Comprendre l'automatisation en boucle fermée dans un réseau défini par logiciel basé sur le cloud

Table des matières

Introduction

Informations générales

Nécessité de l'automatisation

Présentation de la solution

- 1. Fonctionnalités et avantages de la solution
- 2. Composants de la solution
- 3. Composants de la solution en détail
  - 3.1. Matrice : Gestion des performances
  - 3.2. Vitria : Gestion et assurance des pannes
  - 3.3. Contrôleur de réseau croisé (CNC) : Collecte, assurance, topologie
  - 3.4. Kafka : bus de messagerie
  - 3.5. ZTP : Activation des périphériques et mise en service du réseau
  - 3.6.TAF :Cadre d'automatisation des tests
  - 3.7. Portail unifié : Tableau de bord commun

Orchestrer la solution

Exemple d'utilisation de l'automatisation en boucle fermée (CLA)

Défis

- 1. Passer au cloud
- 2.Hésitation pour l'automatisation

Résumé

Informations connexes

Introduction

Ce document décrit le fonctionnement de l'automatisation en boucle fermée dans les réseaux définis par logiciel basés sur le cloud dans un scénario de déploiement 5G.

Informations générales

Le cloud révolutionne le fonctionnement de la technologie dans le monde traditionnel. Avec l'avènement de la 5G, le paradigme a changé dans les environnements des fournisseurs de services. La plupart des modes d'exploitation manuels et hérités d'un réseau permettent une automatisation complète, qui donne un avantage proactif aux réseaux, en les amenant sur une voie d'auto-réparation. Le document fournit une structure d'automatisation en boucle fermée basée sur SDN qui combine différents produits de l'écosystème de Cisco afin de fournir une

analyse, une visualisation et une correction en temps réel, le tout avec les solutions elles-mêmes déployées sur le cloud.

La 5G ne transforme pas seulement la technologie mobile, mais crée également des opportunités considérables pour de nombreux secteurs et prépare le terrain pour des bouleversements à grande échelle.

La 5G améliore considérablement le travail et l'expérience au quotidien grâce à une vitesse plus élevée, une bande passante plus large et une latence ultra-faible.

La 5G ne se limite pas au monde mobile, elle s'étend au-delà de la communication mobile pour couvrir toutes les formes de services de communication ; en fait, il soutient véritablement l'avenir du monde numérique en permettant tous les types de services, en promouvant le changement économique dans tous les secteurs et en utilisant diverses technologies (Wi-Fi, 4G et technologies radio).

Le document ne se concentre pas sur les phases de déploiement. L'accent est mis sur l'automatisation et l'architecture d'orchestration 5G en termes de fonctionnalité et d'observabilité de bout en bout.

Nécessité de l'automatisation

À ce stade, la 5G en est principalement à la phase initiale de test et de déploiement, mais il est nécessaire de comprendre les défis associés. Le nombre d'éléments réseau nécessaires pour exécuter un réseau 5G dans tous les domaines est énorme. Le déploiement de la plupart des réseaux 5G exige une automatisation pour garantir une mise en oeuvre rentable et efficace avec un fonctionnement transparent de tous les composants impliqués.

Dans un scénario de déploiement automatisé, la plupart des tâches manuelles lourdes de planification préalable peuvent être éliminées.

Les systèmes d’intelligence artificielle (IA), basés sur l’apprentissage automatique (ML), peuvent modéliser le fonctionnement des fonctions réseau dans des conditions normales et de charge élevée.

Grâce aux données de performances d'exécution, le système peut assurer le déploiement automatique de nouveaux éléments en fonction des besoins. Pour une optimisation et une assurance de service continues, le système peut collecter et analyser les flux d'équipement de tous types et examiner leurs performances, en déterminant s'ils correspondent aux paramètres que les fournisseurs de services exigent et attendent.

L'automatisation réussie repose sur trois composants essentiels.

1. Visibilité : si une dégradation des performances ne peut pas être détectée, ce qui a un impact sur la qualité du service sans une visibilité en temps réel sur ce qui se passe sur le réseau chaque seconde, vous ne pouvez pas l'automatiser.
2. Insight : les analyses réseau et la corrélation des données pertinentes ont généré des informations pour aider à détecter les anomalies.

3. Action : cette phase prend des mesures pour boucler la boucle afin de savoir que la modification apportée a le bon impact.

L'essentiel est d'avoir l'assurance et ensuite est l'apprentissage automatique qui peut prédire ce que le réseau essaie de réaliser, ce qui conduit à la base de l'automatisation en boucle fermée.

Présentation de la solution

La solution proposée est une solution logicielle offrant des fonctionnalités d'automatisation et d'assurance de pointe qui incluent :

1. Mise en service automatique : activation automatique des nouveaux périphériques, génération de la configuration et mise en service du réseau.
2. Workflow CI/CD : gestion de la configuration, sauvegarde des périphériques et historique des audits de restauration.
3. Visibilité en temps réel - Tableaux de bord et rapports de statistiques de performances et d'indicateurs de performance clés (KPI).
4. Analyse des pannes : déduplication des événements, réduction du bruit, corrélation des événements, gestion des pannes et analyse des causes premières.
5. Tendances et prédictions - Reconnaissance des modèles AI/ML, détection des anomalies, tendances statistiques et prévisions.

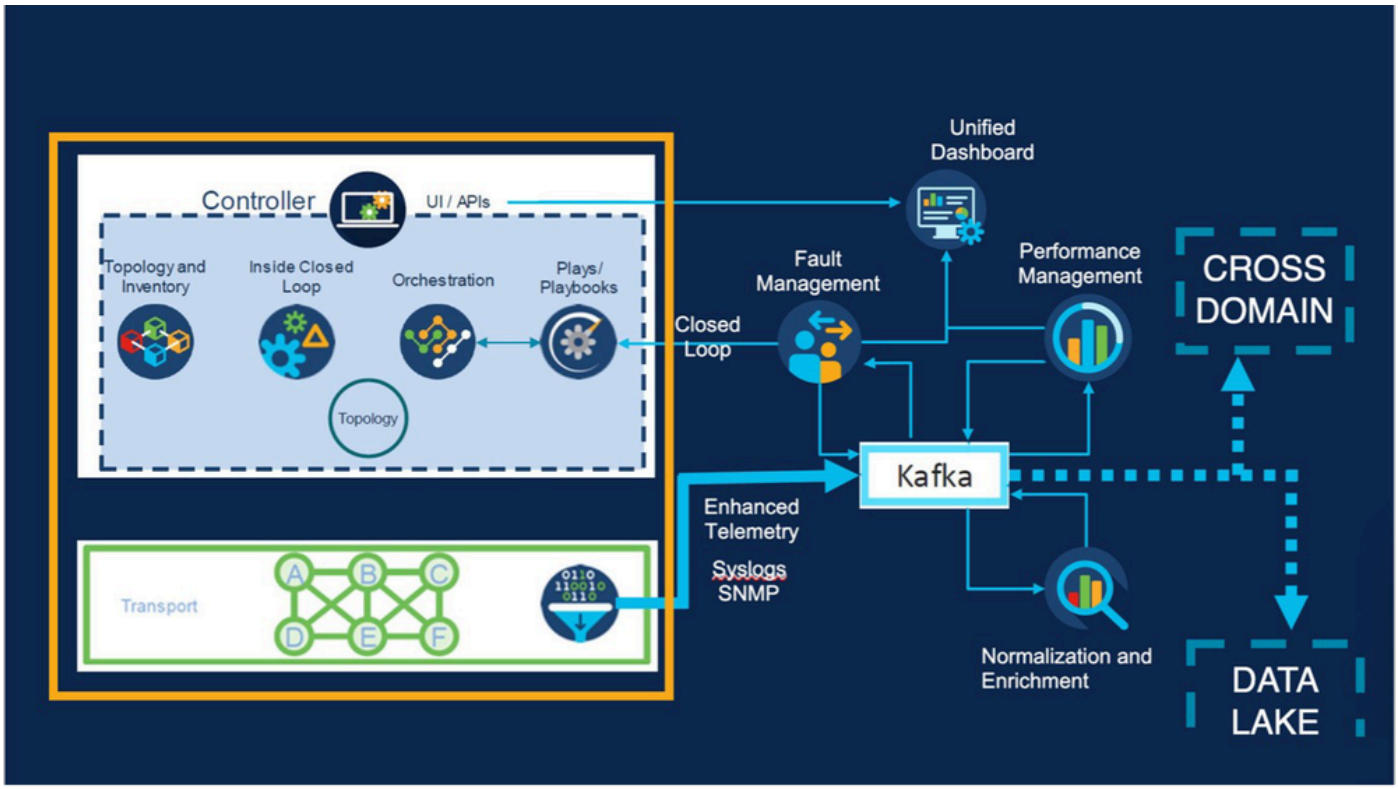
1. Fonctionnalités et avantages de la solution

- Provisionnement sans intervention - Permet un déploiement à grande échelle
- Intégration sans intervention : délai de commercialisation plus rapide
- Workflows automatisés (CICD) : plus de contrôle, moins d'erreurs
- Observabilité (gestion des pannes, gestion des performances, topologie) - Gestion et planification des capacités efficaces
- Corrélation des événements et réduction du bruit : correction des boucles fermées et réseau à rétablissement automatique

2. Composants de la solution

- Matrice (gestion des performances)
- Vitria (Gestion et assurance des pannes)
- CNC - Contrôleur réseau croisé (collecte, assurance, topologie)
- Kafka - Bus de messages
- Composants d'assurance de service ZTP (Zero-Touch Provisioning)
- Cadre d'automatisation des tests (TAF)
- Portail unifié

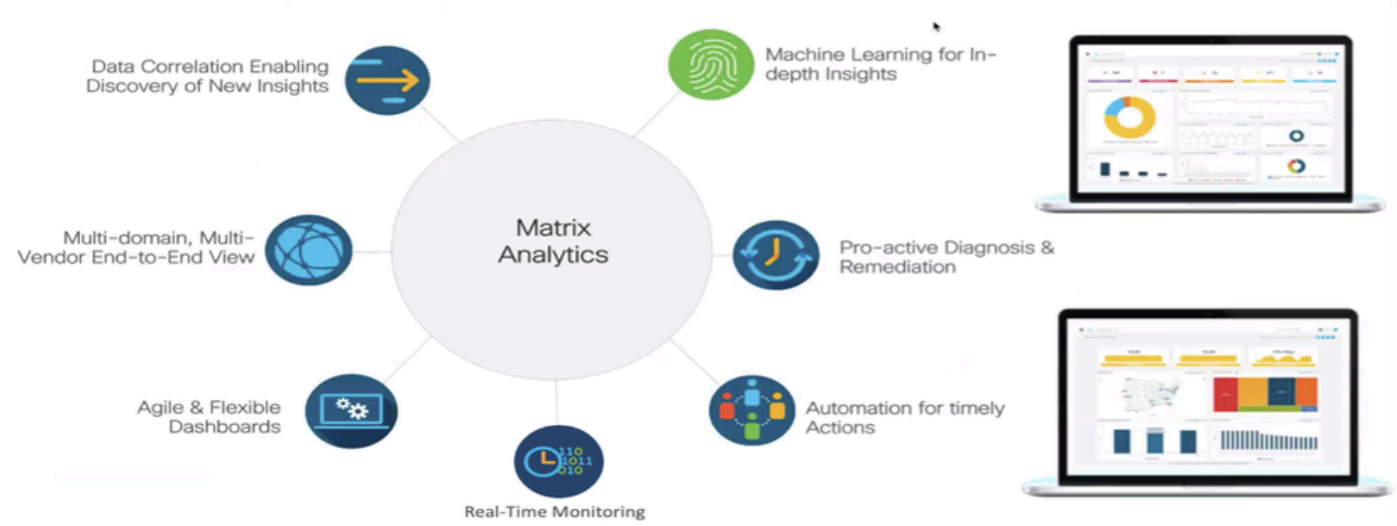
Même si Vitria peut également gérer les performances pour la meilleure solution, Matrix et Vitria font partie de la solution proposée, où Matrix est le meilleur outil de gestion des performances et Vitria le meilleur outil de gestion des pannes.



3. Composants de la solution en détail

3.1. Matrice : Gestion des performances

Matrix est une structure d'analyse générique développée par Cisco qui permet une adaptation facile à différents types de sources de données et permet l'intégration de fonctions d'analyse d'applications dans la solution. Matrix dispose de ces fonctionnalités clés qui vous permettent de créer ou de personnaliser les cas d'utilisation en fonction des besoins.



3.2. Vitria : Gestion et assurance des défaillances

Avec le réseau complexe de systèmes interconnectés composés d'infrastructures virtuelles et physiques, de réseaux internes et publics et d'applications interdépendantes, la gestion des

pannes est un défi constant.

La gestion traditionnelle des pannes repose sur des outils de surveillance cloisonnés qui s'adressent chacun à une couche distincte au sein de la pile technologique. Chaque système de surveillance génère des volumes d'alarmes. Les ingénieurs SRE (Service Reliability Engineers) examinent les alarmes et déterminent si un ticket doit être ouvert.

Les problèmes interconnectés entre les systèmes entraînent l'ouverture de plusieurs tickets et la prise de mesures par des équipes distinctes qui risquent de ne pas répondre à la véritable cause première, ce qui représente une perte de temps et de ressources. Lorsqu'il est finalement déterminé que les problèmes apparemment indépendants peuvent être liés, une équipe interfonctionnelle est formée afin de déterminer la véritable cause première et d'engager l'agent de correction ou la tâche appropriée afin de résoudre le problème. Alors que ce processus traditionnel de gestion des pannes se déroule, la frustration des clients augmente. Ce processus lent et exigeant en main-d'oeuvre n'est plus efficace. Elle est excessivement longue et coûteuse.

Afin de réduire le temps de détection des problèmes, d'accélérer leur résolution et de réduire les coûts, les signaux transmis à travers l'environnement d'exploitation depuis les éléments informatiques jusqu'au réseau et à l'application doivent être assimilés, corrélés et analysés. Une gestion efficace des pannes nécessite une réduction du bruit sur l'ensemble des couches de service, l'automatisation pour réduire le niveau d'intervention humaine et l'intégration aux processus et systèmes de gestion existants.

3.3. Contrôleur de réseau croisé (CNC) : Collecte, assurance, topologie

Un nouveau tournant dans le monde des réseaux a été l'avènement du routage de segment, qui a simplifié les opérations en remplaçant les méthodes traditionnelles comme la commutation multiprotocole par étiquette (MPLS). Le routage par segment a réduit la complexité des opérations en éliminant un grand nombre de protocoles et a entraîné une réduction significative des dépenses d'exploitation globales.

La nouvelle gamme de solutions de Cisco appelée CNC est un contrôleur SDN pour les réseaux de routage de segment. Une fois qu'un réseau est activé pour la SR, le CNC entre dans le vif du sujet avec une gamme de solutions qui permettent de visualiser le réseau, de déployer des services et des politiques, et une foule d'autres fonctionnalités.

Cisco CNC permet aux clients de simplifier et d'automatiser le provisionnement, la surveillance et l'optimisation des services réseau basés sur des intentions dans un environnement réseau multifournisseur avec une interface utilisateur graphique et une API communes.

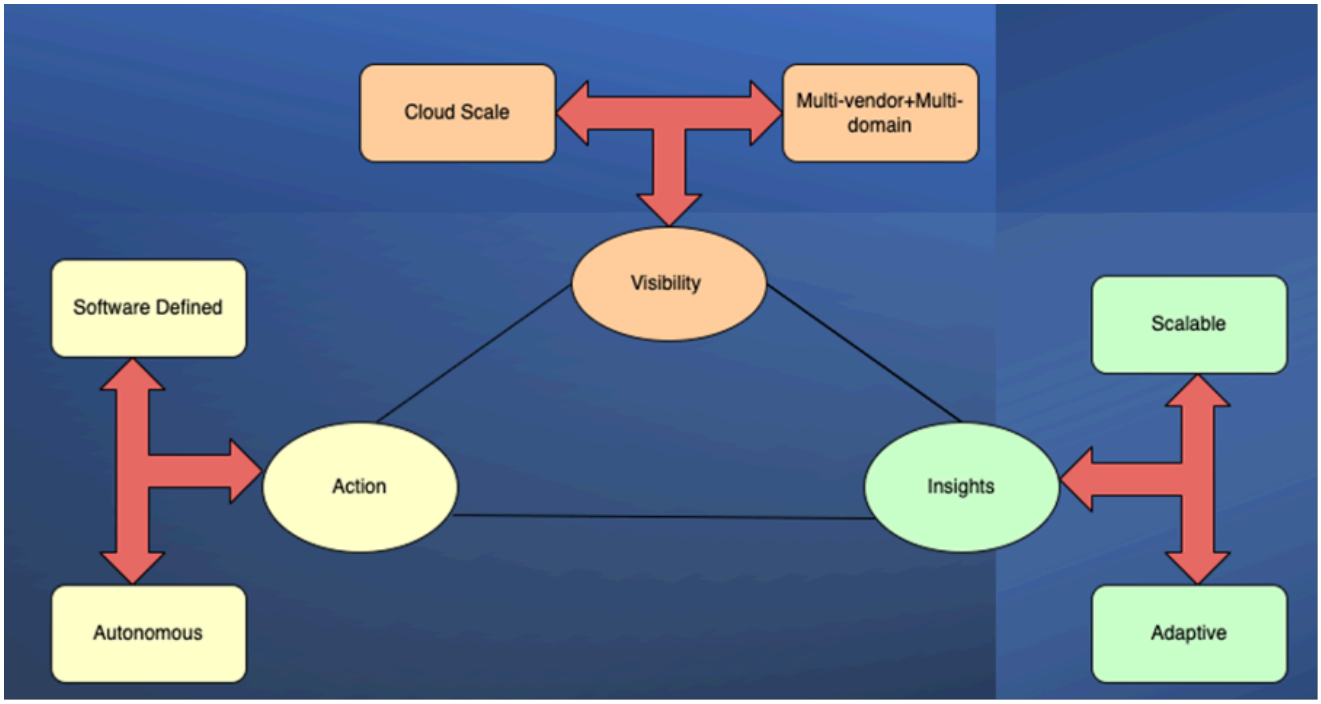
La solution combine l'automatisation du réseau basée sur l'intention afin de fournir des fonctionnalités critiques pour l'orchestration et l'exécution des services, y compris l'optimisation du réseau, le calcul du chemin de service, le déploiement et la gestion des périphériques et la détection des anomalies avec la correction automatique.

La solution entièrement intégrée combine les fonctionnalités de base de plusieurs produits innovants et de pointe, notamment Cisco Network Services Orchestrator (NSO), Cisco Segment Routing Path Computation Element (SR-PCE), Cisco Crosswork Data Gateway (CDG) et

l'infrastructure de Cisco Crosswork et d'une suite d'applications. Son interface utilisateur unifiée permet de visualiser en temps réel la topologie et les services du réseau, ainsi que le provisionnement des services et du transport, via une interface unique.

Les principes du travail croisé peuvent être résumés en trois principes d'automatisation :

- Visibilité
- Idées
- Action



Grâce à sa puissante suite de solutions, CNC offre un mécanisme complet de contrôle global du réseau. Les solutions varient selon les spectres et offrent des capacités étendues, qui répondent aux trois principes mentionnés précédemment.

1. Topologie active

Les réseaux traditionnels ne disposaient pas de composants permettant de visualiser les réseaux une fois déployés. Les opérateurs devaient se connecter physiquement aux routeurs pour vérifier diverses choses. Avec la topologie active du réseau croisé, les opérateurs obtiennent une visualisation en direct/en temps réel de l'ensemble du réseau, ainsi que des liens, de l'utilisation, des débits de trafic, de l'état de santé des noeuds et des liens, de l'état des politiques de routage de segment (SR) et RSVP, et de la visualisation du chemin. Tout ce que l'opérateur doit faire maintenant est de se connecter à une interface graphique intuitive et d'avoir le réseau à portée de main.

2. Moteur d'optimisation du travail croisé (COE)

Solution permettant d'optimiser le réseau en temps réel et qui aide les opérateurs à gérer efficacement l'utilisation de leur réseau. L'objectif final de COE est de permettre l'autoréparation des réseaux sans intervention manuelle importante.

3. Crosswork Data Gateway (CDG)

Imaginez avoir d'énormes réseaux avec des milliers de périphériques qui génèrent une tonne de données. Les données étant la nouvelle huile, le CDG fournit un mécanisme de collecte de toutes ces données à partir d'appareils qui peuvent être exploités par Crosswork lui-même ou peuvent même être envoyés à de nombreuses autres applications tierces pour analyse et autres transformations. CDG prend en charge la collecte de données via plusieurs protocoles tels que SNMP, CLI, gRPC Network Management Interface (GNMI), MDT, syslog, etc.

4. Crosswork Health Insights (HI)

Lorsque le réseau était opérationnel, le mode traditionnel consistait à prendre des mesures réactives après qu'un événement réseau particulier s'était produit. Cela a souvent un coût énorme pour les clients. HI permet d'effectuer automatiquement la surveillance dynamique des indicateurs de performance clés, la génération d'alertes et le dépannage. L'utilisateur peut définir sa propre logique et HI déclenche alors des alertes en fonction de sa surveillance. Cela permet une analyse automatisée de l'état du réseau.

5. Automatisation des modifications transversales

Les opérations manuelles courantes, telles que l'application des modifications de configuration, l'installation de nouvelles versions de logiciels, les mises à niveau et autres peuvent être automatisées et accélérées grâce à l'automatisation des modifications. Cela permet d'utiliser les guides Ansible intégrés dans, et les modifications de configuration sont ensuite répercutées sur les périphériques en tirant parti de Cisco NSO.

6. Mise en service sans intervention (ZTP) du réseau croisé

Les clients sont toujours favorables à la réduction du délai de déploiement et d'exploitation. Lorsque vous avez des dizaines à des milliers de nouveaux périphériques à déployer sur le réseau, au lieu du processus manuel habituel qui pourrait être truffé d'erreurs et de temps, le Crosswork ZTP stimule l'ensemble du processus avec une solution entièrement automatisée pour le provisionnement et l'intégration de nouveaux périphériques Cisco IOS® XR. Les périphériques peuvent être mis en place avec une configuration de jour 0, puis rapidement ajoutés à l'inventaire des périphériques CNC, après quoi la surveillance, ainsi que la gestion de ces périphériques devient plus facile.

Il existe quelques autres séries de produits qui fonctionnent en tandem avec le CNC afin d'atteindre les objectifs. Le principal d'entre eux est le Segment Routing Path Computation Element (SR-PCE), un PCE Cisco IOS XR qui prend en charge SR et RSVP. En fait, c'est le SR-PCE qui facilite la collecte des topologies via le protocole BGP-LS et calcule le chemin afin de permettre au CNC de fonctionner en tant que contrôleur.

Le CNC peut également interagir avec le NSO, ce qui permet de traduire une intention de réseau en configurations spécifiques à un périphérique. Le CNC, lorsqu'il est utilisé conjointement avec le NSO, devient un multiplicateur de force.

3.4. Kafka : bus de messagerie

La surveillance Kafka est activée à l'aide de l'outil Burrow. Burrow est un compagnon de surveillance pour Apache Kafka qui fournit la vérification du décalage client en tant que service sans avoir besoin de spécifier de seuils.

Il surveille les compensations engagées pour tous les consommateurs et calcule l'état de ces consommateurs à la demande. Un terminal HTTP est fourni afin de demander l'état à la demande, ainsi que de fournir d'autres informations de cluster Kafka. Ces API sont interrogées par l'outil de surveillance des performances (PM) afin de générer une surveillance des retards des consommateurs et de fournir des informations sur les clusters Kafka.

L'utilisation du CPU, l'utilisation du stockage et l'utilisation de la mémoire des noeuds Kafka sont également disponibles dans Matrix, qui envoie des alarmes en cas de dépassement des seuils ou de détection d'anomalies.

3.5. ZTP : Activation des périphériques et mise en service du réseau

Il s'agit du processus automatisé d'activation de nouveaux périphériques, de génération de configuration et de mise en service du réseau.

3.6.TAF : cadre d'automatisation des tests

Le cadre TAF (Advanced Test Automation Framework) permet d'exécuter des suites de tests en parallèle sur des milliers de périphériques en même temps, éliminant ainsi la nécessité d'une validation manuelle. Un déploiement gigantesque d'un réseau ne peut jamais évoluer avec une seule validation manuelle et un cadre automatisé comme celui-ci permet de valider les configurations des périphériques et d'autres contrôles de la manière la plus efficace et la plus rapide possible.

Un opérateur peut lancer des centaines de tests sur des milliers de périphériques en un seul clic. La suite de tests effectue tous les tests configurés, valide les données, puis affiche l'ensemble des résultats avec les critères PASS/FAIL dans un rapport Web détaillé. Sur la base du rapport, l'opérateur peut prendre d'autres mesures afin de pallier ces erreurs dans les dispositifs à l'aide d'autres solutions automatisées.

3.7. Portail unifié : Tableau de bord commun

Il s'agit d'une interface utilisateur ouverte pour toutes les applications qui offre la possibilité d'ajouter, de supprimer et de modifier des applications et des icônes sans développement.

Cela permet la prise en charge de l'authentification LDAP et l'accès à la documentation produit.

Orchestrer la solution

Afin d'atteindre les objectifs de l'automatisation 5G, une orchestration interdomaine est nécessaire pour connecter les parties entre les différents domaines composant le réseau.

Une fois les périphériques de transport configurés et installés sur le réseau, au lieu de suivre la

méthode traditionnelle ou héritée de gestion manuelle des périphériques, l'orchestration interdomaine peut être exploitée pour favoriser la simplicité, l'agilité et l'efficacité.

Les périphériques actifs du réseau peuvent être intégrés à CNC avec la spécification des protocoles par lesquels le CDG peut collecter des données à partir des périphériques. Une fois que les périphériques sont intégrés à CNC, la visualisation en temps réel de l'ensemble du réseau L2 et L3 devient facile. La surveillance des périphériques s'accélère avec l'affichage sur l'interface graphique utilisateur lié à de nombreuses facettes de l'état de santé du périphérique. La collecte de données à partir des dispositifs commence à des intervalles prédéterminés et ces données ont une valeur analytique riche. Les données sont collectées via SNMP, SSH, MDT, la télémétrie et divers autres modes, comme indiqué précédemment.

Ces données peuvent ensuite être transmises aux autres applications de l'écosystème. Le CNC permet d'envoyer les données collectées au système Matrix via un bus Kafka. La collection est souscrite à un sujet Kafka et le CDG continue de distribuer les données qu'il recueille à ce sujet, dont le point d'extrémité est à Matrix.

Matrix dispose de plusieurs tableaux de bord intuitifs à partir desquels ces données peuvent être visualisées et plusieurs opérations analytiques peuvent également être effectuées. Ces données peuvent ensuite être regroupées par la solution Cisco Vitria AIOps pour la surveillance des pannes. Chaque fois que des défauts ou anomalies sont détectés, l'outil Vitria génère des alarmes de manière proactive afin que les corrections nécessaires puissent être prises, évitant ainsi les défaillances majeures.

Au sein de la suite de travail croisé, certaines applications peuvent orchestrer de manière proactive le trafic dans un réseau de transport, réduisant ainsi les temps d'arrêt significatifs lors des périodes de charge de pointe. Des packs de fonctionnalités de COE tels que Local Congestion Mitigation (LCM) et Bandwidth on Demand (BWoD) viennent à la rescousse dans de tels scénarios.

Le LCM est un outil très pratique qui permet de réduire l'encombrement au sein d'un réseau et d'appliquer des politiques qui empruntent des chemins alternatifs, libérant ainsi l'interface surchargée. Tout cela se produit automatiquement sans qu'un utilisateur ne tente de détecter l'encombrement après qu'il se soit déjà produit. LCM utilise un seuil configurable au-delà duquel il est considéré comme encombré.

Une fois que l'utilisation d'une interface dépasse ce seuil, LCM fournit des recommandations pour réduire l'encombrement au niveau d'une interface locale. La solution prend soin d'orienter uniquement le volume de trafic requis qui entraîne la congestion sous le seuil. L’avantage de cette méthode est que l’intégralité du trafic dans l’interface n’est pas déviée. L'utilisateur peut analyser l'ensemble de recommandations, puis choisir celle qui lui convient le mieux. Ainsi, les politiques de trafic tactique sont lancées par LCM avec l'aide du composant SR-PCE qui aide à la suppression automatisée de la congestion en temps réel.

La solution BWoD peut fonctionner avec LCM. S'il existe une interface de priorité élevée transportant le trafic vocal ou vidéo, un opérateur veut s'assurer que le chemin dispose toujours d'une quantité spécifiée de bande passante disponible. COE permet à un utilisateur de créer un chemin de stratégie BWoD et, lorsque le BWoD est également configuré avec un seuil, la

surveillance démarre toutes les secondes. Dès que le seuil de l'interface est atteint, BWoD intervient pour créer de nouvelles politiques SR ou réoptimiser le chemin existant qui s'efforce de maintenir la bande passante allouée.

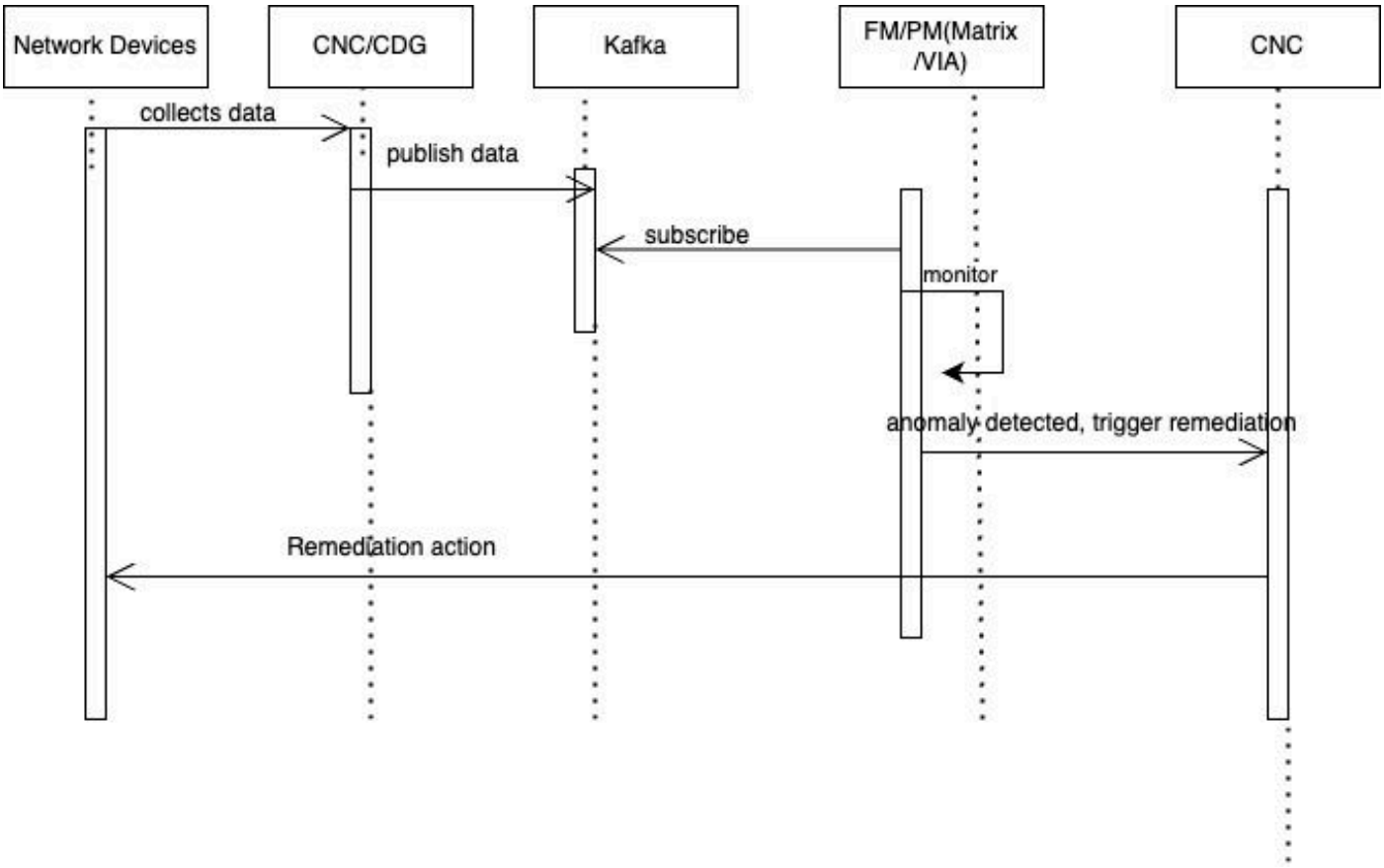
Voici quelques scénarios qui optimisent le chemin de transport et facilitent l'automatisation du transport. Bien que la CNC puisse être utilisée avec d'autres solutions afin de traiter et d'analyser les données, les composants internes de la CNC peuvent également jouer un rôle important dans le développement du réseau de transport avec une automatisation haut de gamme qui augmente la disponibilité et la fiabilité du réseau.

Exemple d'utilisation de l'automatisation en boucle fermée (CLA)

Dans tous les cas d'utilisation d'ALC, les étapes de base comprennent :

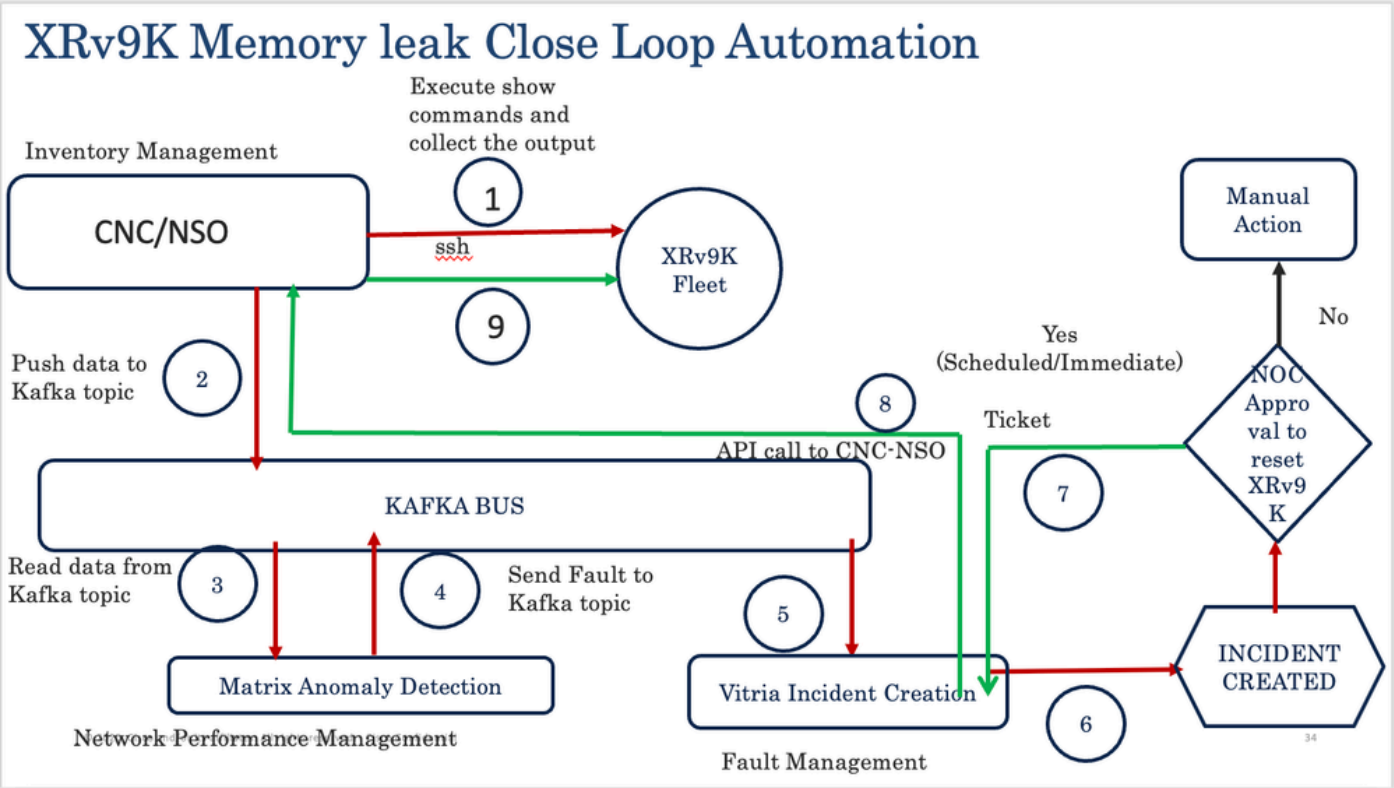
1. Collecte de données à partir du périphérique ou de la source et transfert de ces données vers le bus de messages.
2. Système de gestion des performances pour mettre en oeuvre la logique d'ingestion (analyseur), améliorer le pipeline de traitement et définir un seuil KPI afin de détecter les anomalies pour des processus spécifiques.
3. Les systèmes de gestion des pannes doivent détecter les anomalies détectées et attendre qu'elles se produisent pour appeler les API afin d'agir.
4. Une fois la correction effectuée, les anomalies du flux de détection du système de gestion des performances envoient une alerte d'anomalie avec un état clair.
5. Gestion des pannes Systèmes permettant d'ingérer l'alerte, d'éliminer l'anomalie et de clore l'incident.

Voici une description du flux de cette solution Cisco :



Un exemple réel de la façon dont l'automatisation en boucle fermée peut fonctionner en exploitant les composants Cisco interdomaines est le mieux illustré dans le cas de fuites de mémoire des périphériques. La commande `show processes memory detail` fournit les détails de la consommation de mémoire de tous les processus du routeur.

Une tâche de collecte CLI peut être créée dans CNC afin de permettre à CDG de se connecter au routeur à des cadences spécifiées par l'utilisateur et d'exécuter la commande `show processes memory detail`. Le CDG obtient le résultat de cette commande et transfère les données au bus Kafka. Matrix lit ces données à partir du bus Kafka, et les analyse et les transforme pour afficher les informations de mémoire sur ses tableaux de bord.



Chaque fois que la consommation de mémoire dépasse un seuil défini pour les routeurs, Matrix génère une alarme et transmet l'anomalie au bus Kafka. Vitria AIOps génère ensuite un incident sur son tableau de bord en lisant l'anomalie dans le bus Kafka. Cela peut être visualisé dans le tableau de bord AIOps qui affiche le nom d'hôte du périphérique où l'utilisation de la mémoire a dépassé les limites de sécurité.

À partir de l'interface utilisateur graphique d'AIOps, il est possible d'agir sur cette alarme en intégrant une API de réinitialisation de périphérique Network Service Orchestrator (NSO), un système de gestion de la configuration, qui réinitialise le périphérique.

Il y a aussi une période de refroidissement à Vitria où l'incident reste ouvert pendant un certain temps. Dans ce délai, si Matrix ne signale plus aucune fuite sur le même périphérique, l'incident se ferme automatiquement. Dans le cas contraire, le même processus de réinitialisation du périphérique est répété. Dans le processus, il n'est pas nécessaire d'effectuer une seule intervention manuelle et l'ensemble de la correction est géré par les composants interdomaines eux-mêmes, qui prouvent que l'ensemble de la boucle est automatisé et résolu proactivement de la manière la plus cohérente, en temps réel.

Défis

1. Passer au cloud

L'hébergement de l'application dans le cloud présente les défis suivants :

- De nouvelles solutions de sécurité et de gestion des opérations sont nécessaires
- Recherche de cas d'utilisation et de modèles commerciaux derrière la périphérie du cloud

- Les clouds doivent prendre en charge le haut débit requis
- Les opérations, les processus, la sécurité et la disponibilité doivent répondre aux attentes des fournisseurs de services et de leurs clients
- Les fournisseurs de cloud proposent leurs solutions afin de faciliter la conception de services de migration vers le cloud, parfois difficile à adapter

2. Hésitation pour l'automatisation

- Impossibilité de prévoir le besoin d'automatisation
- Complexité des réseaux des fournisseurs

Résumé

L'automatisation et l'orchestration d'un réseau 5G sont des tâches complexes qui doivent être correctement planifiées et mises en oeuvre dès le début de la conception d'un réseau.

La complexité des réseaux 5G exige l'automatisation et l'orchestration afin de simplifier les tâches et de minimiser la probabilité d'erreurs lors de la planification, de la mise en oeuvre et de l'exploitation.

Informations connexes

- https://www.cisco.com/c/dam/m/en_us/customer-experience/collateral/5G-automation-architecture-white-paper.pdf
- https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/crosswork-network-controller/3-0/Solution-Workflow-Guide/CNC-3-0-Solution-workflow-guide.pdf
- Assistance technique de Cisco et téléchargements

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.