOAD-BALANCED				
sagefrp710lb	TCP	443	443	0
STANDALONE				
Remote De...	TCP		3389	0
WinRM	TCP	5986	5986	0

Configuration Sage 1000

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

- Installez la clé Sage FRP 1000 Cluster
- Créez 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

Configuration d'un service

Identification

Nom du service : DEMOGCF

Référentiel Général Applications / Dossiers Planifications Surveillance Services SDATA HTTP

Général

Démarrer le serveur http intégré Port : 443

Paramètres SSL

Paramétrer le serveur en https Utiliser le magasin Windows Utiliser le fichier certificat

Certificats : <Aucun certificat>

Émetteur du certificat :

Numéro de série :

Fichier cert. autorité interm. :

Paramètres HTTP

Protocole : https: Hôte : sagefrp710 Port : 443 Service :

Il s'agit des informations nécessaires aux utilisateurs pour accéder au service.
Ces informations sont utiles au service pour la construction d'URL de rappel (web services, Workflow, SData...) :

Répartition de charge avec serveur http intégré

Ce service effectue une répartition de charge Port d'écoute inter-service : 8888

Gestion de l'ACL

Nombre de règles : 0 Modifier les règles

Les utilisateurs qui ont le droit de gérer le dossier peuvent ajouter de nouvelles règles à l'exécution

Enregistrer Annuler

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>).

Note: 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.

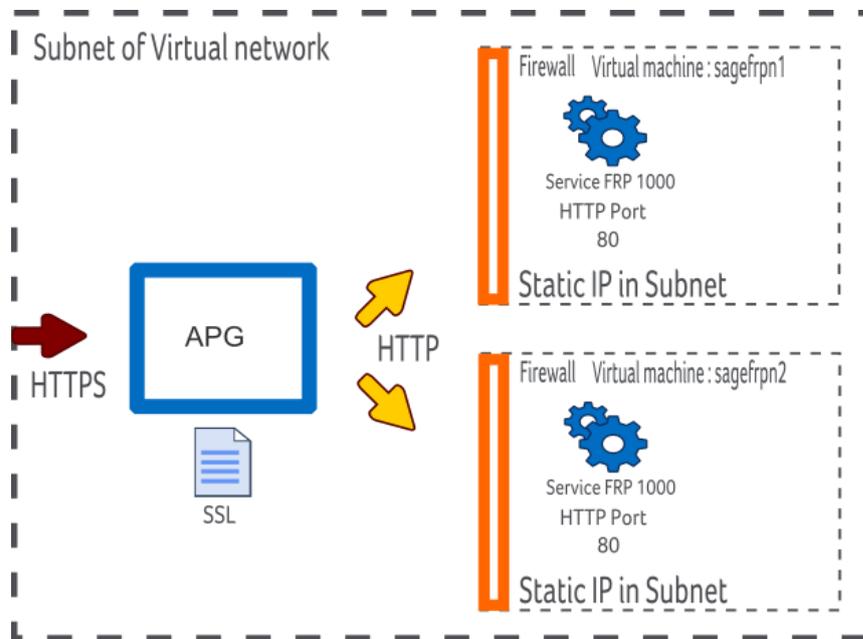
L'ensemble des machines sont hébergées dans le même domaine, les ports publics des end-points doivent être distincts.

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 (i.e.

Cloud Service). Reportez-vous à la documentation Azure sur « Comment créer une image à partir d'une machine virtuelle ».

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.

Configuration des machines virtuelles

- Les IP des machines doivent être statiques
- Vous devez les retirer des « Load Balancer Set » si nécessaire
- Définissez une règle de Firewall pour ouvrir le port 80

Configuration des services Sage FRP 1000

- Modifiez la configuration http pour que le port d'écoute soit http.

Identification

Nom du service :

Référentiel Général Applications / Dossiers Planifications Surveillance Services SDATA HTTP

Point d'écoute HTTP

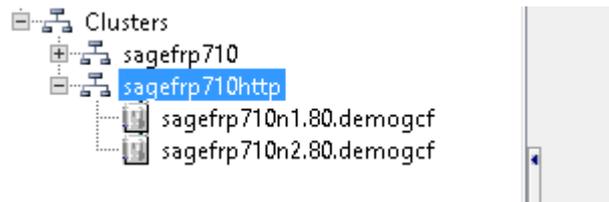
Démarrer le serveur http intégré Paramétrer le serveur en https Port :

Domaine

Protocole : Domaine : Port : Service :

Ces informations sont utiles au service pour la construction d'URL de rappel (OAuth, Web services, Workflow, Outlook ...)

- Créez un Cluster pour les nœuds



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\.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/NetworkConfigurat
ion">
  <VirtualNetworkConfiguration>
    <Dns>
      <DnsServers>
        <DnsServer name="AZURE" IPAddress="100.91.250.140" />
      </DnsServers>
    </Dns>
  </VirtualNetworkConfiguration>
</NetworkConfiguration>
```

```

<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
```

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, cette adresse doit être renseignée dans le CName de votre configuration DNS.

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.

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.

Créez un rôle d'application « Administrateur »

Rôle <Administrateur>

Administrateur

Libellés : Administrateur

Description

Rôle d'application

Rôle de conception

Rôle d'exécution

Droits et interdictions

Droits

	Type de droit	Descriptif
<input checked="" type="checkbox"/>	Additionnel	Droit d'administration
<input type="checkbox"/>	Additionnel	Droit de gérer le dossier

OK Annuler

Associez le compte administrateur au rôle.

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 :

📘 Ajoutez la clé reCAPTCHA à votre site

▼ Clés

Clé du site

Utilisez cette clé dans le code HTML que vous proposez à vos utilisateurs.

6LdbYiATAAAAAAJyb_f1_1cCWFILt8yv5T9-XFio

Clé secrète

Utilisez cette clé pour toute communication entre votre site et Google. Veillez à ne pas la divulguer, car il s'agit d'une clé secrète.

6LdbYiATAAAAAABXMsYp0WQV3pFL1JDfbF0mQJmgv

Dans la console d'administration des services :

The screenshot shows the 'Configuration d'un service' window in the Azure portal. The 'Sécurité' section is active, showing the following configuration:

- Identification:** Nom du service : DEMOGCF
- Mode:** Mode internet, pour un service ouvert sur Internet (Attention, des mesures supplémentaires peuvent être néc
- Recaptcha (Google):**
 - Clef publique : 6LdbYiATAAAAAAJyb_f1_1cCWFILt8yv5T9-XFio
 - Clef privée : 6LdbYiATAAAAAABXMsYp0WQV3pFL1JDfbF0mQJmgv
- Fichiers téléversés par l'utilisateur:**
 - Extensions autorisées : (séparées par ";")
 - Taille maximale du dossier : 50 Mb
- Dossier public:** Répertoire racine des répertoires partagés du service :
- Alertes:** Envoyer les alertes aux adresses emails suivantes (séparées par ";") :
- Affinité du processus:** Affinité du processus :

Buttons: Enregistrer, Annuler

Mise en œuvre de l'Annuaire Sage FRP 1000 Entreprise

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.

Politique d'authentification <P1>

Nom de la politique : P1

Authentification

Composition du mot de passe

Le mot de passe doit être complexe :

Taille minimale du mot de passe : 8

Nombre de mots de passe à historiser : 3

Nombre de mots interdits : 0

Modifier

Durée de vie

Périodicité de changement de mot de passe : 60 jours

Délai minimal entre chaque changement : 8 jours

Essais

Nombre d'erreurs tolérées dans la saisie : 5

Authentification double facteur

Activer l'authentification double facteur (SMS) :

Actions des utilisateurs

Autoriser la réinitialisation de mot de passe : Confirmation pas SMS :

Autoriser l'utilisateur à s'enregistrer :

Demander la confirmation des inf. de contact : Gestion des inf. de contact

Ok Annuler

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.

Politique de contrôle d'accès <PA1>

Nom de la politique : PA1

Contrôle d'accès

Accès simultanés

Les accès simultanés sont interdits :

Lecture seule

Accès en lecture seule :

Types de connexions autorisés

<input type="checkbox"/> Desktop	<input type="checkbox"/> Dashboard
<input checked="" type="checkbox"/> WebTop	<input type="checkbox"/> Mobile
<input type="checkbox"/> Service	<input type="checkbox"/> SOAP
<input type="checkbox"/> Automate	<input type="checkbox"/> SDATA
<input type="checkbox"/> Outlook	
<input type="checkbox"/> Excel	

Horaires autorisés

Nombre d'heures autorisées :

Détection et blocage des tentatives d'intrusion

Nb de tentatives infructueuses :

Plage de calcul (en minutes) :

Durée de blocage (en minutes) :

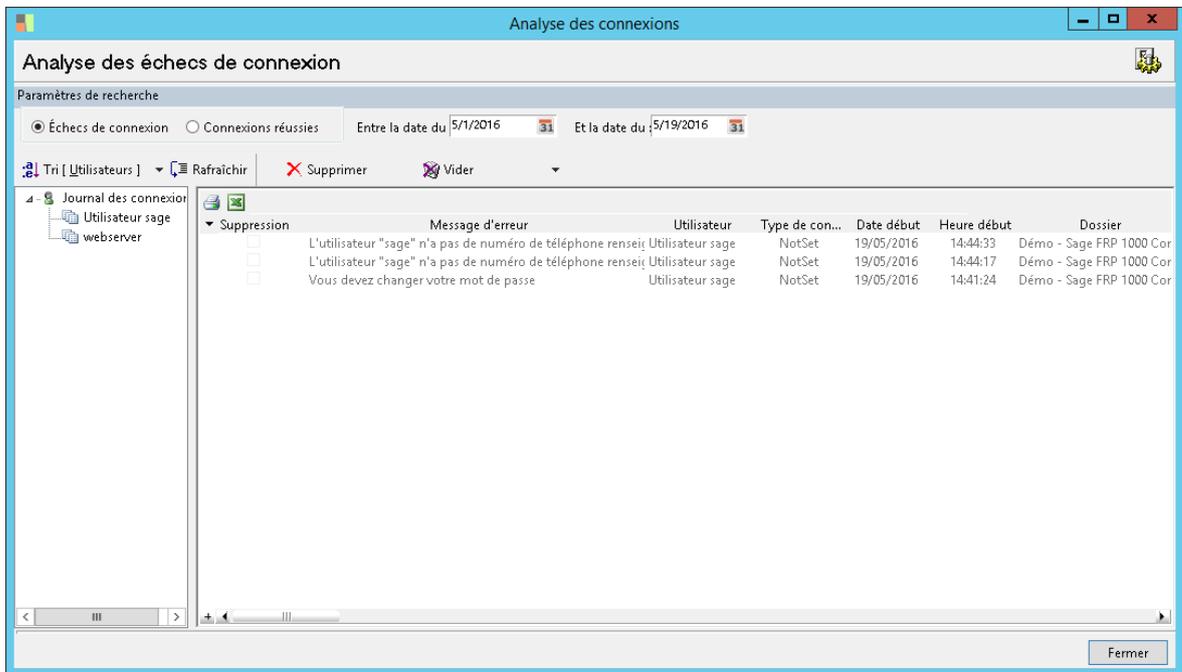
Contacter l'administrateur :

Si n tentatives de connexion infructueuses sur une plage de calcul m sont détectées, la machine (adresse Mac + Adresse IP) est bloquée pour la durée définie.
Pour débloquer une machine avant le terme de la durée de blocage, il faut supprimer les entrées correspondant aux échecs de connexion dans le journal

Important! 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.

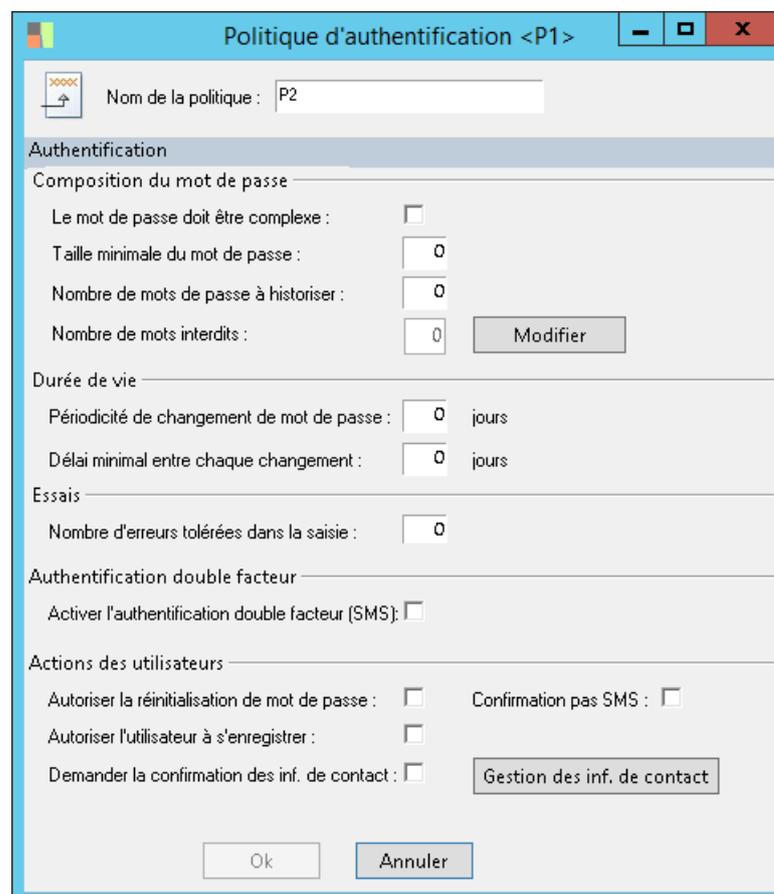
Note: En cas d'erreur d'authentification des utilisateurs, vous pouvez consulter le journal des échecs de connexion.



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

Politique de contrôle d'accès <PA1>

Nom de la politique : PA2

Contrôle d'accès

Accès simultanés

Les accès simultanés sont interdits :

Lecture seule

Accès en lecture seule :

Types de connexions autorisées

Desktop Dashboard
 WebTop Mobile
 Service SOAP
 Automate SDATA
 Outlook
 Excel

Horaires autorisés

Nombre d'heures autorisées : 168

Détection et blocage des tentatives d'intrusion

Nb de tentatives infructueuses : 0
Plage de calcul (en minutes) : 0
Durée de blocage (en minutes) : 0
Contacter l'administrateur :

Si n tentatives de connexion infructueuses sur une plage de calcul m sont détectées, la machine (adresse Mac + Adresse IP) est bloquée pour la durée définie.
Pour débloquer une machine avant le terme de la durée de blocage, il faut supprimer les entrées correspondant aux échecs de connexion dans le journal

Cette politique autorise les accès services.

Associez ces politiques aux utilisateurs de service :

Annuaire <Annuaire d'entreprise>

Nom : Sage1000 Actif Par défaut

Libellé : Annuaire d'entreprise

Politique de contrôle d'accès : PA1 (peut être redéfinie pour chaque acteur)

Politique d'authentification : P1 (peut être redéfinie pour chaque acteur)

Acteurs

Liste des entités actrices de l'annuaire

Nom	Libellé	Politique d'authentification	Politique de contrôle d'a...
admin	Administrateur		
sage	Utilisateur sage		
webserver	webserver	P2	PA2

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.

Annuaire Azure Directory

Créer un annuaire AZD (Ancien portail) :

NOM	ÉTAT	RÔLE	ABONNEMENT	RÉGION DE CENTRE DE D...	PAYS OU RÉGION
sagesyfreazad	✓ Actif	Administrateur général	Partagé par l'ensemble des...	Europe, États-Unis	France

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 est le domaine de l'Application dans cet exemple), notez l'url de réponse :

propriétés

NOM Sage FRP 1000 ?

URL DE CONNEXION <https://www.syfrecorp.com/demogcf/server/portal.l1000> ?

ID CLIENT 4594e274-0ab7-4e38-b1d3-f241acd83a05 ?

AFFECTATION DE L'UTILISATEUR REQUISE POUR ACCÉDER À L'APPLICATION OUI NON ?

clés ?

1 année 25/05/2016 25/05/2017 *****
Sélectionn... VALIDE DEPUIS EXPIRE LE LA VALEUR DE LA CLÉ S'AFFICHERA APRÈS SON ENREGISTREMENT

authentification unique

URI ID D'APPLICATION <https://www.syfrecorp.com> ✓ ?

URL DE RÉPONSE https://www.syfrecorp.com/oauth2_success.l1000 ?
(SAISISSEZ UNE URL DE RÉPONSE)

Notez la clé secrète affichée lors de la validation

Important! C'est le seul moment où cette clé est affichée.

Annuaire Sage FRP 1000

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

Annuaire <AzureAD>

Nom : AzureAD Actif Par défaut

Libellé : AzureAD

Politique de contrôle d'accès : PA1 (peut être redéfinie pour chaque acteur)

Acteurs Paramètres OAuth2

Fournisseur : Azure AD

Paramètres client

Client Id : 4594e274-0ab7-4e38-b1d3-f241acd83a05 **1**

Client Secret : gkPdeV8z3LVLNWbXx2sKovzLfdKtnWtFrTbUTnk:

Voir les paramètres avancés

Paramètres annuaire

Scope : user_impersonation

AccessTokenUrl : https://login.microsoftonline.com/08fc35dc-c87 **2.a**

EndPoint : https://login.microsoftonline.com/08fc35dc-c87 **2.b**

UserInfoUrl : https://login.microsoftonline.com/08fc35dc-c87

UserIdPath : unique_name

Client email : email

Client first name : given_name

Client last name : family_name

Ressource : https://graph.windows.net/

Avancé

Url de redirection : (adresse du service 1000 non publique)

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, ces informations sont accessible sur :



✕

Points de terminaison d'app

Si vous développez une application qui s'intègre à Microsoft Azure AD, mettez votre code à jour afin d'utiliser ces points de terminaison pour l'authentification unique et l'accès aux annuaires.

DOCUMENT DE MÉTADONNÉES DE FÉDÉRATION ?
`https://login.microsoftonline.com/08fc35dc-c877-43ed-af13-cf00dcb5c048`

POINT DE TERMINAISON DE CONNEXION WS-FEDERATION ?
`https://login.microsoftonline.com/08fc35dc-c877-43ed-af13-cf00dcb5c048`

POINT DE TERMINAISON DE CONNEXION SAML-P ?
`https://login.microsoftonline.com/08fc35dc-c877-43ed-af13-cf00dcb5c048`

POINT DE TERMINAISON DE DÉCONNEXION SAML-P ?
`https://login.microsoftonline.com/08fc35dc-c877-43ed-af13-cf00dcb5c048`

POINT DE TERMINAISON DE L'API MICROSOFT AZURE AD GRAPH ?
`https://graph.windows.net/08fc35dc-c877-43ed-af13-cf00dcb5c048`

POINT DE TERMINAISON DE JETON OAUTH 2.0 ? 2.a
`https://login.microsoftonline.com/08fc35dc-c877-43ed-af13-cf00dcb5c048`

POINT DE TERMINAISON D'AUTORISATION OAUTH 2.0 ? 2.b
`https://login.microsoftonline.com/08fc35dc-c877-43ed-af13-cf00dcb5c048`

✓

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

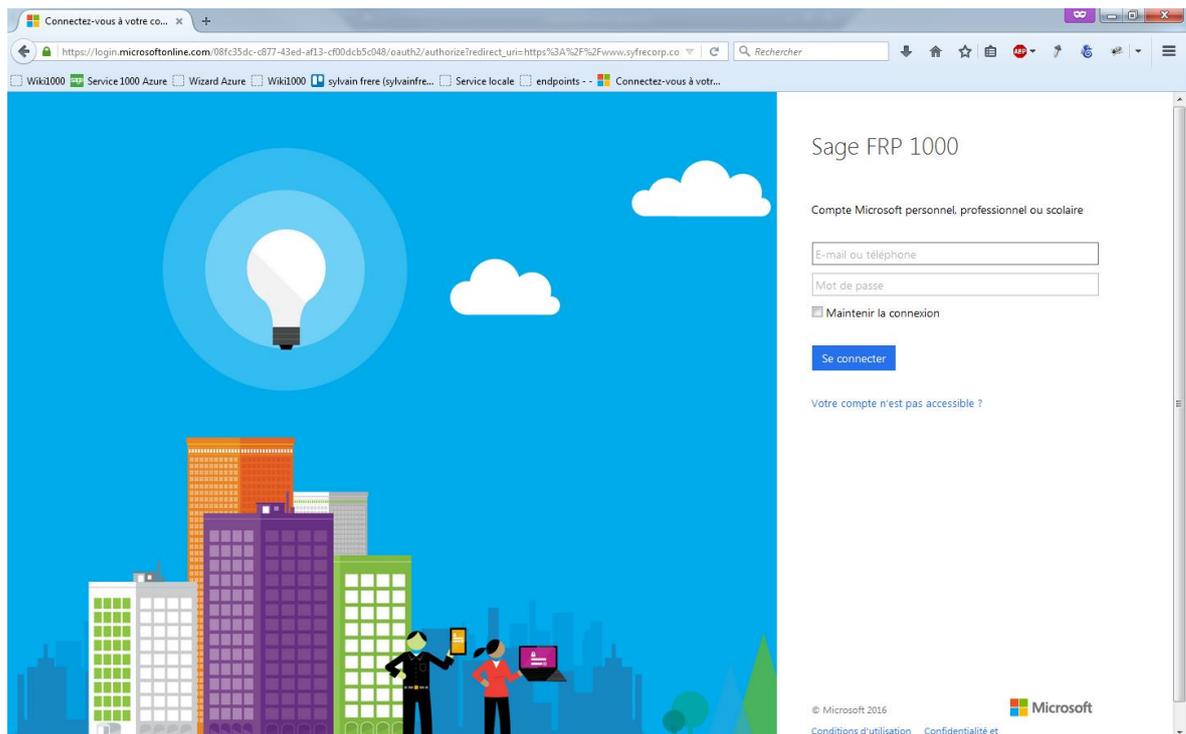
Enregistrement des utilisateurs.

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.

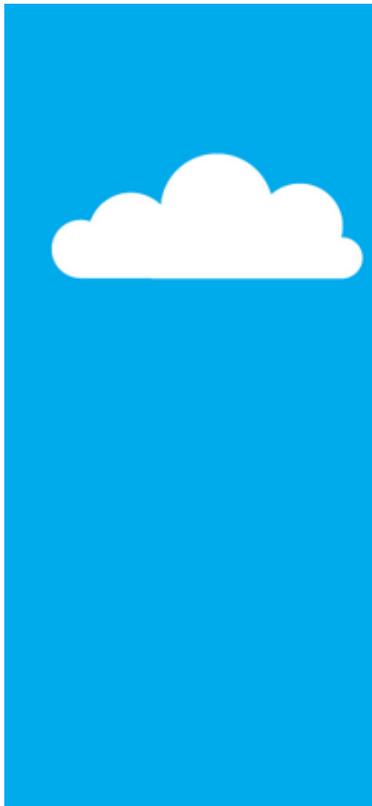


Si l'utilisateur n'est pas connecté sur azure une fenêtre de connexion apparaît :



Cette fenêtre est géré par Azure

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



Sage FRP 1000

Compte Microsoft personnel, professionnel ou scolaire

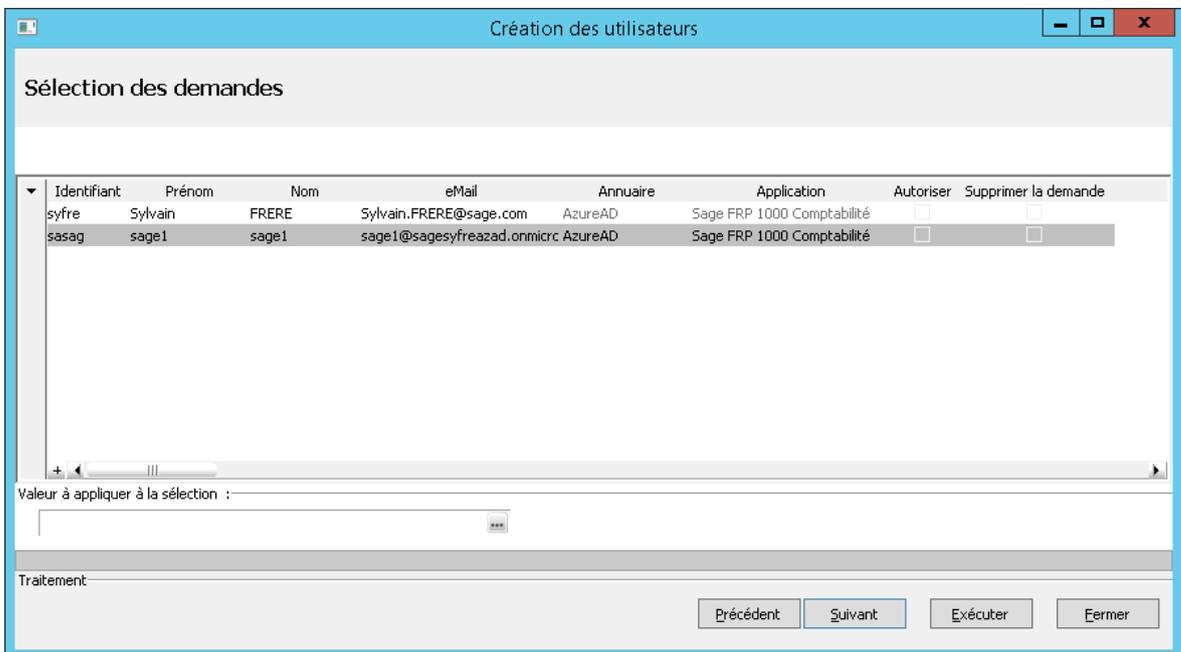
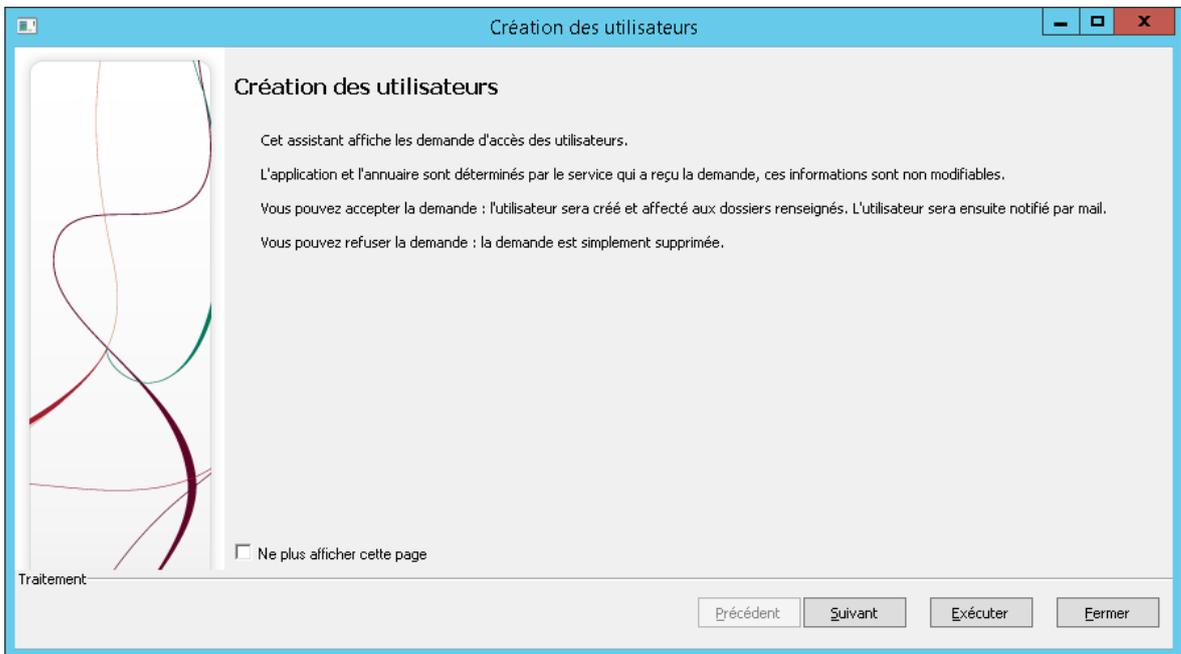
Maintenir la connexion

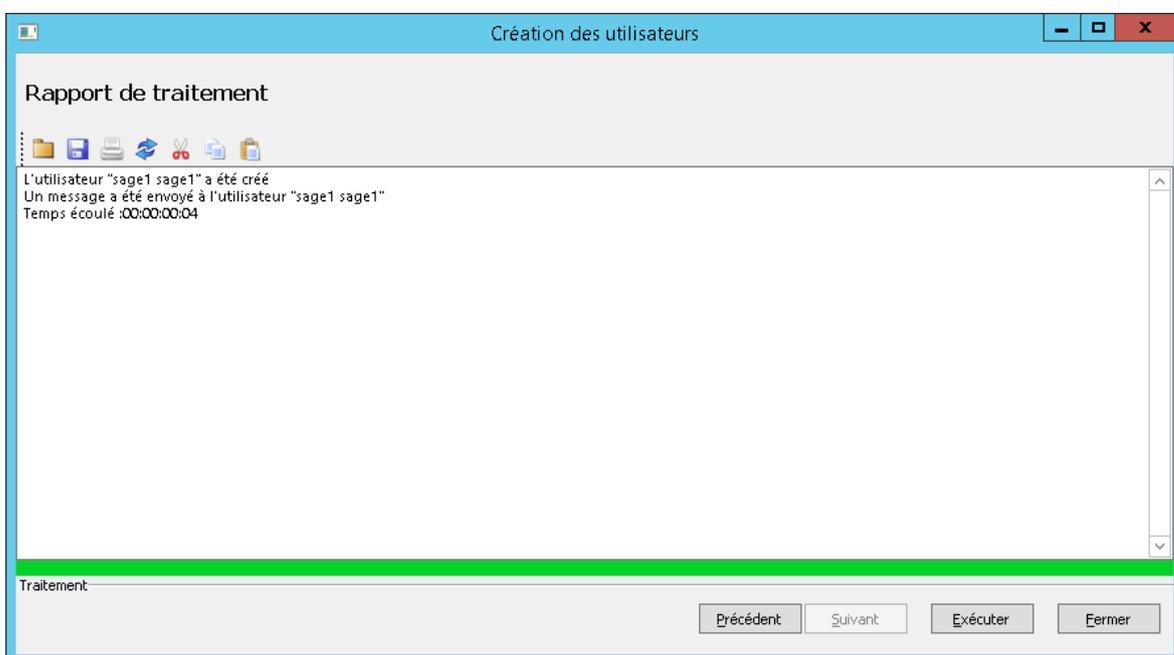
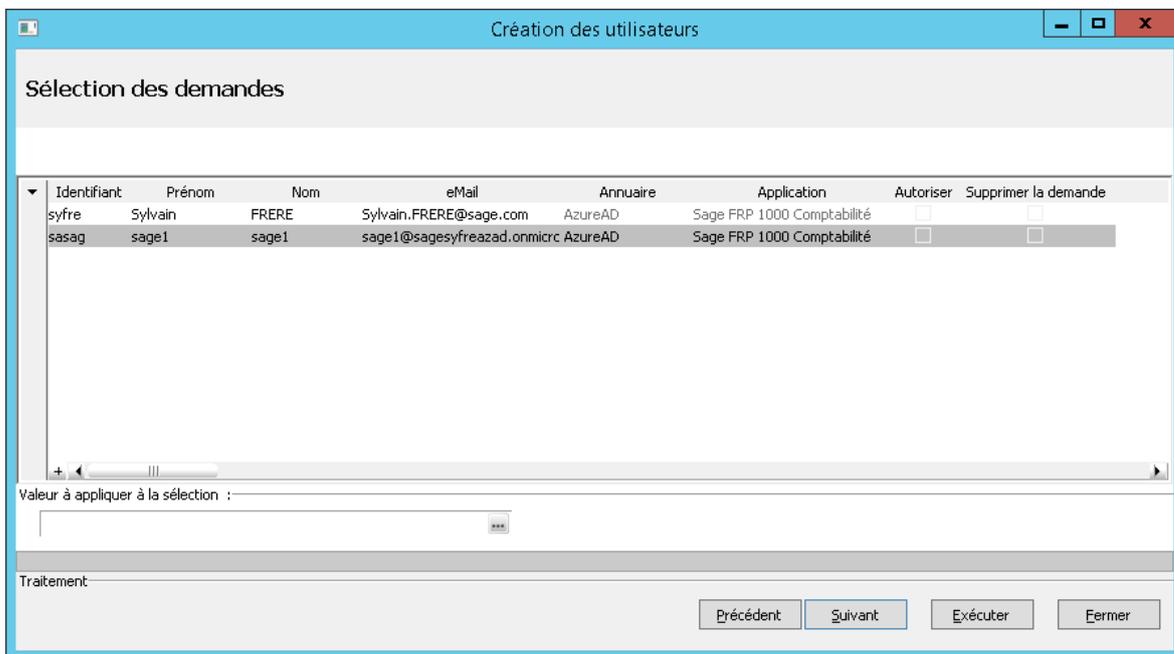
Se connecter

[Votre compte n'est pas accessible ?](#)

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 utiliser « 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.

Sécurité

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.

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 :

- Installez le certificat dans le magasin de Windows (sur chaque nœud)
- Dans la Console des services sélectionnez le certificat

The screenshot shows the configuration interface for Sage FRP 1000 services. The 'HTTP' tab is selected in the top navigation bar. The 'Général' section has 'Démarrer le serveur http intégré' checked with a port of 443. The 'Paramètres SSL' section has 'Paramétrer le serveur en https' checked and 'Utiliser le magasin Windows' selected. The 'Certificats' section shows a dropdown for 'Sujet : www.syfrecorp.com, émetteur : StartCom Cla', a text box for 'Émetteur du certificat : C=IL, O=StartCom Ltd., OU=Secure Digital Certificate Si', a text box for 'Numéro de série : 06A44AEE793EA7', and a text box for 'Fichier cert. autorité interm.' with a browse button. On the right side, there are vertical labels for 'Magasin Windows' and 'Fichiers certificats'.

Configuration DNS

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

Record Set Name X Any Type Aliases Only Weighted

Only

Displaying 1 to 3 out of 3 Record Sets

<input type="checkbox"/>	Name	Type	Value	Evaluate
<input type="checkbox"/>	syfrecorp.com.	NS	ns-979.awsdns-58.net. ns-1253.awsdns-28.org. ns-1558.awsdns-02.co.uk. ns-322.awsdns-40.com.	-
<input type="checkbox"/>	syfrecorp.com.	SOA	ns-979.awsdns-58.net. awsdns-hostmaster.amazon.	-
<input type="checkbox"/>	*.syfrecorp.com.	CNAME	sagefrp710.cloudapp.net	-

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

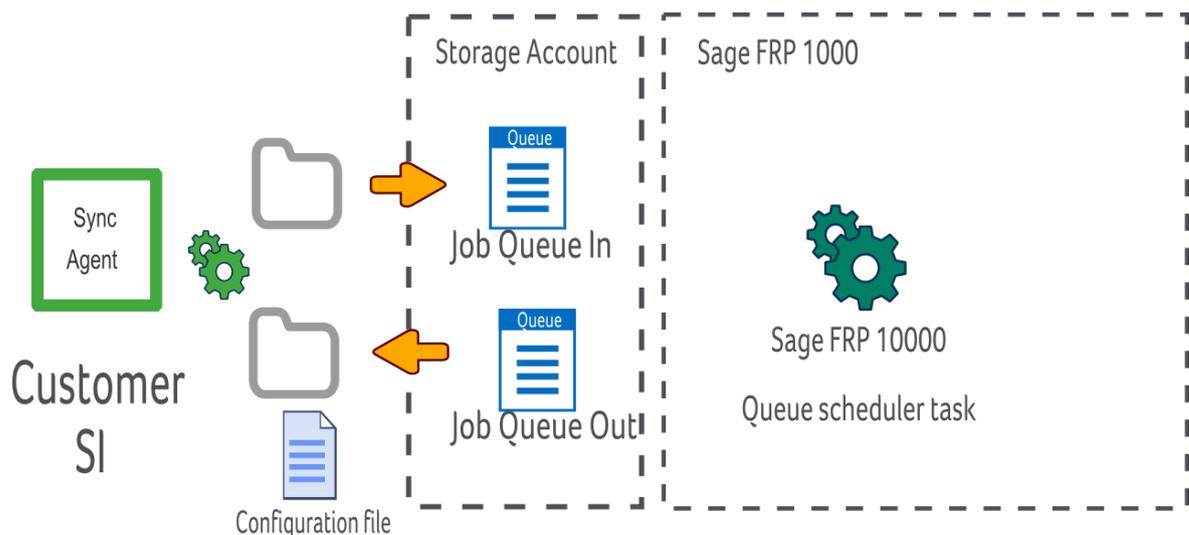
Mise en place au niveau de Microsoft Application Gateway

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

Intégration avec le Système d'information

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.

Important! N'utilisez pas des files d'attente gérées par la base de données, utilisez des files d'attente Azure.

Paramétrage des tâches d'exportation.

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

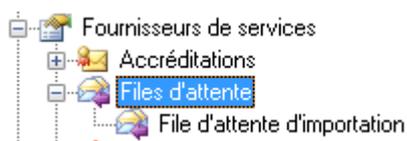
- Configurer les files d'attente
- Configurer un compte de service et obtenir un jeton d'authentification
- Installer et configurer le Sync Agent
- Paramétrer les automates Sage FRP 1000

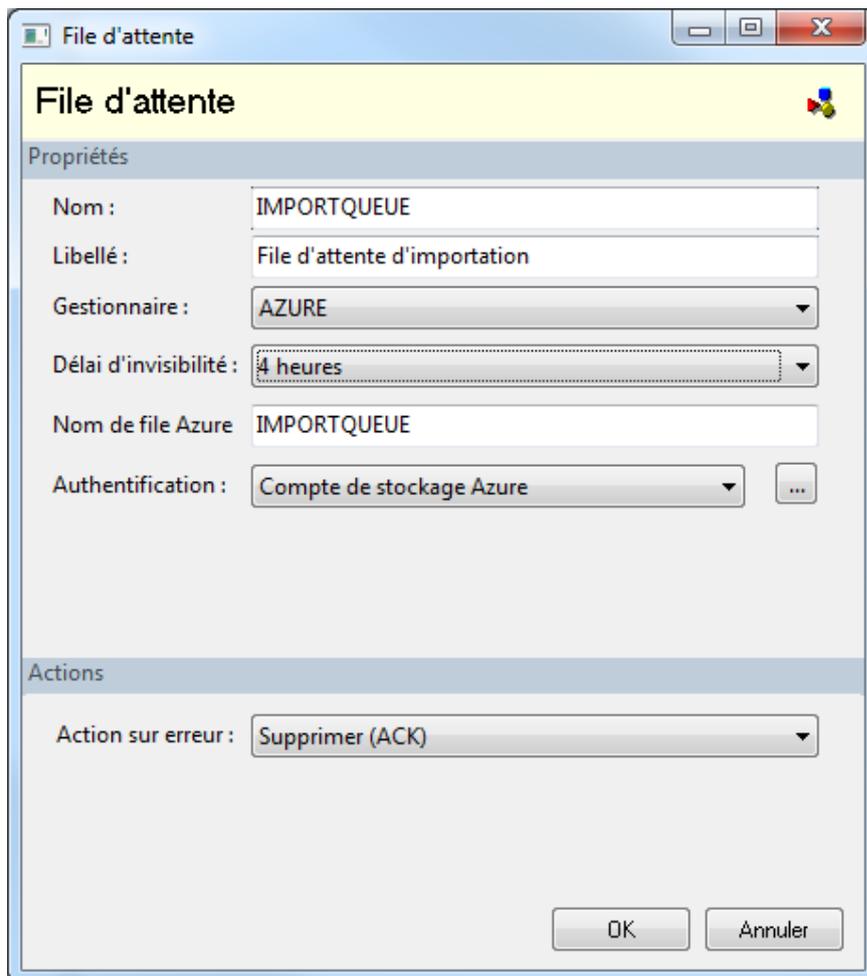
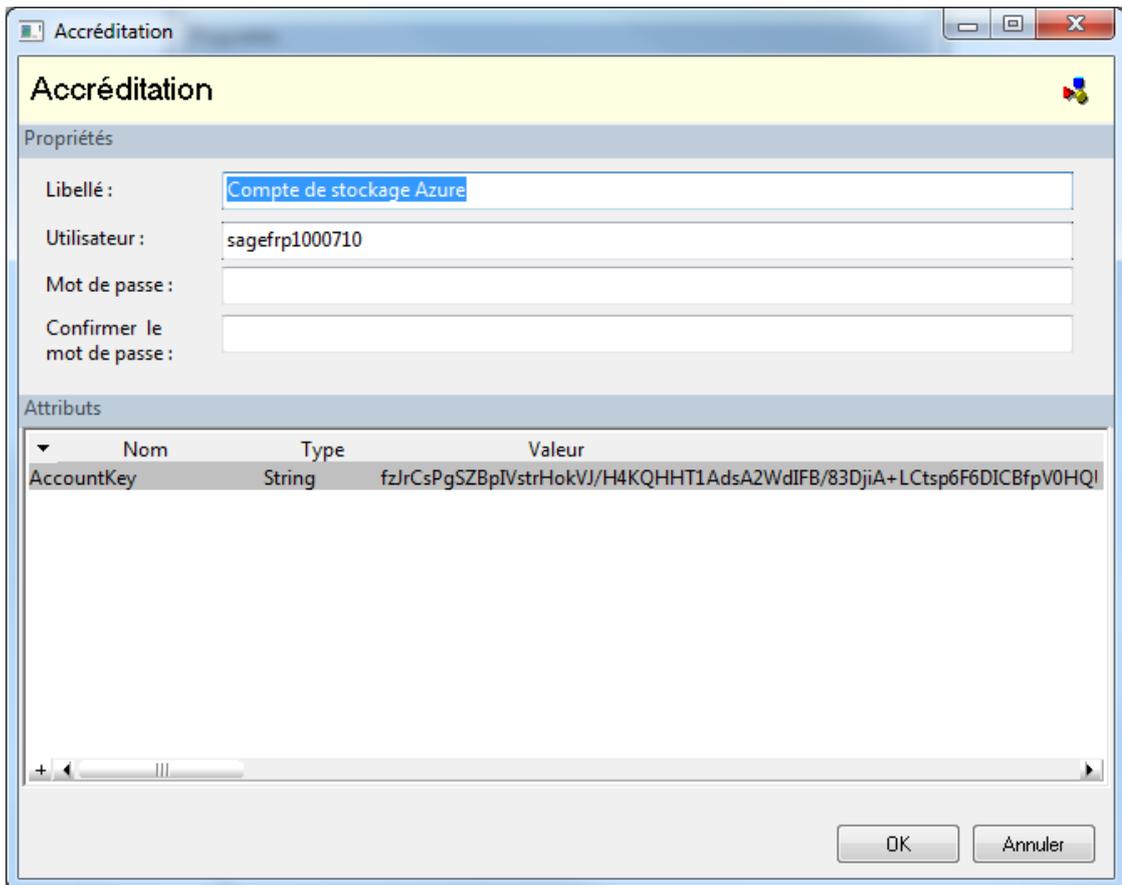
Configuration des files d'attente

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

The screenshot displays the Azure portal interface for a storage account named 'sagefrp1000710'. The 'Essentials' tab is active, and the 'Keys' icon is highlighted with a red box. The 'Manage keys' panel on the right shows the 'STORAGE ACCOUNT NAME' (sagefrp1000710) and 'PRIMARY ACCESS KEY' (fzJrCsPgSZBpIVstrHokVJ/H4KQHHT1AdsA) highlighted with red boxes. Other keys and connection strings are also visible.

Configurez ensuite une file d'attente. Dans la console d'administration :





Configuration d'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.

Jeton d'authentification

Libellé : SyncAgent

Dossier : Démo - Sage FRP 1000 Comptabilité

Base de données : dbDemoGCF710

Société :

Application : Sage FRP 1000 Comptabilité

Utilisateur : syncagentaccount

Expire : 30/12/1899 02:00:00 Désactivé

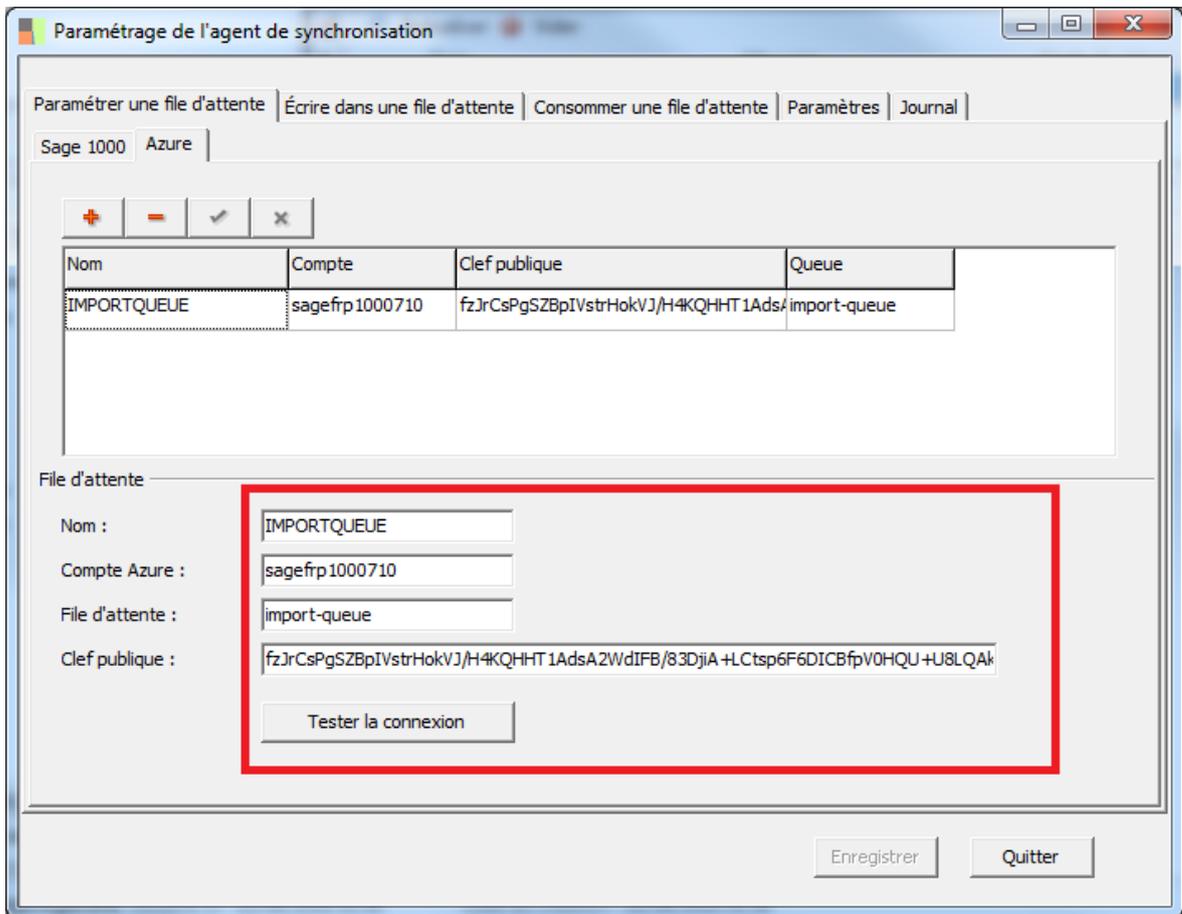
160000001500900130ED1800F700000080F61C9842D7E049670CDE72387AD42EE6
1E7777C0D8AC1C679B59FE11BF0D1D6EBC8CC874C38466DF7D742E1AA9F81C
8EDF33A285840FFCD83364B7633B094A511526382C9A7DC5C797ED4DE61273C
1D0D36BF7D4840EC6E383EB0B40ED1C857B8D7A8FF32580C1D644224C1FFB4B
B4B02AFB374C4C4F4288A36D3DB38841ECEBF6A6EAC1AC14025A0EC43473EB
8E23CA3D16EF073BAF2CCD35BBFC8E03FAD93748F403CD6F0BA5D59FFDE8E3
A32D5A27B694133859A659ACF019F93665B034E5404409DE09D8F822535E22419
5A5D008FFC8F53A1B01EE99BB3B134254F931B2327246C134060C452A4D67440

Copier le jeton OK Annuler

Installation et configuration de Sage Sync Agent.

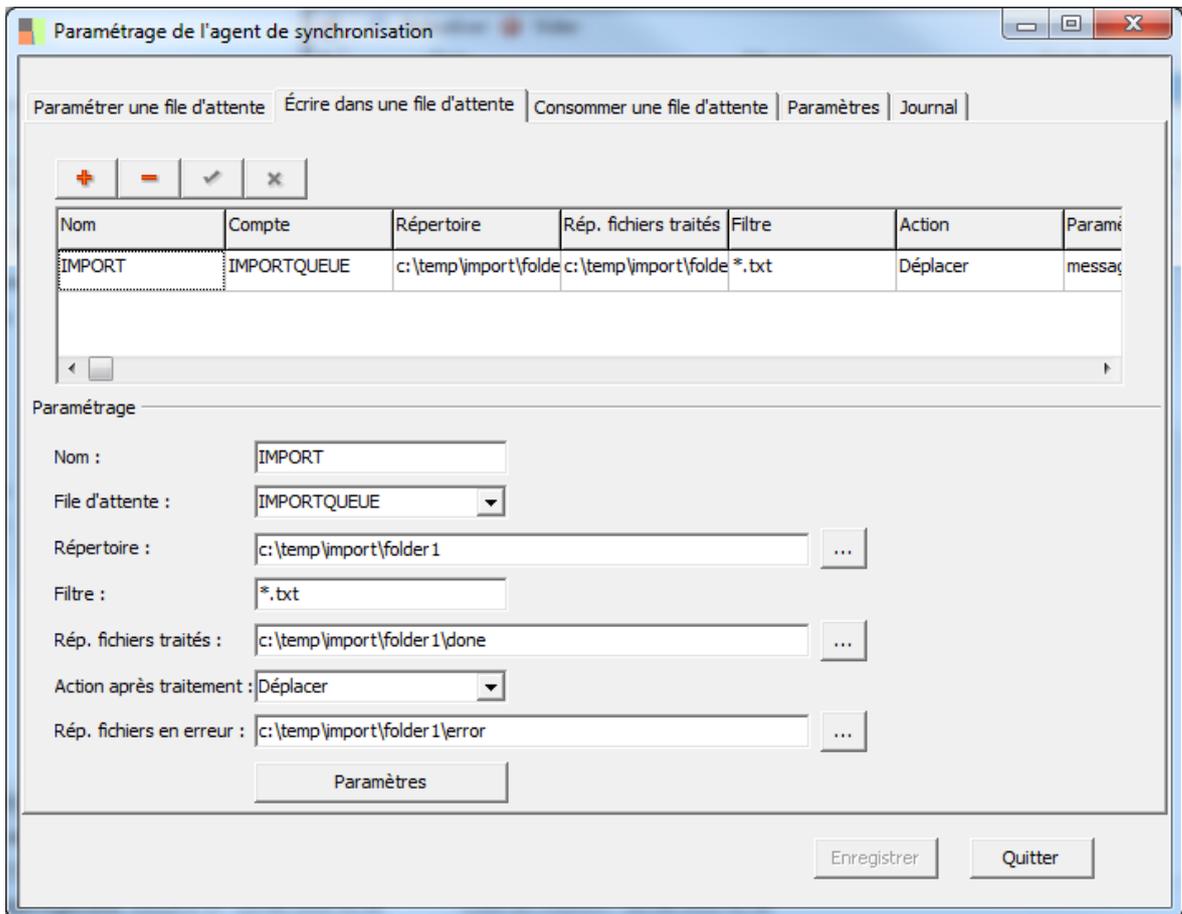
Le « Sync Agent » est un service Windows s'installant sur un poste du système du réseau du Client et permettant de faire le lien entre des fichiers déposés sur le système de fichiers du Client et les files d'attente Azure.

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



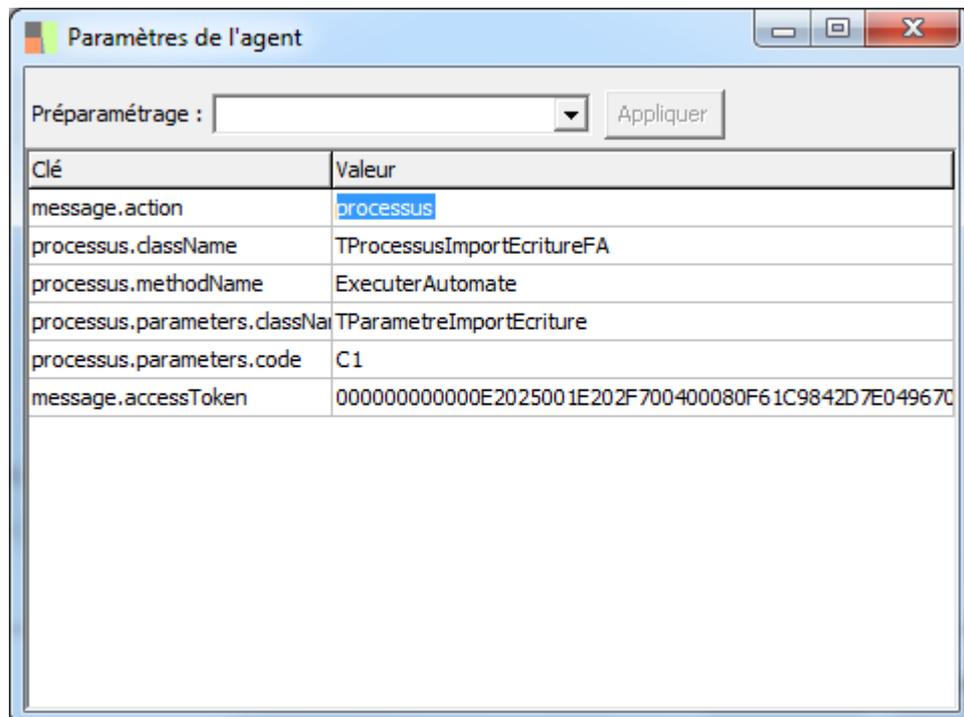
- Compte Azure : Le nom du compte de stockage Azure
- File d'attente : Le nom de la file d'attente Azure
- Clé publique : La clé publique du compte de stockage.

Configurez ensuite un répertoire d'envoi de message :



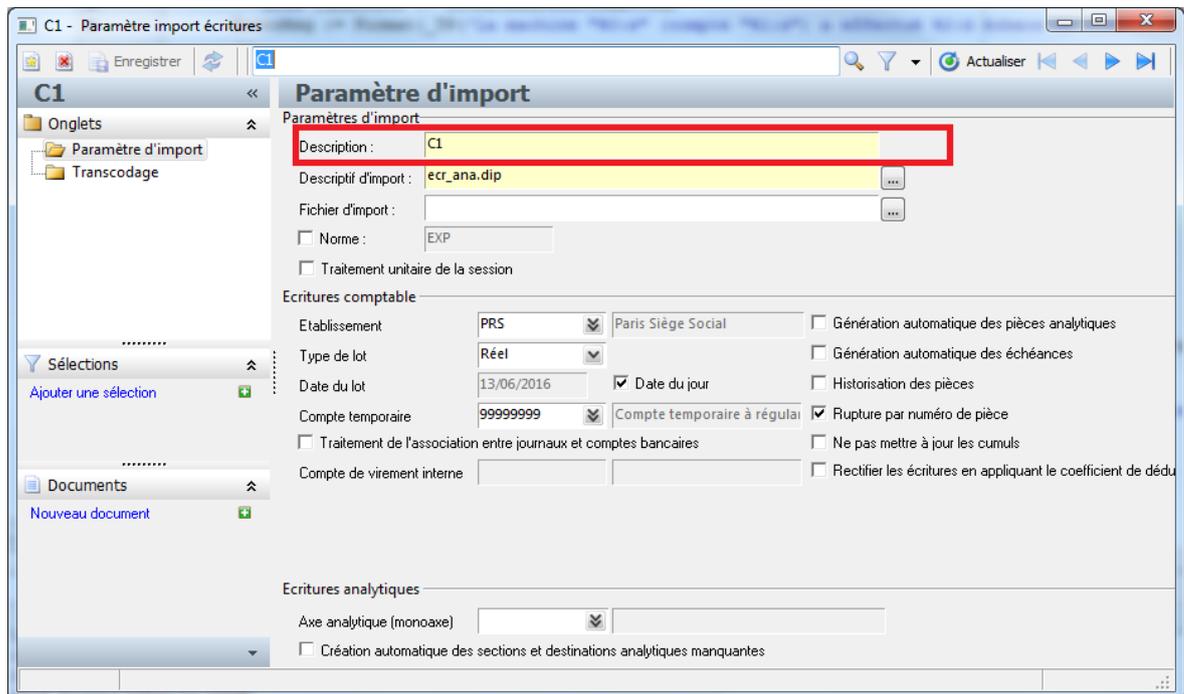
- File d'attente : Le nom de la file d'attente précédemment configurée.

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.

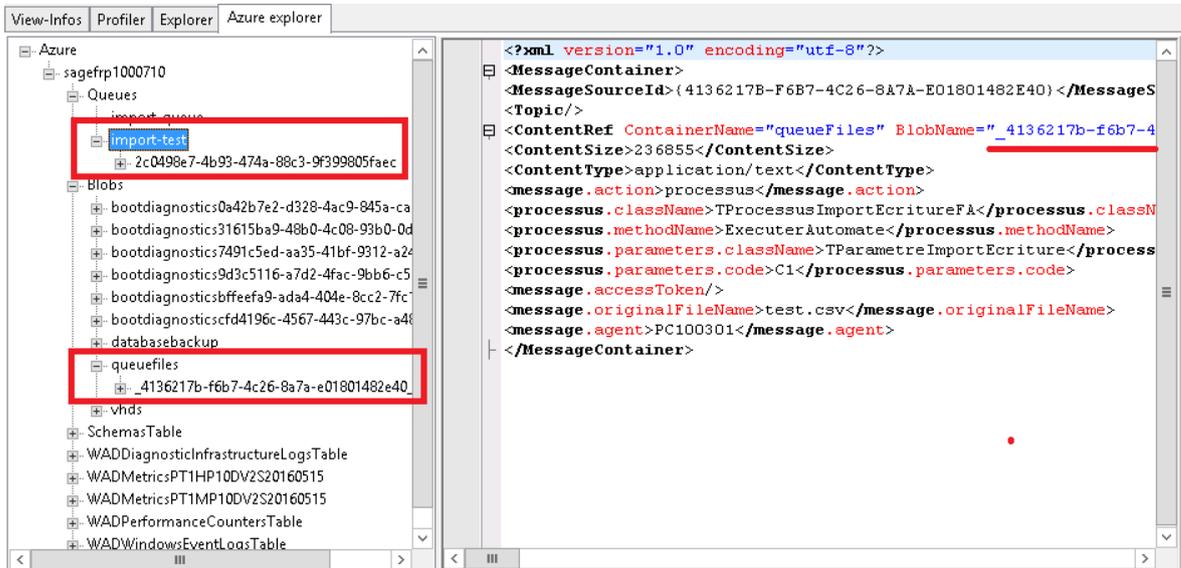
Tester la communication

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 :

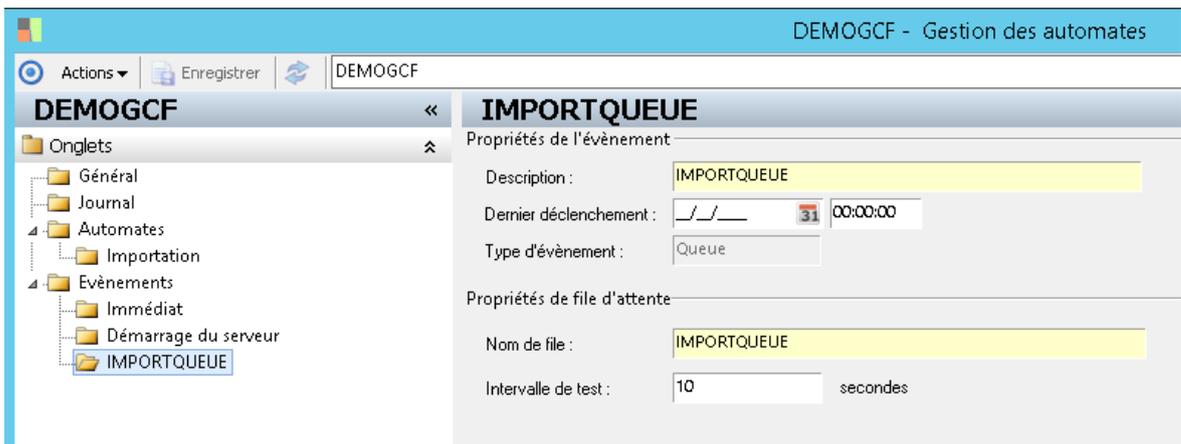
- Paramétrer un nom de file d'attente Azure de test
- Copier un fichier dans le répertoire surveillé
- Vérifier que le fichier et le message ont bien été créés.

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 :

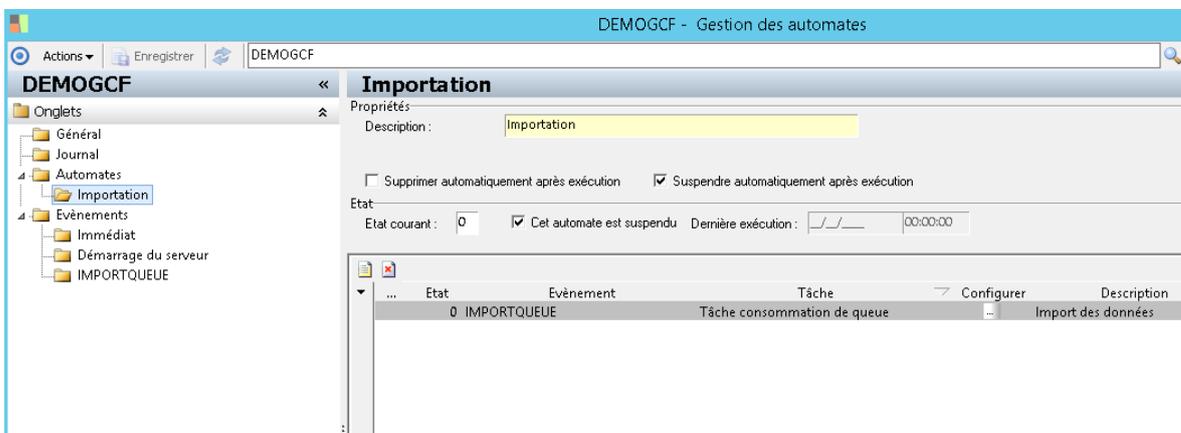


Paramétrage des automates

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



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



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

Journal
Journal des messages d'exécution

Date	Message	Code de retour	Traitement \ Tâche réalisée	Opérateur	Node ID
13/06/2016 07:50:00	OK	0	Import des données		sagefrp710n2.80.demogcf

Tâche "consommation de queue" déclenchée
Exécution du processus "TProcessusImportEcritureFA.ExecuterAutomate"

Paramètres du message:

```
message.action="processus"  
processus.className="TProcessusImportEcritureFA"  
processus.methodName="ExecuterAutomate"  
processus.parameters.className="TParametreImportEcriture"  
processus.parameters.code="C1"  
message.accessToken="000000000000E2025001E202F700400080F61C9842D7E049670CDE72387AD42EE61E7777C0D8AC1C679B59FE11BF0D1D58E56793DEA82F79F5A247817567CC4BD61"  
message.originalFileName="test import direct.txt"  
message.agent="PC100301"  
message.binary.datalength:"390"
```

Import:C1

** Importation de fichier **

Fichier descripteur : ecr_ana.dip
Dossier : Démo - Sage FRP 1000 Comptabilité
Base de données : mssql://sagefrp1000.database.windows.net/dbDemoGCF710?prefix="dbo."
Gestion des partages:
Utilisateur : syncagentaccount
Mode : Insertion.

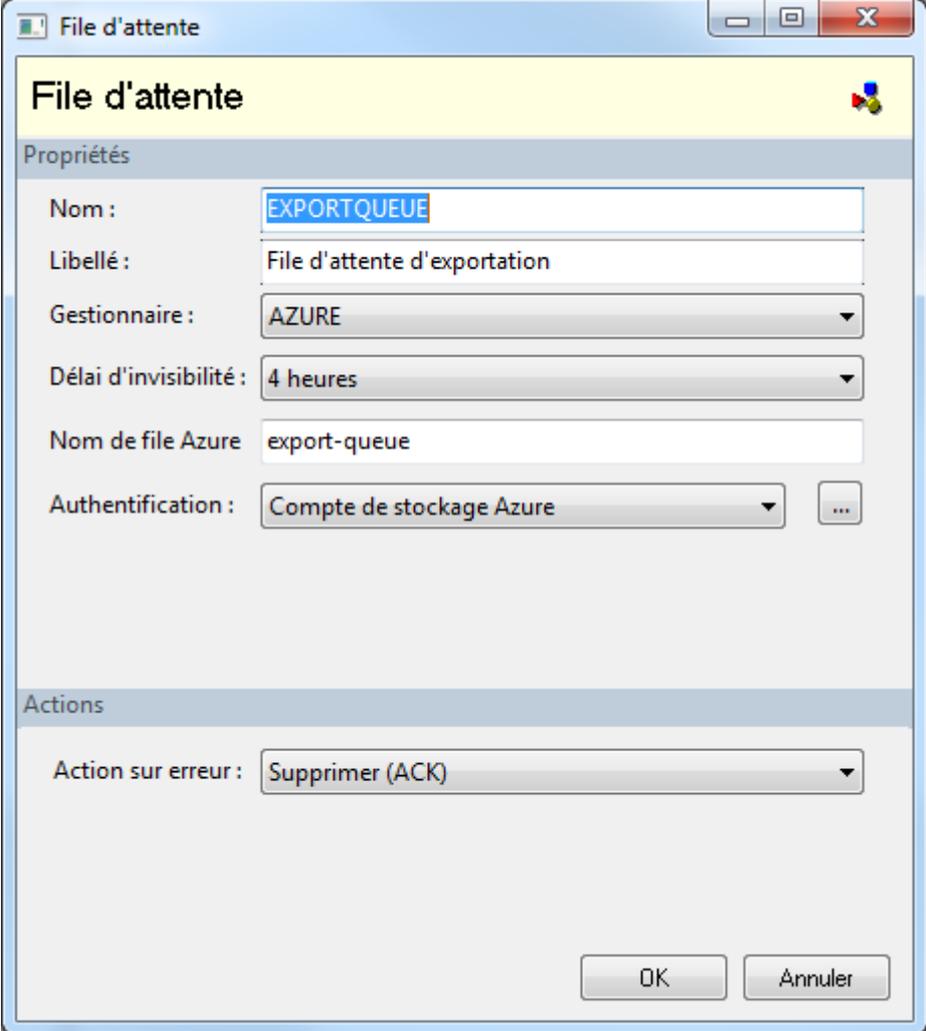
Paramétrage des tâches d'exportation.

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.

Création d'une file d'attente d'exportation.

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



The image shows a Windows-style dialog box titled "File d'attente". It is divided into two main sections: "Propriétés" and "Actions".

Propriétés

- Nom :** A text input field containing "EXPORTQUEUE".
- Libellé :** A text input field containing "File d'attente d'exportation".
- Gestionnaire :** A dropdown menu with "AZURE" selected.
- Délai d'invisibilité :** A dropdown menu with "4 heures" selected.
- Nom de file Azure :** A text input field containing "export-queue".
- Authentification :** A dropdown menu with "Compte de stockage Azure" selected, and a small "..." button to its right.

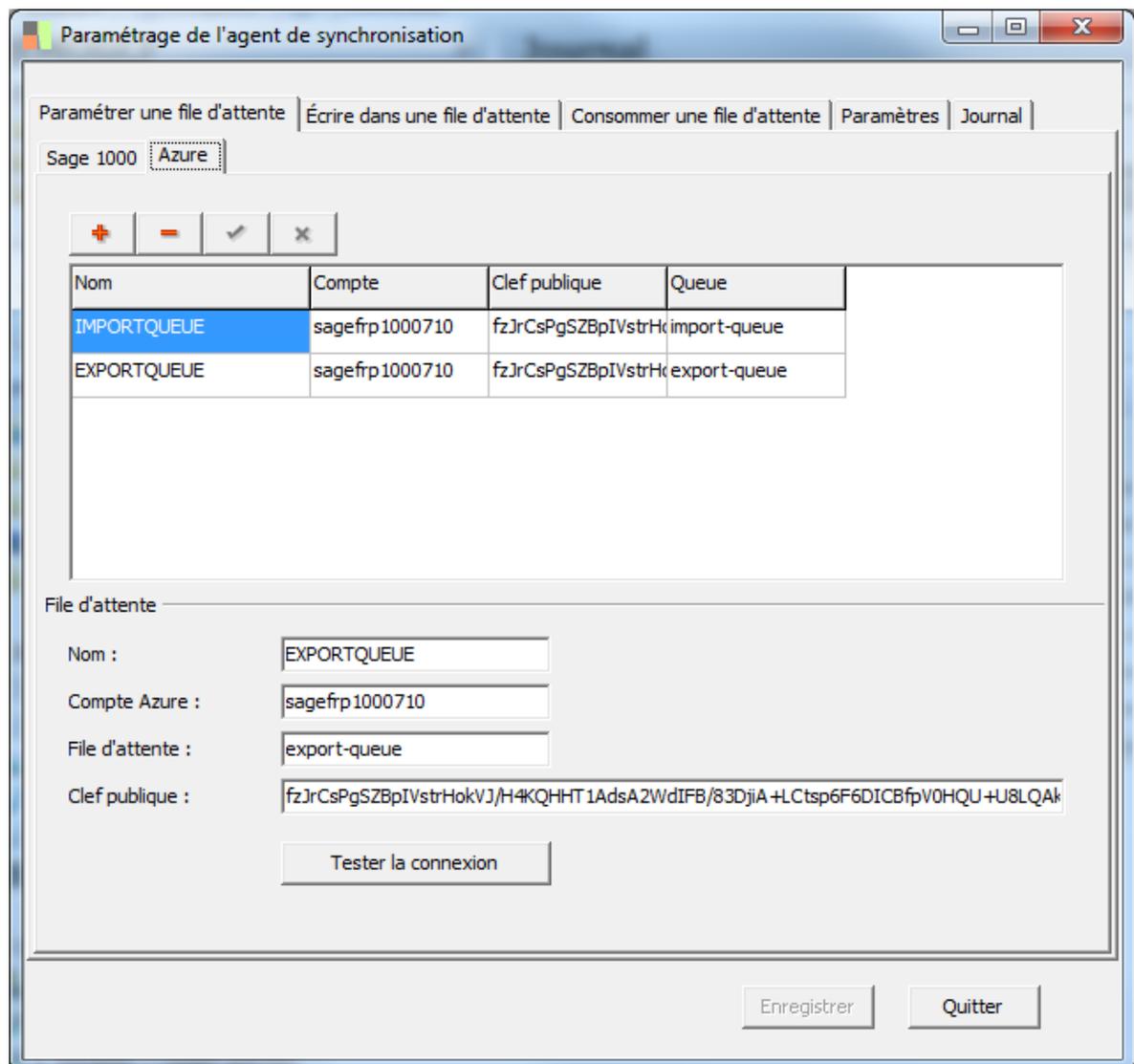
Actions

- Action sur erreur :** A dropdown menu with "Supprimer (ACK)" selected.

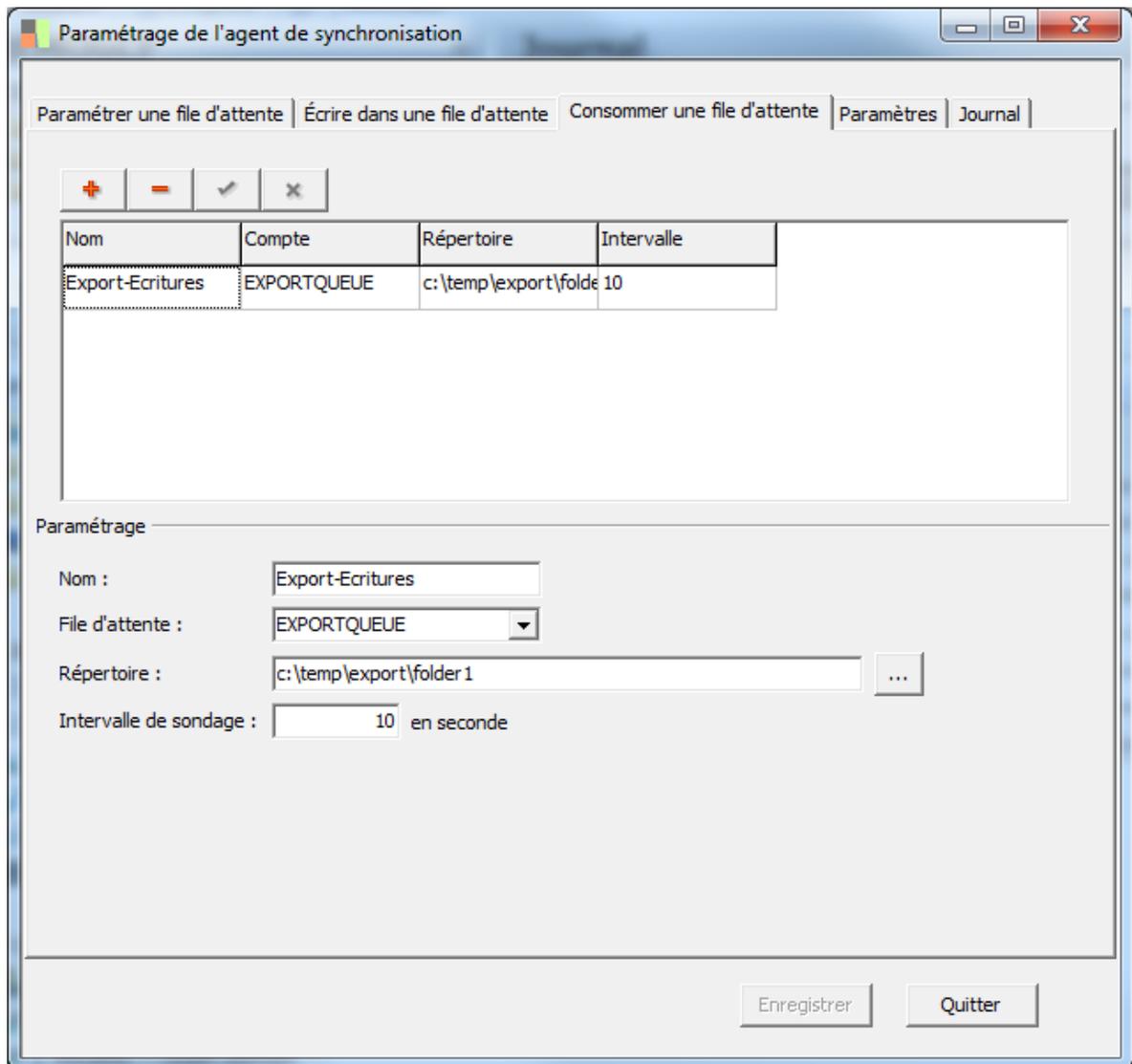
At the bottom right of the dialog, there are two buttons: "OK" and "Annuler".

Configuration du Sync Agent.

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

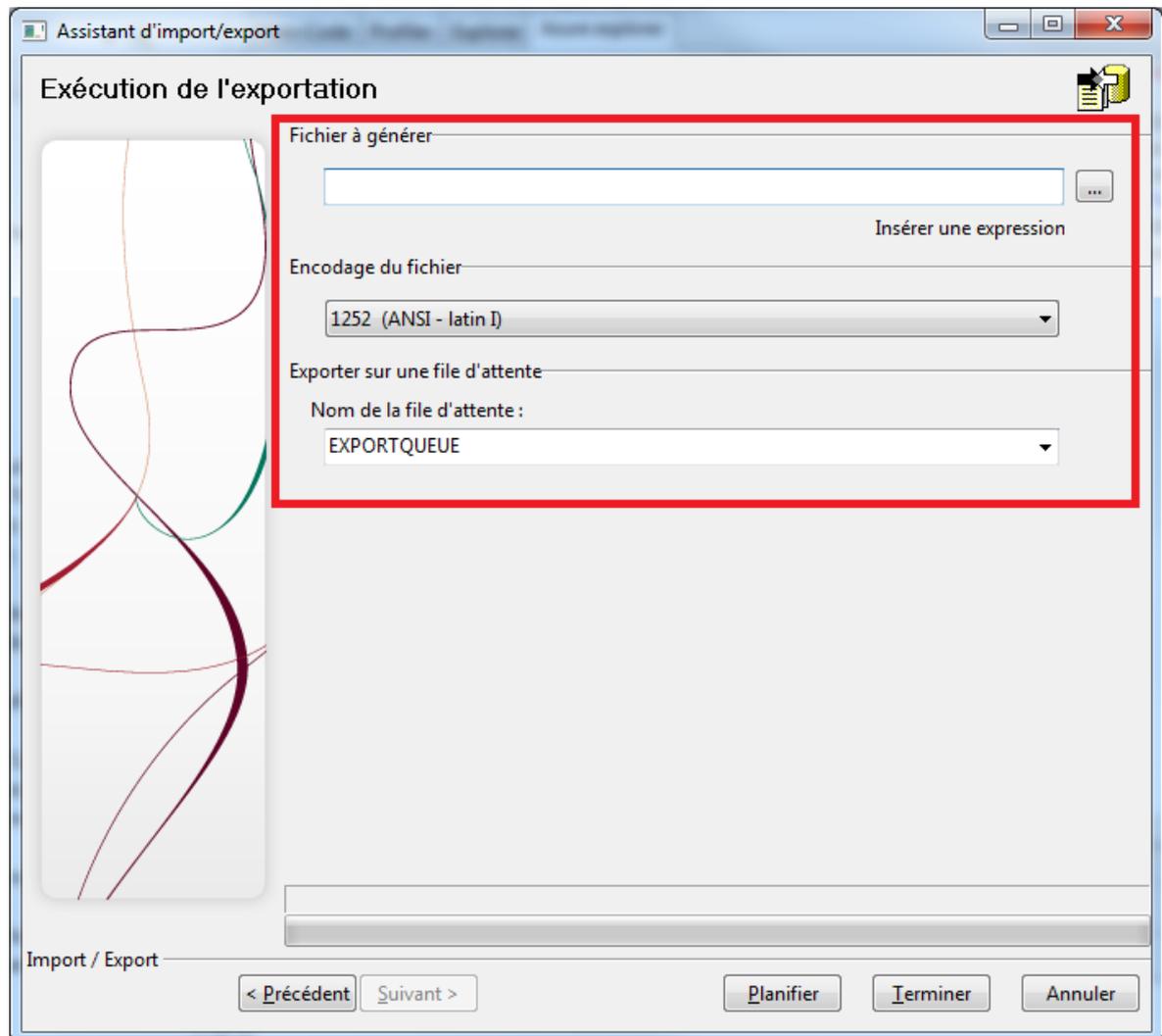


Et ajouter un répertoire pour recevoir les fichiers de cette file :



Création d'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.



10 rue Fructidor
75834 Paris Cedex 17

www.sage.com

© 2016 The Sage Group plc or its licensors. All rights reserved. Sage, Sage logos, and Sage product and service names mentioned herein are the trademarks of The Sage Group plc or its licensors. All other trademarks are the property of their respective owners.