



Au-delà de l'automatisation

Construire des réseaux plus intelligents et autonomes

Livre blanc

Au-delà de l'automatisation : construire des réseaux plus intelligents et autonomes

Alcatel·Lucent 
Enterprise

Introduction

Avec l'essor fulgurant du cloud, la multiplication des objets connectés et l'évolution constante des menaces cyber, les réseaux d'entreprise deviennent de véritables labyrinthes technologiques. Dans ce contexte, la gestion manuelle devient vite un frein : les méthodes traditionnelles ne tiennent plus la cadence face aux exigences des opérations modernes.

Ce document explore **l'évolution de l'automatisation des réseaux traditionnels vers des réseaux autonomes, en soulignant le rôle central de l'intelligence artificielle (IA) et de l'apprentissage automatique (Machine Learning - ML).**

Pour relever ce défi, les réseaux autonomes sont une solution robuste, capable de surveiller, analyser et optimiser les performances en temps réel, tout en réduisant au minimum les interventions humaines

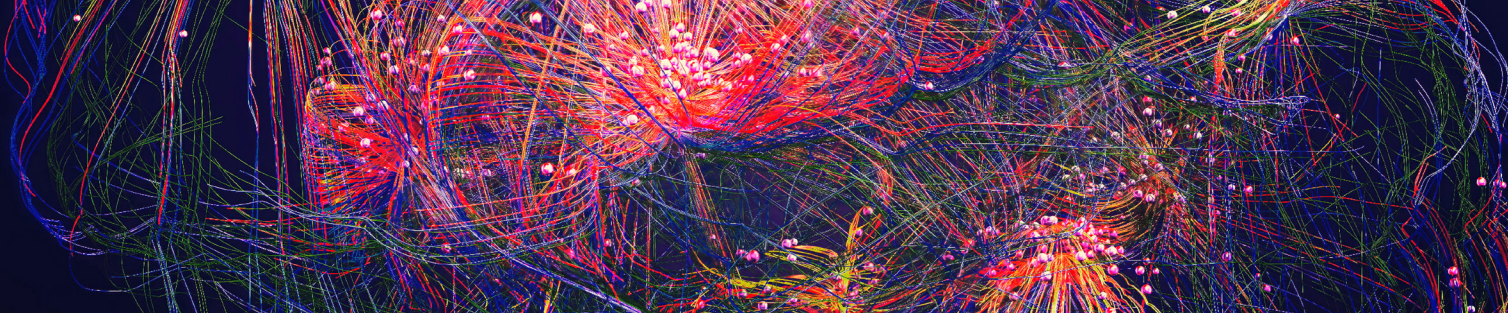
Ce document présente des cas d'usage concrets, basés sur l'intelligence artificielle, qui répondent à des défis critiques de gestion réseau restés hors de portée de l'automatisation conventionnelle. Ces cas illustrent une évolution majeure : le passage d'une IA réactive, qui intervient après coup, à une IA proactive et préventive, capable d'anticiper les problèmes et de les atténuer avant qu'ils n'impactent les opérations. Le parcours culmine avec l'IA prescriptive, où les systèmes intelligents fournissent des recommandations basées sur des données qui étayent une prise de décision stratégique éclairée.

En combinant l'automatisation avec des initiatives d'IA, votre entreprise peut garantir la fiabilité et l'efficacité des opérations de leur réseau, en obtenant une stabilité durable, une résilience et un avantage concurrentiel dans le paysage informatique complexe d'aujourd'hui.

Livre blanc

Au-delà de l'automatisation : construire des réseaux plus intelligents et autonomes





Comprendre le réseau autonome

Un réseau autonome est un système qui fonctionne de manière indépendante. Il fonctionne en conformité avec les objectifs de l'entreprise sans nécessiter d'intervention humaine au-delà de la saisie initiale (sous la forme d'intentions, d'objectifs, de politiques ou de données de configuration spécifiques). Il est conçu pour se gérer lui-même par le biais de diverses opérations d'autogestion, notamment l'autoconfiguration, l'autodiagnostic, l'auto-réparation, l'auto-guérison, l'auto-optimisation et l'auto-protection. Ces capacités sont soutenues par l'aptitude du réseau autonome à découvrir automatiquement les informations opérationnelles et à agir en conséquence.

Un réseau autonome présente les caractéristiques suivantes :

- **Vigilance** - Il surveille en permanence son environnement opérationnel, ses performances et son état interne afin de déterminer s'il atteint les objectifs prédéfinis et convenus.
- **Capacité d'adaptation** - Il ajuste dynamiquement ses activités pour s'adapter aux changements de son environnement à court et à long terme. Il s'agit notamment de modifier ses décisions et ses comportements afin d'assurer une performance opérationnelle durable.
- **Automatisation** - Il peut contrôler de manière indépendante les ressources et les opérations internes et fonctionner sans intervention manuelle.

Le niveau de « capacité » d'un réseau peut varier, allant de l'automatisation de base à l'autonomie complète.

Différence entre automatisation et autonomie

L'automatisation des réseaux et l'autonomie des réseaux sont deux concepts souvent confondus, mais qui présentent des différences distinctes dans leur approche, leur fonctionnalité et leur niveau d'intervention humaine.

L'automatisation des réseaux implique l'utilisation d'outils et de processus logiciels pour gérer l'infrastructure et les services du réseau par programmation. Le processus automatise les tâches répétitives, telles que la configuration, le déploiement et la maintenance, afin d'améliorer l'efficacité et de réduire les erreurs humaines. L'automatisation nécessite généralement **une intervention humaine** pour la prise de décision et l'établissement de règles. Elle fonctionne selon des paramètres et des conditions prédéfinis. L'IA générative peut contribuer à fluidifier la communication entre les administrateurs et le réseau.

L'autonomie du réseau, quant à elle, fait référence à une **architecture de réseau autogérée** qui exploite l'IA/ML pour minimiser ou éliminer l'intervention humaine. Elle peut se configurer, se surveiller, se maintenir et se sécuriser elle-même. Les décisions sont pilotées par le système et les humains sont en dehors de la boucle, sauf s'ils sont nécessaires pour une supervision. La mise en place d'un réseau autonome est un processus progressif. Pour que les administrateurs puissent renoncer complètement au contrôle, le système doit augmenter progressivement son niveau d'autonomie afin de gagner leur confiance.

Chaque concept aborde un scénario de gestion de réseau différent. L'automatisation est utilisée pour des problèmes répétitifs bien connus ; les administrateurs investissent leur temps et leurs efforts pour développer des moyens techniques afin de résoudre ces problèmes. L'autonomie est responsable de problèmes rares, souvent inconnus, qui peuvent être identifiés à l'aide de méthodes d'IA/ML. **Ensemble, ces deux méthodes constituent une base robuste pour le bon fonctionnement des réseaux.**

La gestion de réseau avec automatisation

À la base, l'automatisation permet d'exécuter des tâches sans intervention humaine. Pour ce faire, on introduit des fonctions automatiques ou on améliore, remplace ou modifie les processus manuels à l'aide d'outils d'automatisation, tels que des scripts qui exécutent une séquence de commandes.

L'automatisation fonctionne à différents niveaux de granularité, depuis les tâches et processus individuels jusqu'à la gestion et l'exploitation complètes de l'infrastructure (englobant l'ensemble du cycle de vie des réseaux et des services, y compris l'installation, la configuration, la mise à disposition et la résiliation). Cette automatisation peut être encore améliorée par des innovations telles que la dissociation des plans de contrôle et de données et les techniques de virtualisation, qui apportent une plus grande flexibilité. Cependant, l'un des principaux défis consiste à intégrer ces composants modulaires dans des systèmes d'automatisation cohérents, performants, robustes, extensibles et reconfigurables. Cela souligne la nécessité de disposer d'interfaces, de modèles et de mécanismes normalisés.

La mise au point d'une solution d'automatisation entièrement intégrée reste un défi complexe et ouvert. Ce type de solution passe par une coordination parfaite des fonctions automatisées, avec les caractéristiques suivantes :

- **Automatisation verticale de bout en bout**, couvrant l'ensemble de la pile de protocoles, de la couche service à la couche physique
- **Automatisation horizontale de bout en bout**, couvrant plusieurs technologies et domaines administratifs
- **Reproductibilité et réutilisabilité**, en exploitant des interfaces standardisées et de bonnes pratiques pour une large applicabilité
- **Approvisionnement dynamique** de points de contrôle personnalisables, permettant une supervision humaine au sein de la boucle d'automatisation

Il est important de déterminer dans quelle mesure l'automatisation est motivée par des politiques techniques ou des intentions commerciales. Une seule infrastructure technologique permettra de tout gérer

Grâce à cette infrastructure intégrée, le Bâtiment Intelligent 5.0 gèrera la température, l'éclairage et les stores des fenêtres de chaque pièce à l'aide de plusieurs capteurs. Il s'appuiera sur son architecture véritablement intelligente pour collecter des données, les analyser, en rendre compte et agir de manière

indépendante sur la base de toutes les informations disponibles dans le but de soutenir le fonctionnement courant. En outre, le bâtiment sera capable de prévoir les changements de paramètres d'exploitation nécessaires en se basant sur les données relatives aux conditions environnementales intérieures et extérieures du bâtiment et d'agir en fonction de ces prévisions afin de maintenir les objectifs du bâtiment régénératif.

Automatisation axée sur les politiques

Les actions automatisées peuvent souvent être régies par des politiques. De nombreux déploiements de réseaux intègrent déjà une gestion dynamique des politiques, permettant des ajustements automatisés dans la gestion du cycle de vie et d'autres configurations du réseau.

Au cœur de l'automatisation basée sur des politiques se trouve **le concept de règles prédéfinies qui déclenchent des actions spécifiques** lorsque certaines conditions sont remplies. Ces conditions peuvent inclure :

- Déclencheurs temporels (heure de la journée, jour de la semaine, etc.)
- Seuils de charge du réseau
- Défaillances du système
- Combinaisons des éléments ci-dessus

Lorsqu'une condition de déclenchement se produit, l'entité de gestion locale exécute les actions prédéfinies correspondantes, telles que :

- Déploiement ou arrêt de services/composants
- Redimensionnement des ressources
- Migration des charges de travail
- Remplacement des instances
- Ajustement des configurations
- Gestion des mises à jour de logiciels

Une fois les politiques mises en place, l'automatisation axée sur les politiques permet une gestion entièrement autonome, **sans aucune intervention humaine**. Cependant, l'élaboration de politiques et leur adaptation dynamique à l'évolution des conditions restent un défi complexe. L'application d'intentions métiers générales peut améliorer la situation.



Automatisation basée sur l'intention

L'**automatisation** basée sur l'intention repose sur le concept d'Intent-Based Networking (IBN), qui utilise des logiciels intelligents pour comprendre les objectifs des utilisateurs et les traduire automatiquement en configurations concrètes de services ou de réseaux. L'IBN est un mécanisme relativement nouveau, sa définition varie donc et il n'existe pas de cadre normalisé à l'heure actuelle.

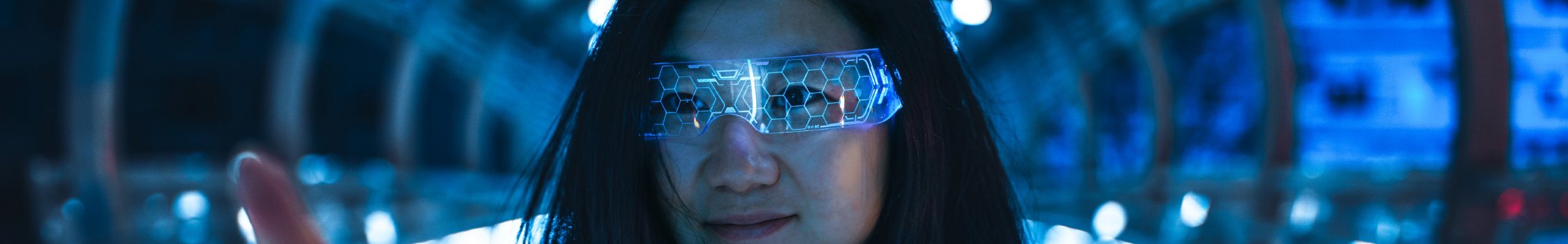
L'IBN est l'étape suivante de la gestion de réseau après l'automatisation basée sur des politiques. Alors que les politiques définissent des règles de décision spécifiques, l'intention représente un objectif déclaratif plus général. Une API basée sur l'intention permet aux utilisateurs de spécifier les résultats souhaités, tandis que le système sous-jacent détermine dynamiquement la configuration optimale du réseau.

Les systèmes de gestion traditionnels nécessitent des modifications de configuration lorsque les exigences d'un service changent. Une approche véritablement axée sur l'intention repose sur une modélisation sémantique qui permet une automatisation basée sur le comportement sans manipulations manuelles de la configuration. Contrairement aux politiques, les intentions ne sont pas affectées par les changements ou les défaillances de l'infrastructure. Les applications de gestion sont ainsi libérées des détails spécifiques au réseau, ce qui simplifie le développement, les tests et le déploiement des services.

Une API d'intention extensible permet à **des services développés** indépendamment d'exprimer leurs exigences dans un langage unifié. Ceci est essentiel pour les environnements modernes qui intègrent SDN, SD-WAN, MPLS, le cloud privé/public et l'Edge Computing.

L'IA générative peut combler le fossé entre les intentions métier en amont et les configurations réseau en aval. Pour ce faire, elle interprète les entrées en langage naturel des utilisateurs et les traduit en politiques techniques exploitables. Par exemple, si un utilisateur spécifie un objectif tel que « donner la priorité au trafic de vidéoconférence », GenAI peut identifier les paramètres de qualité de service (QoS) nécessaires pour mettre en œuvre cette intention. Elle s'appuie sur des modèles entraînés à partir de données réseau et de règles de politique pour garantir des traductions précises et pertinentes. Cela permet aux intervenants non techniques d'exprimer leurs objectifs sans avoir à comprendre la syntaxe complexe de la configuration.

GenAI prend également en compte le contexte de l'environnement réseau, tel que les politiques existantes, les mesures de performance et les exigences de conformité. Cela permet d'éviter les conflits et de s'assurer que les nouvelles configurations s'inscrivent dans la stratégie globale du réseau. Au fil du temps, GenAI peut apprendre des commentaires des utilisateurs et du comportement du réseau pour améliorer ses capacités de génération de politiques. **La gestion du réseau devient ainsi plus intuitive, plus souple et plus conforme aux objectifs de l'entreprise.**



L'IA dans les réseaux

Trois types d'IA sont particulièrement pertinents pour la gestion des réseaux : l'IA prédictive, l'IA générative et l'IA agentique.

IA prédictive

L'IA prédictive utilise des données historiques, des modèles statistiques et des algorithmes d'apprentissage automatique pour prévoir des résultats ou des comportements futurs. Elle identifie les modèles et les tendances afin de faire des prédictions éclairées, telles que l'anticipation des défaillances du système ou de la dégradation des performances.

Les principales applications de l'IA prédictive sont les suivantes :

- **Seuils dynamiques pour la détection des anomalies** : contrairement aux seuils statiques préconfigurés, les seuils basés sur le ML sont ajustés en temps réel en fonction de l'évolution des modèles et des tendances, ce qui garantit une surveillance plus adaptable et plus réactive, et donc une détection efficace des anomalies.
- **Corrélation automatisée des événements** : l'IA identifie les relations cachées entre les événements, fournissant les moyens d'une analyse efficace des causes profondes, ce qui améliore considérablement les temps de réponse aux incidents et réduit les efforts manuels.
- **Analyse intelligente des log** : l'IA peut exploiter les données historiques pour classer et interpréter les messages syslog nouveaux et rares, en identifiant les événements critiques sans qu'il soit nécessaire d'appliquer des règles d'analyse prédéfinies.

IA générative

L'IA générative crée des contenus en apprenant des modèles à partir de données par l'application de grands modèles de langage (Large Language Model - LLM).

Les principales applications de l'IA générative sont les suivantes :

- **Rapports adaptatifs** : l'IA génère en temps réel des rapports contextuels adaptés aux conditions actuelles du réseau, ce qui permet de disposer en permanence d'informations pertinentes.
- **Interface en langage naturel pour les administrateurs** : l'IA traduit les commandes en langage naturel en configurations de réseau ou en requêtes. Elle peut également permettre une interaction intuitive avec les données du réseau par le biais d'invites conversationnelles.

IA agentique

L'IA agentique s'appuie sur une logique avancée pour prendre des décisions et des mesures au nom de l'utilisateur, à l'aide de modèles prédictifs et génératifs. Elle fait preuve d'un comportement orienté vers les objectifs grâce à un raisonnement en plusieurs étapes et à un apprentissage adaptatif, s'améliorant constamment grâce à une boucle de feedback en temps réel qui évalue les résultats et s'ajuste en conséquence.

L'application clé de l'IA agentique est celle des flux de travail intelligents. Un ingénieur réseau délègue un large éventail de tâches de gestion réseau à un agent IA. L'agent détermine de manière autonome comment répondre à la demande, ce qui implique souvent des interactions avec plusieurs systèmes qui collectent des données, exécutent des requêtes de suivi et interprètent les résultats. Une fois le processus terminé, l'agent IA fournit une réponse complète à l'ingénieur.

Gestion de réseau avec autonomie

Traditionnellement, l'automatisation des réseaux s'est concentrée sur la rationalisation des tâches à haute fréquence ou critiques, telles que :

- **Application des règles d'analyse** aux messages syslog les plus courants
- **Génération d'alertes** lorsque les indicateurs clés dépassent des seuils prédéfinis
- **Corrélation d'événements** sur la base de modèles types ou de combinaisons récurrentes

Cependant, cette approche néglige un large éventail de tâches moins bien définies, mais potentiellement cruciales. Pour traiter ces tâches, il faut une stratégie fondamentalement différente, qui exploite les capacités de l'IA et du ML. Ces technologies permettent l'automatisation et l'optimisation même en l'absence de règles explicitement définies pour chaque scénario.

Les trois types d'IA mentionnés ci-dessus, associés à des méthodes d'automatisation et à d'autres technologies, sont intégrés pour mettre en œuvre le moteur principal de l'autonomie du réseau : l'automatisation en boucle fermée.

L'automatisation en boucle fermée est une approche dans laquelle un système recueille en continu des données, les analyse, prend et applique des décisions de configuration, puis répète ce cycle afin d'améliorer les résultats en fonction des retours d'expérience des actions précédentes.

À mesure que les réseaux passent d'un fonctionnement manuel à une autonomie totale, ils passent par plusieurs niveaux tels que l'automatisation assistée, partielle, conditionnelle, élevée et totale. À des niveaux plus élevés, l'automatisation en boucle fermée devient plus sophistiquée, permettant l'autoréparation, l'auto-optimisation et la résolution proactive des problèmes.

Les principales étapes d'une automatisation en boucle fermée sont la surveillance, l'analyse, la décision et l'exécution.

Phase de surveillance : collecte et intégration des données

La phase de surveillance consiste à collecter et à prétraiter les données provenant des périphériques réseau, un processus appelé « ingestion des données ». Il s'agit de transférer des données provenant d'une ou de plusieurs sources vers un référentiel central à des fins de stockage et d'analyse. Les données collectées peuvent prendre différentes formes : événements, journaux, télémétrie et captures de trafic.

Phase d'analyse : extraction d'informations

Au cours de la phase d'analyse, les informations sont dérivées des données en temps réel recueillies lors de l'étape de surveillance, des enregistrements historiques, de la

configuration du réseau et des informations de la base de connaissances décrivant le réseau. Les aperçus fournissent des réponses à des questions clés, telles que :

- « Que s'est-il passé ? » : détection des anomalies ou des comportements inhabituels du réseau
- « Pourquoi cela s'est-il produit ? » : application d'une analyse des causes profondes pour identifier le problème sous-jacent

Cette génération d'informations est un processus continu, affiné en permanence grâce aux nouvelles données provenant de la phase de surveillance.

Phase de décision : détermination des actions

La phase de décision traduit les informations en flux de travail qui guident la réponse du système. Cette étape dicte la marche à suivre appropriée en fonction des problèmes détectés, qui peuvent être :

- **Réactif**: traiter les problèmes dès qu'ils surviennent
- **Proactif** : prévenir les problèmes potentiels en se basant sur la détection de modèles de données normalement observés avant que ces problèmes ne surviennent
- **Prédictif**: anticiper les problèmes réseau futurs en fonction des tendances des données

En exploitant l'IA/ML, les règles et les politiques, la phase de décision transforme les informations recueillies en une liste d'actions, orientant le réseau vers un état optimal.

Phase d'exécution : mise en œuvre des actions

La phase d'exécution met en œuvre les flux de travail déterminés lors de la phase de décision, en appliquant des mesures correctives ou adaptatives au réseau. Ces flux de travail consistent en une ou plusieurs opérations qui doivent être soigneusement orchestrées pour garantir une mise en œuvre sans faille. Les approches modernes basées sur des modèles comme YANG et les protocoles associés comme NETCONF et RESTCONF en sont une partie importante.

Une fois les flux de travail exécutés, la logique d'automatisation en boucle fermée lance un nouveau cycle de Surveillance, Analyse, Décision et Exécution afin de prendre en compte les conséquences des actions du cycle précédent ainsi que les nouvelles conditions du réseau externe.

Livre blanc

Au-delà de l'automatisation : construire des réseaux plus intelligents et autonomes



Conclusion

La transition vers des réseaux autonomes est une étape cruciale pour les entreprises qui cherchent à améliorer l'efficacité opérationnelle, l'agilité et la satisfaction des utilisateurs. L'automatisation traditionnelle des réseaux apporte déjà des avantages significatifs, tels que **la réduction des charges de travail manuelles, la minimisation des erreurs humaines et l'accélération des opérations de routine**. Sur cette base, l'automatisation en boucle fermée permet une surveillance en temps réel et une réponse automatisée aux conditions du réseau, garantissant une résolution plus rapide des problèmes et une fiabilité accrue. Elle permet également une optimisation continue en apprenant du comportement du réseau et en s'adaptant sans intervention manuelle. En conséquence, les réseaux autonomes permettent aux entreprises de disposer de capacités d'autogestion, d'autoréparation et d'auto-optimisation. **Cela permet de réduire les coûts d'exploitation tout en améliorant l'évolutivité et la résilience**. Il sera essentiel pour les entreprises d'adopter cette évolution afin de rester agiles et compétitives dans un environnement de réseau de plus en plus complexe.