Architecture de référence pour le zonage de la sécurité des réseaux

Architecture d’entreprise, direction générale du DPT

État : **En cours**

Version du document : **10**

Date de publication : à déterminer

Classification de sécurité : **NON CLASSIFIÉ**

Approbation du document

Les signataires autorisés indiqués ci-dessous acceptent les modalités et les responsabilités décrites dans le présent document.

|  |  |  |  |
| --- | --- | --- | --- |
| Victor Ulitsky | Directeur général  Architecture d’entreprise  Direction générale du dirigeant principal de la technologie  Services partagés Canada | Date | Signature |
| Mathieu Fortin | Directeur,  Liaison pour l’architecture d’entreprise partenaire  Direction générale du dirigeant principal de la technologie  Services partagés Canada | Date | Signature |

Historique du document

Le présent Document relatif à l’architecture de référence est visé par des mesures officielles de gestion architecturale. À l’achèvement de l’élaboration du présent objet, désigner clairement les participants et les comités auxquels le document a été distribué et qui ont approuvé celui-ci.

| Ver.  no | Date | Personnes consultées/réviseurs  (nom de la personne et du groupe de travail consultés) | Brève description des changements | Auteur de la modification |
| --- | --- | --- | --- | --- |
| 0.1 | 2019-03-31 | Reportez-vous à l’annexe B. | Ébauche initiale | Andrew Wykurz |
| 0.2 | 2019-05-24 | Reportez-vous à l’annexe B. | Mise à jour de la section 4 des modèles d’architecture avec des descriptions améliorées et des modèles plus clairs. Les instructions relatives au contenu du document ont également été supprimées. | Andrew Wykurz |
| 0.3 | 2019-06-18 | Reportez-vous à l’annexe B. | Mise à jour de la section 4, ajout des artefacts de sécurité manquants | Yacin Abdallah |
| 0.4 | 2019-07-18 | Reportez-vous à l’annexe B. | Mise à jour de la section 4, ajout de Connectivité nuage-sol et Internet du GC | Yacin Abdallah |
| 0.5 | 2020-07-15 | Reportez-vous à l’annexe B. | Mise à jour en fonction de l’examen de l’AE | Yacin Abdallah |
| 0.6 | 2020-07-27 | Reportez-vous à l’annexe B. | Mise à jour de la section 4.6.5, modification de la connexion CG-TIP vers le nuage. Nous avons également supprimé AWS du titre de la section, car le modèle prend en charge à la fois AWS et Azure. | Yacin Abdallah |
| 0.7 | 2020-08-19 | Walter Sokyrko | Intégration des commentaires reçus lors de la présentation du Conseil d’architecture (2020-07-27).  Suppression de la mention PROVISOIRE. | Claude Vallée |
| 08 | 2020-09-03 | Reportez-vous à l’annexe B. | Mise à jour de la section 1.1.1 sur la base de la recommandation du Groupe de gestion de la sécurité (GGS) | Yacin Abdallah |
| 09 | 2020-09-22 | Conseil d’examen de l’architecture des services (CEAS) Recommandations | Mis à jour sur la base de la recommandation du CEAS | Yacin Abdallah |
| 10 | 2020-11-08 | Recommandation du Groupe de travail de la recherche sur les politiques (GTRP) | Mis à jour sur la base de la recommandation du GTRP | Yacin Abdallah |

Table des matières

[1 Introduction 1](#_Toc73605204)

[1.1 Organisme faisant autorité 1](#_Toc73605205)

[1.1.1 Rôles, responsabilités (RACI) 2](#_Toc73605206)

[1.2 Objectif 2](#_Toc73605207)

[1.3 Contexte 2](#_Toc73605208)

[1.4 Portée 3](#_Toc73605209)

[1.4.1 Exceptions 4](#_Toc73605210)

[1.5 Vision, buts et objectifs 4](#_Toc73605211)

[1.5.1 Points de vue sur les affaires et la motivation 5](#_Toc73605212)

[1.6 Concept opérationnel de haut niveau 5](#_Toc73605213)

[1.6.1 Architecture opérationnelle 6](#_Toc73605214)

[1.6.2 Perspective opérationnelle 7](#_Toc73605215)

[1.6.3 Modèles d’entreprises générales du gouvernement du Canada 8](#_Toc73605216)

[1.6.4 Modèle d’interopérabilité des ministères du GC 9](#_Toc73605217)

[1.6.5 Définitions 10](#_Toc73605218)

[1.6.5.1 Zone publique (ZP) 10](#_Toc73605219)

[1.6.5.2 Zone d’accès public (ZAP) 11](#_Toc73605220)

[1.6.5.3 Zone des opérations (ZO) 11](#_Toc73605221)

[1.6.5.4 Zone d’accès restreint (ZAR) 12](#_Toc73605222)

[1.6.5.5 Zone d’accès très restreint (ZATR) 12](#_Toc73605223)

[1.6.5.6 Zone extranet d’accès restreint (ZEAR) 13](#_Toc73605224)

[1.6.5.7 Zone de gestion restreinte (ZGR) 13](#_Toc73605225)

[1.6.5.8 Zone d’accès spécial (ZAS) 13](#_Toc73605226)

[1.7 Liens avec d’autres architectures, programmes et initiatives 13](#_Toc73605227)

[2 Principales orientations 15](#_Toc73605228)

[2.1 Principes 15](#_Toc73605229)

[2.2 Facteurs 15](#_Toc73605230)

[3 Normes et politiques 16](#_Toc73605231)

[3.1 Normes 16](#_Toc73605232)

[3.2 Politiques 16](#_Toc73605233)

[4 Modèles d’architecture 17](#_Toc73605234)

[4.1 Vue d’interaction des zones interentreprises départementales 17](#_Toc73605235)

[4.2 Concepts de zone de sécurité 17](#_Toc73605236)

[4.2.1 Les points d’interface de zone (PIZ) et leurs fonctions de sécurité 18](#_Toc73605237)

[4.2.2 Zone d’opérations et PIZ 20](#_Toc73605238)

[4.2.3 Zone d’accès public et PIZ 21](#_Toc73605239)

[4.2.4 Zone d’accès restreint aux applications Internet et PIZ 22](#_Toc73605240)

[4.2.5 Zone restreinte et ZAR PIZ 23](#_Toc73605241)

[4.2.6 ZARD et PIZ 24](#_Toc73605242)

[4.2.7 Gestion ZAR et PIZ 25](#_Toc73605243)

[4.3 Zonage du réseau de haut niveau 25](#_Toc73605244)

[4.4 Zones de gestion restreinte 27](#_Toc73605245)

[4.5 Vues des applications, des informations et des données 28](#_Toc73605246)

[4.5.1 Vues des applications 29](#_Toc73605247)

[4.6 Scénarios de zonage du nuage 29](#_Toc73605248)

[4.6.1 CDE SPC et intégration des services en nuage 30](#_Toc73605249)

[4.6.2 Vue de zonage du nuage hybride du service 31](#_Toc73605250)

[4.6.3 Les services passent à l’hébergement en nuage complet 33](#_Toc73605251)

[4.6.4 Zones infonuagiques 34](#_Toc73605252)

[4.6.5 Connectivité nuage-sol et Internet du GC 37](#_Toc73605253)

[4.7 Internet des objets 38](#_Toc73605254)

[4.8 Interopérabilité de l’accès des organismes gouvernementaux partenaires (OGP) d’autres ministères (AM) 40](#_Toc73605255)

[5 Glossaire des termes et des acronymes 42](#_Toc73605256)

[5.1 Glossaire 42](#_Toc73605257)

[5.2 Acronymes 42](#_Toc73605258)

[6 Références 44](#_Toc73605259)

[Annexe A Notation ArchiMate® 47](#_Toc73605260)

[Annexe B Collaborateurs et réviseurs 50](#_Toc73605261)

Liste des figures

[Figure 1. Modèle de motivation pour le zonage du réseau 5](#_Toc73604129)

[Figure 2. Contexte de la prestation de service GC 6](#_Toc73604130)

[Figure 3. Vue opérationnelle de SPC 7](#_Toc73604131)

[Figure 4. Vue interentreprises du ministère 8](#_Toc73604132)

[Figure 5. Modèle d’interopérabilité des ministères du GC 9](#_Toc73604133)

[Figure 6. Modèle de mise en œuvre de la zone de sécurité du réseau   
dans l’état actuel 10](#_Toc73604134)

[Figure 7. Vue d’interaction des zones interentreprises départementales 17](#_Toc73604135)

[Figure 8. PIZ et fonctions de sécurité 19](#_Toc73604136)

[Figure 9. Vue de la zone des opérations et des services PIZ 20](#_Toc73604137)

[Figure 10. Vue des services ZAP et PIZ de la ZAP 21](#_Toc73604138)

[Figure 11. Vue de la zone restreinte de l’application Internet et des services PIZ 22](#_Toc73604139)

[Figure 12. Vue des services de zone restreinte et de PIZ de la ZAR 23](#_Toc73604140)

[Figure 13. Vue des services ZARD et PIZ 24](#_Toc73604141)

[Figure 14. Vue des services PIZ et ZAR 25](#_Toc73604142)

[Figure 15. Du CDE au nuage SaaS 26](#_Toc73604143)

[Figure 16. Du centre de données virtuel (CDV) au nuage SaaS 27](#_Toc73604144)

[Figure 17. Zones du réseau du GC 28](#_Toc73604145)

[Figure 18. Dépendance des objets d’application pour le zonage du réseau 29](#_Toc73604146)

[Figure 19. Vue de l’intégration des services hébergés dans le nuage 30](#_Toc73604147)

[Figure 20. Vue de zonage du nuage hybride du service 32](#_Toc73604148)

[Figure 21. Aperçu de l’hébergement en nuage complet 33](#_Toc73604149)

[Figure 22. Zones du réseau infonuagiques 35](#_Toc73604150)

[Figure 23. Connectivité nuage-sol et Internet du GC pour AWS 36](#_Toc73604151)

[Figure 24. Internet des objets 38](#_Toc73604152)

[Figure 25. Aperçu de l’interopérabilité de l’accès des OGP/AM 40](#_Toc73604153)

[Figure 26. Concepts ArchiMate® de premier niveau 46](#_Toc73604154)

[Figure 27. Concepts de base ArchiMate® 47](#_Toc73604155)

[Figure 28. Prorogations ArchiMate® 47](#_Toc73604156)

[Figure 29. Relations avec ArchiMate® 48](#_Toc73604157)

Liste des tableaux

[Tableau 1. Rôles, responsabilités (RACI) 2](#_Toc73604158)

[Tableau 2. Revu et endossé par 49](#_Toc73604159)

# Introduction

Une architecture de référence (AR) est une description qui fournit un plan ou un modèle de description de la solution à un problème. Les architectures de référence facilite la gestion de la complexité et sont des outils essentiels qui permettent à SPC et à ses partenaires de diriger, de guider et de contraindre les architectures de solution (SA) en fournissant des informations communes, des conseils, des normes et une orientation qui permettent le développement de solutions efficaces et efficientes. Pour être plus efficaces, les AR doivent être élaborées sur la base de principes architecturaux solides et répondre à des normes communes en termes de forme et de contenu. Le présent document d’architecture de référence (DAR) constitue la première étape de l’établissement de ce processus de création d’AR cohérentes et complètes.

Une AR est un modèle d’architecture éprouvé existant qui représente l’état actuel de l’informatique tel que défini par l’architecture actuelle pour un domaine donné. Dans ce document, le guide de sécurité ITSG-22 est la référence de l’état actuel. Elle contribuera à réduire le temps et les efforts nécessaires à la conception et au développement des solutions.

Le langage de modélisation de l’architecture d’entreprise ArchiMate est utilisé tout au long de ce document pour illustrer les concepts et les exemples. ArchiMate est une norme technique de The Open Group et est basée sur les concepts de la norme IEEE 1471. Elle est soutenue par divers vendeurs d’outils et sociétés de conseil. Une brève introduction à la notation de modélisation ArchiMate est fournie à l’annexe A. Des informations supplémentaires concernant la spécification ArchiMate sont disponibles sur le site [Web de l’Open Group](https://www.opengroup.org/archimate-forum/archimate-overview)[[1]](#footnote-1).

## Organisme faisant autorité

Le présent document contient des contributions de, et a été révisé par, de nombreux experts en la matière, y compris les principales PME listées dans l’annexe B.

Les demandes de renseignements sur le présent document doivent être adressées à la personne désignée qui assure la liaison avec SPC au sein du ministère concerné. Le point de contact exact reste à déterminer.

### Rôles, responsabilités (RACI)

Dans cette section, nous déterminerons les rôles et les responsabilités de la matrice RACI (Responsable, Autorité, Contributeur/ Consultant, Informé)

| Processus d’architecture de référence pour le zonage du réseau | SPC | Cyber SCT | CST/CCC | Partenaires |
| --- | --- | --- | --- | --- |
| Conception/mise en œuvre du service | A/R | C | C | I |
| Conseils et orientation | A/R | R | R | I |
| Conformité (c.-à-d. GC CEAI, ITSG-22) | R | A | R | R |
| Maintenance (mises à jour) | A/R | C | C | C |

Tableau 1. Rôles, responsabilités (RACI)

**R**esponsable : Avoir l’obligation de mener à bien un processus

***A***utorité : Autorité décisionnelle censée garantir la bonne fin d’un processus.

**C**onsulté : Consulté pour obtenir des détails et des informations supplémentaires sur un processus.

**I**nformé : Mise au courant de l’état des conditions

**Conception :** L’objectif principal des concepteurs/ingénieurs est la conception technique globale et l’ingénierie d’éléments précis du service, du projet et des architectures d’entreprise. Ils fournissent à l’architecte de services et à l’architecte de solutions une expertise propre au domaine afin de concevoir les spécifications techniques nécessaires aux exigences liées à l’élaboration et à l’intégration des systèmes.

**Maintenance** : S’assurer que les exigences de cette architecture de référence du zonage du réseau sont alignées avec ITSG-22 chaque fois qu’un changement se produit.

## Objectif

Le présent document d’architecture de référence (DAR) a pour objet de décrire le zonage du réseau afin que les ministères et organismes du gouvernement du Canada (GC) puissent utiliser le zonage du réseau pour améliorer leur posture de sécurité.

## Contexte

Dans le contexte de l’excellence des services, de l’innovation et de l’optimisation des ressources, SPC a le mandat de maintenir et d’améliorer la prestation des services d’infrastructure de TI tout en renouvelant l’infrastructure de TI vieillissante de l’administration fédérale. SPC adopte une véritable perspective d’entreprise à l’égard des projets d’infrastructure de TI de l’État, non seulement pour améliorer le service, mais aussi pour éliminer le double emploi et réduire les coûts. Un des aspects importants de ce travail est l’élaboration de normes de service à l’échelle du ministère, précédemment établies et maintenues par chacune des 43 organisations partenaires dans leur propre milieu de travail, normes qui sont désormais en cours d’élaboration collective à l’échelle du GC.

En collaboration avec ses partenaires et grâce aux conseils offerts par l’industrie, SPC est en train de déterminer les exigences visant l’infrastructure de TI de l’administration fédérale et d’appliquer des pratiques exemplaires pour relever les défis opérationnels et atteindre les objectifs de l’administration en matière de modernisation. L’établissement d’une structure plus sécuritaire et plus solide pour soutenir les activités actuelles renforce aussi la capacité de protéger les renseignements personnels de la population canadienne.

Le zonage fait partie des directives de sécurité du GC, mais n’est généralement pas suivi pour diverses raisons. Compte tenu de l’essor du CDE et du nuage, il est possible et nécessaire de mettre en œuvre cette exigence.

## Portée

La présente architecture de référence s’applique au domaine de la TI du gouvernement fédéral sous la supervision de Services partagés Canada (SPC) pour l’hébergement de SPC, de ses partenaires et clients au sein du domaine protégé. Le domaine protégé se limite à la confidentialité du matériel de niveau Protégé B et de niveau inférieur (préjudice non national moyen ou moindre).

Ce document définit les zones et la circulation de l’information de haut niveau qui est permise entre les zones. Il doit être utilisé de concert avec un document d’accompagnement plus détaillé qui définit les exigences de sécurité au sein des différentes zones de sécurité.

### Exceptions

Les anciens services de SPC (par ex. les services qui n’ont pas été convertis par un programme de SPC tels que le programme de regroupement des centres de données, le Programme de transformation des télécommunications, etc.), peuvent ne pas être conformes à la présente architecture de référence. On s’attend à ce que l’infrastructure non conforme au sein du domaine de la TI du gouvernement du Canada (GC) de niveau Protégé soit transformée avec le temps; transformation pendant laquelle le respect de la présente architecture est requis.

Le présent document ne concerne pas les ministères qui ne sont pas partenaires de SPC, puisque ceux-ci peuvent exploiter leur propre domaine de TI et devraient avoir leur propre norme relative aux zones de sécurité.

## Vision, buts et objectifs

Cette architecture de référence ne constitue pas un document de conception à lui seul. Il s’agit plutôt d’un document de base pouvant être utilisé :

* Pendant la conception générale de l’infrastructure de TI de SPC
* Comme guide lors de la conception du réseau de services et de partenaires.

Ce document d’architecture de référence doit être utilisé de concert avec un document d’accompagnement plus détaillé qui définit les exigences de sécurité au sein des différentes zones de sécurité.

### Points de vue sur les affaires et la motivation

Le modèle de motivation pour le zonage du réseau est l’un des modèles les plus importants, car il représente les liens entre les processus/solutions d’entreprise et les principales parties prenantes d’une architecture.

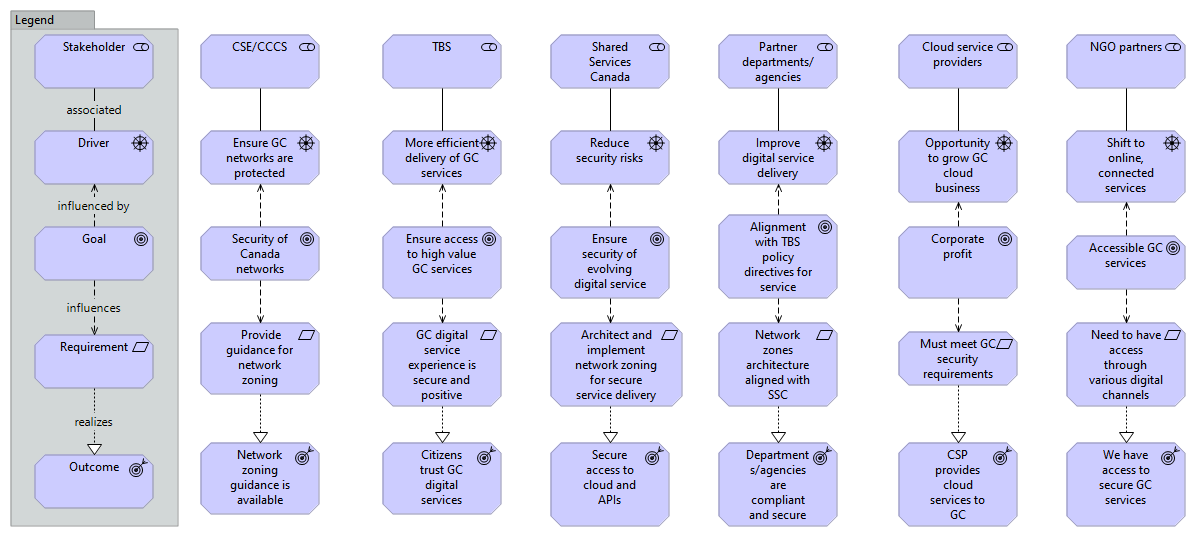


Figure 1. Modèle de motivation pour le zonage du réseau

La figure 1 ci-dessus utilise le langage de modélisation de l’architecture d’entreprise (AE)de The Open Group ArchiMate 3.0.1, qui est un langage visuel avec un ensemble d’iconographies par défaut pour décrire, analyser et communiquer de nombreuses préoccupations de l’AE. Un aperçu des concepts d’ArchiMate figure à l’annexe A ou un lien vers la spécification détaillée est disponible à la réf. E.

La colonne Légende de la figure détermine le type d’élément (objet) pour chaque ligne de ce diagramme matriciel 5x6 et les colonnes sont les perspectives spécifiques des parties prenantes. Les modèles ArchiMate sont utilisés tout au long de ce document AR pour illustrer les concepts et les informations sur les cas d’utilisation spécifiques. Les lecteurs sont invités à se familiariser avec le langage de modélisation ArchiMate AE pour comprendre pleinement les informations fournies dans les figures.

## Concept opérationnel général

### Architecture opérationnelle

La fonction principale des ministères est de fournir des services gouvernementaux aux citoyens et aux entreprises du Canada. Les attentes des consommateurs en matière de service sont plus élevées que jamais et les entreprises ne cessent de relever la barre en matière de prestation de services numériques. Les services gouvernementaux sont sous pression pour fournir en toute sécurité des services de grande valeur. Le modèle suivant montre comment les ministères et les organismes fournissent des services gouvernementaux aux organisations du secteur privé, aux autres ministères/organismes partenaires, aux organisations non gouvernementales et, surtout, aux citoyens ou aux particuliers.

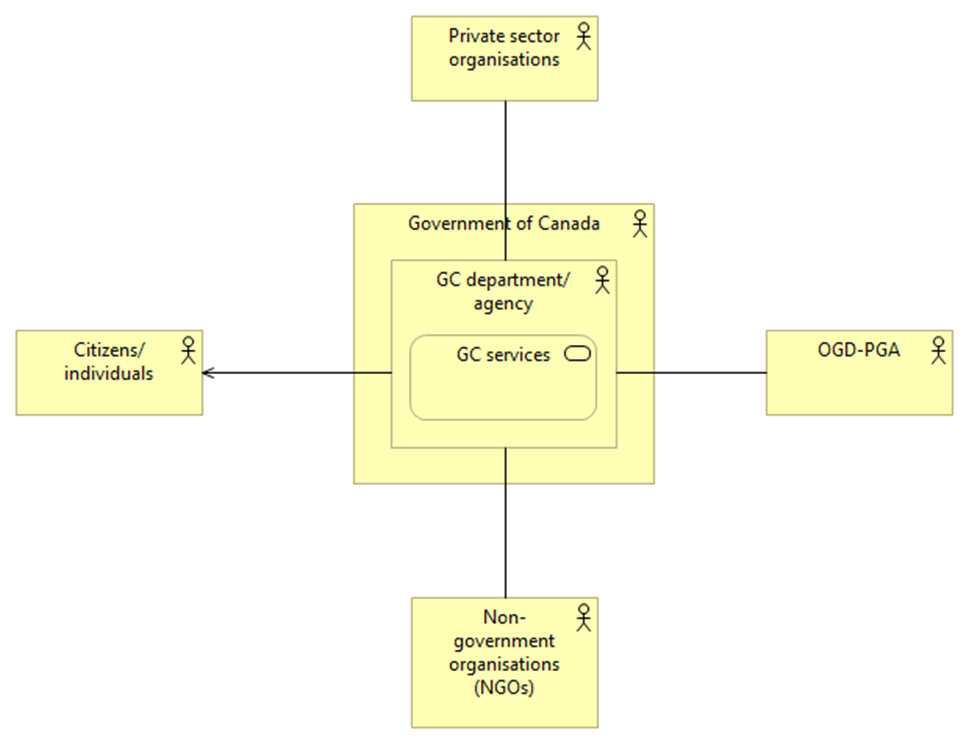


Figure 2. Contexte de la prestation de service GC

### Perspective opérationnelle

Le modèle suivant se concentre sur la vue opérationnelle de SPC, où SPC fournit aux partenaires des services d’infrastructure, de réseau et de sécurité.

Ce point de vue soutient le « nuage d’abord » du GC basé sur les normes architecturales du GC pour l’alignement numérique auxquelles tous les ministères doivent se conformer.

SPC est associé à son « mandat », représenté ici comme un moteur (élément moteur d’ArchiMate), pour regrouper et fournir des services de technologie de l’information et d’infrastructure de réseau. Le modèle dépeint cette relation entre la partie SPC et les services généraux comme une affectation. Les services technologiques pertinents du GC (au zonage réseau) se composent des opérations du centre de données et des services de réseau et de télécommunication qui servent les partenaires du GC. Sur le côté droit, les services de gestion des fournisseurs du GC sont associés à une fonction de courtage qui est associée aux services du nuage du GC, qui à leur tour servent les partenaires du GC de SPC.

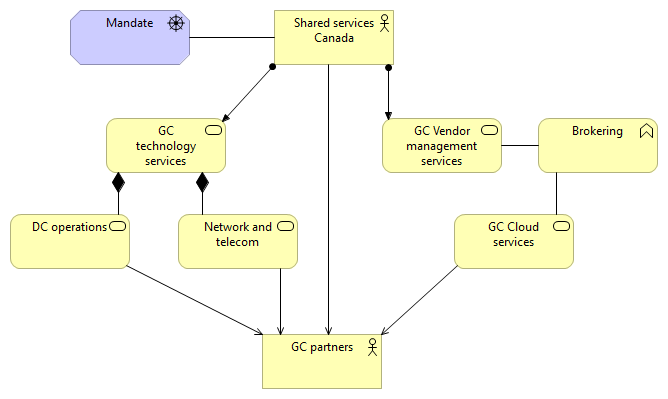


Figure 3. Vue opérationnelle de SPC

### Modèles opérationnels généraux du gouvernement du Canada

Le modèle suivant illustre une intégration générique interentreprises entre un ministère/organisme du GC et des organisations du secteur privé et/ou des organisations non gouvernementales. Il existe un flux d’informations bidirectionnel entre les entités externes et les applications du GC et les données du GC qui est médiatisé à la fois par les services de sécurité et les services technologiques interentreprises.

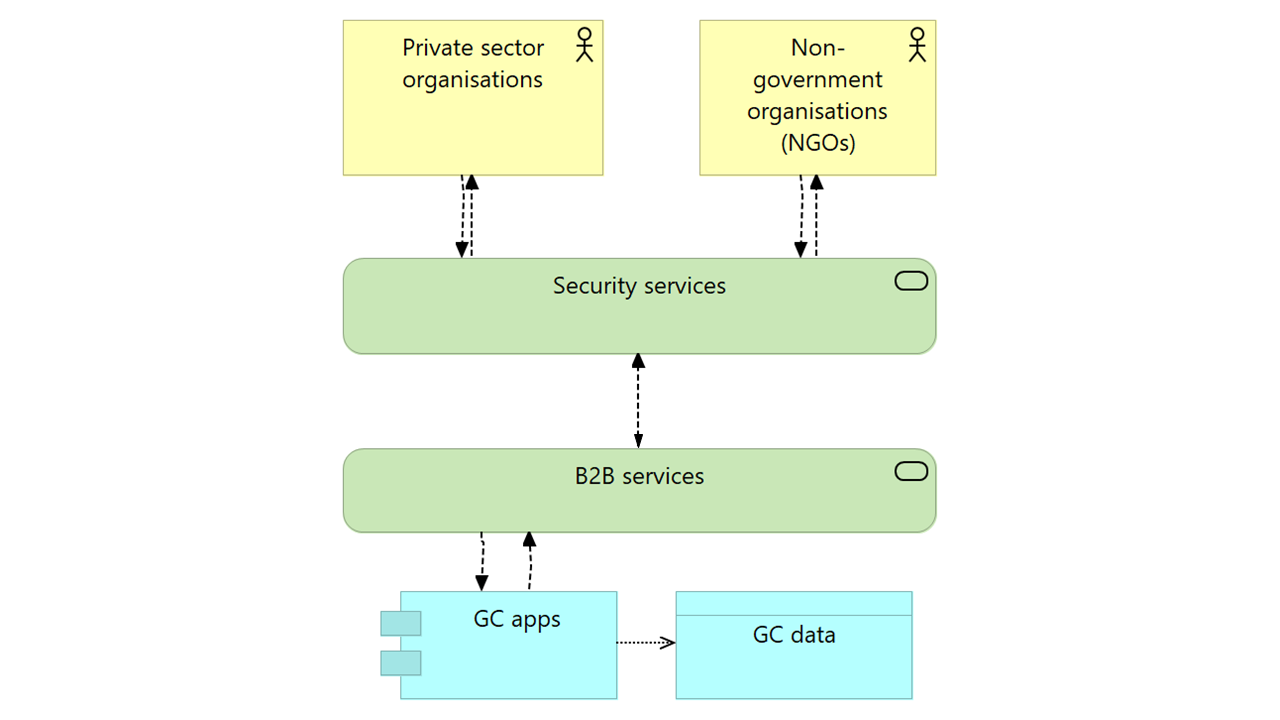


Figure 4. Vue interentreprises du ministère

### Modèle d’interopérabilité des ministères du GC

La figure 5 fournit une vue d’ensemble du modèle d’interopérabilité actuel des ministères du GC. Les ministères du GC travaillent et collaborent avec des partenaires externes ou des organisations non gouvernementales (ONG) et des partenaires gouvernementaux ainsi que des citoyens. L’Internet des objets (IdO) connaît une croissance rapide avec un nombre croissant d’appareils intelligents connectés aux personnes et aux réseaux dans le monde entier.

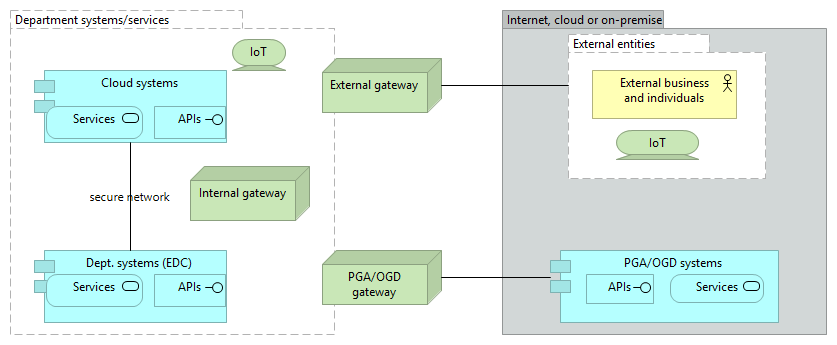


Figure 5. Modèle d’interopérabilité des ministères du GC

### Définitions

Les définitions des types de zones de sécurité et de leurs éléments proviennent de ITSG-22 [Réf. B] qui est la référence de l’état actuel pour ce document. Elles sont reproduites ici pour des raisons pratiques. D’autres définitions sont fournies à la section 5 Glossaire des termes et des acronymes.

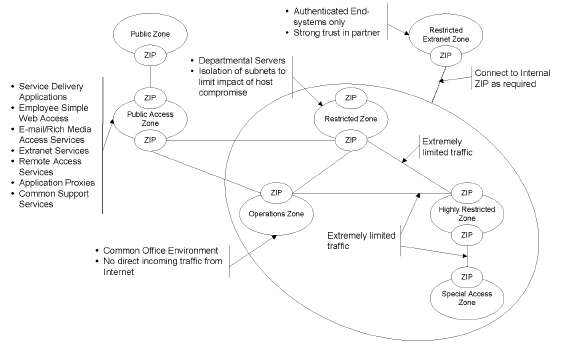


Figure 6. Modèle de mise en œuvre de la zone de sécurité du réseau dans l’état actuel[[2]](#footnote-2)

#### Zone publique (ZP)

La zone publique (ZP) est entièrement ouverte. Elle englobe les réseaux tels qu’Internet, le réseau téléphonique commuté et d’autres réseaux fédérateurs et services publics de télécommunication. La mise en place ou l’application de restrictions et d’exigences pour cette zone est très difficile, voire impossible, car elle échappe normalement au contrôle que peut exercer le GC en tant que propriétaire du système. L’environnement de la ZP est présumé extrêmement hostile. Tous les systèmes installés dans une ZP ou qui interagissent avec un système d’une ZP devraient être renforcés pour résister aux attaques.

Le fait que la ZP soit supposément extrêmement hostile n’interdit pas à une autorité de zone de sécurité de réseau d’utiliser les services de sécurité des fournisseurs publics. En fait, cette pratique est encouragée, car elle renforce la posture de défense en profondeur. Cependant, il serait extrêmement imprudent de négliger l’ampleur de la menace que représente une ZP lors de l’élaboration des exigences de sécurité de base.

#### Zone d’accès public (ZAP)

Le rôle de la zone d’accès public (ZAP) consiste à négocier les accès entre les systèmes opérationnels du GC et la zone publique. Les interfaces de tous les services du gouvernement en direct devraient être mises en œuvre dans une ZAP. Les services de serveur mandataire qui permettent aux employés du gouvernement d’accéder aux applications Web devraient être mis en œuvre dans une ZAP, de même que les passerelles de courrier électronique externe, d’accès à distance et d’extranet.

Une ZAP est un environnement sous étroite surveillance qui permet de protéger les réseaux et les applications internes du GC contre d’éventuelles attaques hostiles provenant de la ZP. La ZAP sert également d’écran pour masquer les ressources internes de la zone publique et limiter leur exposition.

Il convient de noter que l’accès à distance, mentionné ci-dessus, ne comprend que les mises en œuvre qui fournissent un accès complet aux ressources sur les réseaux internes du GC. Certaines solutions d’accès à distance, notamment l’accès par le réseau téléphonique public commuté, permettent de contrôler à distance des hôtes spécifiques sur des réseaux internes (p. ex., des serveurs de terminaux). Ces mises en œuvre basées sur l’hôte sont plus restrictives et ne fournissent qu’une fenêtre de terminal sur le réseau interne. Ces solutions sont des applications de prestation de services et les exigences de sécurité pour les applications de prestation de services s’appliquent comme indiqué dans le modèle d’architecture fédérée[[3]](#footnote-3).

#### Zone des opérations (ZO)

La zone des opérations (ZO) est l’environnement standard dans lequel sont exécutées les activités courantes du GC. C’est là que sont installés la plupart des systèmes d’utilisateur et des serveurs d’équipes de travail. Lorsque les systèmes d’extrémité sont munis de contrôles de sécurité appropriés, la zone de sécurité peut convenir au traitement de renseignements sensibles. Toutefois, elle ne convient généralement pas aux grands répertoires de données sensibles ni aux applications critiques sans contrôles de sécurité supplémentaires solides et fiables qui dépassent le cadre de la présente ligne directrice[[4]](#footnote-4).

Dans une ZO, le trafic est généralement non restreint et peut provenir de sources internes ou des sources externes autorisées par l’intermédiaire de la ZAP. Parmi les exemples de sources externes de trafic, on peut mentionner l’accès à distance, l’accès mobile et les extranets. Le trafic malveillant peut provenir de sources hostiles internes programmes hostiles importés de la zone publique ou de nœuds malveillants non détectés sur le réseau (par exemple, un hôte compromis ou une connexion sans fil non autorisée à la zone).

#### Zone d’accès restreint (ZAR)

Une zone d’accès restreint (ZAR) procure un environnement de réseau contrôlé habituellement adapté aux services de TI essentiels (ceux pour lesquels on a établi des exigences moyennes sur le plan de la fiabilité, mais où une interruption des services de TI entraînerait un arrêt des activités) ou pour des dépôts volumineux d’informations sensibles (comme un centre de données). Elle permet l’accès depuis des systèmes situés dans la zone publique par l’intermédiaire d’une ZAP. Toutes les entités de la couche réseau d’une ZAR sont authentifiées, soit explicitement, par la mise en œuvre d’un service d’authentification de l’entité homologue, soit implicitement, par une combinaison de mesures de sécurité matérielle et d’un contrôle rigoureux de la configuration. La ZAR réduit les menaces en provenance de l’intérieur du système en limitant les accès et en appliquant des mesures de surveillance administrative. Les services de confidentialité des données sont établis à l’intérieur de la ZAR pour les protéger de l’écoute clandestine par des nœuds non autorisés. Ces services peuvent être mis en œuvre au niveau du réseau ou au moyen de la sécurité des supports.

#### Zone d’accès très restreint (ZATR)

Une zone d’accès très restreint fournit un environnement réseau bien contrôlé qui convient généralement aux applications critiques pour la sécurité (par ex. ceux qui ont des exigences de fiabilité élevées, lorsque l’interruption des services de TI mettrait en danger la santé ou la sécurité humaine) ou aux vastes dépôts d’informations sensibles. Seules les autres zones contrôlées par le GC peuvent accéder à une ZATR (c.-à-d. qu’il n’y a pas d’accès par les systèmes de la zone publique). Toutes les entités de la couche réseau d’une ZATR sont authentifiées, soit explicitement, par la mise en œuvre d’un service d’authentification de l’entité homologue, soit implicitement, par une combinaison de mesures de sécurité matérielle et d’un contrôle rigoureux de la configuration. En général, la ZATR a des exigences plus strictes pour les systèmes finaux que la zone publique. Elle impose également des contrôles plus stricts sur les initiés du système pour faire face aux menaces provenant de cette source. Des services de confidentialité des données, adaptés à la protection des informations sensibles, sont également mis en œuvre dans une ZATR pour protéger le trafic de la zone contre l’écoute par des nœuds non autorisés. Ces services peuvent être mis en œuvre soit au niveau du réseau, soit au niveau de la couche physique. Des mesures peuvent être nécessaires pour prévoir une protection contre l’accès non autorisé aux émissions électroniques.

#### Zone extranet d’accès restreint (ZEAR)

Une ZEAR prend en charge les services extranet directement connectés (c.-à-d. non connectés par une ZAP, voir figure 6) avec des partenaires de confiance. Cette zone peut être considérée comme une extension logique des zones internes vers des organismes partenaires extérieurs au GC. Les exigences et les pratiques liées à de telles zones seraient élaborées au cas par cas et appliquées au moyen d’ententes avec les partenaires;

Les exemples possibles de ZEAR sont les suivants :

* Intégration avec les institutions financières
* Environnements informatiques externalisés
* Interfaces fédérales-provinciales
* Interfaces avec les autres gouvernements.

Les connexions entre les services du GC n’utilisent pas de ZEAR. Une ZEAR est seulement pour les connexions à des organisations en dehors du GC. Les connexions entre les services se feraient par des connexions directes de zone à zone (p. ex. ZO à ZO, ZO à ZAP à ZO, ZAR à ZAR, ZAR à ZAP à ZAR, ZATR à ZATR).

#### Zone de gestion restreinte (ZGR)

Les architectures de réseau ministériel et de réseau de services Internet comportent une zone d’accès restreint conçue spécifiquement pour les activités de gestion, appelée « Zone de gestion restreinte ». Cette zone regroupe les services liés à l’administration des TI nécessaires pour l’exploitation du réseau ministériel ou du réseau de services Internet.

Les services situés dans la ZAR de gestion ne communiquent avec la zone publique par la ZAP que pour les mises à jour provenant d’un site du réseau du fournisseur, en utilisant des mesures de sécurité appropriées qui protègent l’intégrité et la confidentialité de la communication et authentifient l’adresse du réseau du fournisseur.

#### Zone d’accès spécial (ZAS)

Une ZAS est un environnement réseau contrôlé qui convient aux besoins de traitement spéciaux. Les exigences d’une ZAS seraient élaborées au cas par cas pour répondre aux besoins spéciaux de traitement de l’environnement. Des mesures peuvent être nécessaires pour prévoir une protection contre l’accès non autorisé aux émissions électroniques. Les limites de la technologie de sécurité peuvent empêcher les connexions du réseau aux autres zones.

## Liens avec d’autres architectures, programmes et initiatives

Les architectures de référence qui pourraient être informatives sont :

* GCCOF - Cadre d’accueil du nuage GC - SPC/AE
* GC E2E Net - Réseau de bout en bout du GC DAR - SPC/AE
* CDE DAR - SPC/AE
* ADNS – Activation et défense du nuage sécurisé, SPC gestion de la sécurité et de la gouvernance.
* SRAD - Document relatif à l’architecture de référence- SPC gestion de la sécurité et de la gouvernance.

D’autres sources d’information utilisées dans la préparation de cette AR sont :

* GC Stratégies et services d’architecture d’entreprise, y compris :
* UnGC
* Connexion Canada
* Cadre de confiance pancanadien [Réf. L],
* Services d’authentification centralisés internes du GC (GCpass - le service d’authentification centralisé interne du GC [ICAS]) [Réf. K],
* Plateforme d’échange numérique,
* Données ouvertes.
* Normes numériques du GC et principes architecturaux de l’AE du GC
* Stratégie de données du GC
* Instruments des politiques du gouvernement du Canada
* Normes architecturales du GC pour l’alignement numérique [Réf. H]
* Cadre de l’architecture d’entreprise du GC [Réf. I]
* Normes architecturales existantes du gouvernement du Canada [Réf. J]
* Architecture de sécurité et de la protection des renseignements personnels de l’entreprise du GC [Réf. M]
* Architecture de sécurité intégrée (ASI) [Réf. N]
* Gouvernement du Canada - Architecture fédérée - Itération un [Réf. O]

# Principales orientations

## Principes

Les principes sont des définitions générales des valeurs fondamentales qui guident les décisions prises concernant la gestion des affaires, de l’information, des applications, de la technologie, de la sécurité et de la protection des renseignements personnels.

Les principes de l’architecture d’entreprise de SPC qui sont destinés à être utilisés comme guide lors de l’examen de l’introduction de solutions de service ou de changements qui sont permis par les processus, les systèmes ou la technologie.

Les neuf principes prioritaires s’appuient et s’alignent sur les principes directeurs des autres sources stratégiques du GC et de SPC.

1. Adopter une approche opérationnelle
2. L’entreprise d’abord
3. Comprendre les besoins des clients
4. Sécurité et protection des renseignements personnels
5. Fiabilité et disponibilité
6. Variabilité d’échelle et durabilité
7. Couplage souple et modularité
8. Automatiser
9. Mesure et contrôle

Les descriptions détaillées des principes, leur justification et les détails des incidences se trouvent dans les [principes de l’EA](https://gcdocs.gc.ca/ssc-spc/llisapi.dll?func=ll&objaction=overview&objid=60300911) de SPC.

## Facteurs

La figure 1 de la section 1.5.1 ci-dessus fournit un exemple de divers facteurs associés à des intervenants précis.

# Normes et politiques

Les politiques, les directives, les normes et les lignes directrices générales de Services partagés Canada peuvent être consultées sur le site [http://service.ssc.gc.ca/en/policies\_processes/policies](http://service.ssc.gc.ca/fr/politiques_processus/politiques).

## Normes

Les normes de sécurité suivantes de la SPC doivent être examinées afin de s’y conformer lors de l’utilisation de cette AR :

* [Normes de sécurité de SPC](https://gcdocs.gc.ca/ssc-spc/llisapi.dll?func=ll&objId=91128836&objAction=browse&viewType=1)
* [Norme de sécurité relative à la définition de la zone de sécurité](http://service.ssc.gc.ca/fr/policies_processes/policies/zones)

## Politiques

[Instruments de politique de SPC](https://myssc-monspc.ssc-spc.gc.ca/fr/outilstravail-processus/instrument-politique/securite)

[Politique sur la sécurité du gouvernement](https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578)

# Modèles d’architecture

## Vue d’interaction des zones interentreprises ministérielles

La figure 7 décrit un modèle traditionnel d’entreprise à entreprise entre un ministère du GC et des entités non gouvernementales. La zone publique accueille des organisations du secteur privé et des organisations non gouvernementales, chacune ayant des flux d’information bidirectionnels avec les services du GC. La ZAP héberge des services de sécurité d’entreprise afin de réduire les risques associés à la zone publique. Les services ZAP servent de médiateur pour le flux bidirectionnel continu à travers les services interentreprises et finalement les applications et les données GC hébergées dans les ZAR des services.

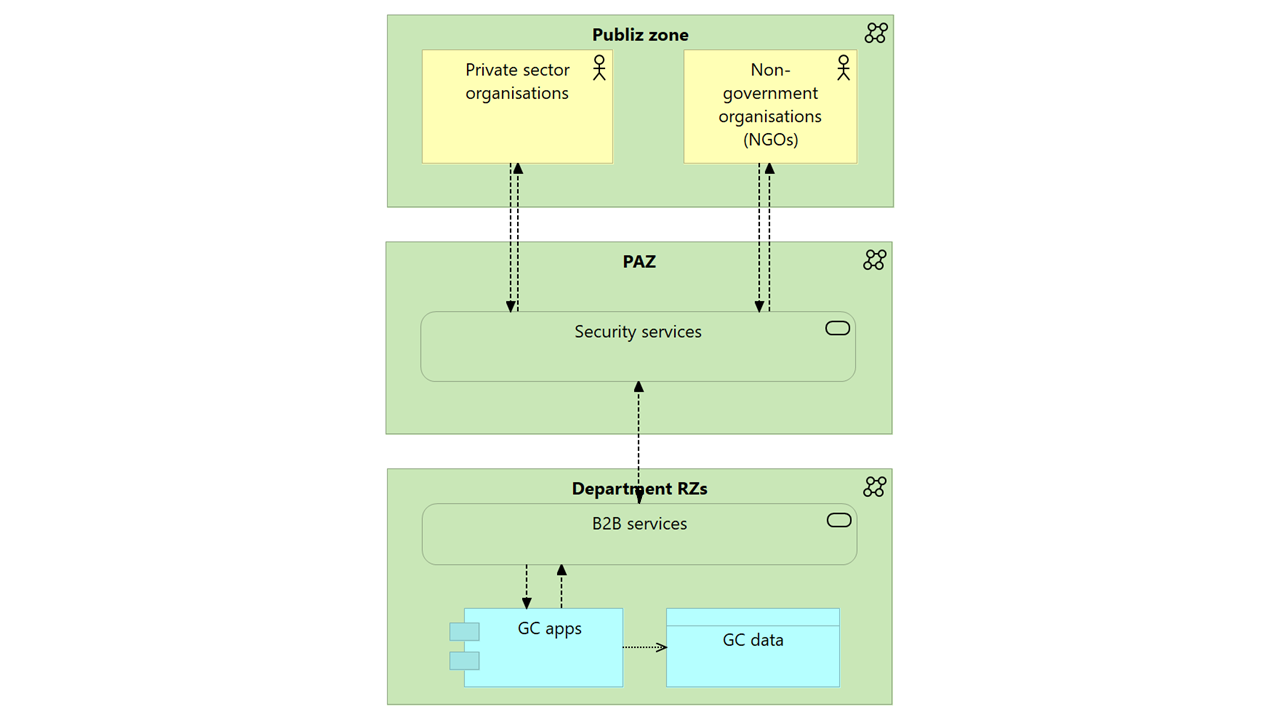


Figure 7. Vue d’interaction des zones interentreprises ministérielles

## Concepts de zone de sécurité

### Les points d’interface de zone (PIZ) et leurs fonctions de sécurité

Le modèle ci-dessous donne un aperçu général des points d’interface de zone (PIZ) et des fonctions de sécurité qu’ils hébergent. Les trois principaux PIZ sont :

1. Zone d’accès public
2. Zone des opérations
3. Zone restreinte

La ZAP est la seule zone qui fournit des contrôles de sécurité pour le trafic réseau bidirectionnel.

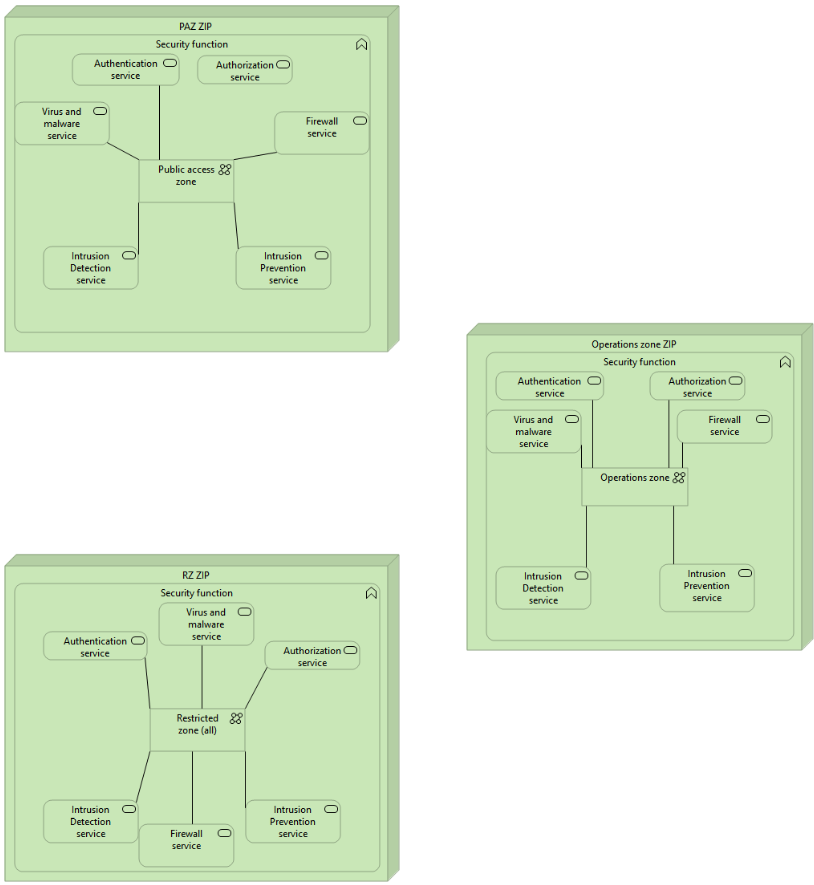


Figure 8. PIZ et fonctions de sécurité

### Zone d’opérations et PIZ

Le modèle ci-dessous décrit les services technologiques qui sont le plus souvent associés à la zone des opérations (ZO) et au PIZ de la ZO.

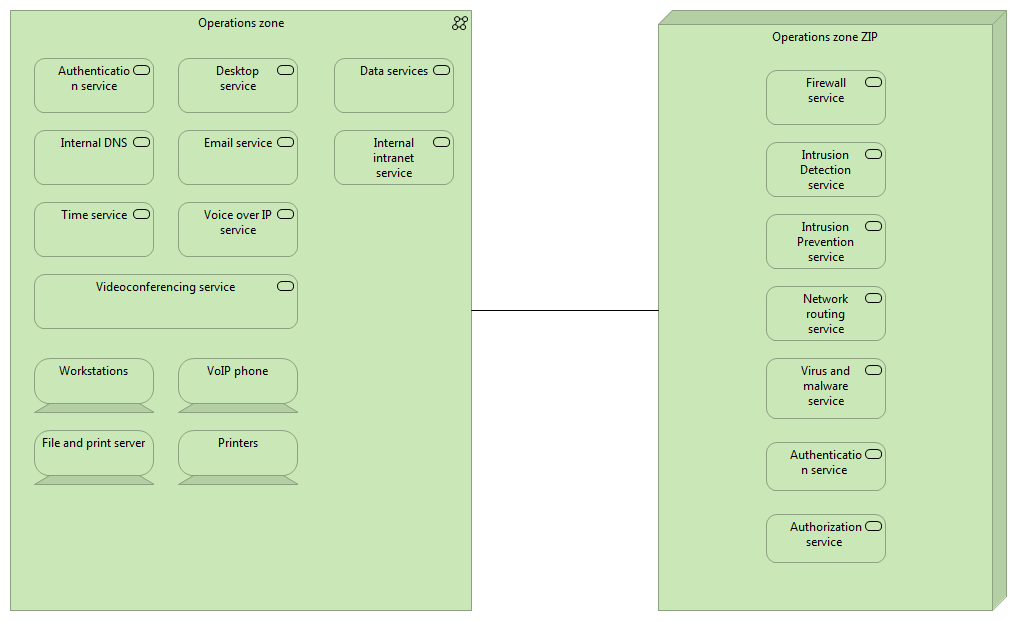


Figure 9. Vue de la zone des opérations et des services PIZ

### Zone d’accès public et PIZ

Le modèle ci-dessous décrit les services technologiques qui sont le plus souvent associés à la zone d’accès publique (ZAP) et au PIZ de la ZAP.

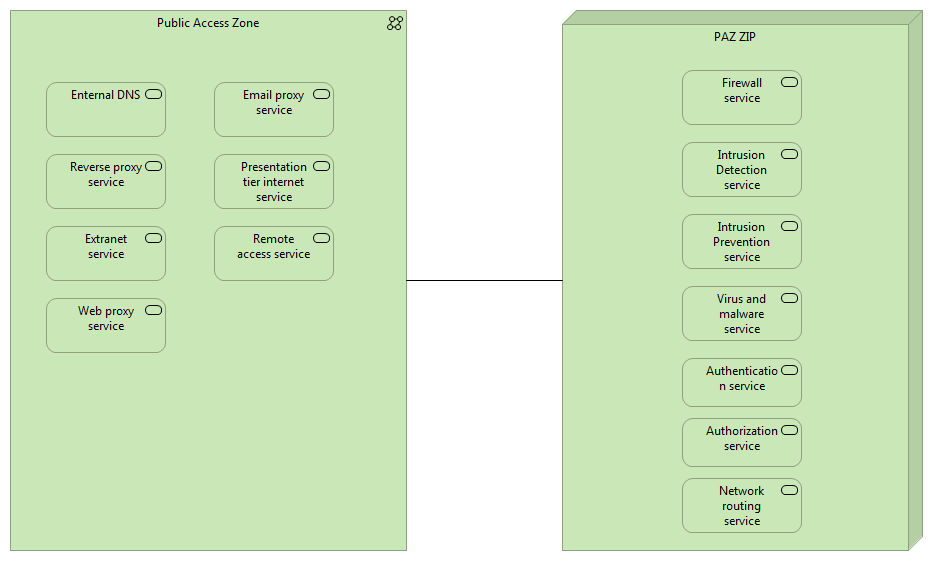


Figure 10. Vue des services ZAP et PIZ de la ZAP

### Zone d’accès restreint aux applications Internet et PIZ

Le modèle ci-dessous décrit les services technologiques qui sont le plus souvent associés à la zone restreinte de l’application Internet (ZRAI) et au PIZ de la ZAR.

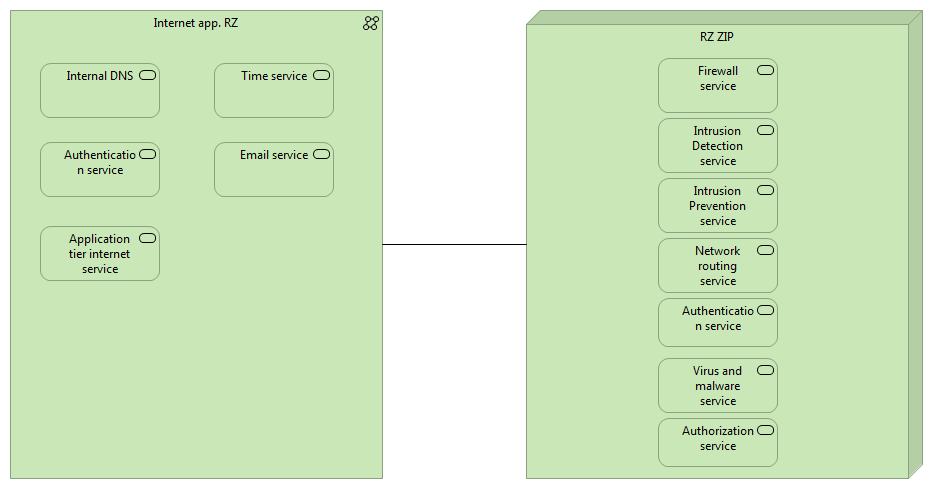


Figure 11. Vue de la zone restreinte de l’application Internet et des services PIZ

### Zone restreinte et ZAR PIZ

Le modèle ci-dessous décrit les services technologiques qui sont le plus souvent associés à la zone d’accès restreinte (ZAR) et au PIZ de la ZAR.

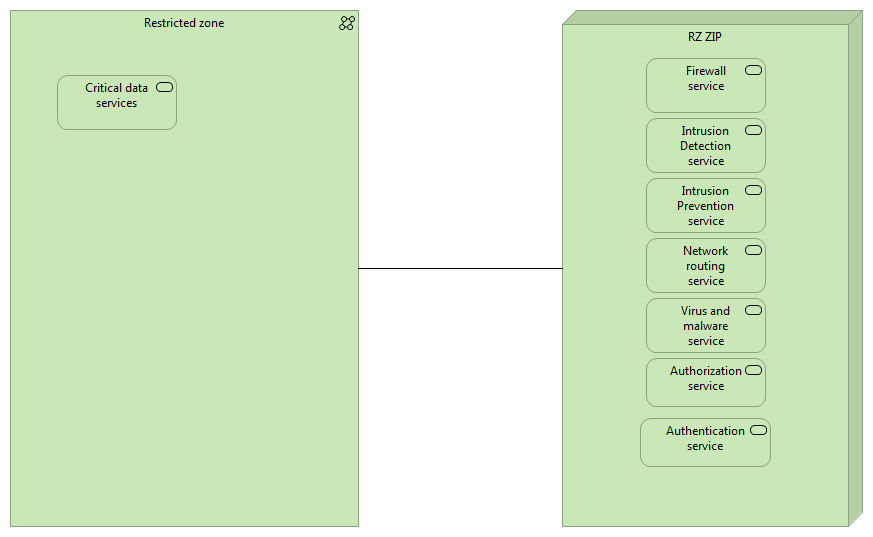


Figure 12. Vue des services de zone restreinte et de PIZ de la ZAR

### ZARD et PIZ

Le modèle ci-dessous décrit les services technologiques qui sont le plus souvent associés à la zone restreinte des données (ZARD) et au PIZ de la ZAR.

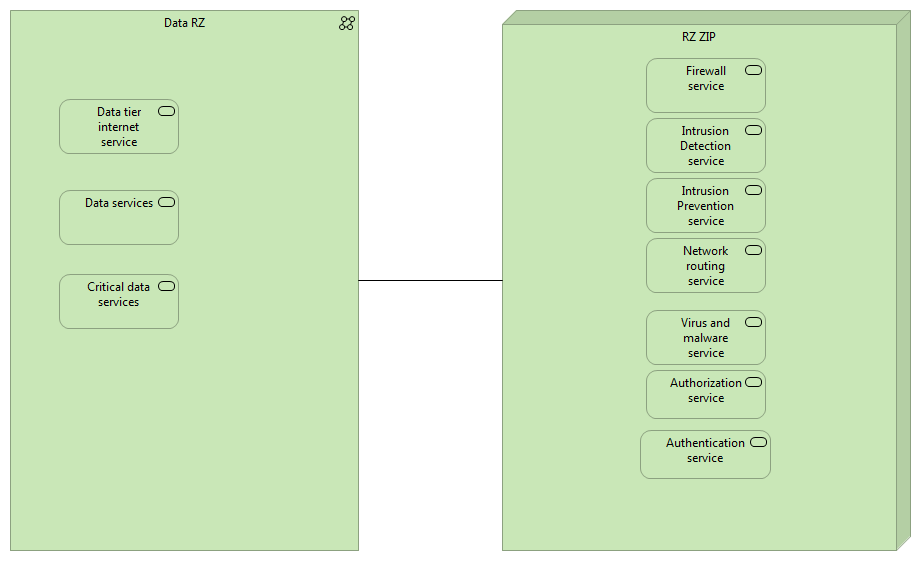


Figure 13. Vue des services ZARD et PIZ

### Gestion ZAR et PIZ

Le modèle ci-dessous décrit les services technologiques qui sont le plus souvent associés à la zone restreinte de la gestion de l’application Internet (ZRG) et au PIZ de la ZAR.

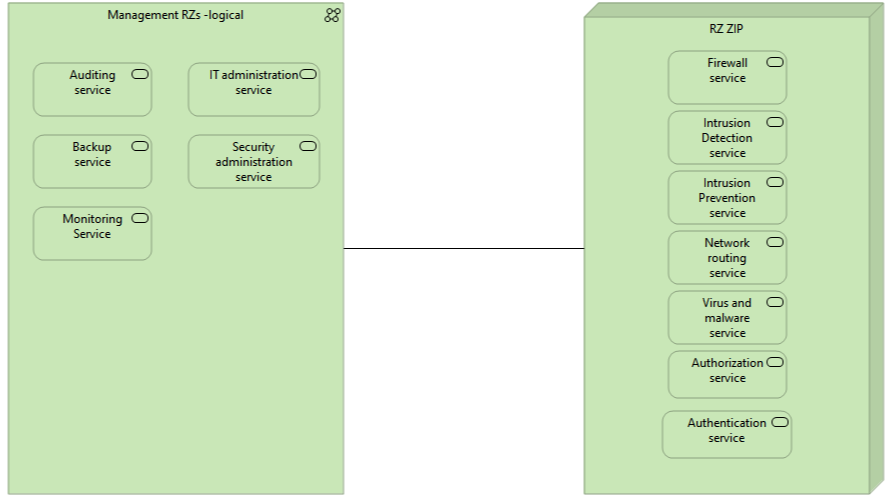


Figure 14. Vue des services PIZ et ZAR

## Zonage général du réseau

Deux modèles sont proposés pour mettre en œuvre la fourniture de services en nuage SaaS. La première option, figure 15, concerne l’intégration entre un service traditionnel hébergé par CDE et la seconde, figure 16, concerne la connectivité entre l’infrastructure en nuage d’un service et une application SaaS. Les services qui utilisent les services SaaS doivent mettre en place un zonage du réseau pour atténuer les risques associés à l’utilisation d’un environnement informatique entièrement contrôlé par une partie tierce.

La figure 15 décrit un service qui utilise le centre de données d’entreprise (CDE) traditionnel de SPC pour l’hébergement principal des services informatiques et des applications de GI. Ce service utilise également une solution SaaS basée sur le cloud qui est accessible par les utilisateurs du ministère et interagit avec les autres systèmes du service.

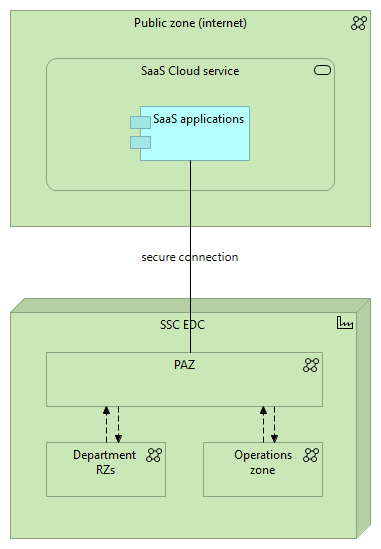


Figure 15. Du CDE au nuage SaaS

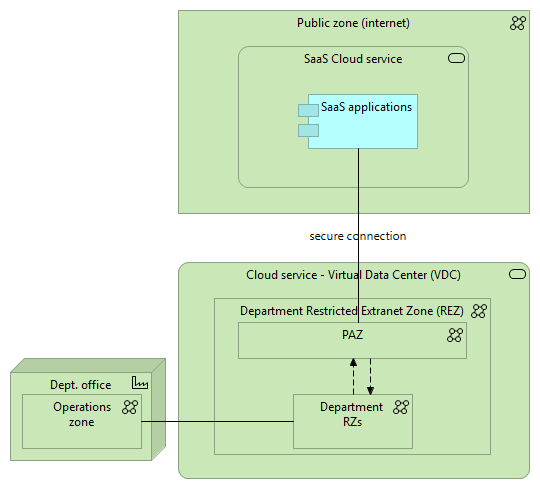


Figure 16. Du centre de données virtuel (CDV) au nuage SaaS

## Zones de gestion restreinte

Le modèle suivant donne un aperçu de toutes les zones de réseau dont disposent les ministères et les organismes du gouvernement du Canada. La zone de gestion est une représentation logique de la zone où commence l’accès administratif aux autres zones et à leurs configurations.

À chaque zone correspond une ZGR. Cela ne signifie pas que les utilisateurs privilégiés disposent d’un certain nombre de postes de travail physiques. Les postes de travail virtuels peuvent être configurés pour prendre en charge l’accès privilégié à des zones spécifiques du réseau.

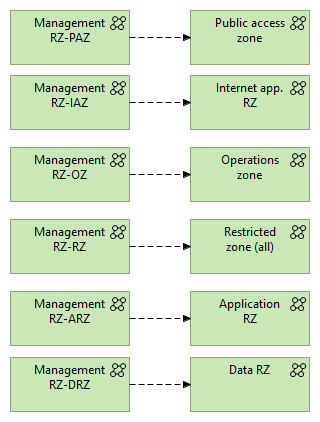


Figure 17. Zones du réseau du GC

## Vues des applications, des informations et des données

### Vues des applications

Les interfaces de programmation d’applications (API) du GC déclenchent de petits services qui accèdent aux informations/données du GC. Ces objets d’application dépendent du zonage du réseau.

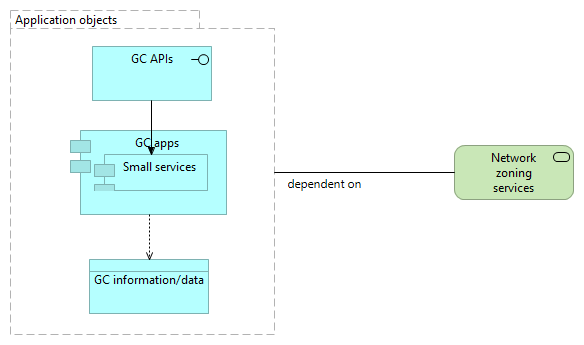


Figure 18. Dépendance des objets d’application pour le zonage du réseau

## Scénarios de zonage du nuage

### CDE SPC et intégration des services en nuage

Le modèle suivant représente un service partenaire dont l’intégration avec les technologies extérieures est limitée, mais qui souhaite tirer parti des services infonuagiques. De bas en haut, ce modèle représente une installation de centre de données d’entreprise SPC où des zones de service communes (ZAP, ZAR et ZGR) sont configurées. Notez que la ZO du service est située dans une installation du service. Ce modèle représente également une association entre le ministère du ZAP et un fournisseur de services de confiance.

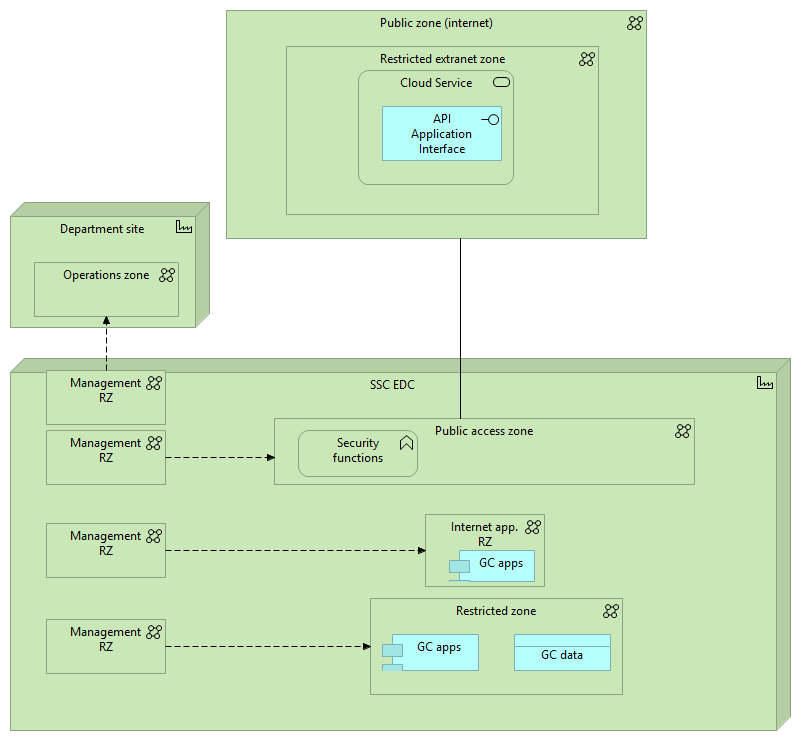


Figure 19. Vue de l’intégration des services hébergés dans le nuage

### Vue de zonage du nuage hybride du service

Ce modèle décrit un partenaire du GC ayant réalisé un investissement important dans des systèmes désuets et prêt à passer à des technologies informatiques modernes telles que l’IA et les offres de nuage hébergées dans un centre de données virtuel.

Les flux d’informations entre le nuage et le sol sont gérés par les fonctions de sécurité des ZAP respectives. La « ZAR de données » supplémentaire que l’on trouve dans le nuage n’est utilisée que pour montrer que les exigences en matière de zonage pourraient être différentes entre les CDV du nuage des ministères/agences et les centres de données des entreprises du GC. Une ZAR de données dans le nuage pourrait être nécessaire pour faciliter l’analyse des données dans le nuage.

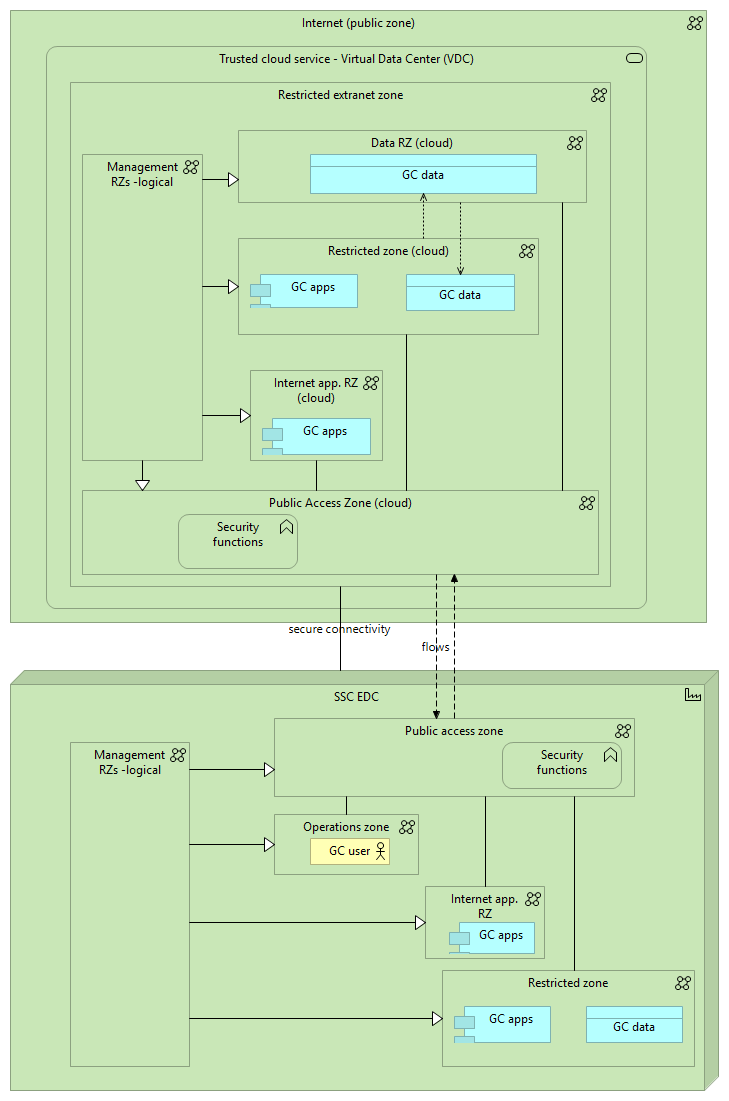


Figure 20. Vue de zonage du nuage hybride du service

### Les services passent à l’hébergement en nuage complet

Certains ministères et organismes partenaires pourraient souhaiter transférer la plupart de leurs systèmes GI/TI vers l’infonuagique. Cela pourrait être un bon modèle pour les ministères et les organismes partenaires qui n’ont pas de services numériques interactifs pour les utilisateurs. Veuillez noter que la zone des opérations (ZO), la zone restreinte de gestion (ZRG) et la zone d’accès public (ZAP) sont toujours nécessaires. De gauche à droite, les utilisateurs du GC utilisent des appareils terminaux dans la zone des opérations laquelle est gérée (spécialisée) à partir de la ZRG. La ZRG gère ou se spécialise également dans les ZAP et les ZAR des ministères hébergés dans le nuage.

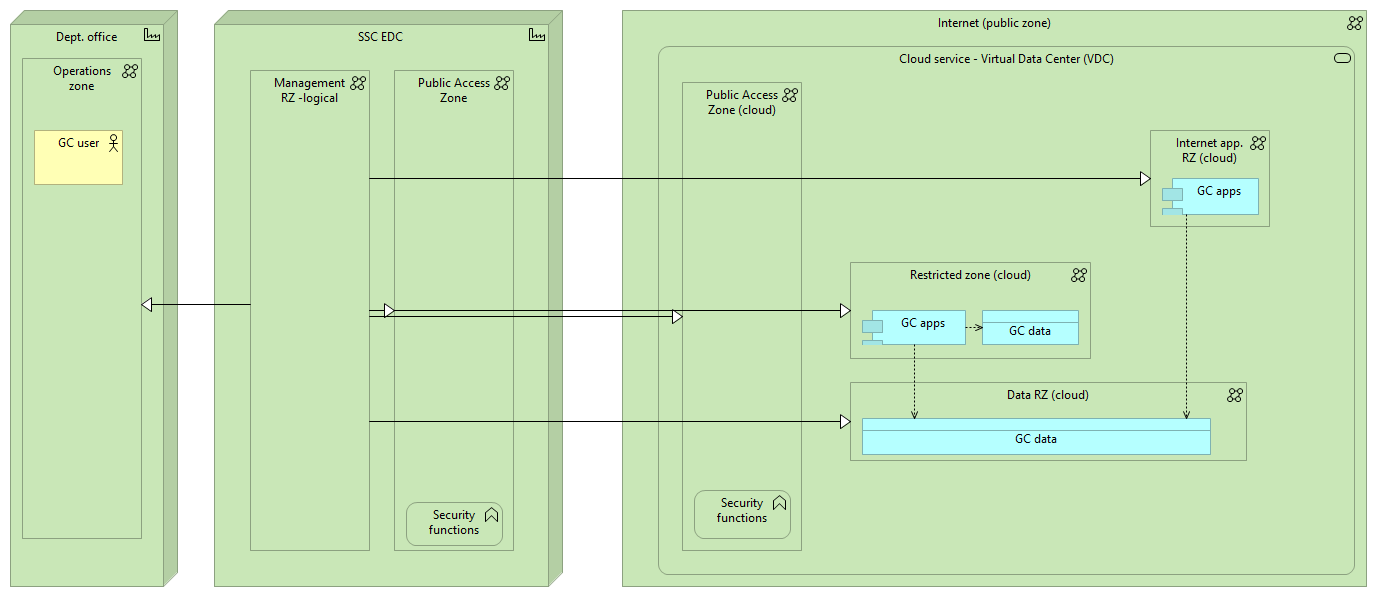


Figure 21. Aperçu de l’hébergement en nuage complet

### Zones infonuagiques

Les lignes directrices du Centre de la sécurité des télécommunications (CST) en matière de zonage du réseau ont été élaborées bien avant que l’infonuagique ne devienne pratique courante et véritablement accessible. Le gouvernement du Canada a adopté une approche « l’infonuagique d’abord » pour le choix des plateformes informatiques et des services de GI-TI. Comme telles, les zones du réseau du GC doivent (également) exister dans le nuage. La norme ITSG-22 (version publiée) porte historiquement sur les zones de sécurité pour une seule organisation. Ainsi, la ZAP applique la politique de sécurité qui vise l’ensemble de l’organisation. Les centres de données virtuels du ministère situés dans le nuage nécessitent le même zonage du réseau que pour un centre de données d’entreprise (CDE) traditionnel.

La figure 22 montre comment les zones traditionnelles et les zones infonuagiques sont déployées pour prendre en charge les flux d’informations bidirectionnels. Une différence notable est que la zone opérationnelle n’est pas hébergée dans le nuage.

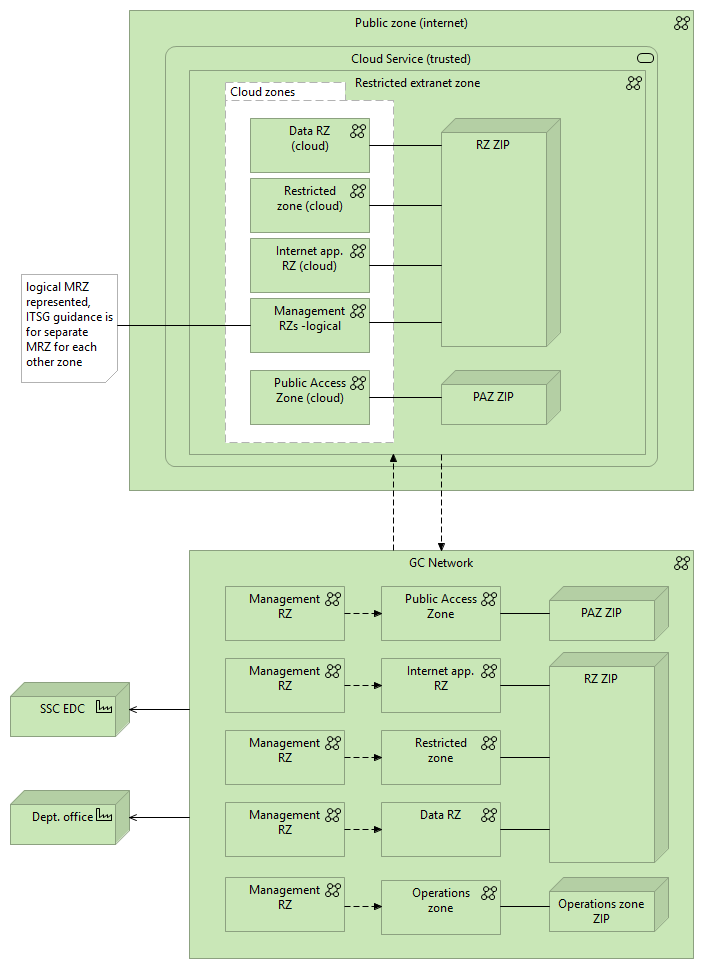


Figure 22. Zones du réseau infonuagiques

### Connectivité nuage-sol et Internet du GC

La figure 23 montre comment un ministère du GC ayant des services numériques infonuagiques interagit avec ses systèmes au sol et l’Internet. En bas à gauche, le modèle montre les applications et les données du ministère hébergées dans les centres de données traditionnels de SPC, connectés au RGC. Depuis l’ADNS, les utilisateurs des points d’interconnexion de confiance du GC se connectent à la zone d’accès public du ministère puis aux ZAR du ministère. En haut à gauche, nous voyons que le trafic Internet se dirige vers la ZAP de SPC (dans le nuage) où le PAN du GC fait office de médiateur du trafic Internet avant d’assurer l’interopérabilité avec la ZAP du ministère, puis avec les ZAR du ministère. Les objets de « compte » en jaune représentent les différents centres de coûts qui utilisent les ressources infonuagiques (utilisées pour la facturation...).

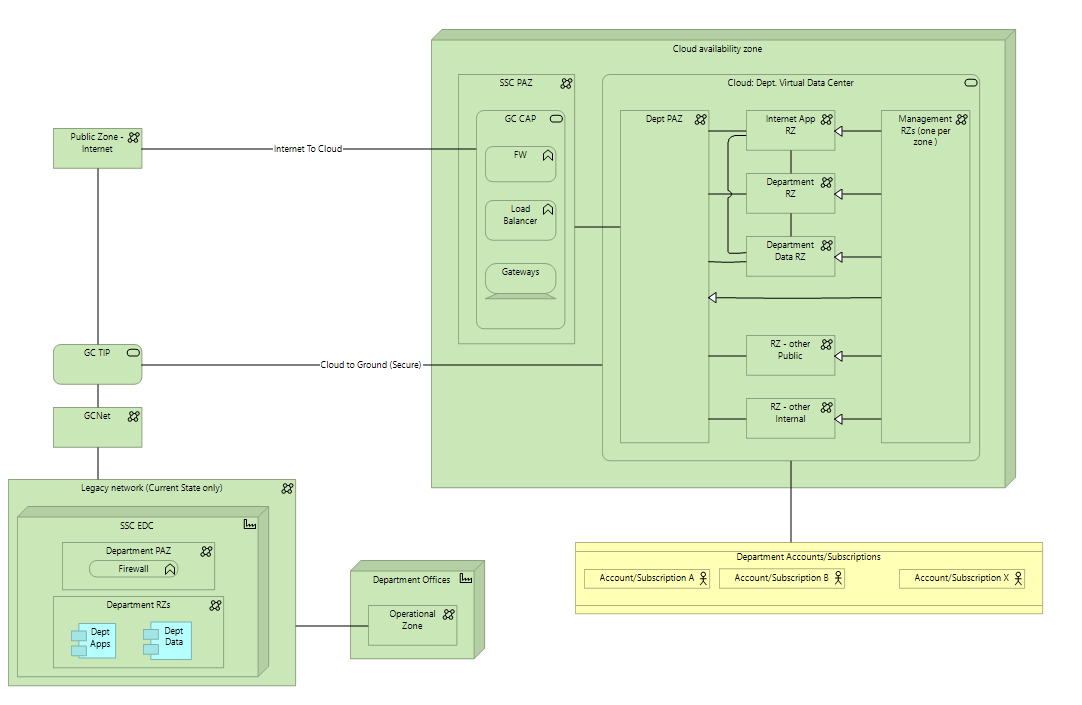


Figure 23. Connectivité nuage-sol et Internet du GC pour AWS

## Internet des objets

L’Internet des objets met à profit tous types d’appareils connectés. De nombreux citoyens ont des appareils portatifs IdO et la réalité des véhicules autonomes ou connectés se fera sentir au cours des prochaines années; la plupart des nouveaux véhicules que l’on vend déjà partout dans le monde sont connectés. Les provinces et les municipalités investissent dans des appareils intelligents qui les aident à améliorer les services gouvernementaux, par exemple le déneigement et l’enlèvement de la glace des routes. Certains services gouvernementaux utilisent des appareils connectés, notamment des instruments scientifiques pour recueillir des mesures de toutes sortes allant des images aux isotopes nucléaires et jusqu’à la température.

Contrairement aux terminaux traditionnels, de nombreux appareils de l’IdO ne sont pas sous le contrôle du GC et par conséquent, on ne peut pas s’y fier. En général, les appareils qui sont connectés à Internet (zone publique) ne sont pas fiables; d’autres appareils de l’IdO qui appartiennent au GC et qui sont sous son contrôle dans les ZO des ministères et des organismes sont de confiance. En règle générale, les appareils de l’IdO qui ne sont pas fiables doivent servir de médiateurs par l’intermédiaire des ZAP du ministère. Les appareils fiables feront partie des ZO des ministères et des organismes, et suivront les modèles des terminaux traditionnels, comme le fait de nos jours un ordinateur portable ou un téléphone intelligent.

La figure 23 montre la connectivité aux appareils d’IdO publics (côté gauche) et le zonage du réseau pour les appareils d’IdO du GC (côté droit et au centre).

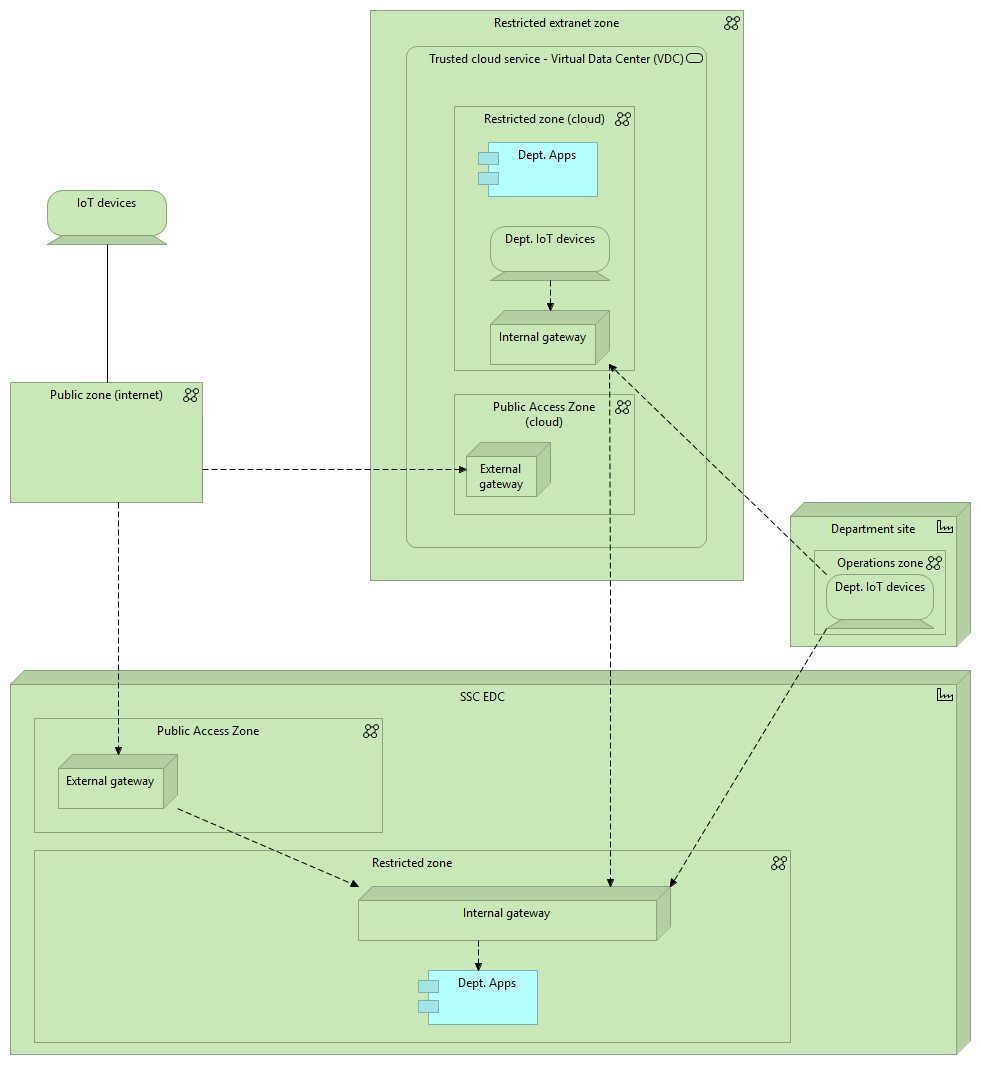


Figure 24. Internet des objets

## Interopérabilité de l’accès des organismes gouvernementaux partenaires (OGP) d’autres ministères (AM)

La figure 25 décrit trois modèles d’intégration fondamentaux : les services infonuagiques tournés vers Internet, les services infonuagiques des ministères et l’intégration de gouvernement à gouvernement (G2G). Nous utilisons deux groupes visuels pour séparer les modèles G2G du reste.

Dans l’élément du groupe G2G, il y a deux zones du réseau des ministères du GC (ministères A et B) dans les centres de données d’entreprise (CDE) de SPC qui utilisent les services de la Plateforme canadienne d’échange numérique (CDXP) commune au GC, également hébergée dans un CDE de SPC pour assurer l’intégration entre les applications du GC (applis du GC). Les services de la plateforme CDXP se connectent à la passerelle d’accès des OGP/AM de chaque ministère pour avoir accès aux applications du GC. Les provinces et les territoires utilisent également les services de la plateforme CDXP pour fournir des services d’identité utilisés par les ministères du GC.

Dans le groupe des services du GC Internet et infonuagiques, nous décrivons de gauche à droite : Les services de TI de confiance du ministère A situés dans le nuage où sont hébergées les applications GC du ministère A. Une passerelle interne sert de médiateur pour l’intégration et l’échange de messages avec d’autres services de confiance dans les zones extranet restreintes (ZER).

La ZER suivante représente les services de la plateforme CDXP hébergés dans le nuage public. Notez qu’une zone d’accès public est incluse dans cette ZER puisque sa connectivité est liée à l’Internet grâce à une passerelle externe sécurisée. Les lignes en pointillés dans le modèle représentent des flux de données ou d’information.

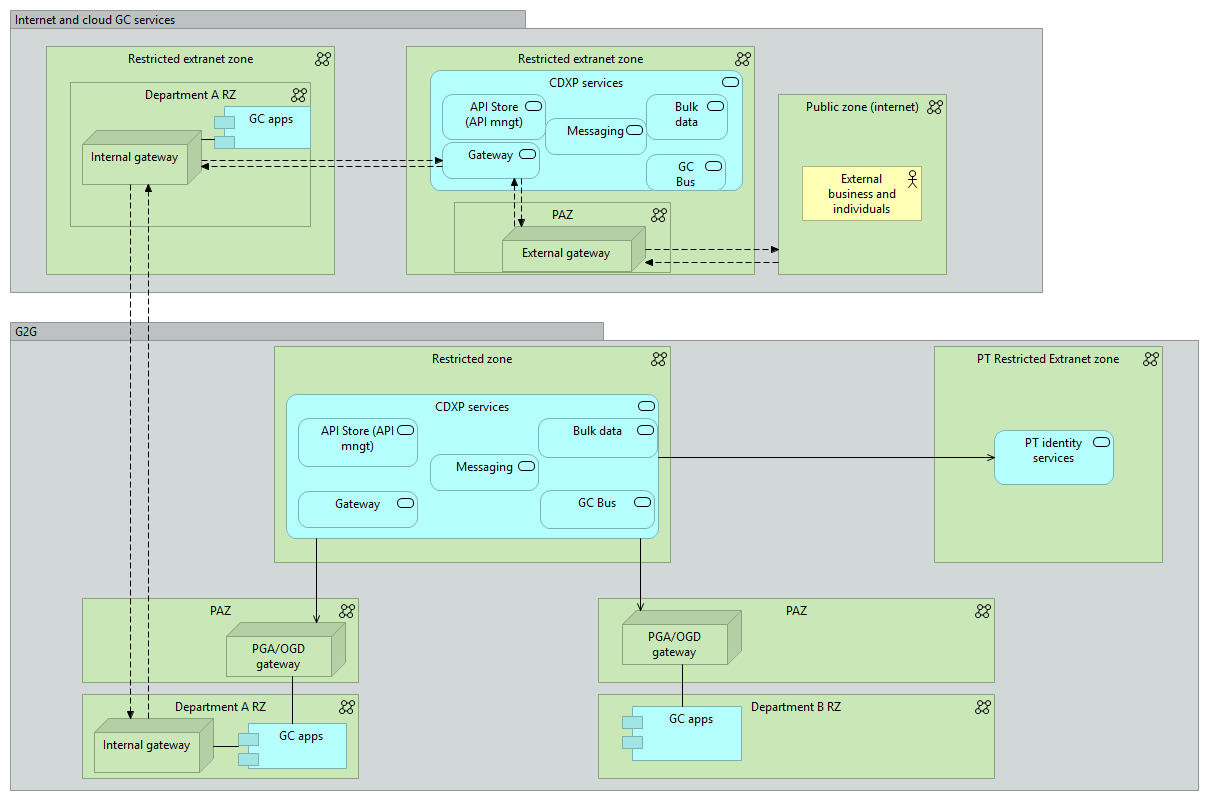


Figure 25. Aperçu de l’interopérabilité de l’accès des OGP/AM

# Glossaire des termes et des acronymes

## Glossaire

| Durée | Description |
| --- | --- |
| CST | Centre de la sécurité des télécommunications (CST) Canada : organisme du ministère de la Défense nationale responsable de l’élaboration de normes et de directives de sécurité liées aux réseaux informatiques. |
| Point d’interface de zone (PIZ) | Interface entre deux zones de sécurité du réseau par laquelle les données peuvent circuler. (Source : ITSG-22) |
| Services externes | Un service qu’un ministère client peut commander auprès de SPC (c.-à-d. dans le catalogue de services de SPC). |
| Système d’extrémité | Système qui, dans un cas particulier de communication, constitue la source ou la destination ultime de la communication. (Source : ITSG-22) |
| Zone d’accès public (ZAP) | Reportez-vous à la section 1.6.5.2. (Source : ITSG-22) |
| Zone d’accès restreint (ZAR) | Reportez-vous à la section 1.6.5.4. (Source : ITSG-22) |
| Zone d’accès spécial (ZAS) | Reportez-vous à la section 1.6.5.8. (Source : ITSG-22) |
| Zone d’accès très restreint (ZATR) | Reportez-vous à la section 1.6.5.5. (Source : ITSG-22) |
| Zone de gestion (ZG) | Reportez-vous à la section 1.6.5.7. (Source : ITSG-22) |
| Zone des opérations (ZO) | Reportez-vous à la section 1.6.5.3. (Source : ITSG-22) |
| Zone extranet d’accès restreint (ZEAR) | Reportez-vous à la section 1.6.5.6. (Source : ITSG-22) |
| Zone publique (ZP) | Reportez-vous à la section 1.6.5.1. (Source : ITSG-22) |

## Acronymes

| Sigle | Description |
| --- | --- |
| AE | Architecture d’entreprise |
| AM | Autre ministère |
| AR | Architecture de référence |
| CCC | Centre canadien pour la cybersécurité |
| CDE | Centres de données d’entreprise |
| CDXP | Plateforme d’échange numérique |
| CST | Centre de la sécurité des télécommunications Canada |
| G2G | De gouvernement à gouvernement |
| GC | Gouvernement du Canada |
| GSG | Gestion de la sécurité et de la gouvernance |
| IPA | Interface de programmation d’applications |
| ITSG | Ligne directrice sur la gestion de la sécurité des technologies de l’information |
| OGP | Organismes gouvernementaux partenaires |
| PIZ | Point d’interface de zone |
| PSTI | Praticien de la sécurité des technologies de l’information |
| PT | Provinces et territoires |
| RSSN | Réseaux, sécurité et services numériques |
| SPC | Services partagés Canada |
| TOGAF | The Open Group Architecture Framework |
| ZAG | Zone d’accès de gestion |
| ZAP | Zone d’accès public |
| ZAR | Zone d’accès restreint |
| ZAS | Zone d’accès spécial |
| ZATR | Zone d’accès très restreint |
| ZEAR | Zone extranet d’accès restreint |
| ZG | Zone de gestion |
| ZO | Zone des opérations |
| ZP | Zone publique |

# Références

La documentation suivante a été utilisée pour élaborer cette description de l’architecture de référence :

| Référence | Titre | Remarques |
| --- | --- | --- |
|  | Mandat | Sécurité des réseaux de SPC - Mandat du groupe de travail sur l’architecture de zonage  <https://gcdocs.gc.ca/ssc-spc/llisapi.dll?func=ll&objaction=overview&objid=33397799> |
|  | ITSG - 22 - Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada | Ligne directrice sur la gestion de la sécurité des technologies de l’information (ITSG) - 22 - Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada, (ITSG-22), juin 2007. <https://cyber.gc.ca/fr/orientation/exigences-de-base-en-matiere-de-securite-pour-les-zones-de-securite-de-reseau-au-sein-du-gouvernement-du-Canada-itsg-22>  Les *exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada* désigne un document *NON CLASSIFIÉ* publié avec l’autorisation du chef du Centre de la sécurité des télécommunications. |
|  | ITSG 38 - Zones de sécurité dans un réseau | Ligne directrice sur la gestion de la sécurité des technologies de l’information (ITSG) - 38 - Zonage de sécurité dans un réseau - Considérations de conception relatives au positionnement des services dans les zones, mai 2009. <https://cyber.gc.ca/fr/orientation/considerations-de-conception-relatives-au-positionnement-des-services-dans-les-zones-itsg-38>  La *zone de sécurité dans un réseau* désigne un document *NON CLASSIFIÉ* publié avec l’autorisation du Chef du Centre de la sécurité des télécommunications. |
|  | ITSG-33 – Gestion des risques liés à la sécurité des TI : une méthode axée sur le cycle de vie | Ligne directrice sur la gestion de la sécurité des technologies de l’information (ITSG) - 33 - Gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie - Aperçu, nov. 2012. <https://cyber.gc.ca/fr/orientation/la-gestion-des-risques-lies-la-securite-des-ti-une-methode-axee-sur-le-cycle-de-vie-itsg-33>  L’*approche de gestion de la sécurité des technologies de l’information* désigne un document *NON CLASSIFIÉ* publié avec l’autorisation du Chef du Centre de la sécurité des télécommunications. |
|  | ArchiMate 3.0.1 | Spécification The Open Group ArchiMate 3.0.1 <http://pubs.opengroup.org/architecture/archimate3-doc/toc.html> |
|  | The Open Group Architecture Framework (certification TOGAF) | The Open Group Architecture Framework « TOGAF, version 9.1 », 2011. [TOGAF](https://www.opengroup.org/togaf/) |
|  | Norme de sécurité relative à la définition de la zone de sécurité | <https://gcdocs.gc.ca/ssc-spc/llisapi.dll?func=ll&objaction=overview&objid=10649608> |
|  | Normes architecturales du GC pour l’alignement numérique | <http://www.gcpedia.gc.ca/wiki/GC_Architectural_Standards_for_Digital_Alignment> |
|  | Cadre de l’architecture d’entreprise du GC | <http://www.gcpedia.gc.ca/wiki/GC_Enterprise_Architecture_Framework> |
|  | Normes architecturales existantes du gouvernement du Canada | <http://www.gcpedia.gc.ca/wiki/GC_Existing_Architectural_Standards> |
|  | GCpass - les services d’authentification centralisés internes (SACI) du gouvernement du Canada | <http://www.gcpedia.gc.ca/gcwiki/index.php?title=GCpass_-_the_GC_Internal_Centralized_Authentication_Service_(ICAS)&redirect=no> |
|  | Cadre de confiance pancanadien | <https://diacc.ca/pan-canadian-trust-framework/> |
|  | Architecture de sécurité et de la protection des renseignements personnels de l’entreprise du GC | <https://wiki.gccollab.ca/GC_Enterprise_Security_and_Privacy_Architecture> |
|  | ASE du GC | ([http://www.gcpedia.gc.ca/wiki/Category:Government\_of\_Canada\_Enterprise\_Security\_Architecture\_[ESA]\_Program)](http://www.gcpedia.gc.ca/wiki/Category:Government_of_Canada_Enterprise_Security_Architecture_(ESA)_Program)) |
|  | Gouvernement du Canada - Architecture fédérée - Itération un | *Gouvernement du Canada - Architecture fédérée - Itération un* [en ligne]. [Ottawa] : Secrétariat du Conseil du Trésor du Canada, juin 2000 [cité le 1er avril 2006]. Disponible sur <http://www.tbs.sct.gc.ca/fap-paf/documents/iteration/iteration_e.asp>. |
|  | Orientation sur l’utilisation sécurisée des services commerciaux d’informatique en nuage : Avis de mise en œuvre de la Politique sur la sécurité (AMOPS) | <https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/orientation-utilisation-securisee-services-commerciaux-informatique-nuage-amops.html> |

1. Notation ArchiMate®

Les détails concernant la notation ArchiMate® 3.0.1 utilisée dans les figures de ce document d’architecture de référence proviennent du chapitre 4 du site Web de The Open Group™ [Réf. F].

* 1. **Aide-mémoire**

Vous trouverez ci-dessous une représentation graphique des principales notations de modélisation utilisées dans ce document.

* + 1. **Structure de la langue de premier niveau**

La figure 26 décrit la structure hiérarchique linguistique de premier niveau :

* Un modèle est un ensemble de concepts. Un concept est un élément ou une relation.
* Un élément est un élément de comportement, un élément de structure, un élément de motivation ou un élément mixte.

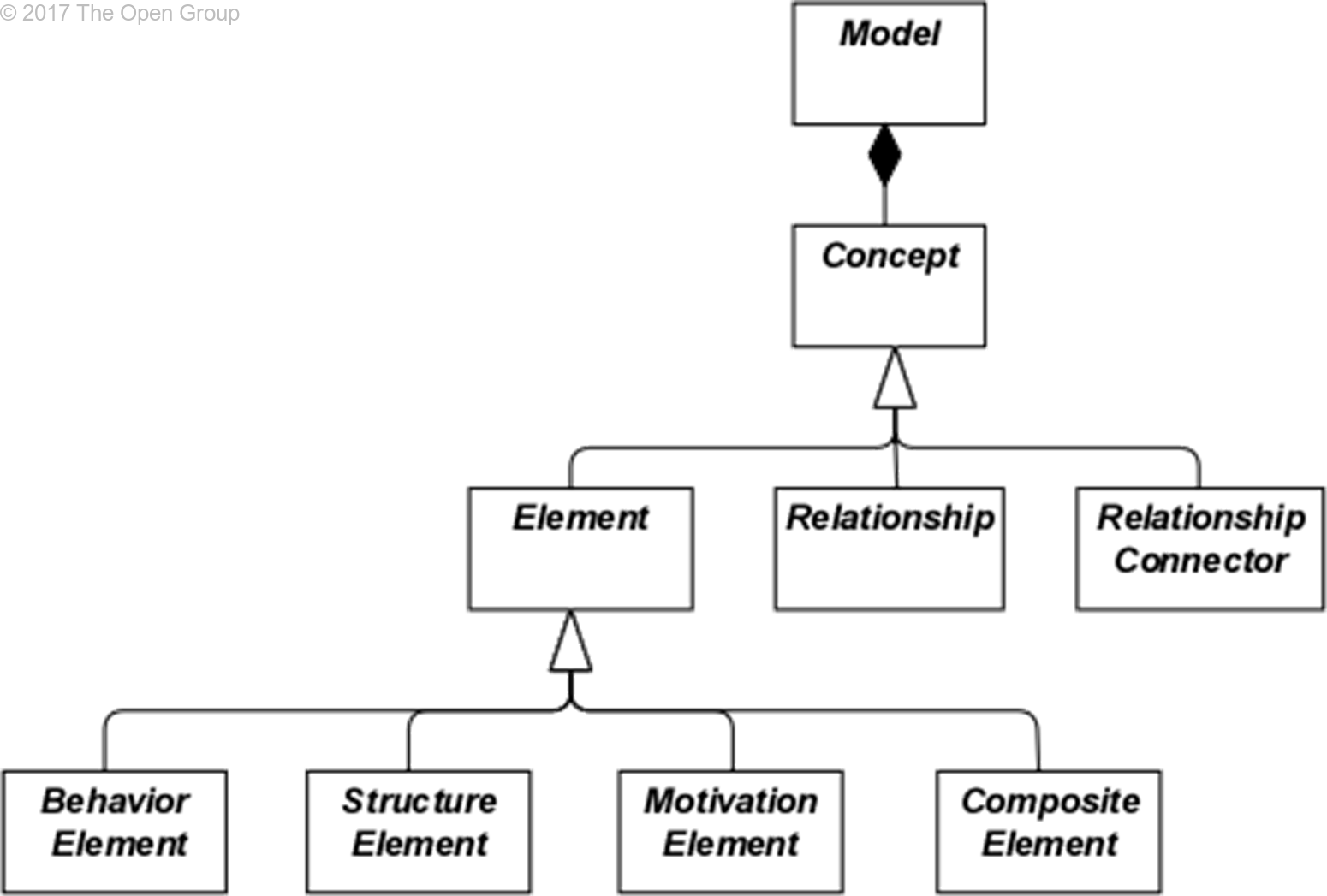


Figure 26. Concepts ArchiMate® de premier niveau

* + 1. **Concepts de base**

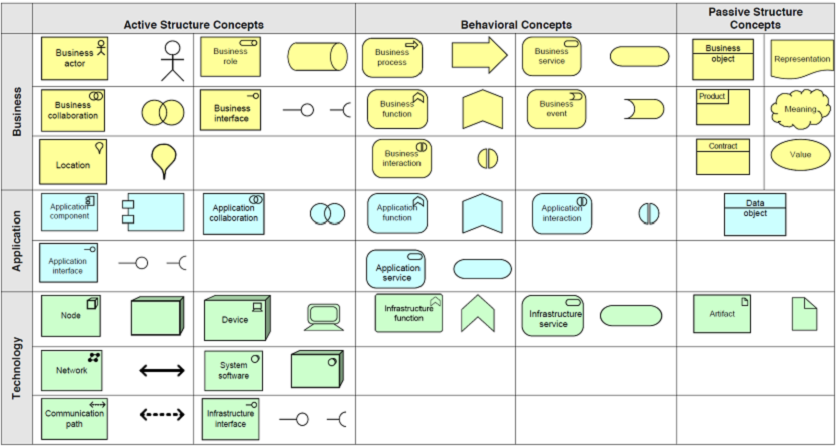
******

Figure 27. Concepts de base ArchiMate®

* + 1. **Prorogations**

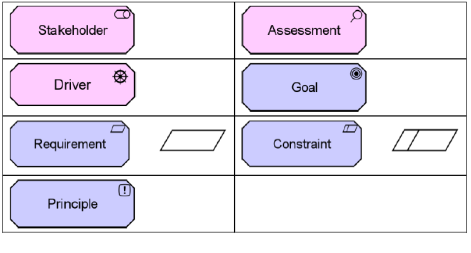
******

Figure 28. Prorogations ArchiMate®

* + 1. **Relations**

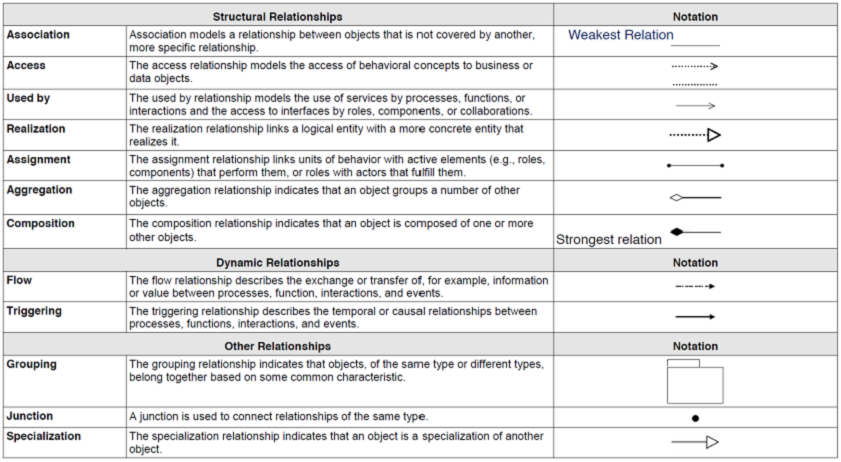
******

Figure 29. Relations avec ArchiMate®

1. Collaborateurs et réviseurs

Les personnes suivantes ont revu et contribué au présent document de l’architecture de référence du zonage de réseau du GC.

Tableau 2. Revu et endossé par

| **Nom du participant au complet – Titre** | **Ministère participant – Division** | **Rôle ou contribution** |
| --- | --- | --- |
| Vanessa Clowe, PMP  [Vanessa.Clowe@cyber.gc.ca](mailto:Vanessa.Clowe@cyber.gc.ca)  Téléphone : 613-998-2837 | CST  Partenariat et atténuation des risques  Architecture des normes et gestion des risques | Contributeur ou réviseur |
| Mike Albert  [Michael.Albert@cyber.gc.ca](mailto:Michael.Albert@cyber.gc.ca) | CST | Contributeur ou réviseur |
| Peter Benisson  [Peter.Bennison@cyber.gc.ca](mailto:Peter.Bennison@cyber.gc.ca) | CST | Réviseur |
| Jim Palmer  [James.Palmer@cyber.gc.ca](mailto:James.Palmer@cyber.gc.ca) | CST | Réviseur |
| David Alton  [David.Alton@cyber.gc.ca](mailto:David.Alton@cyber.gc.ca) | CST | Réviseur |
| Po Tea-Duncan  613-404-2924  [Po.Tea-Duncan@tbs-sct.gc.ca](mailto:Po.Tea-Duncan@tbs-sct.gc.ca) | Cybersécurité/SCT | Contributeur ou réviseur |
| Rahim Charania  [Rahim.Charania@tbs-sct.gc.ca](mailto:Rahim.Charania@tbs-sct.gc.ca) | Cybersécurité/SCT | Réviseur |
| John Biro - Architecte d’entreprise  Bureau : 343-291-7390  Cellulaire : 613-612-4624  [john.biro@cbsa-asfc.gc.ca](mailto:john.biro@cbsa-asfc.gc.ca) | ASFC/ Architecte d’entreprise, technologie et sécurité  Architecture d’entreprise  Direction générale de l’information, des sciences et de la technologie | Contributeur ou réviseur |
| Jianmin Gao,  Conseiller principal, Architecture d’entreprise, ASFC [Jianmin.Gao@cbsa-asfc.gc.ca](mailto:Jianmin.Gao@cbsa-asfc.gc.ca) | ASFC | Contributeur ou réviseur |
| Yacin Abdallah  Conseiller technique,  [yacin.abdallah2@canada.ca](mailto:yacin.abdallah2@canada.ca)  Tél. : 343-548-0839 | SPC/Direction générale du dirigeant principal de la technologie | Contributeur ou réviseur |
| Deoliveira, Fabien  [fabien.deoliveira@canada.ca](mailto:fabien.deoliveira@canada.ca) | SPC/DSIS (Services d’intégration des solutions) | Réviseur |
| Brian McKittrick  [brian.mckittrick@canada.ca](mailto:brian.mckittrick@canada.ca) | Sécurité et services définis par des logiciels / Habilitation numérique | Réviseur |
| James MacLeod  [james.macleod@canada.ca](mailto:james.macleod@canada.ca) | Groupe de gestion de la sécurité | Réviseur |
| Lloyd Low  [lloyd.low@canada.ca](mailto:lloyd.low@canada.ca) | DGSCD – (Direction générale des services de centres de données) | Réviseur |
| Brad Matthews  Conseiller principal  [brad.matthews@canada.ca](mailto:brad.matthews@canada.ca)  Tél. : 506-449-2536 | SPC/Conception et intégration  Direction des réseaux, de la sécurité et des services numériques | Contributeur ou réviseur |
| Brent Lahaise, CISSP, PSCGFCC  Conseiller en sécurité  [brent.lahaise2@canada.ca](mailto:brent.lahaise2@canada.ca)  Tél. : 613-884-3257 | SPC/Architecture de sécurité d’entreprise  Gestion et gouvernance de la sécurité, Direction générale du dirigeant principal de la technologie | Contributeur ou réviseur |
| Andrew Martin  Directeur  [andrew.martin@canada.ca](mailto:andrew.martin@canada.ca) | SPC |  |
| Jason Boutilier  Tél. : 613-219-6227  [jason.boutilier@canada.ca](mailto:jason.boutilier@canada.ca) | SPC | Contributeur ou réviseur |
| Mark McLean  [mark.mclean3@canada.ca](mailto:mark.mclean3@canada.ca) | SPC-DSI (Direction des services d’infonuagique) | Contributeur ou réviseur |
| Ali, Tarek  [tarek.ali@canada.ca](mailto:tarek.ali@canada.ca) | SPC – Recherche infonuagique et développement | Réviseur |
| Hill, Gerald  [Gerald.Hill@canada.ca](mailto:Gerald.Hill@canada.ca), | SPC – Recherche infonuagique et développement | Réviseur |
| Sylvain Bluteau  [sylvain.bluteau@canada.ca](mailto:sylvain.bluteau@canada.ca) | SPC/DSI | Réviseur |
| Rob Bryce (SPC)  [rob.bryce2@canada.ca](mailto:rob.bryce2@canada.ca) | SPC |  |
| David Zinni (SPC)  david.zinni@canada.ca | SPC |  |
| Rick Cairns  rick.cairns@tbs-sct.gc.ca | SCT |  |
| Centurione, Marcello  [marcello.centurione@canada.ca](mailto:marcello.centurione@canada.ca) | SPC/AE | Contributeur ou réviseur |
| Claude Vallée | SPC/AE | Contributeur ou réviseur |
| Walter Sokyrko | SPC/RSSN | Contributeur ou réviseur |
| Earle, Simon  (Consultant affecté à la recherche infonuagique et au développement) | SPC/DSI | Contributeur ou réviseur |
| Nguyen, Tho  [Tho.Nguyen@ssc-spc.gc.ca](mailto:Tho.Nguyen@ssc-spc.gc.ca) | SPC/RSSN | Réviseur |
| Andre Hiotis  (Consultant affecté à l’ADNS)  [andre.hiotis@canada.ca](mailto:andre.hiotis@canada.ca) | SPC | Contributeur ou réviseur |

1. <https://www.opengroup.org/archimate-forum/archimate-overview>. [↑](#footnote-ref-1)
2. Figure tirée de la réf. B ITSG - 22 - Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada, juin 2007. [↑](#footnote-ref-2)
3. *Gouvernement du Canada - Architecture fédérée - Itération un* [en ligne]. [Ottawa] : Secrétariat du Conseil du Trésor du Canada, juin 2000 [cité le 1er avril 2006]. Disponible sur <http://www.tbs.sct.gc.ca/fap-paf/documents/iteration/iteration_e.asp>. [↑](#footnote-ref-3)
4. Voir ITSG-22. [↑](#footnote-ref-4)