SERVICES DE CDE
INFORMATION SUR L'INTÉGRATION TECHNIQUE

Services partagés Canada

Division des services d'intégration de solutions

Gestion et exécution des projets

Révision du document :	v. 0.2
État d'avancement :	ÉBAUCHE
Date de publication :	***2018-01-18***

HISTORIQUE DU DOCUMENT

Commented [TM(1)]: Do we really want to include Doc History in the RFP version of this document?

Auteur(s) et co-auteur(s) du document, poste – Titre

Nom complet	Rôle	Ministère – Poste – Titre
Fabien de Oliveira	Conseiller principal	Division des services d'intégration de solutions
Ray Parent	Intégrateur de solutions	Division des services d'intégration de solutions
Sean Smith	Intégrateur de solutions	Division des services d'intégration de solutions

Historique des modifications

Ver. nº	Date	Consulté/Réviseurs	Brève description de la modification	Auteur de la modification
0.1	2017-12-19	Fabien de Oliveira	Première ébauche	Fabien de Oliveira
0.2	2018-01-18	Fabien de Oliveira	Commentaires de Sean Smith	Fabien de Oliveira

Table des matières

1 Introduction

1.1 Objet

Ce document énonce les exigences et les services techniques de haut niveau de SPC nécessaires pour mettre en œuvre toute solution d'intégration aux centres de données de SPC. Il se penche en particulier sur les services qui sont disponibles aux centres de données à l'état final (CDF).

Toute utilisation d'un quelconque service proposé par SPC dans le Catalogue de services signale une dérogation au modèle opérationnel Installations comme service (IcS) et indique une transition vers des modèles opérationnels Infrastructure comme service (IncS) ou Plateforme comme service (PcS).

2 Aperçu de l'environnement d'intégration de SPC

Figurent ci-après les services existants de SPC qui peuvent être mis à contribution et/ou intégrés aux solutions mises en œuvre dans les CDF :

- Installations de centres de données de SPC
- Services de CDF de SPC
- Infrastructure du réseau de SPC
- Bureau de service d'entreprise de SPC
- Centre des opérations de sécurité de SPC
- Justificatif d'identification Active Directory de SPC
- Composants ICP du GC
- Autres (à mesure de leur disponibilité dans le catalogue de services de SPC)

2.1 Installations de centres de données de SPC

Les Installations de centres de données de SPC comportent les caractéristiques suivantes :

- Capacité de centre de données – volet 3 – haute densité
- Environnement à locataires multiples (partenaires multiples) sans séparation physique
- Alimentation conditionnée sans interruption pour l'infrastructure de TI
- Alimentation sans coupure, systèmes de sauvegarde et redondance N+1 (ou supérieure) complets
- Systèmes robustes de chauffage, de ventilation et d'air conditionné (HVAC)
- Équipement, techniques et procédures de sécurité pour contrôler, surveiller et consigner l'accès aux installations
- Mesure et surveillance de la disponibilité, de l'efficacité, de la capacité et de la sécurité
- Centres d'exploitation et espace de stockage
- Au moins deux points d'accès distincts au réseau aux fins de redondance

2.2 Réseau de centres de données

Services partagés Canada (SPC) doit assumer la responsabilité de fournir la connectivité de l'Internet, du réseau étendu (WAN) et du réseau local (LAN) pour la solution proposée qui sera hébergée au centre de données (CDF) de SPC. Ce modèle de connectivité permettra la circulation à partir et en direction de la solution proposée ainsi que la communication à l'intérieur du CDF.

2.3 Services du CDF

2.3.1 Centres de données

L'autorisation d'exploitation (AE) du centre de données a été reçue au niveau Protégé A, Moyen, Moyen. Les contrôles de sécurité de l'application peuvent être abordés afin de porter l'accréditation de l'application à Protégé B.

Classification de sécurité	Non classifié
État d'avancement :	ÉBAUCHE v0.2
Objet :	Intégration Technique des services de CDE

2.3.2 Visibilité et accessibilité de l'application

La communauté du gouvernement du Canada, les ministères et le public de l'Internet sont en mesure d'avoir accès aux applications en passant par les zones d'accès de sécurité du réseau :

- Entrée depuis la communauté du GC via le NCGC en passant par la zone opérationnelle (OZ) du CDF.
- Entrée depuis l'Internet dans le CDF en passant par la zone d'accès public (ZAP) du CDF

Reportez-vous à la figure 1 à la Section 2.5.1 pour plus de renseignements sur le zonage du CDF.

2.3.3 Environnements de développement minimum

SPC appuie à l'heure actuellement les trois environnements de cycle de développement de systèmes (CDS) normalisés suivants :

- Développement
- Préproduction
- Production

Des environnements supplémentaires quelconques, notamment Essai, Formation, AQ, etc. peuvent être placés dans l'un des trois environnements de base selon les exigences de l'environnement supplémentaire.

2.3.4 Privilège élevé

Les permissions de compte d'administrateur de production et de préproduction s'appliquent exclusivement aux groupes de soutien opérationnel de SPC pour tous les dispositifs (physiques et virtuels) à l'intérieur du CDF. Les administrateurs et les concepteurs des partenaires et/ou des fournisseurs recevront des justificatifs d'identité au niveau de grand utilisateur dans les environnements de production et de préproduction.

2.3.5 Plateforme de virtualisation

L'hyperviseur utilisé actuellement au CDF est le VMware vSphere ESXi version 5.5.

2.3.6 Contrôleur de livraison d'applications (ADC)

La solution de contrôleur de livraison d'applications (ADC) est actuellement mise en œuvre dans une configuration entièrement redondante. Cette redondance augmente la fiabilité et la disponibilité. Ce service vise à optimiser l'utilisation de ressources, à maximiser le débit, à réduire au minimum le délai de réponse et à éviter la surcharge d'une ressource particulière.

- Les caractéristiques disponibles de la solution ADC sont les suivantes : Forward Proxy (proxy de transfert), Load Balancer (compensateur de charge) et SSL Offload Certificate (certificat de déchargement SSL).

2.3.7 Infrastructure de sauvegarde

Tous les serveurs virtuels sont automatiquement protégés par le Service de récupération opérationnelle (SRO) lorsqu'ils sont mis en service au CDF. Le calendrier prévoit une sauvegarde entière par semaine et des sauvegardes supplémentaires les jours restants.

CommVault, la solution d'état final intérimaire, sauvegarde un instantané VMware du serveur virtuel. La version 11.x de CommVault est utilisée actuellement.

Il pourrait être possible de tirer parti de la sauvegarde en mode agent au cas par cas, au besoin.
Les données de sauvegarde sont conservées 30 jours, et le stockage hors site d'une sauvegarde s'effectue au moyen de travaux de copie auxiliaires programmés chaque jour.

2.3.8 Infrastructure de surveillance et d'alerte

SPC surveille la disponibilité en temps réel de l'infrastructure et des applications qui utilisent les outils de surveillance du SSE et le service du CCE. Une partie du SE géré dans le cadre du service de SE géré est surveillée par le biais du service CA agent.
Cette surveillance fournit une option de surveillance de base à l'Infrastructure (UCT, Mémoire, espace du disque et état de pulsation du logiciel Ping).

L'outil qui est actuellement utilisé est le spectre du Système de surveillance d'entreprise (SSE).

2.3.9 Système d'enregistrement

Les journaux d'environnement sont envoyés à un agrégateur de journaux qui les envoie à son tour à un collecteur aux fins d'analyse et d'examen.
Les journaux utilisent la carte d'interface réseau (CIR) de gestion pour envoyer l'information au secteur de service approprié.

2.3.10 Système d'adressage par domaines (DNS)

Un service DNS géré de SPC est disponible pour la résolution d'adresses IP d'applications.

2.3.11 Services de répertoire

Les solutions ont l'option d'interagir avec le logiciel Active Directory (AD) de SPC pour tirer parti des justificatifs d'identité d'AD.
La solution AD qui est en place utilise actuellement les services de répertoire Windows 2012. (L'équipe AD de SPC planifie actuellement l'entrée en service de Windows 2016).

2.3.12 Protection antivirus

SPC utilise actuellement une solution d'analyse antivirus. Si le fournisseur juge que le rendement pourrait être altéré par l'analyse antivirus, il faudrait fournir des exclusions pour le client de l'antivirus.
Une « liste blanche » pour les applications est en cours de mise en œuvre au CDF et exigera que les détails de l'application soient communiqués à l'équipe de la sécurité pour que l'application soit installée et exécutée.

2.3.13 Services correctifs

La correction pour le service Windows est effectuée au moyen du produit SCCM.
La correction pour le service Linux est disponible par l'entremise de Puppet et Satellite pour Red Hat.
Un calendrier de correction est disponible pour les deux versions SE géré.

2.3.14 Redondance

La redondance est intégrée au centre de données. Une conception spéciale est nécessaire pour la configuration GD entre centres de données, au cas par cas.

2.3.15 SE (système d'exploitation) géré

Par défaut, chaque SE géré est configuré avec deux cartes d'interface de réseau (CIR) (gestion et production). Chaque SE géré est étayé par les services susmentionnés de sauvegarde, de surveillance et d'alerte, d'antivirus et de correction.
Toute solution proposée doit fournir toutes les licences et la gestion de logiciel qu'exige la solution dans la catégorie d'application au-dessus du système d'exploitation géré. Les systèmes d'exploitation de SE gérés pris en charge sont les suivants :

- Windows 2012 R2
- Linux Red Hat 6.4

2.4 Service d'accès à distance

L'accès à distance à la Zone restreinte de gestion (ZRG) est réalisé au moyen d'une authentification à deux facteurs faisant appel aux deux facteurs suivants :

- Des justificatifs d'identité de la TI associés aux services de répertoire Windows avec l'accès fondé sur les rôles.
- Un compte ICP maClé

2.4.1 Plateforme de l'administration d'applications

L'accès à l'administration des applications est fourni par une plateforme Citrix, à laquelle il est possible d'avoir accès au moyen d'une authentification à deux facteurs par l'entremise d'un service RPV virtuel fourni par SPC.

La plateforme Citrix a par défaut des applications publiées par RDP et Putty. Ces applications publiées peuvent être utilisées pour accéder aux consoles administratives des serveurs d'infrastructure.

Si le fournisseur l'exige, des applications publiées supplémentaires peuvent être mises à disposition (le fournisseur devrait fournir un programme d'installation et un profil pour le projet au secteur de service Citrix). Il serait possible de les utiliser pour publier de quelconques consoles administratives, etc. dont la solution proposée pourrait avoir besoin.

2.4.2 Administration à distance de SPC

Les centres de données CDF sont réputés être des centres de données fermés. Aucun accès n'est autorisé aux centres de données CDF. Toutes les tâches administratives sont effectuées à distance au moyen des solutions d'administration par accès à distance.

L'administration à distance doit respecter les processus actuellement en place de SPC pour l'accès d'administration à distance à l'infrastructure du CDF.

Ces processus peuvent comprendre, entre autres choses :

- Des justificatifs d'identité de la TI
- Des points de terminaison (postes de travail) fournis par le gouvernement du Canada
- Des justificatifs d'identité ICP maClé

2.5 Conformité au zonage de sécurité

2.5.1 Références aux lignes directrices de l'ITSG

SPC applique les lignes directrices en matière de sécurité du CST (ITSG22, 33, 38…) : https://www.cse-cst.gc.ca/fr/publication/list

Le zonage du réseau de CDF est illustré dans le diagramme ci-après.

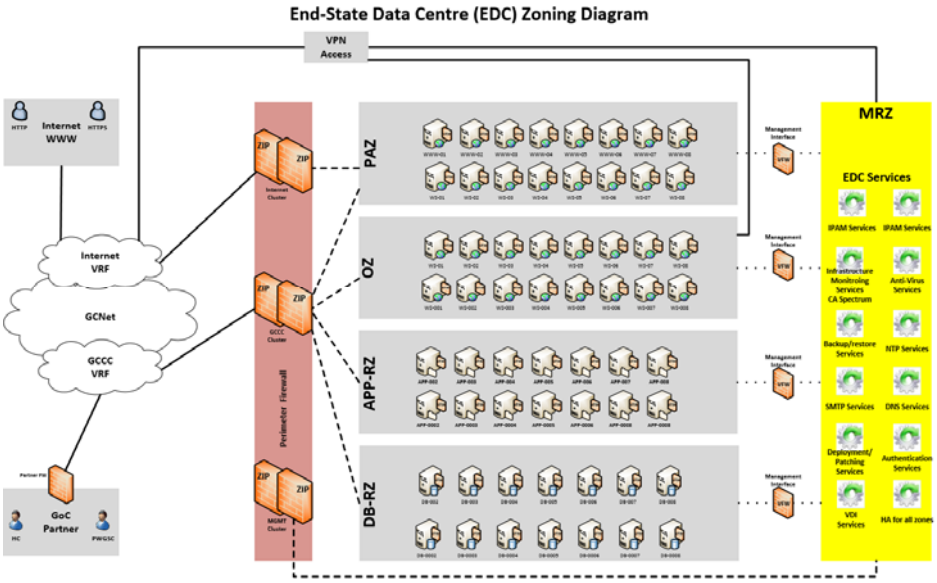

Figure 1 – Diagramme de zonage du CDF

Sigle ou acronyme	Définition
ZR-APP	Zone restreinte d'applications
ZR-BD	Zone restreinte de base de données
NCGC	Nuage commun du gouvernement du Canada
ZRG	Zone restreinte de gestion
ZO	Zone opérationnelle
ZAP	Zone d'accès public
VFW	Pare-feu virtuel
PFV	Routage et acheminement virtuels
PIZ	Point d'interface de zone

Tableau 1 – Définitions des sigles et acronymes du zonage du réseau du CDF

2.6 Plan d'évaluation de la sécurité

Il faudra effectuer une évaluation de la sécurité de toute solution proposée (les détails seront fournis). Veuillez consulter le secteur de service approprié pour un complément d'information.

2.7 Intégration du service externe

2.7.1 Initiative de transformation des services de courriels (ITSC)

Si un service de courriel est nécessaire, le fournisseur devra assurer l'intégration avec un service de courriel hébergé à l'extérieur. Ce service de courriel est actuellement fourni par un fournisseur particulier. Chaque partenaire a un coordonnateur qui est chargé de l'intégration et qui demande un compte de service afin de tirer parti de ce service (veuillez vous reporter au catalogue des services : http://service.ssc.gc.ca/fr/services.

2.7.2 Centre des opérations de sécurité (COS)

SPC héberge le Centre des opérations de sécurité (COS). Le COS est composé de l'Équipe d'intervention en cas d'incidents informatiques du gouvernement du Canada (EIII-GC); de l'Équipe de reprise après incident de sécurité de la TI (ERIS-TI); et du Centre fédéral de protection de l'information (CFPI). L'EIII-GC tient les listes de diffusion pangouvernementale et donne aux ministères et organismes tout conseil et orientation dont ils ont besoin pour atténuer les menaces et les vulnérabilités électroniques.

2.7.3 Service interne de gestion des preuves d'identité (SIGPI)

Au besoin, la solution proposée devrait pouvoir tirer parti de l'infrastructure à clés publiques, maClé du GC.

La solution proposée devrait pouvoir intégrer la GJI maClé aux bureaux des employés.

La CONNEXION maClé (le service d'authentification Web sécurisée), comporte des frais d'intégration supplémentaire en sus du coût de base des services de GJI.

2.7.4 Intégrité de la chaîne d'approvisionnement.

Le processus d'intégrité de la chaîne d'approvisionnement (ICA) a pour objet de veiller à ce qu'aucun équipement, logiciel ou service auquel il ne peut pas être fait confiance ne soit acheté ni ne soit utilisé pour la prestation et/ou à l'appui des services du gouvernement du Canada (GC).