Mesures de sécurité du nuage

Oracle Cloud Infrastructure (OCI)

0.03
May 28, 2020

Shared Services Canada
Services partagés Canada
Canada

Contents

Introduction

Contexte

Le gouvernement du Canada a mis en place une stratégie axée sur le cloud pour aider les ministères et organismes à offrir des services numériques aux Canadiens.

Oracle Cloud Infrastructure (OCI) est un fournisseur de services cloud approuvé.

Services partagés Canada est le point d'entrée unique pour les services infonuagiques. Grâce au portail de courtage dans le cloud, les partenaires peuvent demander des services cloud, notamment des informations publiques, hybrides et privées, non classifiées et jusqu'à Protégé B.

Le but des garde-corps est de garantir que les ministères et organismes mettent en œuvre un ensemble de base de contrôle préliminaire dans leurs environnements cloud.

Ces garde-corps minimaux doivent être mis en œuvre au cours de la période initiale spécifiée par le GC (par exemple, 30 jours) à la réception d'une inscription en vertu de l'Accord-cadre des services cloud du GC.

Ce document fournit un bref aperçu de chaque garde-corps applicable et des instructions sur la façon de les mettre en œuvre lors de l'utilisation d'OCI.

Gestion des accès

Guardrail 1 - Protéger le compte administrateur racine / global

Objectif

Protéger le compte racine ou principal utilisé pour établir le service cloud.

Considérations clés

- ☐ Implémentez le mécanisme d'authentification multifacteur (MFA) pour le compte racine / maître.
- ☐ Consigner une procédure d'urgence de gestion des comptes en cas de bris de verre. Y compris les noms des utilisateurs ayant accès au compte racine ou principal.
- ☐ Obtenir la signature du dirigeant principal de l'information (DSI) et du dirigeant principal de la sécurité (OSC) pour confirmer la reconnaissance et l'approbation des procédures de gestion des comptes d'accès d'urgence.
- ☐ Mettre en œuvre un mécanisme pour appliquer les autorisations d'accès.
- ☐ Configurez les alertes appropriées sur les comptes racine ou principaux pour détecter un compromis potentiel, conformément à GC Event Logging Guidance

Validation

- ☐ Confirmez que la stratégie pour l'authentification multifacteur est activée via des captures d'écran et des rapports de conformité.
- ☐ Confirmer qu'une lettre d'attestation de la procédure de bris de vitre d'urgence a été signée par le DSI ministériel et le CSO.

Considérations supplémentaires

- ☐ Tirez parti des services d'entreprise tels que le système de contrôle d'accès administratif (AACS) pour la gestion des accès privilégiés (PAM), le contrôle d'accès basé sur les attributs (ABAC).

Modèles de service applicables

- IaaS, PaaS, SaaS

Comment protéger le compte administrateur racine et global

1. Pour activer MFA sur le compte d'administrateur global Oracle cloud, suivez les instructions indiquées ici :

   https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/usingmfa.htm

Comment confirmer la stratégie pour l'authentification multifacteur

1. Pour confirmer que MFA est activé pour votre compte administrateur Cloud, envoyez une capture d'écran de votre utilisateur Admin, comme indiqué ci-dessous. Le «champ d'authentification multifacteur» doit être étiqueté «ACTIVÉ».

Guardrail 2 - Gestion des privilèges administratifs

Objectif

Établir des politiques et des procédures de contrôle d'accès pour la gestion des privilèges administratifs.

Considérations clés

- ☐ Documenter un processus de gestion des comptes, des privilèges d'accès et des informations d'identification d'accès pour les utilisateurs organisationnels, les utilisateurs non organisationnels (si nécessaire) et les processus basés sur les principes de séparation des tâches et du moindre privilège (par exemple, procédures opérationnelles et Active Directory) .
- ☐ Implémentez un mécanisme pour appliquer les autorisations d'accès.
- ☐ Mettre en œuvre un mécanisme d'identification et d'authentification unique des utilisateurs organisationnels, des utilisateurs non organisationnels (le cas échéant) et des processus (par exemple, nom d'utilisateur et mot de passe).
- ☐ Implémentez un mécanisme d'authentification multifacteur pour les comptes privilégiés (par exemple, nom d'utilisateur, mot de passe et mot de passe à usage unique) et pour les interfaces externes.
- ☐ Modifiez les mots de passe par défaut.
- ☐ Assurez-vous qu'aucun rôle de propriétaire d'abonnement personnalisé n'est créé.
- ☐ Configurez la politique de mot de passe conformément aux instructions de mot de passe du GC GC Password Guidance.
- ☐ Minimiser le nombre d'utilisateurs invités; ajoutez seulement si nécessaire.
- ☐ Déterminez les restrictions d'accès et les exigences de configuration pour les appareils d'extrémité émis par le GC, y compris ceux des utilisateurs non privilégiés et privilégiés, et configurez les restrictions d'accès pour les appareils d'extrémité en conséquence. Remarque: certains fournisseurs de services peuvent proposer des options de configuration pour restreindre l'accès aux terminaux. Alternativement, une politique organisationnelle et des instruments de procédure peuvent être mis en œuvre pour restreindre l'accès..

Validation

- ☐ Confirmer la politique pour MFA (voir Guardrail 1)
- ☐ Confirmez qu'un plan et un processus de gestion de compte privilégié ont été documentés.
- ☐ Confirmer que la politique de mot de passe est conforme aux instructions de mot de passe du GC, le cas échéant.

Considérations supplémentaires

- ☐ Tirez parti des services d'entreprise tels que le système de contrôle d'accès administratif (AACS) pour la gestion des accès privilégiés (PAM), le contrôle d'accès basé sur les attributs (ABAC).

Modèles de service applicables

- IaaS, PaaS, SaaS

Comment configurer la gestion des privilèges administratifs

1. Pour démarrer avec Identity and Access Management et savoir comment contrôler l'accès à vos ressources cloud, consultez le document «Présentation d'Oracle Cloud Infrastructure Identity and Access Management», situé ici:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm

2. Pour créer des utilisateurs et fournir un accès aux ressources cloud, consultez le document «Gestion des utilisateurs» situé ici:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/managingusers.htm

3. Pour créer des groupes afin de fournir un accès aux ressources cloud, consultez le document «Gestion des groupes» situé ici:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/managinggroups.htm

4. Pour créer des stratégies permettant d'accéder aux ressources cloud, consultez le document «Fonctionnement des stratégies» situé ici:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Concepts/policies.htm

5. Pour organiser et isoler vos ressources cloud, utilisez Compartments, voir le document «Managing Compartments» situé ici:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/managingcompartments.htm

Guardrail 3 - Accès à la console cloud (développeurs / propriétaires d'applications)

Objectif

Limitez l'accès aux appareils gérés par le GC et aux utilisateurs autorisés.

Considérations clés

- ☐ Implémentez un mécanisme d'authentification multifacteur (MFA) pour les comptes privilégiés et l'accès au réseau distant (cloud).

- ☐ Déterminez les restrictions d'accès et les exigences de configuration pour les appareils gérés par le GC, y compris ceux des utilisateurs non privilégiés et privilégiés, et configurez les restrictions d'accès pour les appareils d'extrémité en conséquence.

Note: Certains fournisseurs de services peuvent proposer des options de configuration pour restreindre l'accès aux terminaux. Alternativement, la politique organisationnelle et les instruments de procédure peuvent être mis en œuvre pour restreindre l'accès.

- ☐ Assurez-vous que les actions administratives sont effectuées par les utilisateurs autorisés à l'aide d'un appareil de confiance connecté à un réseau de confiance (par exemple, réseau du CPG).
- ☐ Implémentez un mécanisme pour appliquer les autorisations d'accès.
- ☐ Implémentez des mécanismes de protection par mot de passe pour vous protéger contre les attaques par force brute.

Validation

- ☐ Confirmer la politique pour MFA (voir Guardrail 1)

Considérations supplémentaires

- ☐ Tirez parti des services d'entreprise tels que le système de contrôle d'accès administratif (AACS) pour la gestion des accès privilégiés (PAM), le contrôle d'accès basé sur les attributs (ABAC).

Modèles de service applicables

- IaaS, PaaS, SaaS

Comment limiter l'accès à Cloud Console

1. Pour démarrer avec Identity and Access Management et savoir comment contrôler l'accès à vos ressources cloud, consultez le document «Premiers pas avec Oracle Cloud Infrastructure Identity and Access Management», situé ici:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm

2. Pour créer des utilisateurs et fournir un accès aux ressources cloud, consultez le document «Gestion des utilisateurs» situé ici:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/managingusers.htm

3. Pour créer des groupes afin de fournir un accès aux ressources cloud, consultez le document «Gestion des groupes» situé ici:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/managinggroups.htm

4. Pour créer des stratégies permettant d'accéder aux ressources cloud, consultez le document «Fonctionnement des stratégies» situé ici:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Concepts/policies.htm

5. Pour organiser et isoler vos ressources cloud, utilisez Compartments, voir le document «Managing Compartments» situé ici:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/managingcompartments.htm

Guardrail 4 - Comptes de surveillance d'entreprise

Objectif

Créez un compte basé sur les rôles pour permettre la surveillance et la visibilité de l'entreprise.

Considérations clés

- ☐ Attribuez des rôles aux parties prenantes approuvées du GC pour permettre la visibilité de l'entreprise. Les rôles incluent le lecteur de facturation, le contributeur / lecteur de politique, le lecteur de sécurité et le lecteur global.
- ☐ Assurez-vous que le mécanisme d'authentification multifacteur pour les comptes de surveillance d'entreprise est activé.

Validation

- ☐ Confirmer la présence de comptes d'entreprise basés sur les rôles du GC créés par le Ministère pour les intervenants approuvés par le GC.
- ☐ Confirmer que les comptes disposent d'un accès en lecture approprié à l'environnement des locataires du Ministère.

Modèles de service applicables

- IaaS, PaaS, SaaS

Comment créer des comptes de surveillance d'entreprise

1. L'équipe SSC Cloud Brokering créera un compte utilisateur en lecture seule dans votre location cloud qui donnera accès aux données de facturation et d'audit. Le nom d'utilisateur est intitulé «SSC Admin» et disposera des privilèges de lecture requis.

   Aucune action ou configuration supplémentaire n'est requise.

Artefacts de gestion des accès

- Procédures d'urgence sur les comptes d'accès d'urgence approuvées par le CIO / CSO
- Plan de gestion des comptes privilégiés
- Rapport de conformité

Protection des Données

Guardrail 5 - Localisation des données au Canada

Objectif

Établir des politiques pour limiter les charges de travail sensibles du GC aux emplacements géographiques approuvés.

Considérations clés

- ☐ Conformément à la Directive sur la résidence des données électroniques (ITPIN 2017-02), «Toutes les données électroniques sensibles sous le contrôle du gouvernement, qui ont été classées comme Protégé B, Protégé C ou classifiées, seront stockées dans une installation informatique approuvée par le GC située dans les limites géographiques du Canada ou dans les locaux d'un ministère du GC situé à l'étranger, comme une mission diplomatique ou consulaire."

Validation

- ☐ Confirmer la politique et le balisage pour l'emplacement des données.

Modèles de service applicables

- IaaS, PaaS, SaaS

Comment activer la localisation des données au Canada

1. Lorsque vous vous inscrivez à Oracle Cloud Infrastructure, Oracle crée une location pour vous dans une région de votre choix, c'est votre région d'origine. Vous ne pouvez provisionner des ressources cloud que dans votre région d'origine. En outre, vous pouvez provisionner des ressources dans d'autres régions cloud, mais avant de bénéficier de cette capacité, vous devez d'abord vous abonner à l'autre région cloud. Pour activer la localisation des données au Canada, sélectionnez une région canadienne comme région d'origine. Si vous souhaitez provisionner des ressources cloud dans d'autres régions, abonnez-vous uniquement aux régions canadiennes. Pour savoir comment vous abonner à la région cloud, consultez le document Oracle situé ici:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/managingregions.htm

Comment montrer que l'emplacement des données est au Canada

1. Connectez-vous à votre console Oracle Cloud et sélectionnez le menu hamburger dans le coin supérieur gauche et choisissez **Administration**, puis **Region Management**.
2. Prenez une capture d'écran de la page "Régions d'infrastructure".
3. Vous pouvez éventuellement utiliser l'API ListRegions pour répertorier les régions auxquelles vous êtes abonné. La documentation de l'API se trouve ici :

https://docs.cloud.oracle.com/en-us/iaas/api/#/en/identity/20160918/Region/ListRegions

Guardrail 6 - Protection des données au repos

Objectif

Protégez les données au repos par défaut (par exemple, le stockage) pour les charges de travail basées sur le cloud.

Considérations clés

- ☐ Demandez conseil aux responsables de la protection de la vie privée et de l'accès aux informations au sein des institutions avant de stocker des informations personnelles dans des environnements en nuage.
- ☐ Implémentez un mécanisme de cryptage pour protéger la confidentialité et l'intégrité des données lorsque les données sont au repos dans le stockage de votre solution.
- ☐ Utilisez des algorithmes et protocoles cryptographiques approuvés par le CSE, conformément à 40.111 et 40.062.
- ☐ Mettre en place des procédures de gestion des clés

Validation

- ☐ Confirmer la politique de chiffrement (par exemple, stockage et / ou VM sur la base d'une évaluation basée sur les risques).

Modèles de service applicables

- IaaS, PaaS, SaaS

Comment activer la protection des données au repos

1. La posture de sécurité d'Oracle Cloud est de crypter automatiquement toutes les données au repos. Aucune autre action n'est donc requise pour activer la protection des données au repos. Des informations supplémentaires concernant ce contrôle de sécurité sont disponibles ici:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Security/Concepts/security_guide.htm

2. Les services de base de données sont également chiffrés par défaut à l'aide du chiffrement transparent des données (TDE). Aucune autre action n'est donc requise. La clé principale est stockée dans Oracle Wallet. Vous pouvez choisir de définir un mot de passe sur Oracle Wallet. Consultez le document suivant pour plus d'informations:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Security/Reference/dbaas_security.htm

Guardrail 7 - Protection des données en transit

Objectif

Protéger les données transitant par les réseaux en utilisant un cryptage et des protections réseau appropriés.

Considérations clés

- ☐ Implémentez un mécanisme de cryptage pour protéger la confidentialité et l'intégrité des données lorsque les données sont en transit vers et depuis votre solution.
- ☐ Utilisez des algorithmes et protocoles cryptographiques approuvés par le CSE.
- ☐ Chiffrement des données en transit par défaut (par exemple TLS v1.2, etc.) pour tous les sites accessibles au public et les communications externes conformément à la direction relative à la mise en œuvre de HTTPS pour les connexions Web sécurisées (ITPIN 2018-01).
- ☐ Chiffrement pour tous les accès aux services cloud (par exemple, stockage cloud, systèmes de gestion de clés, etc.).
- ☐ Envisagez le chiffrement pour la communication de zone interne dans le cloud en fonction du profil de risque et conformément aux instructions du zonage de sécurité réseau CCCS dans ITSG-22 et ITSG-38
- ☐ Mettre en place des procédures de gestion des clés

Validation

- ☐ Confirmer la politique de transmission réseau sécurisée.

Modèles de service applicables

- IaaS, PaaS, SaaS

Comment protéger les données en transit

1. VPN connect fournit un VPN IPSec de site à site entre votre réseau sur site et Oracle Cloud. Le protocole IPSec crypte tous les paquets réseau en transit entre sur site et Oracle Cloud. Vous trouverez de plus amples informations sur VPN Connect ici:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Network/Tasks/overviewIPsec.htm

2. Pour configurer VPN Connect, suivez les instructions situées ici:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Network/Tasks/quickstartIPsec.htm

3. Si vous utilisez FastConnect pour connecter votre site à Oracle OCI, veuillez suivre les instructions du document pour activer le chiffrement à l'aide de FastConnect.:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Resources/Assets/whitepapers/encrypted-fastconnect-public-peering.pdf

Artefacts de protection des données

- Rapport de conformité

Sécurité Internet

Guardrail 8 – Segmenter et séparer

Objectif

Segment et informations séparées en fonction de la sensibilité des informations.

Considérations clés

- ☐ Développer une conception de sécurité du réseau cible qui prend en compte la segmentation via les zones de sécurité du réseau, en alignement avec ITSG-22 et ITSG-38.
- ☐ Mettre en œuvre des niveaux de protection accrus pour les interfaces de gestion.

Validation

- ☐ Confirmer que le service dispose d'un diagramme d'architecture de réseau cible avec une segmentation appropriée entre les zones du réseau.

Modèles de service applicables

- ☐ IaaS, PaaS

Comment isoler vos ressources infonuagique

1. Pour organiser et isoler vos ressources cloud, utilisez Compartments, voir le document «Managing Compartments» situé ici:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/managingcompartments.htm

Guardrail 9 - Services de sécurité du périmètre

Objectif

Établir des périmètres réseau externes et internes et surveiller le trafic réseau.

Considérations clés

- ☐ Assurez-vous que les points de sortie / d'entrée vers et depuis les environnements cloud du GC sont gérés et surveillés. Utilisez les services de sécurité réseau provisionnés de manière centralisée, le cas échéant.
- ☐ Implémentez des mécanismes de protection des limites du réseau pour toutes les interfaces externes qui appliquent une politique de refus de tout ou d'autorisation par exception.

- ☐ Les services de sécurité du périmètre tels que la protection des limites, les services de prévention des intrusions, les services proxy, l'inspection du trafic TLS, etc. doivent être activés en fonction du profil de risque, conformément aux exigences de connectivité sécurisée du GC et aux ITSG-22 et ITSG-38.
- ☐ L'accès au stockage Cloud sera limité aux adresses IP source autorisées uniquement (généralement GC uniquement).

Validation

- ☐ Confirmer la politique de protection des limites du réseau.
- ☐ Confirmer la politique de limitation du nombre d'adresses IP publiques.
- ☐ Confirmer la politique de limitation aux adresses IP source autorisées (par exemple les adresses IP du GC).

Modèles de service applicables

- ☐ IaaS, PaaS, SaaS

Comment configurer les périmètres de réseau externe et interne

1. Il existe plusieurs façons de contrôler la sécurité de votre réseau cloud. Pour obtenir des informations générales sur la sécurité du réseau et comprendre les concepts, consultez ce document Oracle.: https://docs.cloud.oracle.com/en-us/iaas/Content/Network/Concepts/waystosecure.htm

2. Les services réseau offrent deux fonctionnalités de pare-feu virtuels pour contrôler le trafic au niveau des paquets, appelées listes de sécurité et groupes de sécurité réseau, qui utilisent tous deux des listes de sécurité. Pour créer et gérer des listes de sécurité, utilisez le document Oracle suivant:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Network/Concepts/securitylists.htm

3. Pour envoyer du trafic en dehors de votre réseau Oracle Cloud, des tables de routage sont utilisées, le document Oracle suivant fournit des informations supplémentaires:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Network/Tasks/managingroutetables.htm

Comment surveiller le trafic réseau

1. Vous pouvez utiliser les journaux de flux VCN pour surveiller et afficher le trafic réseau au sein de votre Oracle Virtual Cloud Network (VNC). Pour utiliser les journaux de flux, suivez les instructions contenues dans ce document:

   https://blogs.oracle.com/cloud-infrastructure/announcing-vcn-flow-logs-for-oracle-cloud-infrastructure

2. De plus, vous pouvez utiliser l'inspecteur de réseau OCI. Pour utiliser l'inspecteur de réseau OCI, suivez les instructions contenues dans ce document:

https://docs.cloud.oracle.com/en-us/iaas/Content/Compute/References/oci-network-inspector.htm

Artefacts de sécurité réseau

- Diagramme d'architecture de réseau cible

Operations

Guardrail 10 – Services de cyberdéfense

Objectif

Établir un protocole d'entente pour les services défensifs et les services de protection de surveillance des menaces.

Considérations clés

- ☐ Signer un protocole d'entente avec CCCS.
- ☐ Suivez les conseils d'intégration.

Validation

- ☐ Confirmation du CCCS que le protocole d'entente a été signé par le ministère.

Comment configurer les services de cyberdéfense

1. Contact the CCCS to obtain guidance on implementation of cyber defense services for the Oracle Cloud Infrastructure.
2. Communiquez avec le SCCC pour obtenir des conseils sur la mise en œuvre de services de cyberdéfense pour Oracle Cloud.

Modèles de service applicables

- ☐ IaaS, PaaS, SaaS

Guardrail 11 - Journalisation et surveillance

Objectif

Activez la journalisation pour l'environnement cloud et pour les charges de travail basées sur le cloud.

Considérations clés

- ☐ Mettre en place un niveau adéquat de journalisation et de reporting, y compris une fonction de journal d'audit de sécurité dans tous les systèmes d'information.

- ☐ Identifier les événements de la solution qui doivent être audités conformément à la journalisation des événements du GC

Note: Vous devrez peut-être configurer votre solution pour envoyer les enregistrements du journal d'audit à une fonction de journalisation centralisée, si elle est disponible, où les mécanismes d'audit existants seront appliqués.

- ☐ Configurez les alertes et les notifications à envoyer au contact / à l'équipe appropriée dans l'organisation.
- ☐ Configurez ou utilisez une source de temps faisant autorité pour l'horodatage des enregistrements d'audit générés par les composants de votre solution.
- ☐ Surveillez en permanence les événements et les performances du système.

Validation

- ☐ Confirmez que la politique de journalisation des événements est mise en œuvre.
- ☐ Confirmez que les journaux d'événements sont générés.
- ☐ Confirmez que les informations de contact de sécurité ont été configurées pour recevoir des alertes et des notifications.

Modèles de service applicables

2. IaaS, PaaS, SaaS

Journalisation de la configuration

1. 1. Le service Oracle Infrastructure Audit enregistre automatiquement les appels vers tous les points de terminaison de l'interface de programmation d'application publique (API) Oracle Cloud Infrastructure pris en charge sous forme d'événements de journal.
   Aucune configuration supplémentaire n'est requise.
   Pour un aperçu des fonctionnalités d'audit, consultez ce document Oracle:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Audit/Concepts/auditoverview.htm

2. Pour afficher les journaux d'audit, consultez le document suivant:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Audit/Tasks/viewinglogevents.htm

Guardrail 12 – Configuration des places de marché de l'infonuagique

Objectif

Limitez les logiciels des places de marché de l'infonuagique aux produits approuvés par le GC.

Considérations clés

- ☐ Seuls les produits des places de marché de l'infonuagique approuvés par GC doivent être consommés. Il est interdit d'ouvrir le marché commercial.
- ☐ Soumettez des demandes d'ajout de produits tiers sur le marché à SSC Cloud Broker.

Validation

- ☐ Confirmez que les restrictions du marché tiers ont été mises en œuvre.

Modèles de service applicables

- IaaS, PaaS, SaaS

Comment configurer la place de marché de l'infonuagique

L'équipe SSC Cloud Brokering mettra sur liste blanche les images de la place de marché Oracle Cloud dont la consommation est approuvée.

Les images en liste blanche peuvent être provisionnées au sein de votre location cloud.

Aucune action ou configuration supplémentaire n'est requise.

Artefacts d'opérations

- MOU signé avec CCCS
- Rapport de conformité

Références

Garde-corps d'Infonuagique

ID.	Guardrail
01	Protéger le compte racine ou des administrateurs généraux
02	Gestion des privilèges d'administration
03	Accès à la console du nuage
04	Comptes de surveillance organisationnels
05	Hébergement des données
06	Protection des données au repos
07	Protection des données en transit
08	Segmenter et séparer *
09	Services de sécurité du réseau
10	Services de cyberdéfense *
11	Journalisation et surveillance
12	Configuration des marchés de l'informatique en nuage

* Ne fait pas partie de ce document

- Cloud Guardrails on Git

Processus d'audit de conformité (SSC)

Lorsqu'un département procède au contrat Protégé B, il a jusqu'à 30 jours pour mettre en œuvre les garde-corps Cloud, se mettre en conformité et montrer comment ils sont conformes.

TBS a publié une procédure d'exploitation standard (SOP) pour la validation des garde-corps Cloud. La section suivante donne un aperçu du processus d'audit SSC

1. Le ministère achète Protégé B
2. L'équipe des opérations des fournisseurs de cloud de SSC envoie un e-mail de bienvenue au département
3. Dans les 30 jours suivant l'achat:
    a. Les départements créent un document avec des sections pour chaque garde-corps
    b. Les départements envoient un e-mail à SSC (boîte de réception cloud) avec un package complet
    c. Recevoir une réussite ou un échec en matière de conformité
4. SSC envoie un rapport de conformité mensuel au TBS