

Choisir un service AWS de mise en réseau et de diffusion de contenu



Choisir un service AWS de mise en réseau et de diffusion de contenu:

AWS Guide de décision

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques commerciales et la présentation commerciale d'Amazon ne peuvent pas être utilisées en relation avec un produit ou un service extérieur à Amazon, d'une manière susceptible d'entraîner une confusion chez les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon sont la propriété de leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Introduction 1

Comprenez 2

Tenez compte 4

Choix 9

Utiliser 10

Explorez 22

Historique du document 23

..... xxiv

Choisir un service AWS de mise en réseau et de diffusion de contenu

Objectif :

Aidez à déterminer les services de mise en AWS réseau et de diffusion de contenu les mieux adaptés à votre organisation.

Dernière mise à jour :

16 janvier 2025

Services couverts :

- [Amazon API Gateway](#)
- [AWS Client VPN](#)
- [AWS Cloud WAN](#)
- [Amazon CloudFront](#)
- [AWS Terminal de transfert de données](#)
- [AWS Direct Connect](#)
- [Elastic Load Balancing](#)
- [AWS Firewall Manager](#)
- [AWS Global Accelerator](#)
- [AWS Network Firewall](#)
- [AWS PrivateLink](#)
- [Amazon Route 53](#)
- [AWS Shield](#)
- [AWS Site-to-Site VPN](#)
- [AWS Transit Gateway](#)
- [Accès vérifié par AWS](#)
- [Amazon VPC](#)
- [Amazon VPC IPAM](#)
- [Amazon VPC Lattice](#)

- [AWS WAF](#)

Le choix d'une approche en matière de mise en réseau dans le cloud et de diffusion de contenu peut s'avérer complexe, en particulier si vous êtes habitué à gérer et à configurer des réseaux avec du matériel sur site. Heureusement, la [création de réseaux dans le cloud](#) partage des concepts fondamentaux avec la création sur site, tels que l'adressage IP, l'équilibrage de charge et le routage. La connaissance de ces concepts vous aidera à comprendre ce dont Services AWS vous avez besoin.

Amazon Web Services (AWS) propose plus de 20 services de mise en réseau et de diffusion de contenu spécialement conçus que vous pouvez utiliser pour créer, exploiter et sécuriser vos réseaux cloud dans tous vos environnements cloud et sur vos sites cloud et périphériques distribués dans le monde entier. Vous pouvez également créer une infrastructure réseau qui étend votre environnement sur site à AWS.

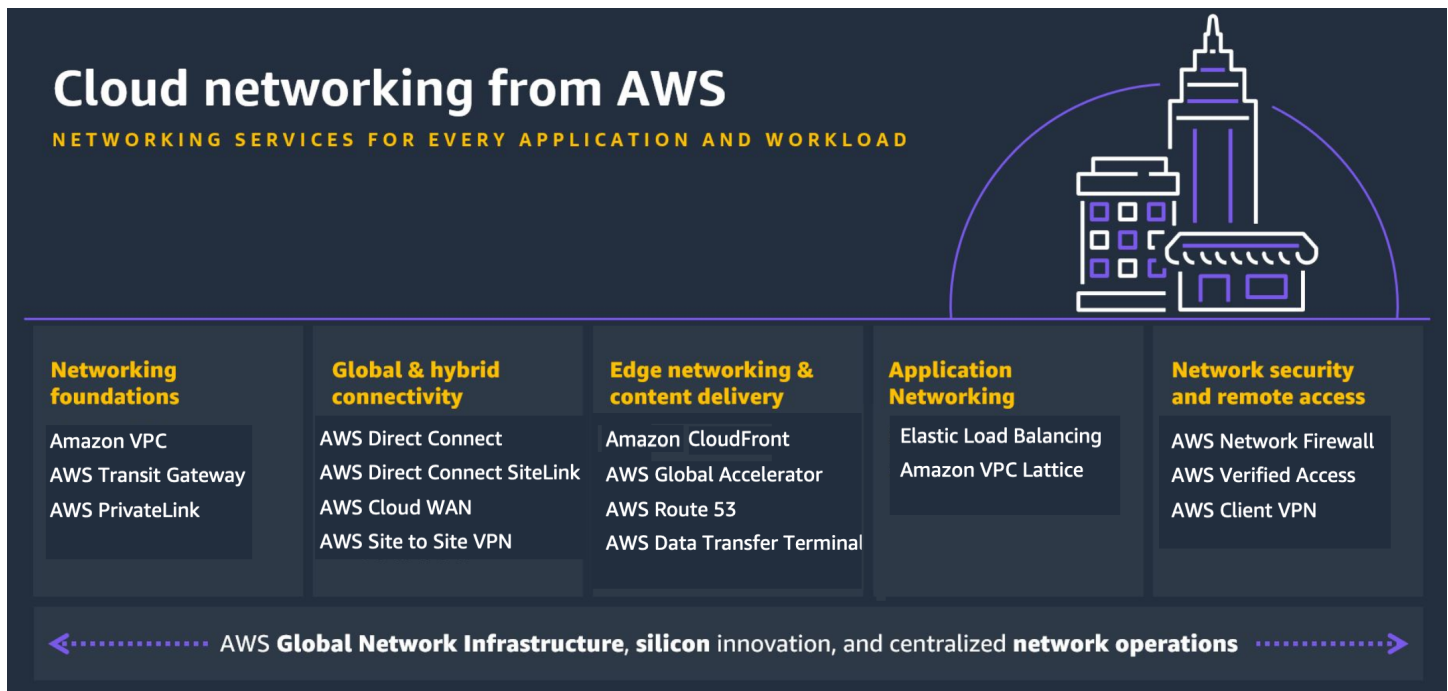
Ce guide de décision vous aidera à vous poser les bonnes questions pour choisir les services et outils de mise en réseau et de diffusion de contenu qui répondent à vos besoins.

[Cette vidéo propose une introduction de quatre minutes au AWS réseautage.](#)

Comprenez

Ce que vous intégrez AWS dépend des besoins de votre entreprise. Dans ce guide, nous utilisons le terme charges de travail pour désigner tout ensemble de ressources et de code apportant une valeur commerciale, comme une application destinée aux clients ou un processus principal.

Les services de mise en réseau et de diffusion de contenu se AWS répartissent en quatre catégories : les bases de la mise en réseau, la connectivité globale et hybride, la mise en réseau de pointe et la diffusion de contenu, et la mise en réseau d'applications.



Fondements du réseautage

Dans AWS, vos charges de travail s'exécutent dans un ou plusieurs [Amazon Virtual Private Cloud \(VPCs\)](#). Une fois que vos charges de travail sont arrivées VPCs, vous pouvez les connecter à d'autres, par VPCs exemple, [AWS Transit Gateway](#) ou vous pouvez les connecter à des services SaaS (Software as a Service), y compris d'autres Services AWS, tels que. [AWS PrivateLink](#) Amazon VPC vous permet de fournir une section privée et isolée dans AWS Cloud laquelle vous pouvez lancer des AWS ressources sur un réseau virtuel à l'aide de plages d'adresses IP définies par le client. Amazon VPC vous propose plusieurs options pour connecter vos réseaux AWS virtuels à d'autres réseaux distants.

Connectivité globale et hybride

Vous pouvez utiliser les services de cette catégorie pour vous connecter en toute sécurité depuis des réseaux locaux à vos charges de travail dans le. AWS Cloud Vous pouvez créer un [réseau privé virtuel \(VPN\)](#) pour connecter des utilisateurs distants en utilisant [AWS Client VPN](#), connecter des réseaux locaux à l'[AWS Site-to-Site VPN](#) aide ou créer un réseau étendu (WAN) mondial avec [AWS Cloud WAN](#). Vous pouvez également configurer une connexion privée directe avec l'utilisateur [AWS Direct Connect](#), AWS Cloud fournissant ainsi une connexion directe et sécurisée au cloud avec des performances prévisibles. Vous devrez peut-être également connecter vos centres de données sur site, vos sites distants et le cloud. [Un réseau hybride](#) peut connecter ces différents environnements.

Mise en réseau de pointe et diffusion de contenu

Les services de cette catégorie contribuent à améliorer les performances grâce à la mise en cache et à l'optimisation du transport. [Amazon](#) en est un bon exemple CloudFront. Vous souhaiterez également que le trafic client soit acheminé de manière optimale pour garantir la disponibilité à l'aide de services tels qu'[Amazon Route 53](#). En outre, il est important que le trafic client soit acheminé afin de tirer le meilleur parti de l'infrastructure AWS mondiale à l'aide de services tels que [AWS Global Accelerator](#). AWS Le [terminal de transfert de données](#) est un emplacement physique prêt à être connecté au réseau où vous pouvez emporter vos périphériques de stockage de données pour un transfert de données rapide vers et depuis le. AWS Cloud

Mise en réseau d'applications

Au fur [AWS App Mesh](#) et à mesure que vous adopterez le AWS Cloud, vous devrez réfléchir à la manière de connecter les charges de travail à grande échelle, en utilisant [Amazon VPC](#) Lattice, d'intégrer les charges de travail de VPCs votre ordinateur à l'[API](#) aide d'[Amazon API Gateway](#) et de gérer l'utilisation des adresses IP des ressources qui s'exécutent sur vous à l' VPCs aide d'[Amazon VPC](#) IP Address Manager (IPAM). À mesure que la demande des clients augmente, vous pouvez faire en sorte que les charges de travail de votre entreprise VPCs puissent évoluer et garantir une haute disponibilité en utilisant [Elastic Load Balancing](#).

Sécurité réseau et accès à distance

Amazon VPC vous aide à sécuriser l'accès à vos charges de travail, mais les services de cette catégorie offrent une protection améliorée contre les acteurs malveillants et les utilisateurs non autorisés en utilisant [AWS Network Firewall](#), [AWS Shield](#), [Accès vérifié par AWS](#) et. [AWS WAF](#) Pour garantir la sécurité du réseau, pensez à utiliser le pare-feu DNS Amazon Route 53, [AWS Network Firewall](#) [AWS Firewall Manager](#), les [listes de contrôle d'accès au réseau](#) et les groupes de sécurité.

Tenez compte

Il est important que vous choisissiez les services réseau qui répondent aux besoins de votre entreprise. Voici certains des critères à prendre en compte lors du choix des services réseau.

Business objectives

Les services réseau que vous choisirez dépendront de vos objectifs commerciaux. Évaluez votre situation actuelle et celle que vous souhaitez atteindre en termes de sécurité, de fiabilité, d'accessibilité et de performance de vos charges de travail exécutées dans le AWS Cloud.

- Déterminez dans quelle mesure les services réseau que vous utilisez s'adaptent à vos stratégies de migration et d'intégration. Une [architecture réseau hybride](#) peut vous aider à répondre à ce besoin en intégrant votre centre de données sur site et AWS.
- Consultez les [blogs sur le réseautage et la diffusion de contenu](#) dans Let's architect ! AWS série de blogs pour voir ce que d'autres construisent dans le AWS Cloud.
- Examinez les options tierces disponibles pour vous aider à accélérer l'adoption de vos services réseau. [AWS Marketplace](#) fournit un catalogue numérique organisé que vous pouvez utiliser pour trouver, acheter et déployer des solutions réseau.
- Décidez s'il serait avantageux de travailler avec une [AWS Partner](#) entreprise spécialisée dans le réseautage et la diffusion de contenu. Les membres du AWS Partner Network sont des experts stratégiques et des constructeurs expérimentés qui peuvent vous aider à répondre à vos besoins avec le AWS Cloud.
- Découvrez les [cours AWS de mise en réseau en ligne](#) sur AWS Skill Builder qui couvrent des services tels qu'Amazon VPC, AWS Cloud WAN et Amazon Route 53.

Workload characteristics

Les services réseau que vous choisirez dépendront des caractéristiques de vos charges de travail.

- Les services de mise en réseau ont chacun un rôle particulier à jouer. Des services tels que AWS Cloud WAN AWS Transit Gateway sont adaptés à la connexion des charges de travail en VPCs cours d'exécution. Amazon API Gateway crée un environnement public APIs afin que vos clients puissent se connecter à vos charges de travail. AWS Global Accelerator peut vous aider à améliorer la fiabilité, la sécurité et la latence de vos charges de travail.
- À mesure qu'Internet continue de croître, le besoin d'adresses IP pour les appareils augmente également. Le format le plus courant pour les adresses IP est IPv4. Le format le plus récent pour les adresses IP est IPv6. IPv6 fournit plus d'espace d'adressage et résout le problème de l'[épuisement des IPv4 adresses](#). Services AWS la prise en charge IPv6 inclut la prise en charge de la configuration à double pile (IPv4 ou IPv6) ou des configurations IPv6 uniquement. Le nombre de Services AWS ces aides IPv6 ne cesse de croître. Pour consulter les services actuellement pris en charge IPv6, consultez [Services AWS ce support IPv6](#).

Data protection

Il est important de prendre en compte la protection de vos données dans le AWS Cloud.

- Les entreprises doivent protéger les données de leurs clients contre l'évolution des cyberrisques. Amazon VPC vous aide à sécuriser l'accès aux charges de travail en cours d'exécution VPCs, mais envisagez des mesures de protection des données améliorées, telles que, AWS Network Firewall AWS Shield AWS WAF, et Amazon Route 53 Resolver le pare-feu DNS.
- Il est recommandé d'utiliser le chiffrement au niveau de l'application (TLS), quel que soit le transport, comme mesure de défense approfondie afin de garantir la confidentialité. end-to-end
- Si les charges de travail que vous VPCs avez besoin de vous connecter à d'autres services Services AWS, vous pouvez vous connecter à ces services par programmation en utilisant des points de terminaison d'API sur Internet public. Toutefois, si vous souhaitez envoyer des données via une connexion privée, utilisez AWS PrivateLink. De nombreux membres AWS Partner Network proposent leurs solutions SaaS via AWS PrivateLink.

Availability

La disponibilité est la capacité d'une application à maintenir le temps de disponibilité. Il est important que vos clients puissent utiliser les produits et services que vous avez intégrés VPCs avec un minimum ou aucun temps d'arrêt.

- L'infrastructure AWS mondiale repose sur [Régions AWS des zones de disponibilité](#). Lorsque vous déployez vos charges de travail sur votre VPCs, vous devez les déployer dans plusieurs zones de disponibilité afin de garantir que votre charge de travail est toujours disponible en cas de défaillance d'une seule zone de disponibilité.
- Pour améliorer la disponibilité, l'évolutivité, la sécurité et les performances des charges de travail exécutées sur votre ordinateur VPCs, pensez à l'[équilibre de charge](#) (Elastic Load Balancing). Vous pouvez utiliser différents types d'équilibreurs de charge en fonction des besoins de vos applications. Chaque équilibreur de charge prend en charge différents types de trafic via différents protocoles et couches réseau alignés sur le modèle d'[interconnexion des systèmes ouverts \(OSI\)](#). Pour plus d'informations sur les différences entre les types d'équilibreurs de charge, consultez les [comparaisons de produits](#).

Performance

Vous pouvez utiliser les services réseau pour optimiser les exigences de latence, de débit et de bande passante de vos charges de travail exécutées sur l'infrastructure AWS mondiale.

- Si vous souhaitez minimiser le temps de latence pour les clients locaux utilisant des applications Web dans le monde entier, pensez à utiliser Amazon CloudFront. CloudFront est un [réseau de diffusion de contenu](#) qui fournit du contenu aux clients avec la latence la plus faible possible.
- Si vous utilisez des charges de travail liées aux jeux, à l'Internet des objets (IoT) ou à la voix sur IP (VoIP), pensez à utiliser AWS Global Accelerator. Ce service vous aide à améliorer la disponibilité et les performances de vos charges de travail.
- Si les charges de travail que vous souhaitez vous VPCs connecter à d'autres services Régions AWS, vous pouvez vous connecter à ces services par programmation à l'aide de points de terminaison d'API publics.

Operational excellence

Au fur et à mesure que vous augmentez le taux d' AWS Cloud adoption, vous devez comprendre à tout moment ce qui se passe dans l'ensemble de vos charges de travail. Des outils et des services tels que [Reachability Analyzer](#) et [CloudWatch Amazon](#) Internet Monitor peuvent vous aider à suivre l'évolution des besoins et des priorités de votre entreprise à mesure que vos charges de travail augmentent.

- La gestion des adresses IP des charges de travail exécutées en plusieurs parties VPCs peut s'avérer difficile. Déterminez si vous devez automatiser la gestion des adresses IP pour l'ensemble de vos charges de travail (Amazon VPC IPAM).
- Si vous utilisez une [architecture de microservices](#), la gestion de la connectivité, de la sécurité et de la surveillance entre les microservices peut s'avérer difficile. Déterminez si vous devez automatiser l'interaction avec les microservices (AWS App Mesh et Amazon VPC Lattice).

Connectivity

Vous pouvez utiliser les services réseau pour vous connecter aux réseaux AWS Cloud, connecter des charges de travail ou connecter des réseaux.

- Tenez compte des points suivants pour vous connecter à AWS Cloud :
 - Si vous souhaitez connecter en toute sécurité des utilisateurs distants à votre VPCs, pensez à utiliser AWS Client VPN.
 - Si vous souhaitez connecter en toute sécurité un réseau local complet à votre VPCs, pensez à utiliser AWS Site-to-Site VPN.

- Si vous avez besoin de performances plus constantes que celles fournies par Internet, envisagez une connexion directe entre votre réseau local et AWS (AWS Direct Connect).
- Si vous devez transférer rapidement des données vers ou depuis le AWS Cloud, pensez à utiliser un terminal de transfert de AWS données.
- Tenez compte des points suivants pour connecter des réseaux :
 - Si vous opérez en plusieurs Régions AWS, si vous souhaitez gérer vos propres configurations de routage ou si vous préférez utiliser votre propre automatisation, pensez à utiliser AWS Transit Gateway.
 - Si vous souhaitez unifier votre centre de données, vos succursales et vos AWS réseaux à l'aide d'un WAN, pensez à utiliser AWS le Cloud WAN. Cela vaut également la peine d'être pris en compte si vous ne souhaitez pas gérer des configurations de routage complexes ou créer vos propres automatisations pour la connectivité multirégionale.

Security

AWS fournit une base sûre pour créer et déployer vos applications, mais vous êtes responsable de la mise en œuvre de vos propres mesures de sécurité pour protéger vos données, vos applications et votre infrastructure réseau, de la même manière que vous le feriez dans un centre de données sur site.

- Passez en revue et comprenez le [modèle de responsabilitéAWS partagée](#) et son application à la sécurité dans le AWS Cloud.
- AWS les groupes de sécurité et les listes de contrôle d'accès au réseau (NACLs) peuvent être utilisés ensemble ou séparément pour sécuriser un réseau, ce qui vous permet de créer une stratégie de défense approfondie.
- Les entreprises doivent protéger leurs applications réseau contre l'évolution des cyberrisques. Déterminez si vous devez protéger vos charges de travail contre les attaques malveillantes ou les logiciels malveillants (avec [AWS Network Firewall](#)), les attaques par déni de service (DDoS) distribué (avec AWS Shield) ou les attaques par injection SQL et par script intersite (avec AWS WAF

Amazon Route 53 [AWS Firewall Manager](#), les [listes de contrôle d'accès au réseau](#) et les groupes de sécurité sont également importants à prendre en compte pour garantir la sécurité du réseau.

Choix

Maintenant que vous connaissez les critères selon lesquels vous allez évaluer vos options de services réseau, vous êtes prêt à choisir les services qui vous conviennent le mieux.

Catégorie de services	Pour quoi est-il optimisé ?	AWS services de mise en réseau et de diffusion de contenu
Fondements du réseau	Optimisé pour démarrer avec les services AWS réseau et vous connecter VPCs en toute sécurité.	Amazon VPC AWS PrivateLink AWS Transit Gateway
Connectivité globale et hybride	Optimisé pour garantir une connectivité réseau privée, sécurisée et mondiale.	AWS Client VPN AWS Cloud WAN AWS Direct Connect AWS Site-to-Site VPN
Mise en réseau de pointe et diffusion de contenu	Optimisé pour une faible latence et un routage fiable du trafic vers et depuis vos charges de travail.	Amazon CloudFront AWS Global Accelerator Amazon Route 53 AWS Terminal de transfert de données
Mise en réseau d'applications	Optimisé pour garantir que vos charges de travail sont hautement disponibles, qu'elles s'adaptent à la demande et qu'elles peuvent communiquer entre elles.	Amazon API Gateway Amazon VPC IPAM Amazon VPC Lattice Elastic Load Balancing
Sécurité du réseau et accès à distance	Optimisé pour protéger vos charges de travail contre les	AWS Firewall Manager

Catégorie de services	Pour quoi est-il optimisé ?	AWS services de mise en réseau et de diffusion de contenu
	malwares, les DDo attaques S, les injections SQL et les attaques par script intersite.	AWS Network Firewall AWS Shield Accès vérifié par AWS AWS WAF

Utiliser

Pour découvrir comment utiliser et en savoir plus sur chacun des services AWS réseau disponibles, nous avons fourni un parcours permettant d'explorer le fonctionnement de chacun des services. La section suivante fournit des liens vers une documentation détaillée, des didacticiels pratiques et des ressources pour vous aider à démarrer.

Les services suivants couvrent le réseau mondial et la connectivité VPC.

Amazon CloudFront

- Qu'est-ce qu'Amazon CloudFront ?

Découvrez comment accélérer la distribution de contenu.

[Explorer le guide](#)

- Commencer à utiliser Amazon CloudFront

Découvrez les étapes de base pour diffuser du contenu avec CloudFront.

[Explorer le guide](#)

- Hébergement de vidéos en streaming à la demande avec Amazon S3 CloudFront, Amazon et Amazon Route 53

Découvrez comment héberger des vidéos pour les visionner à la demande de manière sécurisée et évolutive.

[Démarrer avec le didacticiel](#)

- Diffusez du contenu plus rapidement avec Amazon CloudFront

Découvrez comment réduire le temps de latence de vos applications Web pour les utilisateurs finaux.

[Démarrer avec le didacticiel](#)

AWS Cloud WAN

- Qu'est-ce que AWS le Cloud WAN ?

Découvrez comment créer, gérer et surveiller un réseau mondial unifié.

[Explorer le guide](#)

- Présentation du AWS Cloud WAN

Découvrez les principaux cas d'utilisation du AWS Cloud WAN et comment démarrer.

[Lisez le blogue](#)

- Commencer à utiliser AWS le Cloud WAN

Créez votre premier réseau mondial et connectez un VPC.

[Démarrer avec le didacticiel](#)

AWS Direct Connect

- Qu'est-ce que c'est AWS Direct Connect ?

Découvrez comment connecter un réseau local à AWS

[Explorer le guide](#)

- Commencer avec AWS Direct Connect

Regardez une brève introduction AWS Direct Connect et découvrez comment préparer votre réseau local pour qu'il puisse s'y connecter AWS.

[Regardez la vidéo](#)

- Connectez votre centre de données à AWS

Connectez votre centre de données à AWS l'utilisation AWS Direct Connect.

[Démarrer avec le didacticiel](#)

AWS Global Accelerator

- Qu'est-ce que c'est AWS Global Accelerator ?

Découvrez comment améliorer les performances de vos charges de travail.

[Explorer le guide](#)

- Commencer à utiliser un accélérateur standard

Créez un accélérateur pour améliorer les performances réseau d'une charge de travail exécutée sur une EC2 instance.

[Démarrer avec le didacticiel](#)

- Améliorez la disponibilité et les performances des applications à l'échelle mondiale pour votre trafic

Regardez une brève démonstration sur la configuration AWS Global Accelerator pour améliorer les performances du réseau.

[Regardez la vidéo](#)

AWS PrivateLink

- Qu'est-ce que c'est AWS PrivateLink ?

Découvrez comment connecter votre VPC à des services en privé.

[Explorer le guide](#)

- Commencez avec AWS PrivateLink

Envoyez une demande depuis une EC2 instance d'un sous-réseau privé à Amazon à CloudWatch l'aide PrivateLink de.

[Démarrer avec le didacticiel](#)

- Accélérez votre IPv6 adoption grâce à des PrivateLink services et à des terminaux

Les clients ayant une forte présence sur Internet ressentent la pression de l'épuisement des IPv4 adresses publiques. Découvrez comment augmenter l' IPv6 utilisation dans le cadre de VPCs l'utilisation PrivateLink.

[Lisez le blogue](#)

Amazon Route 53

- Qu'est-ce qu'Amazon Route 53 ?

Découvrez la résolution de noms de domaine hautement disponible et évolutive.

[Explorer le guide](#)

- Tutoriels de cas d'utilisation d'Amazon Route 53

Comment utiliser Route 53 pour les cas d'utilisation basés sur le trafic et la latence.

[Démarrer avec le didacticiel](#)

- Comment enregistrer un nom de domaine auprès d'Amazon Route 53

Ce didacticiel vous aide à enregistrer un nouveau nom de domaine pour une application Web.

[Démarrer avec le didacticiel](#)

- Présentation d'Amazon Route 53

Regardez une brève introduction à la résolution des noms de domaine et à Route 53.

[Regardez la vidéo](#)

AWS Data Transfer Terminal

- Qu'est-ce qu'un terminal de transfert de AWS données ?

Découvrez comment charger ou télécharger rapidement de grands ensembles de données sur vos AWS Cloud propres périphériques de stockage.

[Explorer le guide](#)

- Présentation du terminal AWS de transfert de données

Découvrez les principaux cas d'utilisation et comment démarrer.

[Lisez le blogue](#)

AWS Site-to-Site VPN

- Qu'est-ce que c'est AWS Site-to-Site VPN ?

Découvrez comment connecter des utilisateurs distants à AWS un VPN.

[Explorer le guide](#)

- Commencer avec AWS Site-to-Site VPN

Configurez une connexion Site-to-Site VPN entre un appareil sur site et AWS.

[Démarrer avec le didacticiel](#)

- AWS Site-to-Site VPN, en choisissant les bonnes options pour optimiser les performances

Choisissez les meilleures options lors de la configuration d'une connexion VPN à AWS.

[Lisez le blogue](#)

AWS Transit Gateway

- Qu'est-ce qu'une passerelle de transit ?

Découvrez comment vous connecter aux passerelles VPCs de transport en commun.

[Explorer le guide](#)

- Exemples de cas d'utilisation des passerelles de transit

Consultez les cas d'utilisation courants des passerelles de transport en commun.

[Explorer le guide](#)

- AWS Transit Gateway atelier

Dans cet atelier pratique, découvrez comment déployer Transit Gateway dans des configurations à une seule région et à un seul compte, à plusieurs comptes et à plusieurs régions.

[Démarrez l'atelier](#)

Amazon VPC

- Qu'est-ce qu'Amazon VPC ?

Découvrez les clouds privés virtuels et les fonctionnalités d'Amazon VPC.

[Explorer le guide](#)

- Commencez avec Amazon VPC

Un guide pour démarrer rapidement avec Amazon VPC.

[Explorer le guide](#)

- Exemples de configurations VPC

Consultez des exemples de configurations VPC basés sur différents cas d'utilisation.

[Explorer le guide](#)

- Architecture VPC modulaire et évolutive

Construisez une base de réseau virtuel basée sur les AWS meilleures pratiques pour votre AWS Cloud infrastructure.

[Démarrer avec le didacticiel](#)

Amazon VPC IPAM

- Qu'est-ce qu'IPAM ?

Découvrez comment suivre et gérer l'utilisation des adresses IP.

[Explorer le guide](#)

- Bonnes pratiques du gestionnaire d'adresses IP Amazon VPC (IPAM)

Découvrez comment créer un plan de gestion des adresses IP évolutif.

[Lisez le blogue](#)

- Création de pools pour gérer votre espace IP

Regardez une brève vidéo de présentation du VPC IPAM.

[Regardez la vidéo](#)

Les services suivants concernent la mise en réseau au niveau des applications.

Amazon API Gateway

- Qu'est-ce qu'Amazon API Gateway ?

Découvrez comment créer APIs pour vos charges de travail.

[Explorer le guide](#)

- Création APIs avec Amazon API Gateway

Découvrez comment commencer APIs à intégrer AWS.

[Regardez la vidéo](#)

- Configuration des intégrations privées avec Amazon API Gateway HTTP APIs

Découvrez comment créer une API pour contrôler l'accès privé aux ressources d'un VPC.

[Lisez le blogue](#)

AWS Client VPN

- Qu'est-ce que c'est AWS Client VPN ?

Découvrez comment connecter des réseaux AWS via un VPN.

[Explorer le guide](#)

- Commencer avec AWS Client VPN

Téléchargez l' AWS Client VPN application et connectez-vous AWS via VPN.

[Explorer le guide](#)

- Scénarios et exemples pour AWS Client VPN

Consultez des exemples de création et de configuration d'un accès VPN client pour vos clients.

[Explorez les exemples](#)

Elastic Load Balancing

- Qu'est-ce qu'Elastic Load Balancing ?

Découvrez comment répartir le trafic entrant entre vos charges de travail.

[Explorer le guide](#)

- Commencer à utiliser Elastic Load Balancing

Découvrez la différence entre les différents types d'équilibreurs de charge et créez un équilibreur de charge.

[Explorer le guide](#)

- Comment choisir le bon équilibreur de charge pour vos AWS charges de travail

Choisissez la bonne option pour équilibrer le trafic par rapport à vos charges de travail.

[Regardez la vidéo](#)

AWS Firewall Manager

- Commencer à utiliser les AWS Firewall Manager politiques

Découvrez comment AWS Firewall Manager activer différents types de politiques de sécurité.

[Explorer le guide](#)

- Comment auditer et limiter en permanence les groupes de sécurité avec AWS Firewall Manager

Ce billet de blog explique comment AWS Firewall Manager limiter les groupes de sécurité afin de garantir que seuls les ports requis sont ouverts.

[Explorer le guide](#)

- AWS Firewall Manager À utiliser pour déployer une protection à grande échelle dans AWS Organizations

Cet article fournit des step-by-step instructions pour déployer et gérer les politiques de sécurité dans l'ensemble de votre AWS Organizations implémentation en utilisant AWS Firewall Manager.

[Explorer le guide](#)

AWS Network Firewall

- Qu'est-ce que c'est AWS Network Firewall ?

En savoir plus sur le pare-feu réseau et la détection des intrusions.

[Explorer le guide](#)

- Commencer avec AWS Network Firewall

Créez et gérez rapidement un pare-feu réseau pour un VPC.

[Démarrer avec le didacticiel](#)

- AWS Network Firewall vidéo explicative animée

Regardez une brève vidéo de présentation de AWS Network Firewall.

[Regardez la vidéo](#)

AWS Shield

- Qu'est-ce que c'est AWS Shield ?

En savoir plus sur la protection DDo S.

[Explorer le guide](#)

- Exemples d'architectures résilientes DDo S de base

Découvrez certaines architectures DDo S-Resilient courantes.

[Explorer le guide](#)

- AWS Shield vidéo explicative animée

Regardez une brève vidéo de présentation de AWS Shield.

[Regardez la vidéo](#)

Accès vérifié par AWS

- Tutoriel : Premiers pas avec Verified Access

Dans ce didacticiel, vous allez apprendre à créer et à configurer des ressources d'accès vérifié.

[Explorer le guide](#)

- Accès vérifié par AWS Intégration avec des fournisseurs d'identité tiers

Ce billet de blog explique comment intégrer Verified Access (AVA) au fournisseur d'identité Okta tiers.

[Explorer le guide](#)

- Intégration Accès vérifié par AWS avec les fournisseurs de confiance en matière d'appareils

Ce billet de blog explique comment concevoir une connectivité à distance basée sur le Zero Trust AWS.

[Explorez les exemples](#)

Amazon VPC Lattice

- What is Amazon VPC Lattice?

Découvrez comment connecter, sécuriser et surveiller les microservices de vos charges de travail.

[Explorer le guide](#)

- Configuration d'Amazon VPC Lattice

Configurez et lancez VPC Lattice pour la première fois.

[Explorer le guide](#)

- Créez une connectivité multi-comptes multi-VPC sécurisée pour vos applications avec Amazon VPC Lattice

Présentation de la façon dont vous pouvez utiliser VPC Lattice pour résoudre les problèmes de connectivité VPC.

[Lisez le blogue](#)

- Explicateur animé Amazon VPC Lattice

Regardez une brève vidéo animée sur VPC Lattice.

[Regardez la vidéo](#)

AWS WAF

- Qu'est-ce que c'est AWS WAF ?

Découvrez comment contrôler l'accès à vos charges de travail.

[Explorer le guide](#)

- Commencer avec AWS WAF

Regardez une courte vidéo expliquant comment protéger vos charges AWS WAF de travail contre les exploits Web et les robots.

[Regardez la vidéo](#)

- Vidéo de présentation de AWS WAF

Regardez une brève vidéo de présentation de AWS WAF.

[Regardez la vidéo](#)

Explorez

- Schémas d'architecture

Explorez les diagrammes d'architecture de référence pour vous aider à développer vos architectures de mise en réseau et de diffusion de contenu AWS.

[Explorez les diagrammes d'architecture](#)

- Livres blancs

Consultez les livres blancs pour vous aider à démarrer, à découvrir les meilleures pratiques et à comprendre vos options de mise en réseau et de diffusion de contenu.

[Découvrez les livres blancs](#)

- AWS Des solutions

Découvrez des solutions approuvées et des conseils en matière d'architecture pour les cas d'utilisation courants en matière de mise en réseau et de diffusion de contenu.

[Découvrez les AWS solutions](#)

Historique du document

Le tableau suivant décrit les modifications importantes apportées à ce guide de décision. Pour recevoir des notifications concernant les mises à jour de ce guide, vous pouvez vous abonner à un flux RSS.

Modification	Description	Date
Guide mis à jour	AWS Terminal de transfert de données ajouté.	16 janvier 2025
Publication initiale	Guide publié pour la première fois.	12 décembre 2023

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.