Sage FRP 1000

Déploiement SAAS Azure

Sage

Avril 2015

Table des matières

[1.0 Introduction 4](#_Toc417022224)

[1.1 Périmètres du projet 4](#_Toc417022225)

[2.0 Architecture 5](#_Toc417022226)

[2.1.1 Architecture Single tenant 5](#_Toc417022227)

[2.2 Vue réseau 5](#_Toc417022228)

[2.3 Ressources 6](#_Toc417022229)

[2.3.1 Ressources par tenant 6](#_Toc417022230)

[2.3.2 Eléments de configuration 7](#_Toc417022231)

[2.4 Dimensionnement 7](#_Toc417022232)

[3.0 Interfaces et notifications 8](#_Toc417022233)

[3.1 Interface données 8](#_Toc417022234)

[3.2 Notifications utilisateurs 8](#_Toc417022235)

[4.0 Configuration / Sécurité 9](#_Toc417022236)

[4.1 Eléments de configuration 9](#_Toc417022237)

[4.1.1 Mot de passe du compte OS de la machine virtuelle 9](#_Toc417022238)

[4.1.2 Certificats SSL du point d’accès https 9](#_Toc417022239)

[4.1.3 Mot de passe de base de données 9](#_Toc417022240)

[4.1.4 Utilisateur démarrant le service 9](#_Toc417022241)

[4.1.5 Jetons d’authentification d’accès service 10](#_Toc417022242)

[4.2 End points 10](#_Toc417022243)

[4.2.1 Point d’accès HTTPS 10](#_Toc417022244)

[4.2.2 Point d’accès Remote desktop 10](#_Toc417022245)

[4.3 Ports ouverts en sortie 10](#_Toc417022246)

[4.3.1 SMTP 10](#_Toc417022247)

[4.3.2 HTTP 10](#_Toc417022248)

[4.4 ACLs 10](#_Toc417022249)

[4.5 Annuaires 10](#_Toc417022250)

[4.6 Localisation des éléments de sécurité 11](#_Toc417022251)

[4.7 Fichier de configuration 11](#_Toc417022252)

[4.8 Impersonnalisation des machines virtuelles 11](#_Toc417022253)

[5.0 Sauvegardes 14](#_Toc417022254)

[5.1 Point in time 14](#_Toc417022255)

[6.0 Supervision 15](#_Toc417022256)

[6.1 Evènements dans Sage FRP 1000 15](#_Toc417022257)

[6.2 Journaux 15](#_Toc417022258)

[6.3 Monitoring alertes 16](#_Toc417022259)

[6.4 Health probe 16](#_Toc417022260)

[7.0 Déploiement 17](#_Toc417022261)

[Procédure manuelle 17](#_Toc417022262)

[Création d’un nouveau tenant 17](#_Toc417022263)

[7.1 Création de l’image 17](#_Toc417022264)

[7.2 Déploiement d’un tenant 17](#_Toc417022265)

1. Introduction
	1. Périmètres du projet

Le but de ce projet est de migrer des clients Immobilisation Abel et Facet actuellement déployés avec des solutions On Premise vers une solution hébergée SAAS.

Les paramètres du projet :

* Solution Mono Application (Immobilisation)
* Solution Mono Dossier
* Solution pour un nombre réduit d’utilisateurs (2 typique)
* Hébergement Azure
* Architecture single tenant
1. Architecture
	* 1. Architecture Single tenant

La solution est basée sur une architecture « single tenant » chaque client (tenant) dispose :

* D’une machine virtuelle
* D’un service Sage FRP 1000
* D’une base de données SQL Database

Le but de l’architecture est :

* D’assurer l’isolation entre les tenants
* De diminuer les coûts d’hébergement
* D’automatiser les procédures d’administration



* 1. Vue réseau

Pour assurer l’isolation entre les tenants et pour maximiser la sécurité, on met en œuvre une architecture réseau basée sur un réseau virtuelle (VN de la solution) au sein duquel les ressources d’un tenant (virtuelle machine) sont incluses dans un sous réseau.



* L’ensemble de la solution est inclue dans un Virtual Network (10.X.0.0/16)
* Chaque tenant est inclus dans un subnet du VN (10.X.a.0/29)
* Le management est inclus dans un subnet (10.X.0.0/29)

Cette configuration permet :

* D’isoler les tenants (pas de routage entre les tenants)
* De sécurisé les données (fw sur les bases de données)
* Jusqu’à 7 IP pour un tenant
* Jusqu’à 8192 sous réseaux (29-16=13 bits ; une solution 24-16 permet 256 sous réseaux de 256 IPs)
	1. Ressources
		1. Ressources par tenant

Chaque tenant nécessite un ensemble de ressource Azure



* Un sous réseau au sein du réseau virtuel de la solution
* Une machine virtuelle
* Une base de données
* Un containeur dans un espace de stockage pour la journalisation
	+ 1. Eléments de configuration

Le service Sage FRP 1000 dédié à un tenant est hébergé sur la machine virtuelle du tenant, les éléments de configuration présents sur cette machine sont :

* Le fichier de configuration du service Sage FRP 1000 (voir plus loin, l’utilisation du serveur de configuration)
* Le certificat HTTPS / SSL correspond au domaine du tenant
	1. Dimensionnement

Pour réduire au maximum les coûts le dimensionnement suivant est envisagé :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Configuration | Users | Virtual machine | Database | DTU |
| Small  | Up to 2 | A1 ; 1 cpu 1.7 Go | S1 / S2 | 20 / 50 |
| Medium | Up to 20 | A2 ; 2 cpu 3.5 Go | S2 / S3 | 50 / 100 |

Azure SQL Server ont un quota de DTU ce qui limite le nombre de tenants par serveur (2000 dtu)

1. Interfaces et notifications
	1. Interface données

L’application Immobilisation autonome nécessite les interfaces suivantes :

* Import de biens comptables
* Import de biens physiques
* Export d’écritures comptables

L’application Immobilisation ne nécessite pas d’accès Service

Ces interfaces sont réalisées via des automates Sage FRP 1000 à travers des files d’attente gérée en base de données.

Ces files d’attentes sont ensuite alimentées / consommées par le Sync Agent.



* 1. Notifications utilisateurs
1. Configuration / Sécurité
	1. Eléments de configuration
		1. Mot de passe du compte OS de la machine virtuelle

Ce mot de passe est défini à la création de la machine virtuelle, il permet la connexion RDS à la machine.

* + 1. Certificats SSL du point d’accès https

Le certificat SSL est stocké dans le magasin de Windows (préférable à un stockage fichier)



Deux cas possibles :

Certificat wild card

* Le même certificat est installé sur toutes les machines, il peut être dans l’image

Un certificat avec sous domaine

* Le certificat est propre au client et doit être installé spécifiquement
	+ 1. Mot de passe de base de données

Le mot de passe de base de données est stocké dans le fichier de configuration, modifier ce mot de passe nécessite de redémarrer le service.

* + 1. Utilisateur démarrant le service

L’utilisateur démarrant le service et son mot de passe

* + 1. Jetons d’authentification d’accès service

La file d’attente de traitement des travaux batch nécessite une authentification par jeton Sage 1000 ; ce jeton est stocké dans le référentiel.

* 1. End points
		1. Point d’accès HTTPS

Ce point d’accès est utilisé par le client :

* Pour le client Web Sage FRP 1000
* Pour les accès Mobile (optionnel)
	+ 1. Point d’accès Remote desktop

Ce point d’accès est utilisé :

* Pour la configuration des éléments non configurable en Web
* Par la Host team

|  |  |  |  |
| --- | --- | --- | --- |
| End point | Used by | Used for | ACL |
| HTTPS | Customer | Web access | SupportCustomer |
| Remote desktop | Host teamSupport | Configuration | Host team |
|  |  |  |  |

TODO supprimer le point d’accès RDS

* 1. Ports ouverts en sortie
		1. SMTP
		2. HTTP
	2. ACLs

Les ACLs du point d’accès publique sont gérés le service, deux niveaux sont définis :

* Un niveau Client géré par le Client via l’interface d’Administration
* Un niveau « Hosting team » géré en exception et s’ajoutant à la liste d’ACLs client.
	1. Annuaires

L’annuaire d’identité utilisé est l’annuaire interne, la politique d’authentification est paramétrée ainsi :

|  |  |
| --- | --- |
| Policy property | Value |
| Complex password | Yes |
| Minimum password size | 8 |
| Password history | 3 |
| Password live time | 90 days |
| Input max error | 3 |
| Forbidden password list | To be set |

* 1. Localisation des éléments de sécurité

|  |  |  |
| --- | --- | --- |
| Item | Located | Need restart on change |
| OS password | Windows |  |
| SSL Certificate | Windows Store | Yes |
| Repository database account | Configuration file | Yes |
| Product database account | Repository database | Yes |
| ACL hosting team  | Configuration file | Yes |
| ACL Customer | Repository database | No |
| API Authentication token | Repository database | No |
| SMTP credentials | Configuration file | Yes |
| End points | Azure management | - |
|  |  |  |

(\*) repository and product database will be merged

* 1. Fichier de configuration

Eléments spécifiques au tenant dans le fichier de configuration :

|  |  |
| --- | --- |
| Item |  |
| Master base | url of the repository database |
| Master user | Account user of the repository database |
| Master password | Account password of the repository database |
| Server User | Sage FRP 1000 Account to start se server |
| Server Password | Sage FRP 1000 password of the server account |

* 1. Impersonnalisation des machines virtuelles

L’impersonnalisation des machines virtuelles consiste à supprimer toute référence au tenant sur les machines virtuelles.

Pour ceci la configuration du service est déportée vers un serveur de configuration.

Au démarrage du service, le fichier de configuration est obtenu via l’interrogation d’un serveur de configuration.

Pour que l’impersonnalisation soit complète il faut que le certificat soit commun (wild card) ou installé via la configuration.



La mise en œuvre du serveur de configuration résout plusieurs problématiques :

* Absence de stockage de la configuration sur les VMs tenant
* Facilité de modifications groupées des paramètres du SAAS
* Facilité de modification des mots de passes et des certificats

Boot process:



1. Sauvegardes
	1. Point in time

Les bases de données standard SQL dispose de la fonctionnalité « Point-in time restore » sur 14 jours.

1. Supervision
	1. Evènements dans Sage FRP 1000

La gestion des évènements dans Sage FRP 1000 est organisée ainsi :



Les évènements sont générés par les différents modules qui composent le Service, ils sont collectés par un gestionnaire qui les dispatch sur des enregistreurs

|  |  |  |
| --- | --- | --- |
| Event category |  | Action |
| Error | Fatal error, service is dead | Mail alert |
| Warning | Not fatal, but attention required | Mail alert |
| Information | Not critical message | not logged |
| Audit success | Normal activity audit message | Log to Audit table |
| Audit failure | Failure activity audit message | Log to Audit table |
| Monitoring | Monitoring message  | Trigger mail alert  |

* 1. Journaux

Les évènements peuvent être journalisé par catégories :

* Journal d’audit d’activité
* Journal des exceptions

Ces journaux sont stockés dans des Tables Azure

* 1. Monitoring alertes

Les évènements de monitoring sont générés par l’horloge de performance.

Les alertes sont déclenchées lorsque des compteurs de performances dépassent des seuils prédéfinis.

Les compteurs de performance pouvant déclenchant une alerte :

|  |  |
| --- | --- |
| Event category | Signification |
| system.memory.virtualSetSize | Almost out of memory |
| exceptions.hit | Major problem causing a lot of exceptions |
| http.acl.deny.count | A significant number of rejected accesses is reach |
| http.acl.deny.hit | Could be a dos attack |
| http.hit | Could be a dos attack |
| authenticate.failure.hit | Could be a brute force attack |
|  |  |

* 1. Health probe

TODO

1. Déploiement

Procédure manuelle

Création d’un nouveau tenant

* 1. Création de l’image
* Exécuter sysprep

Ceci arrête la machine

* Capturer la machine

Ceci supprime la machine

* 1. Déploiement d’un tenant

Près requis :

* Les données client ont été migré sur une base de données « On premise »

Les opérations pour créer un tenant :

* Déterminer le nom/code/codification du tenant

Il est important d’adopter une convention de nom cohérente

* Modifier l’url des bases de données cible dans TdbmDatabase
* Migrer la base de données avec l’assistant inclus dans « SQL Management Studio »

L’assistant migre la base vers une base niveau Web ou Business, on veut une base type Standard S1

* Dans le Portail Azure, Changer le niveau de la base en S1
* Dans le Portail Azure, Créer la VM tenant à partir de l’image
* Se connecter en Terminal Server sur la nouvelle VM
* Modifier le servicel1000.ini de la VM pour pointer sur la base de données restauré

|  |  |  |
| --- | --- | --- |
| 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 |