Exemple d'utilisation de bande passante à la demande automatisée via la pile logicielle d'automatisation en boucle fermée

Table des matières

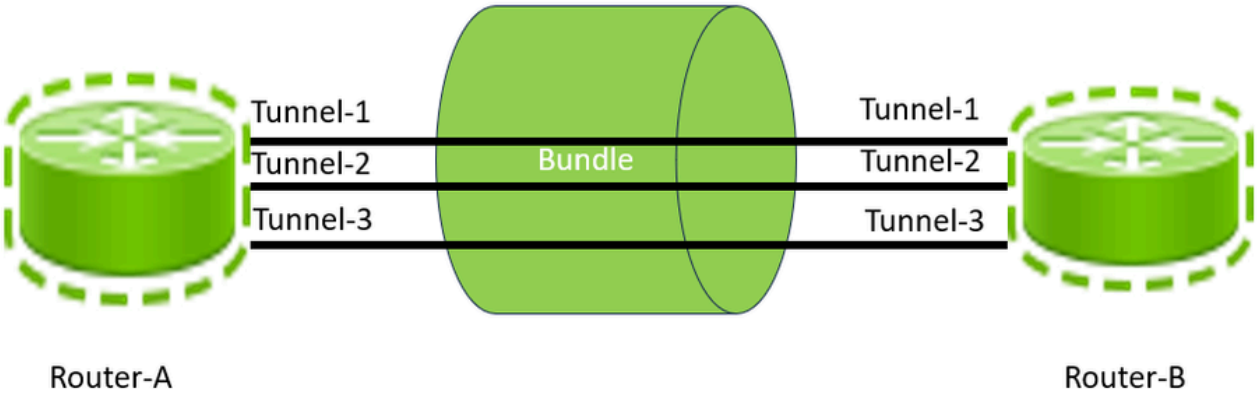
Introduction

Ce document décrit les composants d'une solution d'automatisation en boucle fermée Cisco pour l'automatisation de l'évolutivité du tunnel GRE (Generic Routing Encapsulation) et son adaptabilité à d'autres cas.

Informations générales

Les fournisseurs de services souhaitent contrôler l'utilisation de leur bande passante sur les tunnels GRE de leur réseau et les surveiller étroitement pour faire évoluer les tunnels en fonction des besoins, à l'aide d'une solution d'automatisation intelligente en boucle fermée.

GRE est un protocole de tunneling qui fournit une approche générique simple pour transporter des paquets d'un protocole sur un autre à l'aide de l'encapsulation. Ce document se concentre sur l'exemple basé sur le tunnel GRE pour la plate-forme Cisco IOS® XRv, mais peut également être généralisé à d'autres plates-formes. GRE encapsule une charge utile, un paquet interne qui doit être livré à un réseau de destination à l'intérieur d'un paquet IP externe. Le tunnel GRE se comporte comme une liaison point à point virtuelle avec deux points d'extrémité identifiés par l'adresse source et l'adresse de destination du tunnel.



Tunnels GRE entre routeurs

La configuration d'un tunnel GRE implique la création d'une interface de tunnel et la définition de la source et de la destination du tunnel. Cette image montre la configuration de trois tunnels GRE entre les routeurs A et B. Pour cette configuration, vous devez créer trois interfaces, chacune sur le routeur A, telles que Tunnel-1, Tunnel-2 et Tunnel-3, et créer de même trois interfaces sur le routeur B, telles que Tunnel-1, Tunnel-2 et Tunnel-3. Entre deux routeurs de fournisseur de services, il peut y avoir plusieurs tunnels GRE. Chaque tunnel, comme toute autre interface réseau, a une capacité définie qui est basée sur la capacité de l'interface. Par conséquent, un tunnel ne peut transporter qu'un trafic maximal égal à sa bande passante. Le nombre de tunnels est souvent basé sur la prédiction initiale de la charge de trafic et de l'utilisation de la bande passante entre deux sites (routeurs). Cette utilisation de la bande passante devrait changer en fonction des modifications apportées au réseau et à son extension. Pour optimiser l'utilisation de la bande passante du réseau, il est important d'ajouter de nouveaux tunnels ou de supprimer des tunnels supplémentaires entre deux périphériques en fonction de l'utilisation de la bande passante mesurée sur tous les tunnels entre les deux périphériques.

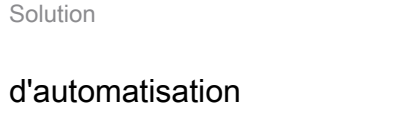
À partir de cet exemple, vous pouvez dire que la capacité totale des trois tunnels entre les routeurs A et B est la somme des capacités de tunnel-1, tunnel-2 et tunnel-3, qui est appelée bande passante agrégée ou bande passante de niveau de regroupement GRE. Notez que le mot clé « bundle » fait ici référence aux tunnels entre une paire de routeurs ; aucune relation implicite avec le regroupement de liaisons LACP/Etherchannel n'est prévue. En outre, le trafic réel entre les deux routeurs est le trafic agrégé total entre les tunnels 1, 2 et 3. En général, vous pouvez concevoir un concept d'utilisation de la bande passante au niveau du bundle, qui peut être un rapport entre le trafic total à travers les tunnels et la capacité totale de tous les tunnels entre deux routeurs. En général, tout fournisseur de services souhaite prendre des mesures correctives en ajoutant ou en supprimant des tunnels entre deux routeurs s'il constate que la bande passante est surutilisée ou sous-utilisée. Cependant, pour ce document, considérez que le seuil inférieur est de 20 % pour une faible utilisation et de 80 % pour une utilisation élevée pour l'utilisation de niveau de regroupement entre deux routeurs.

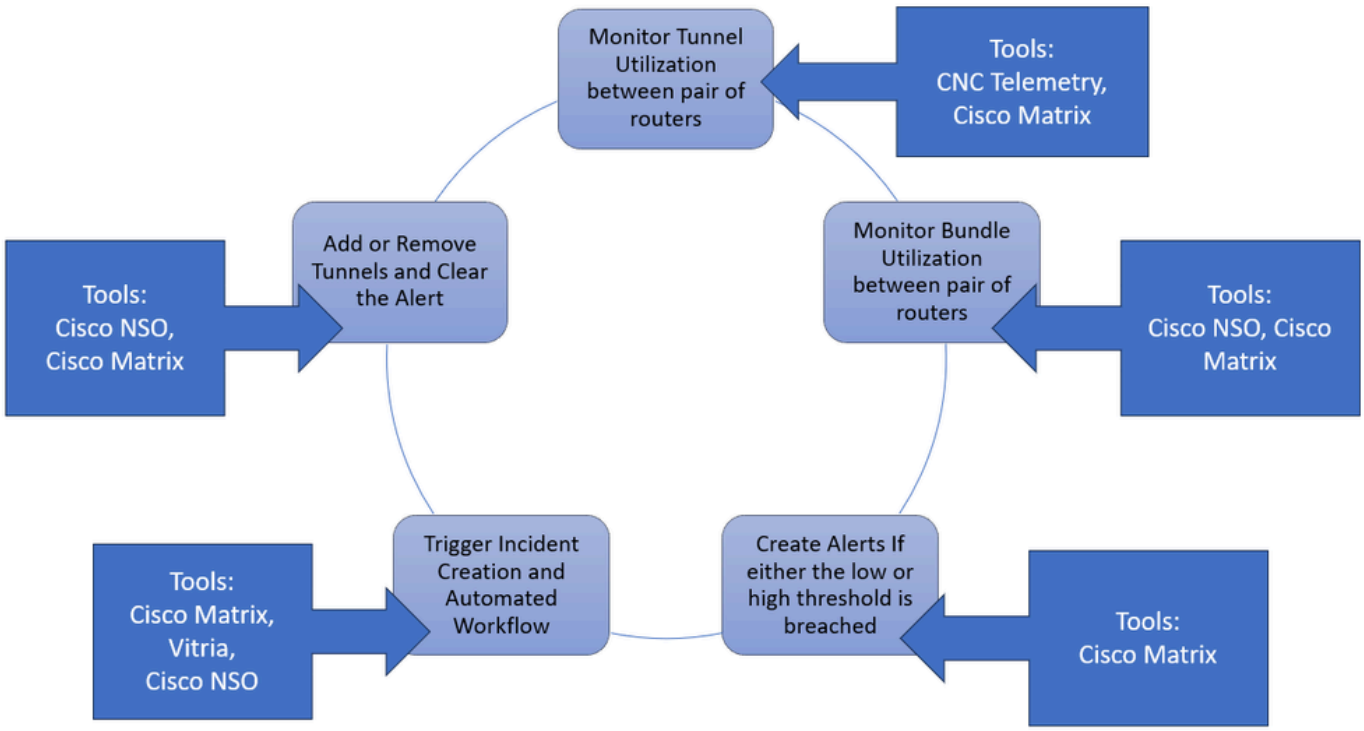
Exigences

1. La solution en boucle fermée est nécessaire pour automatiser de bout en bout l'ensemble GRE sur XRv9K, où le système peut collecter des données de télémétrie, surveiller les données sous la forme d'indicateurs de performance clés (KPI), appliquer l'agrégation, créer des alertes TCA (Threshold Cross Alerts) et effectuer une configuration de correction automatisée, puis fermer l'alerte.
2. La solution peut calculer un indicateur de performance clé de réseau (KPI) pour fournir l'utilisation de la bande passante individuelle d'entrée de tunnel (Rx) et de sortie de tunnel (Tx) de chaque tunnel qui est basée sur le débit brut des tunnels à une fréquence souhaitée.
3. La solution peut calculer des indicateurs de performance clés personnalisés pour fournir l'utilisation de la bande passante en entrée (Rx) et en sortie (Tx) de chaque bundle, qui correspond à l'utilisation de la bande passante agrégée de tous les tunnels entre une paire de routeurs.
4. La solution peut détecter et créer des alertes si les seuils de niveau d'offre groupée définis sont dépassés. Ces alertes sont disponibles à des fins de surveillance.
5. L'alerte doit entraîner le déclenchement d'un workflow automatisé qui peut déclencher une configuration supplémentaire sur le périphérique pour ajouter ou supprimer des tunnels en fonction des conditions d'alerte.
6. Enfin, le système doit fermer automatiquement les alertes avec les mises à jour requises.

Solution

La solution d'automatisation en boucle fermée fait appel à plusieurs outils qui travaillent sur l'objectif spécifique de cette solution complète. Cette image montre quels composants et outils nous aident à réaliser l'architecture finale et décrit le rôle de haut niveau. Vous pouvez examiner chaque composant et son utilisation dans les sections suivantes.





en

boucle fermée

Cisco

Outil	Objectif
Contrôleur réseau Cisco Crosswork (CNC)	Le contrôleur de réseau Crosswork offre une visibilité en temps réel sur le cycle de vie des services et des périphériques, grâce à une navigation intuitive sur la topologie du réseau, l'inventaire des services, les politiques de transport, l'état de santé des services et des périphériques, et plus encore, en prenant en charge un large éventail d'utilisations avec une expérience utilisateur commune et intégrée. Dans cette solution, il est utilisé comme un outil principalement pour la gestion des périphériques et la collecte de données de performance de tunnel à l'aide de gNMI (gRPC Network Management Interface) ou MDT. Plus de détails : https://www.cisco.com/site/us/en/products/networking/software/crosswork-network-controller/index.html
Matrice Cisco	Les services d'analyse CX (packs de fonctions) sont fournis à l'aide de la solution Matrix, qui est une solution d'analyse multidomaine et multifournisseur. Dans cette Solution, la Matrice consomme les données de Kafka envoyées par CNC sur les Rubriques Kafka et effectue en outre l'agrégation des KPI basés sur les

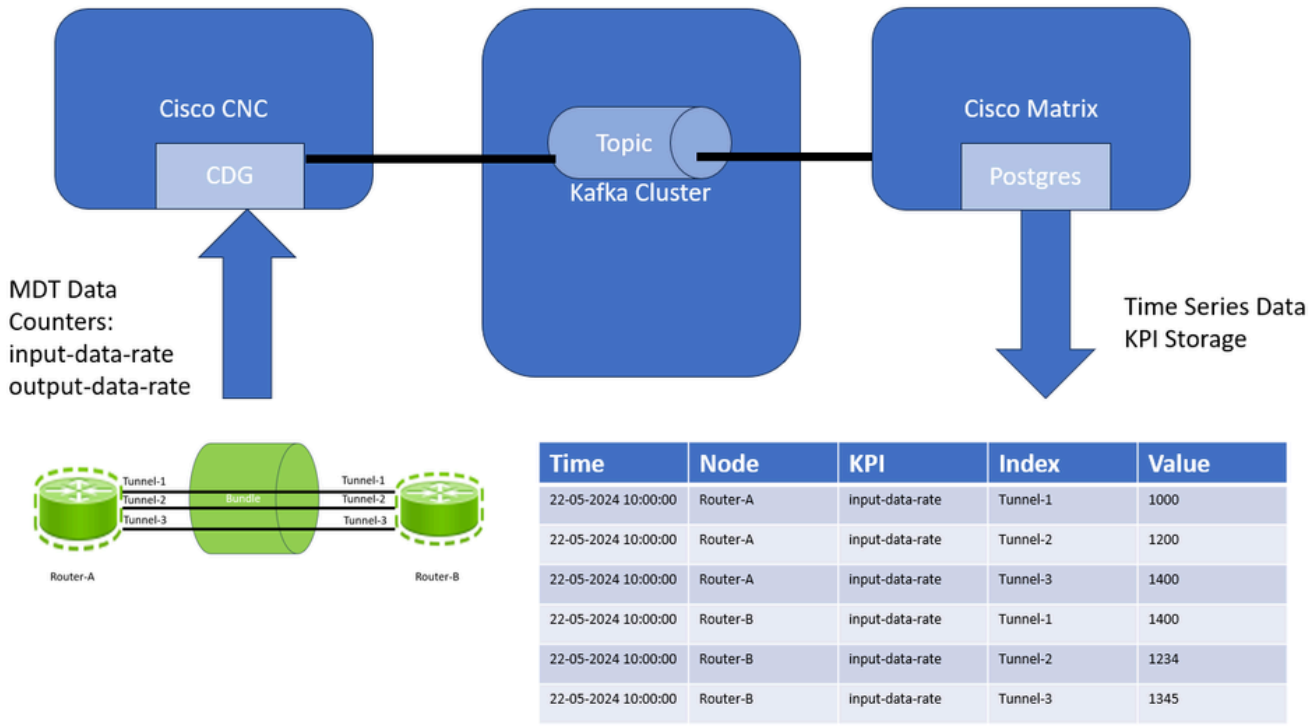
	tunnels dans les KPI de niveau Bundle en utilisant des recherches de topologie et les stocke sous forme de données de séries chronologiques et les stocke dans la base de données Postgres. Une fois stockées, ces données sont disponibles pour la visualisation et Matrix détecte les anomalies à l'aide d'alertes de franchissement de seuil qui nous permettent de configurer des seuils pour les indicateurs de performance clés que nous collectons à partir du réseau.
Grappe De Kafka	Un cluster Kafka est un système qui comprend différents sujets de courtiers, et leurs partitions respectives. Un producteur envoie ou écrit des données/messages au sujet dans le cluster. Un consommateur lit ou consomme des messages du cluster Kafka. Dans cette solution, CNC agit en tant que Producteur qui envoie des données à des sujets Kafka prédéfinis sous la forme de données utiles JSON après avoir converti les données de télémétrie collectées à partir de routeurs. Dans cette solution, Matrix agit en tant que consommateur qui consomme ces données, les traite, les agrège et les stocke en vue d'un traitement ultérieur et d'une détection des anomalies.
Cisco NSO	Cisco Crosswork Network Services Orchestrator (NSO) NSO fait partie de la gamme Crosswork d'outils d'automatisation conçus pour les fournisseurs de services et les grandes entreprises. Dans cette solution, NSO collecte des informations relatives à tous les tunnels et périphériques et crée une table topologique personnalisée pour cette solution. En outre, dans cette solution, NSO et les fonctionnalités d'automatisation des processus d'entreprise sont utilisées pour déclencher un workflow de correction et prendre des mesures telles que l'ajout ou la suppression d'un tunnel à partir du périphérique et la suppression des alertes dans la matrice Cisco. Plus de détails : https://www.cisco.com/c/en/us/products/cloud-systems-management/network-services-orchestrator/index.html
Vitria VIA AIOps	Vitria VIA AIOps pour Cisco Network Automation fournit une analyse automatisée qui permet de remédier rapidement aux événements affectant les services sur toutes les couches technologiques et applicatives. Dans cette solution, VIA AIOps est utilisé pour corréler les événements de seuil KPI générés par Cisco Matrix pour créer un incident, une notification et déclencher une action automatisée vers Cisco NSO pour augmenter ou diminuer le nombre de tunnels GRE. Plus de détails : https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/crosswork-network-automation/solution-overview-c22-2403404.html

La solution effectue ces étapes pour répondre à ce cas d'utilisation, qui sont détaillées dans les sections suivantes.

1. Surveillance de l'utilisation du tunnel entre les paires de routeurs
2. Surveillance de l'utilisation des ensembles entre les paires de routeurs
3. Créer des alertes de dépassement de seuil
4. Déclenchement du workflow d'incident et de résolution automatisée
5. Ajouter ou supprimer des tunnels et effacer l'alerte

Surveillance de l'utilisation du tunnel entre les paires de routeurs

Les applications demandent la collecte de données via des tâches de collecte. Cisco Crosswork attribue ensuite ces tâches de collecte à une passerelle de données Cisco Crosswork pour répondre à la demande. Crosswork Data Gateway prend en charge la collecte de données à partir de périphériques réseau à l'aide de la télémétrie pilotée par modèle (MDT) pour consommer des flux de télémétrie directement à partir de périphériques (pour les plates-formes basées sur Cisco IOS XR uniquement). Cisco Crosswork vous permet de créer des destinations de données externes qui peuvent être utilisées par les tâches de collecte pour déposer des données.Kafka peut être ajouté en tant que nouvelles destinations de données pour les tâches de collecte créées par l'API REST. Dans cette solution, CDG collecte les données des routeurs liées aux statistiques de l'interface de tunnel et envoie les données à la rubrique Kafta.Cisco Matrix consomme les données de la rubrique Kafka et attribue les données à l'application de travail Matrix qui traite les données en tant qu'indicateur de performance clé (KPI) et les enregistre de manière chronologique, comme illustré dans la figure suivante qui décrit le flux du processus.



Time	Node	KPI	Index	Value
22-05-2024 10:00:00	Router-A	input-data-rate	Tunnel-1	1000
22-05-2024 10:00:00	Router-A	input-data-rate	Tunnel-2	1200
22-05-2024 10:00:00	Router-A	input-data-rate	Tunnel-3	1400
22-05-2024 10:00:00	Router-B	input-data-rate	Tunnel-1	1400
22-05-2024 10:00:00	Router-B	input-data-rate	Tunnel-2	1234
22-05-2024 10:00:00	Router-B	input-data-rate	Tunnel-3	1345

Solution Cisco d'automatisation en boucle fermée

Les données de séries chronologiques ont des attributs ICP qui sont stockés dans la base de données matricielle.

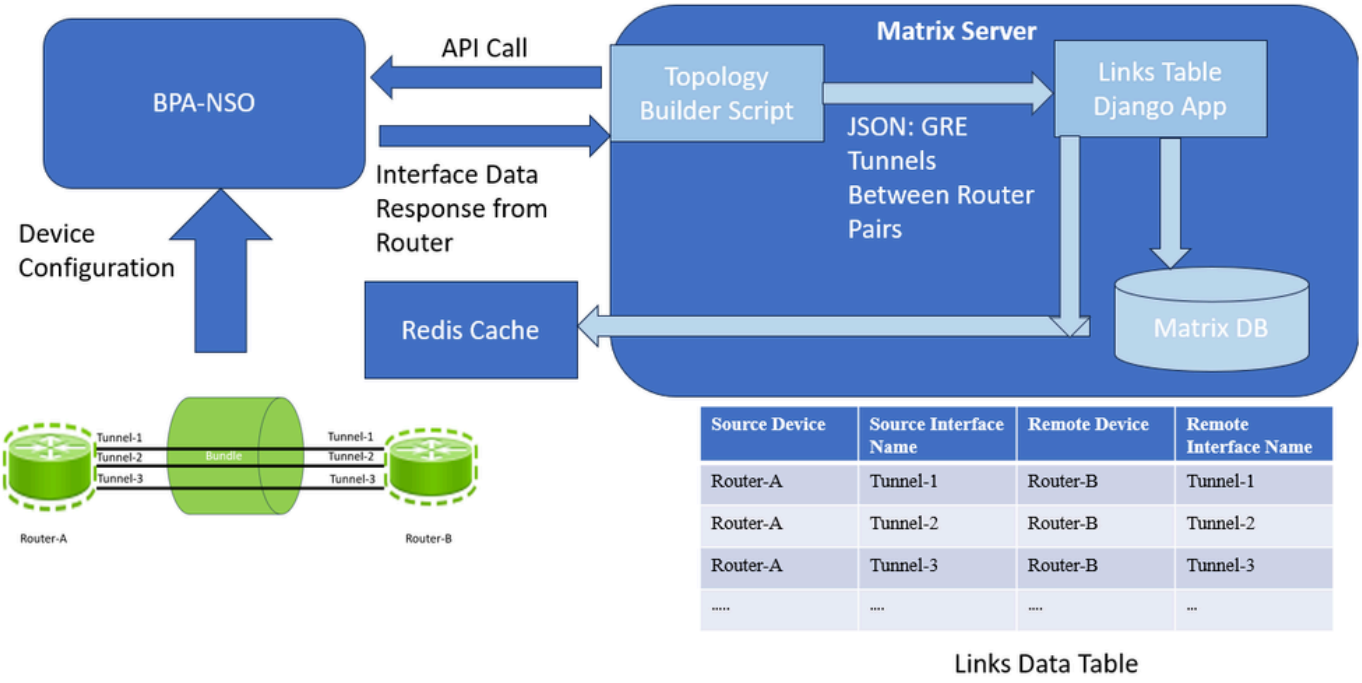
Attributs ICP	Objectif
Noeud	Périphérique ou source pour lequel l'indicateur de performance clé est stocké Exemple : Routeur-A
Heure	L'heure à laquelle les données sont collectées Exemple : 22-05-2024 10:00:00
Indice	Identificateur unique Exemple : Tunnel-1
Valeur	Valeur de l'indicateur de performance clé - Valeur numérique
ICP	Nom KPI Exemple : utilisation du tunnel

Surveillance de l'utilisation des ensembles entre les paires de routeurs

Une fois que vous avez les données de série temporelle comme mentionné dans la section précédente, vous avez les statistiques de trafic collectées par interface de tunnel. Cependant, vous devez identifier quel périphérique avec quelle interface de tunnel source est connecté à quel autre périphérique et quel est le nom de l'interface distante. Il s'agit de l'identification de liaison, qui permet d'identifier le nom du périphérique source. Nom de l'interface source, Nom du périphérique distant et Nom de l'interface distante. Pour interpréter avec précision les informations de liaison et les routeurs, vous avez besoin d’un exemple de référence tel que décrit.

Périphérique source	Nom d'interface source	Périphérique distant	Nom de l'interface distante
Routeur-A	Tunnel-1	Routeur-B	Tunnel-1
Routeur-A	Tunnel-2	Routeur-B	Tunnel-2
Routeur-A	Tunnel-3	Routeur-B	Tunnel-3
....	...	...	.

Pour créer cette table de liens de topologie dans cette solution, vous pouvez remplir une table personnalisée, Table de données de liens, intégrée à Matrix en fonction d'un script exécuté sur le serveur tous les jours à l'heure souhaitée. Ce script effectue un appel d'API à BPA-NSO et récupère une sortie JSON des groupes GRE entre les paires de routeurs. Il analyse ensuite les données d'interface pour créer la topologie au format JSON. Le script prend également cette sortie JSON et l'écrit dans la table de données de liens tous les jours. Chaque fois qu'il charge les nouvelles données dans la table, il les écrit également dans un cache Redis afin de réduire les recherches dans la base de données et d'améliorer l'efficacité.



Source Device	Source Interface Name	Remote Device	Remote Interface Name
Router-A	Tunnel-1	Router-B	Tunnel-1
Router-A	Tunnel-2	Router-B	Tunnel-2
Router-A	Tunnel-3	Router-B	Tunnel-3
.....	....	....	...

Links Data Table

Processus de table de données de liens

Par conséquent, toutes les liaisons entre les deux mêmes périphériques font nécessairement partie de l'offre groupée identifiée comme appartenant à la même offre groupée.Une fois que les indicateurs de performance clés de niveau tunnel brut sont disponibles, vous avez créé une application KPI_aggregate personnalisée sur Matrix qui effectue le travail de calcul des utilisations de niveau offre groupée et de stockage en tant qu'indicateur de performance clé.

Cette application prend les entrées suivantes :

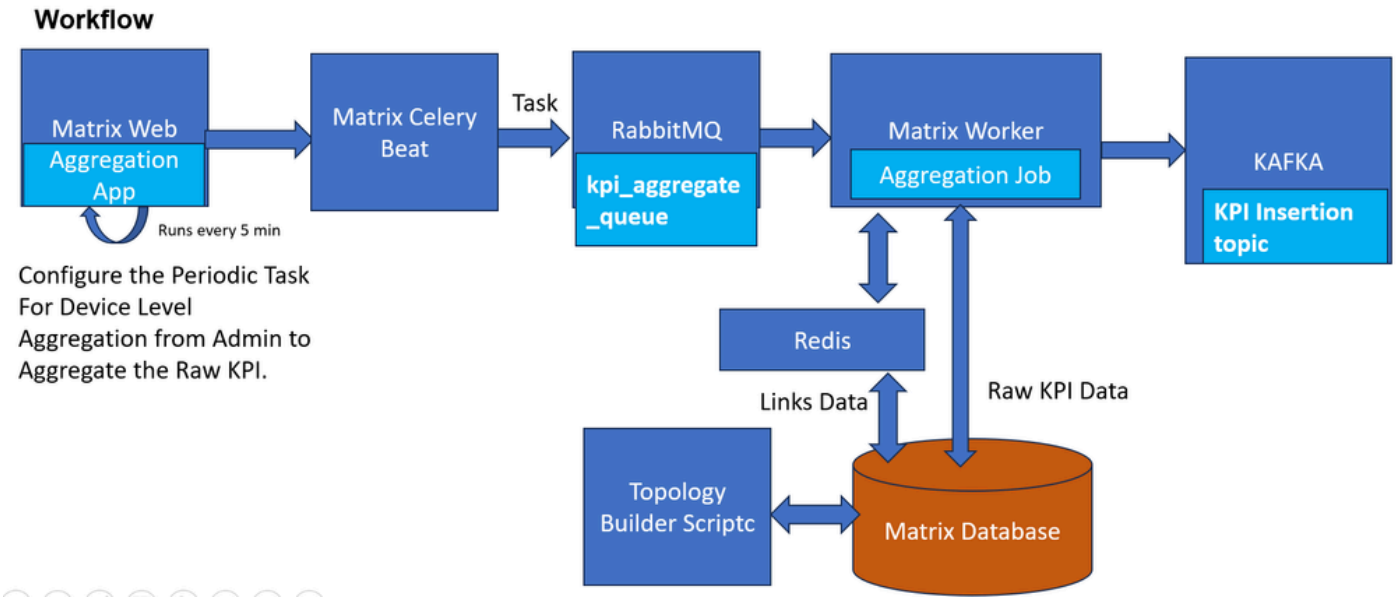
Attribut de configuration	Objectif
Onglet Croisé	Fréquence à laquelle la tâche périodique d'agrégation doit s'exécuter
Case Activé	Activer/Désactiver cette configuration

Nom ICP interface tunnel	Nom de l'indicateur de performance clé brut utilisé pour calculer l'indicateur de performance clé agrégé. Le nom d'indicateur de performance clé d'agrégation est automatiquement créé sous la forme <Raw_KPI_Name>_agg
Plage de dates	Fréquence des données brutes.

La tâche d'agrégation prend les entrées de la base de données de liens et de données brutes KPI et identifie les tunnels qui font partie du même lot et les ajoute à un groupe basé sur cette logique.

```
KPI Name: <Raw_KPI_Name>_agg

Example: tunnel_utilization_agg

Value = sum (tunnel_interface_tx_link_utilization of all the interfaces on the device connected to same

Index: <local device> _<remote device>

Router-A _Router-B

Node: <Local-Device>

Router-A
```

Par exemple, dans ce cas, le nom de l'indicateur de performance clé est généré sous la forme « tunnel-utilisation_agg » pour l'indicateur de performance clé de tunnel brut tunnel tunnel-utilisation. Une fois que le calcul est terminé pour toutes les valeurs KPI brutes pour tous les routeurs et les combinaisons de tunnels, ces données sont envoyées pour chaque lien vers la rubrique Kafka, qui doit être la même rubrique qui ingère l'indicateur KPI traité. De cette façon, ces informations persistent comme tout autre ICP normal reçu de sources valides. Le consommateur de base de données utilise cette rubrique et conserve l'indicateur de performance clé dans la table des résultats d'indicateur de performance clé de la base de données matricielle pour les indicateurs de performance clés agrégés.



Processus d'agrégation ICP pour les ICP d'agrégation de niveau offre

Créer des alertes de dépassement de seuil

Le seuil d'indicateur de performance clé configuré dans Matrix est de 85 %, ce qui signifie que lorsque la valeur de cet indicateur de performance clé dépasse le seuil, une alerte critique est générée et lorsqu'elle passe sous le seuil, une alerte claire est générée. Ces alertes sont enregistrées dans la base de données Matrix et également transmises à Vitria dans cette solution pour l'exemple d'utilisation de l'automatisation en boucle fermée. Si la valeur calculée de l'IPC dépasse le seuil, une alerte est envoyée à Vitria (VIA-AIOPs) via Kafka avec l'état actuel comme Critique dans le message. De même, si la valeur retourne dans les valeurs de seuil à partir des valeurs critiques, elle doit envoyer une alerte aux VIA-AIOP via Kafka avec l'état actuel comme Clear dans le message. Un exemple de message a été envoyé au système et ses attributs sont les suivants.

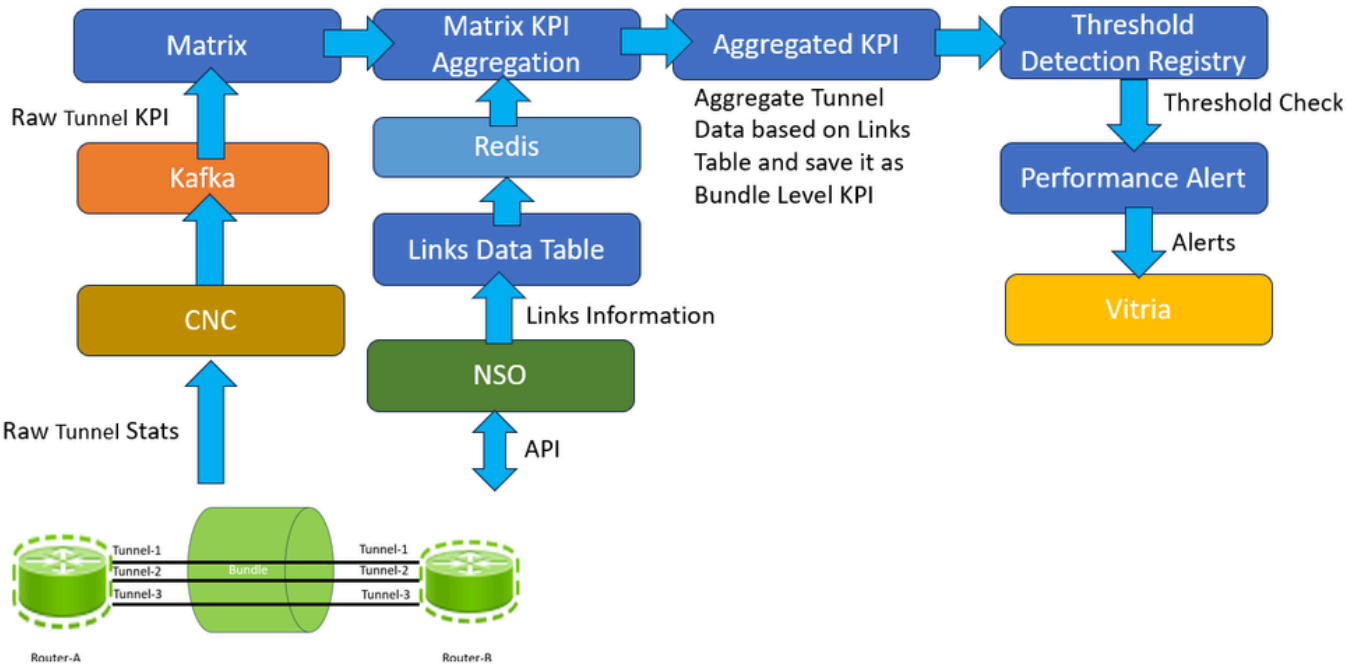

```
{
   "node" : "Router-A",
   "node_type" : "Routeur",
   "kpi" : "tunnel_use_agg",
   "kpi_description" : "Utilisation au niveau du bundle",
   "schéma" : "",
   "index" : "Routeur-A_Routeur-B",
   "heure" : "2023-08-09 05:45:00+00:00",
   "valeur" : "86.0",
```

```
   "état_précédent" : "EFFACER",
   "current_state" : "CRITIQUE",
   "link_name" : "Routeur-A_Routeur-B"
}
```


Attribut de message d'alerte Kafka	Exemple de valeur	Objectif
noeud	Routeur-A	Nom du périphérique réseau
type_noeud	Routeur	Type de périphérique
ICP	agg_utilisation_tunnel	Nom KPI
kpi_description	Utilisation au niveau du bundle	Description ICP
Schéma	S. O.	S. O.
index	Routeur-A_Routeur-B	<périphérique_local>-<périphérique_distant>
Heure	"2023-08-09 05:45:00+00:00"	Heure
valeur	86.0	valeur ICP
état_précédent	DÉGAGER	État d'alerte précédent
état_actuel	CRITICAL (CRITIQUE)	État d'alerte actuel
nom_lien	Routeur-A_Routeur-B	Attribut de corrélation

l'attribut link_name est un nom alphabétique des périphériques présents dans la valeur d'index. Cela permet d'établir une corrélation au niveau des AIO VIA, où les AIO VIA doivent corréler les

alertes provenant de la même liaison de bundle. Par exemple, lorsque plusieurs alertes arrivent sur des AIOP VIA avec le même link_name, cela signifie que les alertes appartiennent à la même liaison groupée dans le réseau désignée par des noms de périphériques dans le nom de la liaison.



Génération d'alertes d'agrégation KPI avec le registre de détection de matrice

Déclenchement du workflow d'incident et de résolution automatisée

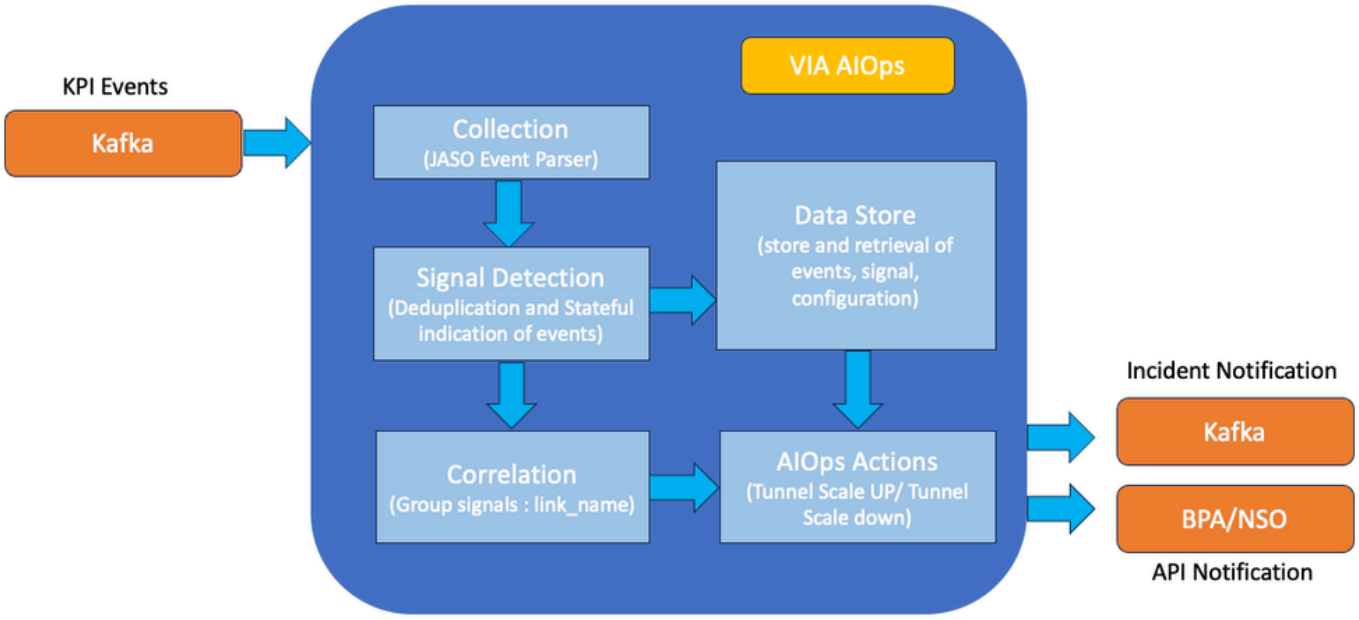
VIA AIOps doit être configuré pour la réception d'événements d'anomalie d'indicateur de performance clé (KPI) à partir d'un sujet Kafka désigné. Ces événements, tels qu'ils sont reçus par les messages Kafka, sont traités par VIA AIOps par l'intermédiaire de l'analyseur d'événements JASO pour une réception ultérieure. Il est essentiel pour les AIO VIA d'identifier précisément les événements d'anomalie KPI liés aux tunnels GRE, de déterminer leur association avec des paires de périphériques spécifiques (par exemple, Routeur A - Routeur B), et de déterminer si l'anomalie nécessite le lancement de l'automatisation de l'évolutivité du tunnel GRE - soit une mise à niveau, soit une mise à niveau inférieure.

L'analyseur d'événements JASO dans VIA AIOps doit être configuré pour extraire et interpréter les dimensions pertinentes de l'événement d'anomalie KPI de la matrice, à savoir l'« hôte », l'« indicateur de performance clé », l'« index » et la « valeur ». Une dimension supplémentaire, appelée « automation_action », doit être configurée pour être mise à jour dynamiquement par l'analyseur d'événements JASO, en fonction de la métrique « value » présente dans l'événement d'anomalie ICP de la matrice. Cette dimension est essentielle pour déterminer si une réponse automatisée doit être mise en oeuvre, en particulier si des procédures « GRE Tunnel Scale Up » ou « GRE Tunnel Scale Down » doivent être déclenchées en traitant le champ « Valeur ICP ». Dans VIA AIOps, un signal représente une consolidation des états des événements. Pour améliorer ce processus de corrélation, nous devons configurer des signaux distincts avec état qui correspondent aux dimensions « host », « link name », « kpi » et « automation_action ». Le tableau illustre les signaux, les groupes de corrélation et leurs configurations de corrélation respectives.

Par exemple, le signal identifié comme GRE_KPIA_SCALEUP serait émis après l'ingestion d'un message d'anomalie ICP spécifié, tel que détaillé dans la section 3, par le système AIOps de VIA.

Nom du signal VIA AIOps	Touches de corrélation des signaux	Nom de règle de groupe de corrélation
GRE_KPIA_SCALEUP	Hôte,IPC, Nom du lien, Automated_action	Extension du tunnel GRE
GRE_KPIB_SCALEUP	Hôte,IPC, Nom du lien, Automated_action	
GRE_KPIA_SCALEDOWN	Hôte,IPC, Nom du lien, Automated_action	Diminution de l'évolutivité du tunnel GRE
GRE_KPIB_SCALEDOWN	Hôte,IPC, Nom du lien, Automated_action	

La règle de groupe de corrélation est conçue pour faciliter l'agrégation de signaux concernant le dispositif A, le dispositif B et leurs tunnels respectifs A, B et C en un incident unifié. Cette règle de corrélation garantit que, pour tout couplage spécifique du périphérique A et du périphérique B, un maximum de deux incidents distincts sont générés : un incident pour une mise à l'échelle du tunnel GRE impliquant le périphérique A et le périphérique B, et un autre incident pour une mise à l'échelle du tunnel GRE pour le même couplage de périphériques. L'infrastructure d'agent VIA AIOps peut interagir avec Business Process Automation (BPA) et Network Services Orchestrator (NSO).



Corrélation et notification d'événements KPI via AIOps

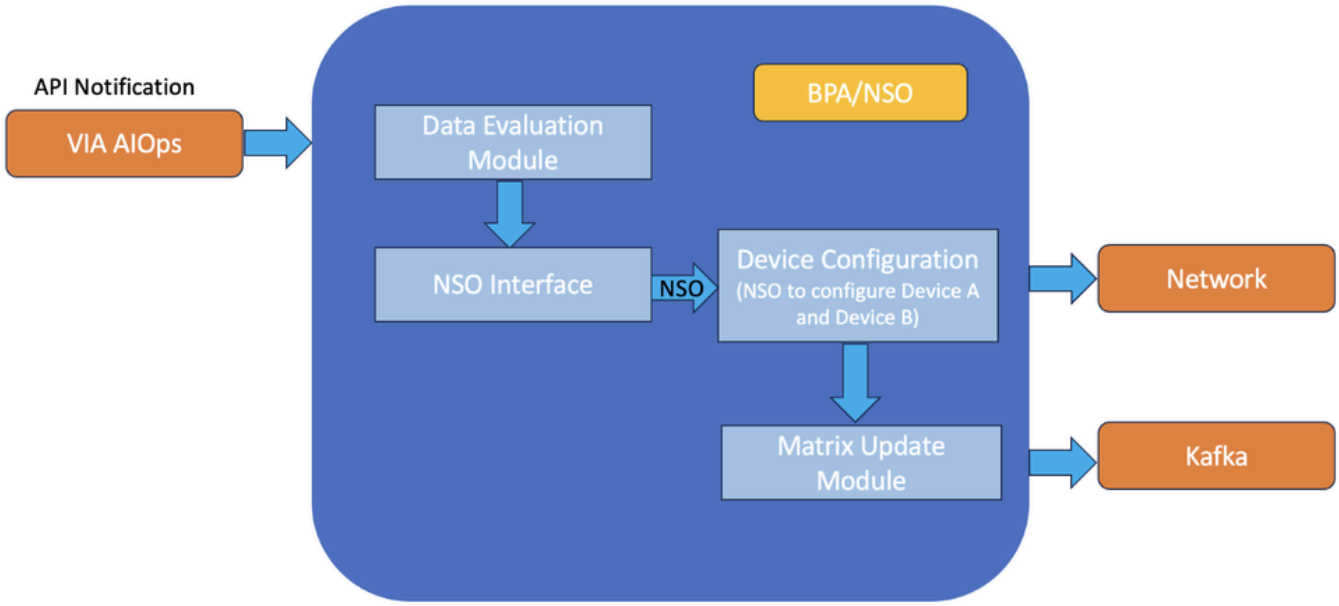
Voici un exemple de notification d'API d'extension de tunnel GRE envoyée à BPA/NSO depuis VIA AIOps.

```
{
  "create": [
    {
      "gre-tunnels-device-cla": [
        {
          "index": "RouterA-RouterB",
          "tunnelOperation": "SCALE UP",
          "MatrixData": [
            { "node": "RouterA", "kpi": "tunnel_utilization_agg" },
            { "node": "RouterB", "kpi": "tunnel_utilization_agg" }
          ]
        }
      ]
    }
  ]
```

```
}
```

Ajouter ou supprimer des tunnels et effacer l'alerte

À la réception d'un appel d'API de VIA AIOps, Cisco Business Process Automation (BPA) lance les directives d'évolutivité requises, par le biais de requêtes internes adressées à Cisco Network Service Orchestrator (NSO). Le BPA évalue la charge utile des données fournies par VIA AIOps, qui inclut les détails de fonctionnement du tunnel, un index et des données matricielles. Les informations d'opération d'index et de tunnel sont utilisées pour établir une interface avec le NSO, fournissant des paramètres pour l'opération d'échelle. Simultanément, les données de la matrice sont traitées par le « module de mise à jour de la matrice », qui est chargé de résoudre les événements d'anomalie d'indicateur de performance clé en établissant une interface avec les API de la matrice.

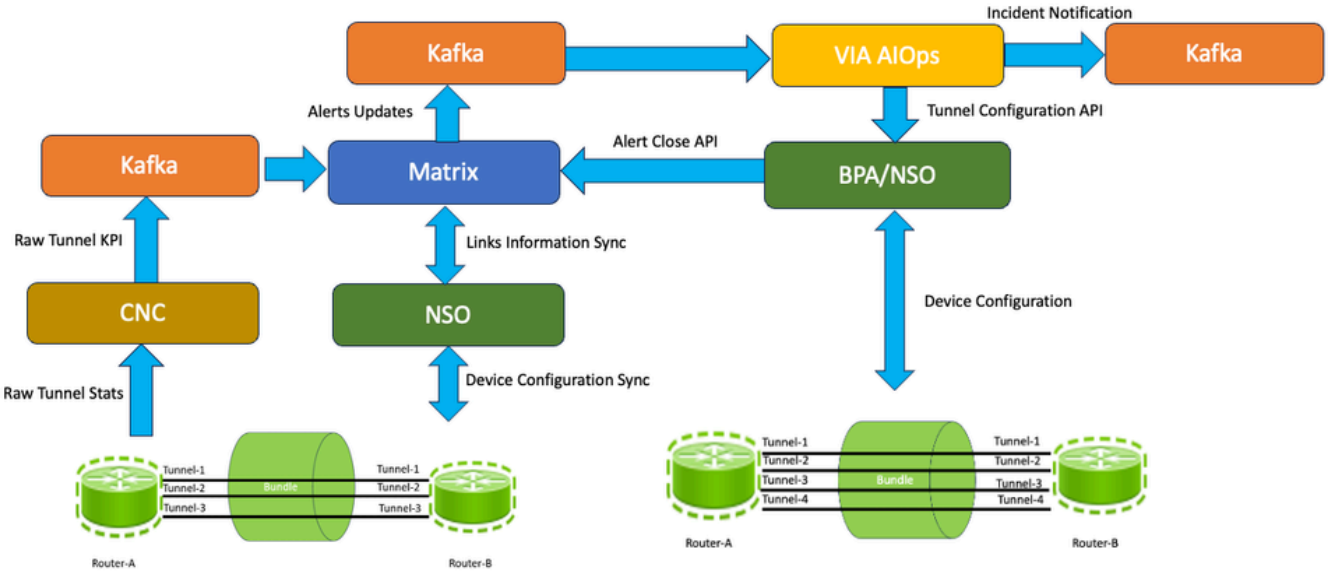


Validation des données et configuration des périphériques à l'aide de BPA-NSO

Avant d'entreprendre des opérations de mise à l'échelle, un modèle d'action YANG doit être élaboré pour l'ONS. Ce modèle définit les actions spécifiques que le NSO doit effectuer pour augmenter ou diminuer le nombre de tunnels entre les routeurs A et B. Le système Business Process Automation (BPA) commence à faire évoluer les opérations en s'engageant avec l'orchestrateur de services réseau (NSO) pour effectuer un « essai à blanc ». Il s'agit de la phase initiale de l'opération au cours de laquelle le BPA demande à l'ONS de simuler les modifications de configuration prévues sans les appliquer. L'essai à sec fonctionne comme une étape de validation essentielle, garantissant que les actions d'échelle proposées, telles que définies par le modèle d'action YANG, peuvent être exécutées sans provoquer d'erreurs ou de conflits dans la configuration du réseau.

Si le test à sec est considéré comme réussi, ce qui indique que les actions de mise à l'échelle sont validées, le BPA passe alors à l'étape « commit ». À ce stade, le BPA demande au NSO

d'implémenter les modifications de configuration réelles nécessaires pour augmenter ou diminuer le nombre de tunnels GRE entre les routeurs A et B. Le BPA déclenche le « Matrix Update Module » vers Matrix à l'aide d'un appel API pour fermer l'événement KPI en tandem avec VIA AIOps. Une fois cette anomalie fermée sur Matrix, Matrix envoie également une alerte avec la gravité « Effacé » à VIA AIOps, qui ferme l'incident à sa fin. De cette manière, le cycle de correction au niveau du réseau est terminé. Une version généralisée du flux de données au sein de l'application, utilisée dans cette automatisation en boucle fermée, est représentée dans cette image.



Flux de données pour un bundle de tunnel GRE Automatisation de boucle fermée

Fermer la boucle pour ouvrir de nouvelles possibilités de correction automatique

La solution abordée dans ce document est délibérément abordée avec un exemple de mise à l'échelle du bundle GRE basée sur les anomalies du réseau pour nous aider à établir des liens avec les différents blocs de construction de cette solution. Nous étudions en résumé comment Cisco Technology Stack, qui inclut Cisco NSO, Cisco Matrix et Cisco BPA, peut s'intégrer en toute transparence à des composants tels que VIA AIOps, Kafka et une autre pile logicielle pour nous aider à surveiller et à résoudre automatiquement les problèmes de réseau. Cette solution ouvre des possibilités pour tous les autres cas d'utilisation du réseau qui peuvent être des problèmes typiques se produisant dans les réseaux de fournisseurs de services ou d'entreprises.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.