Services partagés Canada

services ET GESTION DES produits infonuagiques

Processus de préparation à la connectivité

Version 1.5

GCDOCS <# 68861147>

2020-12-01

Historique des versions

| Numéro de version | Description | Date de modification | Auteur |
| --- | --- | --- | --- |
| 1.0 | Version originale (extraite de l’ébauche du Secrétariat du Conseil du Trésor (SCT) – Scott Levac) | 2020-02-17 | Bureau du dirigeant principal de l’information (BDPI) du SCT |
| 1.1 | Modifications par Opérations des services infonuagiques | 2020-02-28 | Services infonuagiques de Services partagés Canada (SPC) |
| 1.2 | Modifications par le BDPI du SCT  | 2020-02-28 | BDPI du SCT |
| 1.3 | Modifications suggérées par l’équipe sur l’infonuagique de l’Agence des services frontaliers du Canada (ASFC) | 2020-03-06 | Services infonuagiques de SPC à l’ASFC |
| 1.4 | Le champ de données FSI a été changé en texte de forme libre | 2020-10-23 | Services infonuagiques de Services partagés Canada (SPC) |
| 1.5 | Modifications par Opérations des services infonuagiques | 2020-11-30 | Services infonuagiques de Services partagés Canada (SPC) |
|  |  |  |  |

Table des matières

[1 Objectif 1](#_Toc34985629)

[2 Vue d’ensemble du processus 1](#_Toc34985630)

[2.1 Obtenir un compte infonuagique 1](#_Toc34985631)

[2.2 Mettre en place des garde-fous 2](#_Toc34985632)

[2.3 Obtenir une autorisation de fonctionner (ADF) pour l’infrastructure infonuagique 2](#_Toc34985633)

[2.4 Préparation à la connectivité 3](#_Toc34985634)

[2.4.1 Entente sur la connectivité 3](#_Toc34985635)

[2.4.2 Liste de vérification sur l’état de préparation à l’infonuagique 3](#_Toc34985636)

[2.5 Déploiement de solutions infonuagiques hybrides 4](#_Toc34985637)

[2.6 Exploitation et entretien 4](#_Toc34985638)

[3 Foire aux questions 5](#_Toc34985639)

[Appendice A - Liste de vérification sur l’état de préparation à l’infonuagique 8](#_Toc34985640)

[Appendice B - Liste de vérification sur l’état de préparation à l’infonuagique (exemple) 10](#_Toc34985641)

[Annexe C - Glossaire des acronymes 13](#_Toc34985642)

[Liste des acronymes 13](#_Toc34985643)

# Objectif

Les ministères sont tenus d’établir un modèle de TI hybride. Le 31 janvier 2020, le Comité d’examen de l’architecture d’entreprise du gouvernement du Canada (CEAI GC) a approuvé la recommandation de demander aux ministères de démontrer leur état de préparation à l’infonuagique avant l’établissement de toute interconnexion entre l’environnement infonuagique d’un ministère et les centres de données du gouvernement du Canada (GC). Dans le cadre du processus d’intégration, la priorité sera donnée aux ministères ayant terminé leurs activités de préparation à l’infonuagique. Le processus de préparation s’inscrit dans la continuité des activités déjà prévues par le cadre d’opérationnalisation de l’infonuagique protégé B, y compris la mise en œuvre et la validation des [garde-fous](https://github.com/canada-ca/cloud-guardrails) infonuagiques obligatoires.

Les ministères auront la possibilité de consulter les résultats des évaluations de la préparation à l’infonuagique dans le [Centre d’infonuagique](https://wiki.gccollab.ca/cloud) du BDPI du SCT.

# Vue d’ensemble du processus

Afin d’assurer que les ministères intégrés au fournisseur de services d’infonuagique Exchange (FSIE) exploitent pleinement les capacités offertes par celui-ci, ils seront tenus de démontrer qu’ils sont prêts à utiliser les services du FSIE.

On a demandé au Réseau d’expertise en informatique en nuage et en informatique (REINI) d’examiner les différents processus de préparation proposés. Dans la présente section, nous approfondirons les responsabilités du ministère, telles qu’illustrées à la figure 1 ci-dessous.

**Figure 1 : Rôle ministériel dans le cadre d’opérationnalisation de l’infonuagique**



La figure 1 a été extraite de la diapositive 5 sur l’[état de préparation et l’établissement des priorités en vue de la connectivité au FSIE](https://gcconnex.gc.ca/file/download/59833196) du CEAI du GC.

## Obtenir un compte infonuagique

Par l’intermédiaire d’un [courtier en matière d’informatique en nuage du GC](https://cloud-broker.canada.ca/), le ministère présente une demande d’obtention de compte infonuagique pour accéder à différents services infonuagiques IaaS (infrastructure en tant que service) ou PaaS (plateforme en tant que service) offerts par un fournisseur de services d’infonuagique (FSI) approuvé par le GC. On attribue à chaque client deux « utilisateurs désignés » nommés par le dirigeant principal de l’information (DPI) du ministère, qui ont accès au portail de demandes et qui peuvent présenter des demandes au nom de ce client.

Les ministères peuvent demander à ce que leur soit attribué un éventail d’adresses IP, conformément à la [stratégie de Gestion des adresses IP d’informatique en nuage](https://gccollab.ca/file/view/3690502/encloud-internet-protocol-address-management-cloud-ipamfrgestion-des-adresses-de-protocole-internet-dans-le-cloud-cloud-ipam) de SPC. Il est essentiel que les ministères intègrent les adresses IP fournies dans leurs conceptions futures puisqu’elles permettront de faciliter l’acheminement réseau entre leur environnement infonuagique et les réseaux du GC.

## Mettre en place des garde-fous

Conformément au cadre d’opérationnalisation de l’infonuagique protégé B, les ministères et les agences visées par la portée de la [Politique sur les services et le numérique](https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32603) doivent mettre en œuvre à l’échelle de l’entreprise les [garde-fous infonuagiques initiaux](https://github.com/canada-ca/cloud-guardrails) minimums obligatoires de 30 jours du GC.

Les garde-fous forment un sous-ensemble des contrôles de base recommandés pour l’infonuagique, conformément à l’[Orientation sur l’utilisation sécurisée des services commerciaux d’informatique en nuage : Avis de mise en œuvre de la Politique sur la sécurité (AMOPS) de février 2017](https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/orientation-utilisation-securisee-services-commerciaux-informatique-nuage-amops.html) et au [Profil des mesures de sécurité pour les services du GC fondés sur l’informatique en nuage avec une catégorie de sécurité de Protégé B, intégrité moyenne et disponibilité moyenne](https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/services-informatique-nuage/profil-controle-securite-services-ti-fondes-information-nuage.html) (PBMM).

Les garde-fous doivent être appliqués en fonction des [profils d’utilisation de l’infonuagique](https://www.gcpedia.gc.ca/gcwiki/images/8/84/GC_Cloud_Guardrails.pdf). Dans la mesure du possible, il est nécessaire de mettre à profit les modèles approuvés par le GC (par exemple, les accélérateurs du GC). L’utilisation des accélérateurs du GC soutiendra le déploiement de l’infrastructure sous forme de code, qui comporte les garde-fous techniques nécessaires.

Les accélérateurs du GC sont accessibles ici :

AWS : <https://github.com/canada-ca/cloud-guardrails-aws>

Azure : <https://github.com/canada-ca/cloud-guardrails-azure>

La vérification de la mise en œuvre des garde-fous est effectuée par Opérations d’informatique en nuage de SPC. Des outils permettant de soutenir les vérifications automatisées de la conformité sont accessibles dans les répertoires Github présentés ci-dessus.

En particulier pour la segmentation et la séparation liées à la mesure de sécurité 8, on doit sélectionner un pare-feu qui comprend des capacités de réseau privé virtuel (RPV), notamment des [*algorithmes de chiffrement conformes aux normes de chiffrement du GC*](https://cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-pour-linformation-non-classifie-protege-et-protege-b). Disposer d’un pare-feu ou d’un appareil de gestion unifiée des menaces doté de cette capacité est une condition préalable pour la connectivité au service infonuagique sécurisé de SPC (PIF du GC et PAN du GC).

Pour satisfaire à cette exigence, les clients doivent d’abord se procurer des licences par l’intermédiaire des mécanismes de passation de marchés actuels du GC. Ensuite, ils doivent envoyer une demande « Apportez votre licence » au Service de courtage infonuagique du GC pour l’activation de la licence dans le nuage public. Les clients devront fournir des renseignements sur le mécanisme de passation de marchés qu’ils ont utilisé pour acquérir les licences. Pour plus de renseignements au sujet de la demande « Apportez votre licence », veuillez communiquer avec ssc.cloud-infonuagique.spc@canada.ca.

## Obtenir une autorisation de fonctionner (ADF) pour l’infrastructure infonuagique

On s’attend à ce que les ministères continuent à appliquer des mesures de protection progressives proportionnelles aux risques menaçant leur information et leurs biens de TI en ayant recours à des mesures de protection plus rigoureuses à mesure qu’augmentent la valeur des biens, les exigences de la prestation de services et les menaces à la confidentialité, à la disponibilité ou à l’intégrité.

Le point de départ initial des mesures de sécurité de la couche de plateforme infonuagique (votre environnement infonuagique), en tant que sous-ensemble du profil PBMM de l’infonuagique du GC, sera accessible dans tous les ministères :

* Dans le cas d’Azure, le point de départ est accessible au moyen de la [Blueprint Canada PBMM](https://azure.microsoft.com/fr-ca/updates/new-canada-federal-pbmm-azure-blueprint-is-now-available/).
* Dans le cas d’AWS, la ***zone d’atterrissage*** est préconfigurée par le fournisseur de tous les clients du GC.

On prévoit l’adoption d’une approche itérative relativement à la conception, à l’élaboration et à l’évaluation de votre environnement infonuagique. En ce qui a trait aux activités d’ingénierie de système, on générera des données probantes permettant de fournir des garanties concernant la mise en œuvre des contrôles.

L’utilisation de l’ébauche de la [stratégie d’appellation et d’étiquetage](https://gccollab.ca/file/view/3634499/ennaming-and-tagging-standardsfr) aidera également à s’assurer que les différents profils d’utilisation de l’infonuagique que peut comporter un locataire de service infonuagique sont adéquatement étiquetés et que les garde-fous et les contrôles sont appliqués.

La réalisation d’une évaluation et autorisation de sécurité (EAS) sur l’infrastructure infonuagique facilitera l’établissement d’un modèle de transmission de la sécurité qui pourra être utilisé pour le déploiement de futurs systèmes d’information. L’évaluation doit être approuvée par les autorités pertinentes au sein de l’organisation.

Les ministères prévoient fournir des données probantes, comme une lettre d’autorisation dûment signée, pour démontrer que l’organisation avait approuvé l’utilisation de l’infrastructure infonuagique au moment de la signature de l’[entente de sécurité sur l’interconnectivité](https://wiki.gccollab.ca/File%3AInterconnection_Security_Agreement_for_Cloud_Connectivity_v1.2.docx).

Le Secrétariat du Conseil du Trésor du Canada a mis à la disponibilité des autres ministères une certaine partie de ses [documents sur l’évaluation de la sécurité](https://gccode.ssc-spc.gc.ca/GCCloudEnablement/Microsoft/tree/master/TBS%20Cloud%20Environment) sur Azure pour qu’ils puissent en tirer profit.

## Préparation à la connectivité

Cette activité nécessite la signature des ententes pertinentes et la prestation de renseignements sur les flux de réseau.

### Entente sur la connectivité

L’entente de sécurité sur l’interconnectivité énonce les exigences techniques et de sécurité de l’interconnexion. Elle établit les responsabilités des organisations, en plus de décrire les niveaux de service et l’accessibilité des systèmes. Le document de l’entente de sécurité sur l’interconnectivité est publié par le [Centre d’infonuagique](https://wiki.gccollab.ca/GC_Cloud_Infocentre).

**\* L’entente de sécurité sur l’interconnectivité doit être remplie, signée et renvoyée à l’adresse** **ssc.cloud-infonuagique.spc@canada.ca** **et l’objet du courriel en question doit être : « Entente de sécurité sur l’interconnectivité ».**

### Liste de vérification sur l’état de préparation à l’infonuagique

Le ministère doit être en mesure de décrire l’application et les flux de réseau au moyen du modèle figurant à l’Appendice A. Ces détails devraient être suffisants pour permettre à SPC de définir les flux de réseau allant de l’environnement infonuagique aux applications et services des centres de données existants ou organisationnels. Ces derniers devraient comprendre des adresses IP, des ports et des protocoles. N’oubliez pas d’inclure les flux associés au soutien de différents services comme le stockage d’identité.

**\* La Liste de vérification sur l’état de préparation à l’infonuagique doit être remplie, chiffrée et renvoyée à l’adresse** **ssc.cloud-infonuagique.spc@canada.ca** **et l’objet du courriel en question doit être : « Liste de vérification sur l’état de préparation à l’infonuagique ».**

Après avoir terminé le cadre d’opérationnalisation de l’infonuagique protégé B, signé l’entente et rempli la Liste de vérification sur l’état de préparation à l’infonuagique, on considérera que vous aurez fourni à SPC tous les documents nécessaires pour démontrer l’achèvement du processus d’état de préparation.

Veuillez noter : Les ministères peuvent demander à ce que leur soit attribué un éventail d’adresses IP, conformément à la [stratégie de Gestion des adresses IP d’informatique en nuage](https://gccollab.ca/file/view/3690502/encloud-internet-protocol-address-management-cloud-ipamfrgestion-des-adresses-de-protocole-internet-dans-le-cloud-cloud-ipam) de SPC.

## Déploiement de solutions infonuagiques hybrides

On lancera alors les activités de connectivité dans votre ministère, ou si les capacités nécessaires pour la réalisation de ces activités ne sont pas disponibles, la réalisation de ces activités dans votre ministère sera traitée en priorité et inscrite au calendrier.

## Exploitation et entretien

Les ministères doivent gérer les risques de sécurité touchant l’information et les actifs de la technologie de l’information (TI), ce qui comprend la surveillance continue des services fondés sur l’infonuagique en tant qu’élément essentiel d’une stratégie de sécurité de la TI efficace. La surveillance continue englobe des activités telles que :

* surveiller les menaces et les vulnérabilités;
* passer en revue les résultats de la surveillance du système;
* effectuer l’auto-évaluation et la vérification interne;
* élaborer des plans de mesures correctives pour remédier aux insuffisances, au besoin.

# Foire aux questions

Q1 : En quelles circonstances un processus de préparation est-il nécessaire?

Le nombre de demandes d’intégration au fournisseur de services d’infonuagique Exchange (FSIE) surpasse les ressources accessibles dans les ministères d’intégration. Voilà pourquoi le processus de préparation a été créé pour veiller à ce que ces ministères en processus d’intégration au FSIE soient, d’emblée, en mesure de pleinement profiter des capacités du FSIE.

Q2 : Qu’entendez-vous par connectivité?

Dans le cadre du présent document, il s’agit de la connectivité aux environnements infonuagiques de la plateforme IaaS. Il ne s’agit pas de la connectivité à SaaS (logiciel en tant que service), qui est associée à un plan différent. La connectivité vise à aborder un, ou plusieurs, des défis suivants pour les ministères :

1. Une architecture hybride est nécessaire si différentes applications de l’infonuagique communiquent avec les applications d’un centre de données géré par SPC.
2. Les portails Internet actuels ont une bande passante insuffisante pour soutenir les besoins d’un ministère relativement à ses activités infonuagiques.
3. La latence de réseau de la connectivité nuage-sol est à un niveau acceptable.

La plupart des organisations n’ont pas encore eu à composer avec le deuxième défi. Bien que les portails Internet soient soumis à des pressions considérables, l’ampleur de l’utilisation de l’infonuagique dans la plupart des ministères n’est pas assez importante pour complètement saturer les portails Internet. L’accent est habituellement accordé au premier scénario. Il touche les profils d’utilisation 5 et 6.

Q3. Qu’est-ce qu’un fournisseur de services d’infonuagique Exchange (FSIE)?

Le fournisseur de services d’infonuagique Exchange (FSIE) est un service qui relie l’extrémité du réseau du GC au réseau du fournisseur de services d’infonuagique. Le GC utilise un FSIE qui rassemble un grand nombre de réseaux de fournisseurs de services d’infonuagique en un seul emplacement, ce qui permet de simplifier les efforts. On s’attend à ce que les ministères terminent le processus de configuration de connexion dédiée en établissant des services de FSI, comme ExpressRoute ou DirectConnect.

Q4. Que dois-je faire pour connecter différents environnements infonuagiques avec différents fournisseurs de services?

Chaque environnement va avoir ses propres séries d’adresses IP, évaluations de sécurité, etc. Bien qu’il vous serait possible d’utiliser le processus de préparation avec deux environnements en parallèle, cette façon de faire doublerait votre charge de travail. Demandez-vous si vous êtes prêt à pleinement exploiter les deux environnements et si vous êtes prêts à pleinement exploiter les capacités de FSIE dans ces deux environnements. Il pourrait être préférable de commencer par l’environnement le plus prioritaire.

Q5. Passerez-vous en revue mon évaluation de sécurité?

Non. La gestion des évaluations de sécurité est une responsabilité ministérielle. Il reviendra à votre organisation d’établir sa propre tolérance aux risques.

Q6. Mon évaluation de sécurité comprend-elle l’ensemble de mes applications?

Non, on s’attend à ce que vous réalisiez l’évaluation de votre environnement infonuagique avant de transférer ou d’élaborer des applications.

Q7. Pourquoi mon cas doit-il passer en priorité?

Dans l’éventualité où un certain nombre de ministères termineraient le processus de préparation et qu’il y aurait un arriéré de demandes, on établira un ordre de priorité.

Q8. Quel est le cadre d’opérationnalisation?

Le cadre d’opérationnalisation a été approuvé par le CEAI du GC le 19 septembre 2019. Avant l’ouverture du cadre d’opérationnalisation de l’infonuagique aux ministères, le GC a mis en œuvre un ensemble de garde-fous minimums obligatoires que tous les ministères devront appliquer dans leur environnement afin d’assurer le respect de mesures de protection minimales.

Q9. Ces procédures m’aideront-elles à adopter Office 365?

Non. On déploie une solution d’architecture de réseau différente, appelée un fournisseur de services d’infonuagique Exchange (FSIE), pour le SaaS et les grands fournisseurs de contenu Internet.

Q10. Le processus de préparation sera-t-il aboli un jour?

Peut-être un jour. Si l’on revient à la question 1, le processus de préparation permet de s’assurer que les ministères intégrés au FSIE sont prêts à utiliser les capacités du FSIE. Le processus de préparation a été créé parce que l’intégration est supérieure à l’approvisionnement auxquels les organisations d’intégration ont accès. Si la demande venait à chuter ou alors si les capacités d’intégration venaient à augmenter ou à s’automatiser, le besoin de processus de préparation serait grandement réduit.

Q11. Comment SPC pourra-t-il savoir si je suis prêt à l’intégration?

Si vous avez signé les ententes exigées et rempli le cadre d’opérationnalisation avec SPC, vous avez donc effectué toutes les activités nécessaires. Il se passera l’une de ces deux choses :

1. Vous passerez en priorité;
2. Les activités de connectivité seront lancées.

Q12. Que dois-je faire si j’ai besoin d’un niveau de service supérieur à ce que prévoit l’entente de service?

Vous aurez donc besoin d’un service différent. L’entente sur les niveaux de service vise à indiquer le niveau de service que vous pouvez espérer obtenir en soutien à vos services.

Q13. Combien doit-il s’écouler de temps entre la démonstration de la préparation et la mise en place de la connectivité?

Si l’on suppose qu’il n’y a pas d’arriéré d’intégration, l’expérience antérieure démontre qu’il faudra environ deux mois pour réaliser la connectivité.

# Appendice A - Liste de vérification sur l’état de préparation à l’infonuagique

**La colonne de l’évaluation ne peut être remplie que par l’évaluateur.**

|  |  |
| --- | --- |
| **Aperçu du projet, de l’initiative ou de l’application** | **Évaluation** |
| Nom du ministère : \_\_\_\_\_\_\_\_\_\_\_\_\_Nom de l’activité ou du projet de la TI du GC (outil Clarity du SCT) : \_\_\_\_\_\_\_\_\_\_\_\_\_Identifiant de l’activité ou du projet de la TI du GC (outil Clarity du SCT) : \_\_\_\_\_\_\_\_\_\_\_\_\_Description du projet, de l’initiative ou de l’application : (2 ou 3 paragraphes) | Réussite : [ ] Échec: [ ]  |
| **Obtenir un compte d’informatique en nuage** | **Évaluation** |
| Les deux utilisateurs désignés ont-ils reçu leurs comptes dans le portail de courtier de l’infonuagique du GC? [ ] Veuillez fournir votre numéro de demande de gestion des relations avec les clients : \_CRXXXXX\_\_\_\_\_\_\_\_\_\_\_\_FSI (ne choisir qu’une seule option) : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Modèle de services d’infonuagique : IaaS [x]  PaaS [ ]  SaaS [ ]  Réservation du service de GAIP terminée : Oui ☐ Non ☐  | Réussite : [ ] Échec : [ ]  |
| **Mettre en place des garde-fous** | **Évaluation** |
| Avez-vous présenté les données probantes associées aux garde-fous de 30 jours? [ ]  Date de présentation : \_\_\_\_\_\_\_\_\_\_\_\_\_Déploiement du pare-feu ou de l’appareil de gestion unifiée des menaces dotés de capacités RPV : Oui ☐ Non ☐ | Réussite : [ ] Échec : [ ]  |
| **Terminer l’autorisation d’exploitation de l’infrastructure en nuage**  | **Évaluation** |
| Avez-vous rempli votre autorisation d’exploitation de l’infrastructure en nuage? [ ]  | Réussite : [ ] Échec : [ ]  |
| **Préparation à la connectivité** | **Évaluation** |
| Avez-vous signé et présenté l’entente de sécurité sur l’interconnectivité? [ ]  | Réussite : [ ] Échec : [ ]  |
| **Tendances en matière de connectivité (**[**référence**](https://www.gcpedia.gc.ca/gcwiki/images/7/75/GC_Cloud_Connection_Patterns.pdf)**)** | **Évaluation** |
|

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| A1 [ ]   | A2 [ ]   | A3 [ ]  | A4 [ ]  | A5 [ ]  | A6 [ ]  |
| B1 [ ]  | B2 [ ]  | B3 [ ]  | B4 [ ]  | B5 [ ]  | B6 [ ]  |
| C1 [ ]  | C2 [ ]  | C3 [ ]  | C4 [ ]  | C5 [ ]  | C6 [ ]  |
| D1 [ ]  | D2 [ ]  | D3 [ ]  | D4 [ ]  | D5 [ ]  | D6 [ ]  |
| E1 [ ]  | E2 [ ]  | E3 [ ]  | E4 [ ]  | E5 [ ]  | E6 [ ]  |

 | Réussite : [ ] Échec : [ ]  |
| **Tableau sur les flux de réseau** | **Évaluation** |
|

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No du flux** | **Description du flux d’applications** | **Zone source** | **Nom du serveur source** | **IP de la source** | **Besoin d’équilibreurs de charge ou d’intermédiaire?** | **Zone de destination** | **Nom du serveur de destination** | **IP de la destination** | **Port(s)** |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

 | Réussite : [ ] Échec : [ ]  |
| **Diagramme du flux de données**  | **Évaluation** |
| [insérer le diagramme ici] | Réussite : [ ] Échec : [ ]  |
| **Section réservée à l’administration** | **Évaluation** |
| Résultats globaux | Réussite : [ ] Échec : [ ]  |

#

# Appendice B - Liste de vérification sur l’état de préparation à l’infonuagique (exemple)

Cet appendice donne un exemple, à titre illustratif, d’une liste de contrôle dans le cadre d’un scénario fictif.

|  |  |
| --- | --- |
| **Aperçu du projet, de l’initiative ou de l’application** | **Évaluation** |
| Nom du ministère : \_\_\_SPC\_\_\_\_\_\_\_Nom de l’activité ou du projet de la TI du GC (outil Clarity du SCT) : \_\_Examens du GC\_Identifiant de l’activité ou du projet de la TI du GC (outil Clarity du SCT)  : \_\_\_30887\_\_\_Description du projet, de l’initiative ou de l’application : La nouvelle application permettra aux Canadiens d’un bout à l’autre du pays de présenter des examens des produits et services du GC. Les citoyens seront également en mesure de consulter la base de données et d’effectuer des recherches dans cette dernière en fonction du nom, de la catégorie ou de la notation des produits. L’application a été élaborée par le ministère lors du deuxième trimestre de 2019. Les essais auprès des utilisateurs ont été réalisés en septembre au moyen d’un locataire de service infonuagique non classifié et ont donné des résultats favorables. Le ministère demande maintenant l’approbation de faire passer cette application à l’étape de la production. L’application mettra à profit les services d’IaaS dans l’infonuagique publique. La plateforme infonuagique sera basée sur Windows (IIS, .NET, MS SQL) et permettra l’échange de données avec les applications Apache/J2EE au sol. Cela permettra d’assurer la transition harmonieuse des différentes fonctionnalités de l’actuel centre de données à l’infonuagique. Les systèmes actuels seront mis hors service une fois que la transition de l’ensemble des fonctionnalités aura été effectuée (au troisième trimestre du prochain exercice). Une fois la production lancée, tous les nouveaux examens présentés seront entreposés dans la plateforme infonuagique. Les recherches effectuées dans les bases de données permettront d’interroger, à la fois, les enregistrements de la base de données infonuagique et ceux de l’ancienne base de données (au sol). Étant donné que les enregistrements sont récupérés du sol (au moyen de recherches), ils seront entreposés (mémoire cache) dans la base de données infonuagique et seront marqués pour suppression dans l’actuelle base de données. Ce mécanisme engendrera la migration des données, qui passeront du sol à l’infonuagique en fonction de la fréquence et de la demande.  | Réussite : [x] Échec : [ ]  |
| **Obtenir un compte d’informatique en nuage** | **Évaluation** |
| Les deux utilisateurs désignés ont-ils reçu leurs comptes dans le portail de courtier de l’infonuagique du GC? [x] Veuillez fournir votre numéro de demande de gestion des relations avec les clients : \_CR7883457\_\_\_\_\_\_\_\_\_\_\_\_FSI (ne choisir qu’une seule option) : Microsoft Azure Modèle de services d’infonuagique : IaaS [x]  PaaS [x]  SaaS [ ]   | Pass: [x] Fail: [ ]  |
| **Mettre en place des garde-fous** | **Évaluation** |
| Avez-vous présenté les données probantes associées aux garde-fous de 30 jours? [x]  Date de présentation : \_\_2020-02-26\_\_\_\_\_\_\_\_\_\_\_ | Réussite : [x] Échec : [x]  |
| **Terminer l’autorisation d’exploitation de l’infrastructure en nuage**  | **Évaluation** |
| Avez-vous rempli votre autorisation d’exploitation de l’infrastructure en nuage? [x]  | Réussite : [x] Échec : [ ]  |
| **Préparation à la connectivité** | **Évaluation** |
| Avez-vous signé et présenté l’entente de sécurité sur l’interconnectivité? [x]  | Réussite : [x] Échec : [ ]  |
| **Tendances en matière de connectivité (**[**référence**](https://www.gcpedia.gc.ca/gcwiki/images/7/75/GC_Cloud_Connection_Patterns.pdf)**)** | **Évaluation** |
|

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| A1 [ ]   | A2 [ ]   | A3 [ ]  | A4 [ ]  | A5 [x]  | A6 [ ]  |
| B1 [ ]  | B2 [ ]  | B3 [ ]  | B4 [ ]  | B5 [ ]  | B6 [ ]  |
| C1 [ ]  | C2 [ ]  | C3 [ ]  | C4 [ ]  | C5 [ ]  | C6 [ ]  |
| D1 [ ]  | D2 [ ]  | D3 [ ]  | D4 [ ]  | D5 [ ]  | D6 [ ]  |
| E1 [ ]  | E2 [ ]  | E3 [ ]  | E4 [ ]  | E5 [ ]  | E6 [ ]  |

 | Réussite : [x] Échec : [ ]  |
| **Tableau sur les flux de réseau** | **Évaluation** |
|

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No du flux** | **Description du flux d’application** | **Zone source** | **Nom du serveur source** | **IP de la source** | **Besoin d’équilibreurs de charge ou d’intermédiaire?** | **Zone de destination** | **Nom du serveur de destination** | **IP de la destination** | **Port(s)** |
| 1 | Flux de l’Internet à l’infonuagique (extérieur) | Zone publique (ZP) | Tous | Tous | Oui, VIP | Services de réseau essentiels (infonuagique) | LB1 | 201.141.10.10 | 443/tcp |
| 2 | Flux de l’Internet à l’infonuagique (intérieur) | Services de réseau essentiels (infonuagique) | LB1 | 172.16.0.1 | Oui | ZAP infonuagique | www1 – www5 | 172.16.1.3-172.16.1.8(échelle définie) | 80/tcp |
| 3 | Bassin d’applications IIS à .NET  | ZAP infonuagique | www1 – www5 | 172.16.1.3-172.16.1.8 | Non | Cloud App-RZ | App1-App7 | 172.16.2.3 – 172.16.2.10(échelle définie) | 80/tcp |
| 4 | .NET à SQL | Cloud App-RZ | App1-App7 | 172.16.2.3– 172.16.2.10 | Non | Cloud DB-RZ | SQL1 | 172.16.3.5 | 1433/tcp |
| 5 | .NET à LB1 | Cloud App-RZ | App1-App7 | 172.16.2.3– 172.16.2.10 | Oui | Services de réseau essentiels (infonuagique) | LB1 | 172.16.0.1 | 443/tcp |
| 6 | LB1 à intermédiaire REV | Services de réseau essentiels (infonuagique) | LB1 | 172.16.0.1 | Oui, SNAT | ZAP au sol | Apache1 | 142.22.41.3 | 443/tcp |
| 7 | Apache1 à JavaApp2  | ZAP au sol | Apache1 | 142.22.41.3 | Non | Ground App-RZ | JavaApp2  | 142.22.44.3 | 443/tcp |

 | Réussite : [x] Échec : [ ]  |
| **Diagramme du flux de données**  | **Évaluation** |
|  | Réussite : [x] Échec : [ ]  |
| **Section réservée à l’administration** | **Évaluation** |
| Résultats globaux | Réussite : [x] Échec : [ ]  |

# Annexe C - Glossaire des acronymes

**Glossaire**

|  |  |
| --- | --- |
| **Terme** | **Définition** |
| FSIE | Les fournisseurs de services d’infonuagique Exchange (FSIE) sont de tierces entreprises à réseau étendu qui fournissent une connectivité à la fois spécialisée, peu coûteuse, à large bande et à faible latence à un grand nombre de fournisseurs de services d’infonuagique (FSI).  |
| IaaS | L’infrastructure en tant que service désigne différents services infonuagiques, comme l’entreposage, le réseautage et la virtualisation. |
| PaaS | La plateforme en tant que service désigne différents outils matériels et logiciels qui sont accessibles en ligne pour permettre aux clients de développer, d’exécuter et de gérer des applications, sans devoir composer avec les tâches complexes d’établir et de maintenir l’infrastructure qui sont habituellement associées au développement et au lancement des applications. |
| Infonuagique privée | L’infonuagique privée désigne des services informatiques offerts en ligne ou par l’intermédiaire d’un réseau interne privé à des utilisateurs précis plutôt qu’au grand public. L’infonuagique privée peut donc être déployée « sur place » dans un centre de données protégé par un pare-feu. |
| Infonuagique publique | L’infonuagique publique est un service informatique offert par des fournisseurs tiers sur l’Internet public. Ses services sont donc accessibles à quiconque souhaite les utiliser ou les acheter.  |
| SaaS | Le logiciel comme service est un modèle de gestion de licences et de prestation de services logiciels dans le cadre duquel des logiciels sont concédés sous licence après abonnement et sont hébergés de façon centralisée. Les applications de SaaS sont également connues sous le nom de logiciels Web, sur demande et hébergés. |

## Liste des acronymes

| Acronyme | Nom complet |
| --- | --- |
| RENI | Réseau d’expertise sur le nuage et l’informatique |
| FSI | Fournisseur de services d’infonuagiques |
| FSIE | Fournisseur de services d’infonuagique Exchange (FSIE) |
| CEAE du GC | Conseil d’examen de l’architecture d’entreprise du gouvernement du Canada |
| IaC | Infrastructure en tant que code |
| PaaS | Plateforme en tant que service |
| IaaS | Infrastructure en tant que service |
| SaaS | Logiciel en tant que service |
| SA&A | Évaluation de sécurité et autorisation |