Guide d’obtention des DNS pour les fonctionnaires gouvernementaux

Bureau du directeur de la technologie de l’ICANN

David Huberman
OCTO-013
24 juillet 2020

ICANN

TABLE DES MATIERES

Ce document fait partie de la série de documents de l'OCTO. Veuillez consulter la page de publication de l'OCTO
pour obtenir la liste des documents compris dans la série. Si vous avez des questions ou des suggestions sur ces documents, veuillez les envoyer à octo@icann.org.

1 Introduction

Ce guide a pour but d'aider les fonctionnaires gouvernementaux responsables des marchés publics à faire de bons choix en matière d'obtention de noms de domaine et du système de noms de domaine (DNS) afin d'assurer la sécurité, la stabilité et la résilience du nommage des services et des hôtes des réseaux de leurs gouvernements. L'utilisation de ce guide ne nécessite pas d'expertise sur le DNS. Il est rédigé dans un langage accessible pour les aider à travailler avec leur service informatique (TI) et leurs fournisseurs.

Ce document est publié par la Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN). L'ICANN est une société à but non lucratif qui, au nom de la communauté Internet, supervise la coordination technique du plus haut niveau du système de noms de domaine (DNS) de l'Internet, contribuant ainsi à assurer sa sécurité, sa stabilité et sa résilience.

Ce guide suggère des technologies opérationnelles et de bonnes pratiques. Tous les fournisseurs n'offriront pas tous les services ou technologies énumérés dans ce document. Mais pour vous aider à prendre une décision d'acquisition pleinement informée, vous devriez savoir quelles sont les technologies recommandées prises en charge ou pas.

Ce guide se concentre sur trois étapes pour obtenir et rendre opérationnels les noms de domaine :

- Choix d'un nom de domaine
- Enregistrement d'un nom de domaine
- Opérations du DNS : hébergement pour votre nom de domaine

2 Choix d'un nom de domaine

Les noms de domaine se terminent par un suffixe. Certains exemples de ces suffixes incluent *.com*, *.gov*, *.uk* et *.asia*. Il y a plus de 1300 de ces suffixes dans le DNS qui sont appelés domaines de premier niveau, ou *TLD*. Lorsque vous choisissez un nom de domaine, vous devez d'abord décider quel TLD vous utiliserez, soit-il un nom générique (suffixes comme « .com » ou « .asia » qui ont une signification générique) connu sous le nom *de gTLD*, ou un domaine de premier niveau géographique à deux caractères, appelé ccTLD, d'un territoire reconnu (suffixes tels que *.fr* pour la France ou *.za* pour l'Afrique du Sud, où chaque suffixe correspond aux codes géographiques répertoriés dans la norme ISO-3166-2).[1]

Dans de nombreux cas et afin de respecter les règles et les politiques locales établies, les agences gouvernementales peuvent avoir besoin d'utiliser un nom de domaine sous le ccTLD de leur pays (par exemple, *go.jp* pour une agence gouvernementale au Japon). Les différents gouvernements opèrent leurs ccTLD de différentes manières. Nous vous recommandons de contacter l'opérateur des services de noms de domaine de votre gouvernement, de vous renseigner sur les politiques en place et de vérifier leurs fonctionnalités, leurs fonctions de sécurité et leurs plans de continuité des opérations (comme décrit ci-dessous) afin de pouvoir

[1] Consultez https://www.iso.org/iso-3166-country-codes.html pour plus d'informations sur la norme ISO-3166-2. L'ICANN **n'attribue pas** de codes ISO-3166. Cette attribution est du ressort de l'agence de maintenance de la norme ISO-3166.

les comparer à toutes les autres options de TLD qui pourraient vous être proposées. Les coordonnées des gestionnaires de chaque TLD, y compris pour chaque ccTLD, sont publiées dans un annuaire situé à l'adresse https://www.iana.org/domains/root/db (pour accéder aux informations de contact, vous devez cliquer sur le lien pour le TLD).

L'ICANN a un contrat avec chaque gTLD qui spécifie de nombreuses règles. Plus précisément, les gTLD sont tenus de respecter les conditions générales du contrat de registre de l'ICANN dont ils sont signataires.[2] Ces conditions générales établissent certaines exigences techniques et politiques pour les gestionnaires de gTLD, visant à la fois à améliorer la santé de l'écosystème du DNS et à protéger les détenteurs de noms de domaine. En revanche, les ccTLD n'ont pas signé de contrats avec l'ICANN. Tout recours juridique dont un détenteur de nom de domaine pourrait avoir besoin dépendra vraisemblablement de la juridiction compétente dans laquelle le registre ccTLD fonctionne.

Que vous souhaitiez enregistrer un nom de domaine sous un ccTLD ou un TLD générique, il existe quatre fonctionnalités qu'un TLD peut offrir qui, de notre avis, sont importantes : le soutien des DNSSEC, le soutien de l'IPv6, la mise en œuvre d'une certaine forme de verrouillage du registre et la réputation du TLD.

2.1 Prise en charge des DNSSEC

Les utilisateurs sont mieux protégés si les noms de domaine sont signés cryptographiquement par le propriétaire du nom de domaine, c'est-à-dire votre organisation. Votre organisation peut signer numériquement vos noms de domaine par le biais d'une technologie appelée DNSSEC (Extensions de sécurité du système des noms de domaine). Le document de l'ICANN « DNSSEC : sécurisation du DNS » donne plus d'informations sur l'importance des DNSSEC.[3]

Pour signer votre domaine, le TLD de votre choix doit prendre en charge *la signature DNSSEC*. La bonne nouvelle est que la plupart des TLD (y compris tous les TLD génériques) prennent en charge les DNSSEC. Toutefois, si la prise en charge des DNSSEC n'est pas indiquée comme une option avec le TLD de votre choix, vous devez vous renseigner sur le support actuel ou prévu pour cette option. Certes, il n'est pas toujours simple de s'informer du niveau de support des DNSSEC offert par un TLD. Certains TLD publieront ces informations sur leur site Web ; d'autres, non. Vous pourriez être en mesure de faire des recherches sur le Web pour trouver cette information, ou vous pouvez même devoir leur envoyer un e-mail ou les appeler pour en discuter.

2.2 Prise en charge de l'IPv6

Les machines sur Internet utilisent des adresses IP (Protocole Internet) pour s'identifier. Il existe deux types d'adresses IP : IPv4 et IPv6. Les adresses IPv4 sont les types d'adresses IP les plus courantes. L'IPv6 est un nouveau type d'adresse IP conçu pour aider à la croissance continue de l'Internet à mesure que de plus en plus de dispositifs sont ajoutés.

[2] Il existe plusieurs versions du contrat de registre de l'ICANN, et différents TLD sont signataires de différentes versions. La version actuelle est connue sous le nom de « contrat de registre de base de 2017 », et se trouve à l'adresse suivante : https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html

[3] Consultez https://www.icann.org/en/system/files/files/octo-006-en.pdf

Comme certains gouvernements ont des exigences pour que l'infrastructure Internet supporte à la fois l'adressage IPv4 et IPv6, vérifiez auprès de l'opérateur TLD pour vous assurer que les adresses IPv4 et IPv6 sont supportées par vos serveurs DNS. Plus précisément, l'opérateur TLD doit vous offrir le support nécessaire pour que vous puissiez avoir des serveurs de noms faisant autorité qui utilisent des adresses IPv6. Si tel est votre cas mais votre opérateur TLD ne supporte pas l'IPv6, le monde ne pourra pas atteindre les sites de votre domaine.

2.3 Verrouillage du registre

Une autre considération importante lors du choix d'un TLD est de demander à l'opérateur de TLD s'il prend en charge une fonctionnalité appelée *verrouillage du registre*.

Un opérateur de TLD gère un « registre » qui contient tous les domaines de second niveau, par exemple, example.tld, au sein du TLD.[4] Le verrouillage du registre permet aux propriétaires de noms de domaine, connus sous le nom de titulaires de nom de domaine, de dire à l'opérateur du TLD de « verrouiller » le nom de domaine, tout comme le verrouillage des portes de votre voiture. Lorsque votre domaine est verrouillé, personne ne peut y apporter des modifications, le supprimer ou le transférer à un autre titulaire sans une sorte de processus d'autorisation accordé entre vous-même et l'opérateur du TLD. Notez, cependant, qu'il n'existe pas de normes à l'échelle de l'industrie pour la mise en œuvre du verrouillage du registre. Vous devez donc demander à l'opérateur du TLD s'il offre un verrouillage du registre et, le cas échéant, comment il fonctionne.

En général, nous pensons que le meilleur processus pour autoriser des changements implique une autorisation « hors bande », où toutes les parties ne s'appuient pas sur une communication centrée sur Internet, mais plutôt sur des appels téléphoniques ou une autre méthode que les attaquants auraient du mal à pénétrer. Les modifications apportées aux caractéristiques de base d'un nom de domaine devraient être très rares ; il est donc acceptable de se fier à un processus plus lent, comme l'autorisation hors bande. Toutefois, en même temps, il est probablement bon de s'assurer que votre opérateur de TLD a un processus d'escalade clairement rédigé dans le cas encore moins fréquent que certaines données du DNS doivent être modifiées en cas d'urgence.

Nous encourageons fortement tous les titulaires de noms de domaine à utiliser des TLD qui prennent en charge le verrouillage du registre, car cela empêche les attaques connues qui peuvent compromettre des domaines entiers.

2.4 Réputation

Enfin, avant de choisir un TLD, envisagez d'examiner sa réputation. De l'avis de la société anti-abus Spamhaus,[5] un TLD a une mauvaise réputation si trop de noms de domaine enregistrés sont liés à des activités telles que le spam et la distribution de logiciels malveillants. Bien qu'il y ait toujours des noms de domaine malveillants enregistrés dans chaque TLD, des sociétés comme Spamhaus évaluent les portefeuilles de noms de TLD pour déterminer la « méchanceté » ou la « bonté » d'un TLD.

[4] De manière confuse, un opérateur TLD peut également être appelé opérateur de registre
[5] Consultez https://www.spamhaus.org/

Ce qui est important, c'est de choisir un TLD n'ayant pas un nombre significatif d'enregistrements malveillants. Lorsqu'un TLD a une mauvaise réputation dans la communauté technique, il peut être bloqué par des fournisseurs de services Internet (FSI) et des opérateurs de réseau d'entreprise. Si le TLD que vous utilisez a une mauvaise réputation, vous pouvez, par exemple, ne pas être en mesure d'envoyer des e-mails en utilisant votre domaine, car de nombreux serveurs de messagerie sont configurés automatiquement pour bloquer les e-mails provenant de domaines bloqués.

Il existe de nombreuses entreprises anti-abus qui publient des classements de la réputation de TLD, y compris Spamhaus et SURBL.[6]

3 Choix d'un bureau d'enregistrement pour votre nom de domaine

Une fois que vous aurez choisi un TLD pour votre agence, vous enregistrerez ensuite un nom de domaine sous ce TLD. Dans certains ccTLD il est possible d'enregistrer des noms de domaine directement auprès de l'opérateur de TLD. Toutefois, pour de nombreux ccTLD et pour la plupart des gTLD, les noms de domaine doivent être enregistrés par l'intermédiaire d'un « bureau d'enregistrement » de noms de domaine.[7] Dans cette section, nous énumérons certains critères que nous vous suggérons d'étudier lors du choix d'un bureau d'enregistrement potentiel pour votre nom de domaine.

3.1 Accréditation

L'ICANN offre l'accréditation officielle des bureaux d'enregistrement. Obtenir et maintenir avec succès l'accréditation signifie que le bureau d'enregistrement a satisfait tous les critères techniques, opérationnels et financiers nécessaires pour être considéré comme un bureau d'enregistrement.[8] Il est important que le bureau d'enregistrement soit tenu de respecter les conditions générales du contrat d'accréditation de bureau d'enregistrement,[9] qui comprend de nombreuses protections pour les titulaires de noms de domaine.

Si vous enregistrez un nom de domaine sous un gTLD, assurez-vous de choisir un bureau d'enregistrement accrédité par l'ICANN. Vous trouverez une liste des bureaux d'enregistrement accrédités sur le site Web de l'ICANN.[10] Le contrat signé par les bureaux d'enregistrement et l'ICANN leur permet également de travailler avec des « revendeurs », qui sont des sociétés tierces qui offrent des services d'enregistrement de noms de domaine pour le compte d'un bureau d'enregistrement. Toutefois, pour les domaines de grande valeur, nous recommandons

6 Consultez http://www.surbl.org/

7 Vous pouvez considérer la paire opérateur de registre/bureau d'enregistrement comme étant similaire à la division entre commerce grossiste/vente au détail, c'est-à-dire, tout comme les gens achètent des produits chez les détaillants qui proviennent de grossistes, les titulaires achètent des noms de domaine auprès des bureaux d'enregistrement qui obtiennent leur inventaire auprès des opérateurs de registre.

8 Une description des qualifications pour l'accréditation peut être trouvée à https://www.icann.org/resources/pages/policy-statement-2012-02-25-fr#IIA

9 Le RAA actuel est publié à : https://www.icann.org/resources/pages/registrars/registrars-en

10 Consultez https://www.icann.org/registrar-reports/accreditation-qualified-list.html

de travailler directement avec les bureaux d'enregistrement accrédités lorsque cela est possible, car cela réduit le nombre de parties impliquées au cas où il serait nécessaire de résoudre un problème urgent.

Si vous enregistrez un nom de domaine sous un ccTLD, assurez-vous d'utiliser un bureau d'enregistrement ou un revendeur autorisé par l'opérateur du registre ccTLD.

3.2 Fonctions de sécurité de base

Tout bureau d'enregistrement de noms de domaine que vous choisissez devrait supporter des mots de passe sûrs (normalement des chaînes longues avec une combinaison d'une lettre majuscule, d'une lettre minuscule et d'au moins un symbole) et offrir une authentification multifactorielle (un mot de passe plus un jeton de sécurité, qui est souvent un code SMS envoyé à un téléphone mobile) pour les utilisateurs se connectant à leurs portails de compte.

Vous devez également vérifier auprès du bureau d'enregistrement ou du revendeur que les portails de compte client s'exécutent sur un site Web pour lequel les communications sont chiffrées à l'aide de HTTPS. Cela permet de garantir la confidentialité des communications électroniques entre votre personnel du service des technologies de l'information et le bureau d'enregistrement/revendeur.

3.3 Prise en charge des DNSSEC

Si vous avez fait l'effort de vous assurer que votre opérateur de registre prend en charge les DNSSEC, il est important que vous choisissiez un bureau d'enregistrement qui vous permette de fournir les informations nécessaires associées aux DNSSEC et, si vous ne gérez pas vos zones directement, de signer vos zones avec les DNSSEC. Les bureaux d'enregistrement devraient généralement publier les services DNSSEC qu'ils utilisent sur leur site Web. Vous pouvez également faire en sorte que votre personnel technique discute avec le bureau d'enregistrement du niveau de soutien des DNSSEC offert pour vous assurer que vos exigences techniques soient satisfaites.

3.4 Prise en charge de l'IPv6

Le bureau d'enregistrement de noms de domaine doit supporter l'utilisation d'adresses IPv4 et IPv6, c'est-à-dire vous permettre de gérer les enregistrements de ressources d'adresse (« A » et « AAAA ») pour tous les périphériques que vous souhaitez nommer dans votre nom de domaine.

3.5 Exportation de données

En pensant à long terme, vous décidez de ne pas vous engager avec votre bureau d'enregistrement de noms de domaine pour toujours. Vos besoins technologiques peuvent changer, le service du bureau d'enregistrement peut empirer, ou quelque chose d'autre pourrait se produire à l'avenir et vous décidez de transférer vos noms de domaine à un autre bureau d'enregistrement. Dans ce cas, il serait utile que le bureau d'enregistrement vous autorise à « exporter vos données de zone », c'est-à-dire qu'il vous permette de télécharger toutes les données du DNS associées à vos noms de domaine. Cela vous permettra de contrôler les

données du DNS de vos domaines et permettra au personnel des TI de transférer rapidement les services à un nouveau bureau d'enregistrement.

3.6 Réputation

Tout bureau d'enregistrement de noms de domaine que vous aurez choisi devrait avoir une bonne réputation anti-abus et démontrer sa capacité de travailler en collaboration avec les organismes nationaux et internationaux d'application de la loi lorsque l'utilisation malveillante du DNS leur est signalée. Par exemple, vous devriez vous assurer que le bureau d'enregistrement utilise un programme anti-fraude performant lui permettant de détecter et d'arrêter les enregistrements de noms de domaine impliquant l'utilisation d'informations de cartes de crédit volées.

4 Opérations du DNS : hébergement de votre nom de domaine par une tierce partie

Une fois que vous avez enregistré un nom de domaine, il doit être hébergé quelque part. Il peut être hébergé par votre service informatique gouvernemental ou il peut être possible ou même nécessaire de choisir un fournisseur tiers pour héberger vos noms de domaine dans leurs centres de traitement de données. Cet hébergement peut être offert dans le cadre d'un ensemble de services que vous achetez auprès d'un fournisseur de services informatiques. Cette section vise à vous aider à choisir un fournisseur tiers et suggère quelques aspects qui, de notre avis, sont importants.

4.1 Gestion de noms de domaine

Il est important que vous puissiez créer rapidement et facilement des sous-domaines. Un sous-domaine est un nom de domaine qui ressemble à *mail.department.za* ou *elections.government.co.jp* ou similaire. Vous devez vous renseigner sur la facilité de création, de modification et de suppression des sous-domaines, en particulier en masse. Il est également important de pouvoir créer des types d'enregistrement DNS modernes, par exemple le type d'enregistrement d'authentification TLS (TLSA) utilisé par une technologie de sécurité dénommée Authentification d'entités nommées basée sur le DNS (DANE).

4.2 Sécurité des opérations

L'une des considérations les plus importantes lors de l'achat de services DNS est la sécurité. Il est essentiel que votre organisation *conserve le contrôle* de tous vos noms de domaine et des services hébergés sur ces noms à tout moment. La meilleure façon de maintenir ce contrôle est de travailler toujours avec des fournisseurs (du bureau d'enregistrement de noms de domaine à tous les fournisseurs de services informatiques) ayant une culture et un engagement forts vis-à-vis de la sécurité. Lorsque vous perdez le contrôle de n'importe quelle partie de vos technologies DNS, des attaques peuvent se produire très rapidement, ainsi que des violations de données.

Pour un fournisseur d'hébergement tiers, nous remarquons trois éléments de sécurité essentiels pour assurer une sécurité renforcée :

- Il doi0t proposer une authentification multifactorielle pour accéder au compte. Si l'accès aux technologies est disponible via un seul facteur (par exemple, un mot de passe), il n'est pas sécurisé.
- Le fournisseur devrait avoir publié des pratiques et des politiques de sécurité complètes.
- Le fournisseur devrait également offrir une surveillance de sécurité détaillée des éléments de l'infrastructure et des données du DNS. Cette surveillance doit être effectuée régulièrement pour s'assurer que les modifications apportées par un attaquant soient détectées rapidement. En cas de détection d'une activité anormale, le fournisseur doit disposer d'un système d'alerte progressif pour en avertir le personnel technique.

En règles générales, il est également important de poser des questions sur le soutien pour *BCP 38*.[11] BCP 38 est un document qui spécifie les pratiques opérationnelles que les fournisseurs doivent suivre pour réduire la fraude du routage de réseau sur Internet. Tous les fournisseurs de réseau devraient supporter BCP38. Dans certains cas exceptionnels, il peut y avoir des raisons pour lesquelles le BCP38 ne peut pas être suivi, mais dans le contexte des organisations d'hébergement de domaine typiques, ces cas seraient inhabituels et vous devriez demander des explications détaillées.

4.3 Service de noms faisant autorité

Le service de noms faisant autorité est la façon dont vous dites au monde que votre nom de domaine se résout en adresses IP particulières, quel serveur de messagerie vous utilisez pour le courrier entrant, comment l'espace de noms de votre organisation est défini, etc. Que vous souhaitiez configurer vos propres serveurs de noms faisant autorité ou que vous payiez un fournisseur tiers pour héberger les serveurs de noms faisant autorité en votre nom, vous devez tenir compte de quelques considérations :

- La meilleure pratique consiste à disposer de plusieurs serveurs de noms faisant autorité distincts sur des réseaux distincts, géographiquement et topologiquement distincts.
- Assurez-vous que tout service d'hébergement de serveur de noms supporte entièrement les DNSSEC, y compris le téléchargement d'enregistrements DNSKEY et/ou DS vers votre bureau d'enregistrement de noms de domaine.
- Assurez-vous que vous recevrez le support nécessaire pour des ajouts, des modifications ou des suppressions à grande échelle des données du DNS, y compris les enregistrements de ressource et les sous-domaines.
- Comprenez les mesures de protection contre les attaques par déni de service distribué, que vous décidiez d'utiliser vos propres serveurs de noms ou de les configurer avec un fournisseur tiers.

4.4 Prise en charge de l'IPv6

Il est de plus en plus essentiel que les logiciels et les services du fournisseur d'hébergement tiers supportent IPv6. Les Registres Internet régionaux (RIR), qui attribuent les adresses IP au

11 Consultez https://datatracker.ietf.org/doc/bcp38/

premier niveau, ont élaboré de nombreux documents pour vous aider à prendre de bonnes décisions d'acquisition en matière de services qui utilisent des adresses IP. Á savoir :

- AFRINIC, le RIR pour l'Afrique, a un guide sur l'IPv6 adressé aux gouvernements.[12]
- ARIN, le RIR pour l'Amérique du Nord et certaines régions des Caraïbes, a produit une vidéo de 6 minutes expliquant ce qu'est l'IPv6 et pourquoi il est important.[13]
- LACNIC, le RIR pour l'Amérique latine, a publié un guide de déploiement de l'IPv6 en 12 étapes pour les gouvernements et les entreprises.[14]
- RIPE NCC, le RIR pour l'Europe et certaines parties de l'Asie occidentale, a publié un guide sur les exigences de l'IPv6 en matière d'équipement en TIC.[15]

5 Synthèse

Dans ce guide, nous avons abordé de nombreux sujets. Encore une fois, tous les fournisseurs ne seront pas en mesure d'offrir tous les services que nous avons énumérés ici et qui, de notre avis, sont importants. Mais les messages que nous espérons transmettre sont les suivants :

- La sécurité est importante et bien plus qu'un simple mot de passe bien choisi.
- Le support des DNSSEC et de l'IPv6 doit être une exigence de base.
- Les entreprises avec lesquelles vous travaillez doivent s'engager à maintenir une bonne réputation pour atténuer les abus et traiter les plaintes d'abus.

12 Consultez https://afrinic.net/guidebook-gov-ipv6
13 Consultez https://youtu.be/bkLs5_geTM4
14 Consultez https://www.lacnic.net/innovaportal/file/3635/1/10-12-steps-government-ipv6-v3.pdf
15 Consultez https://www.ripe.net/publications/docs/ripe-554

Annexe : Liste de contrôle des acquisitions

Choix d'un registre TLD

- ❑ Il prend en charge les DNSSEC

  Les noms de domaine enregistrés sous ce TLD peuvent être signés par les DNSSEC
- ❑ Il prend en charge IPv4 et IPv6

  Les enregistrements du serveur de noms du TLD peuvent être émis avec des adresses IPv4 et IPv6
- ❑ Il offre le verrouillage du registre

  Dispose d'un processus de verrouillage des enregistrements et nécessite une autorisation hors bande pour apporter des modifications aux enregistrements verrouillés
- ❑ Il a une bonne réputation

  Le TLD lutte activement contre les domaines malveillants enregistrés dans le TLD

Choix d'un bureau d'enregistrement pour votre nom de domaine

- ❑ Il s'agit d'un bureau d'enregistrement accrédité ou autorisé par l'ICANN

  Si un gTLD est accrédité par l'ICANN, et si un ccTLD est autorisé à offrir des domaines
- ❑ Il pratique une bonne cyber-hygiène

  Il exige une authentification multifactorielle pour les connexions de compte d'utilisateur et les pages Web utilisent HTTPS
- ❑ Il prend en charge les DNSSEC

  Les noms de domaine peuvent être signés par les DNSSEC
- ❑ Il permet aux noms de domaine d'être hébergés par des tiers

  Prend uniquement en charge l'enregistrement des noms de domaine et ne vous oblige pas à héberger le nom de domaine sur ses serveurs Web
- ❑ Il permet l'exportation de données

  Les données du DNS peuvent être exportées par votre personnel des services informatiques afin de vous permettre de les transférer facilement vers un nouveau bureau d'enregistrement
- ❑ Il prend en charge les adresses IPv4 et IPv6

  Les enregistrements du serveur de noms peuvent être émis avec des adresses IPv4 et IPv6
- ❑ Il a une bonne réputation

  Il est proactif dans la prévention, la détection et l'atténuation des utilisations malveillantes, et la réponse aux plaintes

Choix d'un fournisseur d'hébergement tiers

- ❑ Il prend en charge la gestion de sous-domaines en masse et les types d'enregistrement DNS modernes

  Peut ajouter, modifier ou supprimer des sous-domaines en masse et ajouter des enregistrements de ressources comme TLSA

- ❑ Il a des opérations sécurisées

  Authentification multifactorielle pour les connexions de l'utilisateur, les pratiques et les stratégies de sécurité publiées, surveillance proactive des données DNS et prise en charge de BCP38

- ❑ Il prend en charge des services DNS faisant autorité

  Serveurs de noms géographiquement disparates, bonne protection contre les attaques, et plus encore

- ❑ Il prend en charge les adresses IPv4 et IPv6

  Accès aux serveurs du fournisseur et mises à jour du serveur de noms supportant IPv4 et IPv6