Principales pratiques Cisco : opérations de gestion de Cisco IOS

Table des matières

Résumé
Introduction
Aperçu
Objectifs
Public
Conditions préalables
Création d'une stratégie d'opérations de gestion Cisco IOS
Identification des livrables
Identification des mesures clés des périphériques
Définir des rôles et des responsabilités
Identification des domaines d'expertise requis
Identification des principaux contributeurs
Identification des responsabilités
Budgétisation des ressources
Suivre les meilleures pratiques du processus d'opérations de gestion de Cisco IOS
Contrôle de version logicielle
Gestion des défaillances
Gestion des problèmes
Normalisation de la configuration
Gestion de la disponibilité
Liste de contrôle des opérations de gestion Cisco IOS
Informations connexes
Services et assistance Cisco

Résumé

Les Méthodes Recommandées de Cisco sont un ensemble de documents codifiés qui fournissent des conseils pertinents et fiables sur les opérations de mise en réseau des produits et solutions Cisco. Les meilleures pratiques sont développées et prises en charge par les ingénieurs primés du centre d'assistance technique Cisco et des services avancés, que vous pouvez utiliser pour créer votre propre ensemble de meilleures pratiques à imiter. Les clients Cisco ont appliqué ces pratiques de pointe dans leur environnement réseau pour améliorer les performances et la disponibilité du réseau.

Il est vivement recommandé de compléter ces pratiques exemplaires par des services de Cisco et de ses partenaires. Pour plus d'informations sur l'optimisation des performances et de la disponibilité de votre réseau, contactez votre représentant commercial des services sur le site

Web des services avancés Cisco et découvrez l'assistance à l'optimisation du réseau : assistance technique ciblée, assistance à l'amélioration de la disponibilité du réseau (NAIS), évaluation du processus de gestion des logiciels (SMPA) et mise en oeuvre NAIS-SMPA.

Introduction

Aperçu

Les processus opérationnels liés à la gestion des logiciels peuvent contribuer à réduire la complexité du réseau, à réduire les problèmes d'assistance réactive et à accélérer la résolution des problèmes. Ce document fournit une stratégie, des recommandations d'outils et des meilleures pratiques pour la gestion globale du logiciel Cisco IOS® (Cisco IOS).

Les sections Création d'une stratégie d'opérations de gestion de Cisco IOS et Respect d'une meilleure pratique Processus d'opérations de gestion de Cisco IOS dans ce document discutent de la méthodologie recommandée pour la mise en route et répertorie les meilleurs outils à utiliser pour la phase d'opérations. La phase d'exploitation inclut les processus de meilleures pratiques pour les éléments suivants :

Process	Description
Contrôle de version logicielle	Le suivi, la validation et l'amélioration de la cohérence des logiciels au sein des « pistes » logicielles identifiées.
Gestion des défaillances	Surveillance proactive et action sur les messages SNMP et Syslog de priorité supérieure générés par Cisco IOS.
Gestion des problèmes	Collecte rapide et efficace d'informations critiques sur les problèmes logiciels afin d'éviter de futurs incidents.
Normalisation de la configuration	« Standardisation » des configurations pour réduire le risque que du code non testé soit utilisé en production et pour standardiser le comportement des protocoles et des fonctionnalités du réseau.
Gestion de disponibilité	Amélioration de la disponibilité en fonction des indicateurs, des objectifs d'amélioration et des projets d'amélioration

Ce document suppose que vous avez mis en oeuvre les meilleures pratiques suivantes pour la planification, la conception et la mise en oeuvre de Cisco IOS :

- Identification des zones logicielles gérables (pistes logicielles) dans votre environnement en fonction des exigences de la plate-forme, du module, des fonctionnalités, du protocole et de la topologie.
- Versions Cisco IOS sélectionnées, certifiées et communiquées par piste logicielle.
- Implémentation cohérente des versions standard de Cisco IOS dans chacune des pistes logicielles.

Objectifs

Cette section vous aide à gérer et à maintenir les versions normalisées de Cisco IOS dans des pistes définies. Vous apprendrez à :

- Développer un processus de contrôle des versions logicielles pour assurer la cohérence des versions logicielles dans les pistes logicielles identifiées.
- Surveiller, notifier et résoudre les processus en fonction des messages et alertes de gestion des pannes des périphériques (SNMP/Syslog) pour aider à résoudre de manière proactive les problèmes logiciels et les pannes potentiels.
- Collecte efficace d'informations sur les problèmes critiques pour les logiciels afin de réduire le temps de résolution des problèmes logiciels.
- Standardiser les configurations des périphériques pour garantir la cohérence des protocoles, des fonctionnalités, de l'accès et de la sécurité dans l'environnement.

Public

Ce document est destiné aux personnes et aux responsables ayant une orientation technique et qui sont responsables du fonctionnement quotidien du réseau. Le document décrit comment établir des processus opérationnels pour vous aider à réduire la complexité du réseau, à diminuer les problèmes de support réactif et à améliorer le temps de résolution des problèmes en renforçant la cohérence du réseau et en améliorant les fonctionnalités de gestion proactive des pannes.

Conditions préalables

Les personnes impliquées dans les opérations de gestion de Cisco IOS doivent avoir une connaissance approfondie de la conception et de l'administration de l'infrastructure réseau, en particulier des équipements Cisco, et doivent avoir accès aux détails de la topologie du réseau cible, de la configuration des périphériques, du profil d'activité, de l'utilisation des applications et de la politique d'utilisation des ressources. L'accès aux outils d'information disponibles sur Cisco Connection Online (CCO) et l'expérience de ces outils sont également requis. Si vous ne vous êtes pas encore inscrit auprès de CCO, nous vous suggérons de le faire pour accéder aux outils décrits dans ce document.

Création d'une stratégie d'opérations de gestion Cisco IOS

De nombreux outils et stratégies de qualité permettent de gérer les environnements Cisco IOS. Ce chapitre se concentre sur trois stratégies clés pour la gestion des opérations Cisco IOS dans des environnements à haute disponibilité et comprend une matrice d'outils opérationnels clés qui sont particulièrement utiles pour la gestion des problèmes Cisco IOS et Cisco IOS.

La première stratégie clé consiste à maintenir l'environnement aussi simple que possible, en évitant autant que possible les variations de configuration et de versions de Cisco IOS. La certification Cisco IOS a déjà été abordée, mais la cohérence de la configuration est un autre domaine clé. Le groupe architecture/ingénierie doit être responsable de la création des normes de configuration. Le groupe chargé de la mise en oeuvre et des opérations est alors chargé de configurer les normes et de les maintenir par le biais du contrôle des versions de Cisco IOS et des normes/contrôles de configuration de Cisco IOS.

La deuxième stratégie clé est la capacité à identifier et à résoudre rapidement les défaillances du réseau. Le groupe des opérations doit généralement identifier les problèmes réseau avant que les utilisateurs ne les signalent, et les problèmes doivent être résolus le plus rapidement possible sans affecter ni modifier l'environnement. Les deux meilleures pratiques clés dans ce domaine sont la gestion des problèmes et la gestion des pannes (ces deux méthodes sont traitées plus loin dans ce document).

Remarque : l'outil Cisco IOS stack decoder peut être utilisé pour diagnostiquer rapidement les pannes du logiciel Cisco IOS.

La troisième stratégie clé consiste à « s'améliorer constamment ». Le principal processus consiste à améliorer un programme d'amélioration de la disponibilité fondé sur la qualité. En effectuant une analyse des causes premières de tous les problèmes, y compris les problèmes liés à Cisco IOS, une entreprise peut améliorer la couverture des tests, les délais de résolution des problèmes et les processus qui éliminent ou réduisent l'impact des pannes. L'entreprise peut également examiner les problèmes courants et mettre en place des processus pour les résoudre plus rapidement.

Identification des livrables

Les éléments livrables du processus de fonctionnement de la gestion du logiciel Cisco IOS sont les suivants :

- Processus et outils de contrôle de version logicielle
- Surveillance et processus de gestion des pannes
- Processus de gestion des problèmes
- Normes de configuration des périphériques et processus d'audit
- Méthodologie de disponibilité du réseau, rapports et processus d'examen

Identification des mesures clés des périphériques

Les indicateurs doivent être définis dans le cadre du plan opérationnel et utilisés pour déterminer si les outils et les processus produisent les résultats escomptés. Voici quelques exemples de mesures utiles de gestion de la plate-forme logicielle Cisco IOS :

- Disponibilité du réseau (en raison de problèmes logiciels)
- % de conformité de la version de Cisco IOS à la norme (par piste)
- % de cohérence de la configuration des périphériques (selon les normes)
- Mesures de gestion des problèmes (MTTR, nombre de tickets, codes de fermeture)

Définir des rôles et des responsabilités

Identifiez, qualifiez et assemblez un groupe interfonctionnel de responsables et/ou de responsables issus des groupes d'architecture réseau, d'ingénierie réseau et d'implémentation/d'exploitation pour garantir la réussite des phases de planification, de conception, d'implémentation et d'exploitation de vos projets de mise à niveau IOS.

Identification des domaines d'expertise requis

Rassemblez un groupe interfonctionnel de responsables et/ou de responsables issus des groupes de gestion, d'ingénierie, de mise en oeuvre et d'exploitation du réseau pour vous aider dans la phase opérationnelle de votre projet de gestion Cisco IOS.

Identification des principaux contributeurs

- Gestionnaire(s) réseau :

  Nom du ou des responsables, service, coordonnées

  Nom, service et coordonnées de la sauvegarde principale

  Nom de la sauvegarde secondaire, service, coordonnées si nécessaire

- Architecte(s) réseau :

  Nom de l'architecte, service, coordonnées

  Nom, service et coordonnées de la sauvegarde principale

  Nom de la sauvegarde secondaire, service, coordonnées si nécessaire

- Ingénieur(s) réseau :

  Nom de l'ingénieur, service, coordonnées

Nom, service et coordonnées de la sauvegarde principale

Nom de la sauvegarde secondaire, service, coordonnées si nécessaire

- Ingénieur(s) des opérations réseau (NOC) :

  Nom de l'ingénieur, service, coordonnées

  Nom, service et coordonnées de la sauvegarde principale

  Nom de la sauvegarde secondaire, service, coordonnées si nécessaire

Identification des responsabilités

- Le ou les gestionnaires de réseau sont responsables de :
  - Tenir à jour le plan du projet
  - Affectation/réaffectation de ressources
  - Gestion du contrôle des modifications
  - Gestion de la progression
  - Gestion des rapports budgétaires
- Les architectes réseau sont responsables de :
  - Analyse des normes réseau et des avertissements
  - Maintenance de la matrice de mise à niveau logicielle
  - Tenir à jour la matrice de gestion des candidats
  - Maintenance de la matrice des besoins en mémoire
- Les ingénieurs réseau (NOC) sont responsables des tâches suivantes :
  - Mise en oeuvre et garantie de la conformité aux normes réseau
  - Identification des problèmes logiciels et de leurs causes premières
  - Recommander une action corrective
  - Surveillance du réseau

Budgétisation des ressources

Les besoins en ressources doivent être déterminés à l'étape des opérations afin d'appuyer la stratégie de gestion des logiciels de l'organisation. Cela comprend le temps nécessaire au personnel et les dépenses d'investissement nécessaires pour soutenir la stratégie logicielle.

Dans de nombreux cas, un retour sur investissement (ROI) ou un plan budgétaire pour les pratiques de gestion des logiciels peut être généré en fonction du coût des temps d'arrêt et des exigences de disponibilité. Si l'entreprise peut déterminer les temps d'arrêt dus à des problèmes logiciels, la majorité de ces coûts peut être compensée par les meilleures pratiques de gestion des logiciels identifiées. Si le coût ne peut pas être entièrement compensé, l'entreprise doit envisager une stratégie de gestion des logiciels plus basique qui contribuera à améliorer la productivité en empêchant les retouches supplémentaires en raison de problèmes logiciels.

Suivre les meilleures pratiques du processus d'opérations de gestion de Cisco IOS

Les Méthodes Recommandées pour suivre un processus Cisco IOS Management Operations sont les suivantes :

Meilleure pratique	Détail
Contrôle de version logicielle	Mise en oeuvre de versions logicielles normalisées et surveillance du réseau pour valider ou éventuellement modifier le logiciel en raison d'une non-conformité de la version.
Gestion des défaillances	La collecte, la surveillance et l'analyse des messages SNMP et Syslog sont des processus de gestion des pannes recommandés pour résoudre davantage de problèmes réseau spécifiques à Cisco IOS difficiles ou impossibles à identifier autrement.
Gestion des problèmes	Processus de gestion des problèmes détaillés qui définissent l'identification des problèmes, la collecte d'informations et un chemin de solution bien analysé. Ces données sont utilisées pour déterminer la cause première.
Normalisation de la configuration	Les normes de configuration représentent la pratique consistant à créer et à gérer des paramètres de configuration standard « globaux » sur des périphériques et services similaires, ce qui permet d'assurer la cohérence de la configuration globale à l'échelle de l'entreprise.

Gestion de la disponibilité	Amélioration de la qualité en utilisant la disponibilité du réseau comme mesure d'amélioration de la qualité.

Contrôle de version logicielle

Le contrôle des versions logicielles consiste à mettre en oeuvre uniquement des versions logicielles normalisées et à surveiller le réseau pour valider ou éventuellement modifier les logiciels en raison d'une non-conformité aux versions. En général, le contrôle de la version du logiciel est effectué à l'aide d'un processus de certification et d'un contrôle des normes. De nombreuses entreprises publient des normes de version sur un serveur Web central. En outre, le personnel chargé de la mise en oeuvre est formé pour examiner la version en cours d'exécution et pour la mettre à jour si elle n'est pas conforme aux normes. Certaines organisations ont un processus de contrôle de la qualité où la validation secondaire est effectuée par le biais d'audits afin de s'assurer que la norme est respectée pendant la mise en oeuvre.

Pendant le fonctionnement du réseau, il n'est pas rare non plus de voir des versions logicielles non standard sur le réseau, en particulier si le réseau est grand et dispose d'un personnel d'exploitation important. Cela peut être dû à l'un des facteurs suivants :

- Personnel nouveau non formé
- Commandes de démarrage mal configurées
- Implémentations non contrôlées

Il est recommandé de valider périodiquement les normes de version logicielle à l’aide d’outils tels que CiscoWorks2000 Resource Manager Essentials (RME) qui peuvent trier tous les périphériques par version de Cisco IOS. Lorsqu'une version non standard est identifiée, elle doit être immédiatement signalée et un rapport d'incident ou un rapport de modification doit être initié pour amener la version à la norme identifiée.

Outils disponibles

CiscoWorks2000 RME Inventory Manager simplifie considérablement la gestion de la version de Cisco IOS des routeurs et commutateurs Cisco grâce à des outils de création de rapports basés sur le Web qui signalent et trient les périphériques en fonction de la version du logiciel, de la plate-forme du périphérique et du nom du périphérique.

Gestion des défaillances

La gestion des pannes est le processus de collecte, de surveillance et d'analyse des messages SNMP et Syslog pour résoudre davantage de problèmes réseau spécifiques à Cisco IOS qui sont difficiles ou impossibles à identifier d'une autre manière.

Collecte des déroutements SNMP

La collecte et la notification des déroutements SNMP constituent un processus de base de la gestion des pannes, utilisé pour identifier les événements logiciels ou matériels et/ou les pannes

sans surcharge ou retard d'interrogation SNMP dus aux intervalles d'interrogation. Les messages d'interruption sont générés directement à partir du périphérique réseau vers un système de gestion de réseau qui fournit des services de notification. La collecte et la notification de ces déroutements sont essentielles à la résolution rapide de nombreux événements réseau, y compris les événements n'ayant pas d'impact sur l'utilisateur, tels que la perte de périphériques principaux ou de liaisons dans un environnement redondant.

Afin de collecter et de surveiller ces déroutements, les déroutements doivent être correctement configurés sur le périphérique ainsi que sur les systèmes de gestion du réseau. Les systèmes de gestion du réseau doivent alerter le groupe des opérations réseau lorsqu'un déroutement a été reçu. La notification peut alors avoir lieu sous la forme d'écrans de radiomessagerie, d'e-mail ou d'événements dans un environnement NOC.

Quelle que soit la manière dont les données sont présentées, ces instances de panne, ou exceptions, doivent être analysées et examinées régulièrement (de préférence quotidiennement) par le personnel d'exploitation et/ou de support réseau. Les causes de toutes les exceptions trouvées doivent être étudiées. Certaines exceptions enregistrées peuvent ne pas être suffisamment critiques pour déclencher immédiatement une alarme dans le Centre d'exploitation du réseau. L'examen, l'investigation et la résolution proactifs des exceptions mineures peuvent aider les groupes d'assistance réseau à réduire ou à prévenir les pannes de réseau.

Collecte des messages Syslog

Les messages Syslog sont envoyés par le périphérique à un serveur de collecte. Il peut s'agir d'erreurs matérielles ou logicielles, ou d'informations (par exemple, lorsqu'un utilisateur a été dans le terminal de configuration d'un périphérique).

La surveillance Syslog nécessite la prise en charge d'outils ou de scripts NMS (Network Management System) pour faciliter l'analyse et la création de rapports sur les données Syslog. Cela inclut la capacité de trier les messages Syslog par date ou heure, période, périphérique, type de message Syslog ou fréquence de message. Dans les réseaux de plus grande taille, des outils ou des scripts peuvent être mis en oeuvre pour analyser les données Syslog et envoyer des alertes ou des notifications aux systèmes de gestion des événements ou au personnel d'exploitation et d'ingénierie. Si des alertes pour un grand nombre de données Syslog ne sont pas utilisées, l'entreprise doit examiner les données Syslog de priorité supérieure au moins quotidiennement et créer des rapports d'incident pour les problèmes potentiels. Afin de détecter de manière proactive les problèmes réseau qui ne peuvent pas être détectés par une surveillance normale, un examen et une analyse périodiques des données Syslog historiques doivent être effectués pour détecter les situations qui peuvent ne pas indiquer un problème immédiat, mais peuvent fournir une indication d'un problème avant qu'il n'affecte le service.

Outils disponibles

Voici quelques-uns des outils de réception d'interruptions SNMP les plus répandus :

- HP OpenView Network Node Manager de Hewlett Packard à l'adresse openview.hp.com
- Spectrum Integrity d'Aprisma à l'adresse www.aprisma.com

- NetView d'IBM Tivoli à l'adresse www.tivoli.com

L’outil Syslog le plus répandu pour la gestion de Cisco IOS est CiscoWorks2000 RME Syslog manager. Parmi les autres outils disponibles, citons SL4NT, un programme shareware de www.netal.com qui laisse cisco.com et Private I de OpenSystems à www.opensystems.com

Gestion des problèmes

La gestion des problèmes, un aspect de la gestion des pannes, est la discipline qui consiste à gérer les problèmes à partir du moment où ils se produisent, en passant par l'identification, le dépannage, la résolution et la fermeture.

De nombreux clients subissent des temps d'arrêt supplémentaires en raison d'un manque de processus dans la gestion des problèmes. Des temps d’arrêt supplémentaires peuvent survenir lorsque les administrateurs réseau tentent de résoudre rapidement le problème en combinant des commandes ou des modifications de configuration ayant un impact sur les services, plutôt que de consacrer du temps à l’identification des problèmes, à la collecte d’informations et à une solution bien analysée. Le comportement observé dans cette zone inclut le rechargement des périphériques ou la suppression des tables de routage IP avant d’étudier un problème et sa cause première. Dans certains cas, cela se produit en raison des objectifs de résolution des problèmes du premier niveau d'assistance. L'objectif de tous les problèmes logiciels doit être de collecter rapidement les informations nécessaires à l'analyse des causes premières avant de restaurer la connectivité ou le service.

Un processus de gestion des problèmes est recommandé et doit inclure un certain degré de description des problèmes par défaut et des collections de commandes « show » appropriées avant de transmettre le problème à un second niveau de support. L'assistance de premier niveau ne doit jamais inclure la suppression de routes ou le rechargement de périphériques. Idéalement, le service d'assistance de premier niveau devrait rapidement collecter des informations, puis transmettre le problème au service d'assistance de second niveau. En passant un peu plus de temps à identifier et à décrire le problème dans le support de niveau 1, une découverte de la cause première est beaucoup plus probable, permettant ainsi une solution de contournement, l'identification de laboratoire et le signalement de bogues. L'assistance de deuxième niveau doit bien connaître les types d'informations dont Cisco peut avoir besoin pour diagnostiquer un problème ou déposer un rapport de bogue, notamment :

- Vidages de mémoire
- Informations de routage
- Sortie de la commande Device show

Normalisation de la configuration

Les normes de configuration globale des périphériques représentent la pratique consistant à maintenir des paramètres de configuration « globale » standard sur des périphériques et services similaires, ce qui permet d'assurer la cohérence de la configuration globale à l'échelle de l'entreprise. Les commandes de configuration globale s’appliquent à l’ensemble du périphérique et

non à des ports, protocoles ou interfaces individuels. Elles ont généralement une incidence sur l’accès au périphérique, son comportement général et sa sécurité. Dans Cisco IOS, cela inclut les commandes suivantes :

- Service
- IP
- VTY
- Port de console
- Journalisation
- AAA/TACACS+
- SNMP
- Bannière

Une convention d'attribution de noms de périphériques appropriée, permettant aux administrateurs d'identifier le périphérique, son type et son emplacement en fonction du nom DNS du périphérique, est également importante dans les normes de configuration globale des périphériques. La cohérence de la configuration globale est importante pour la prise en charge et la fiabilité globales d'un environnement réseau, car elle permet de réduire la complexité du réseau et d'améliorer sa prise en charge. La difficulté de prise en charge est souvent rencontrée sans normalisation de la configuration en raison d'un comportement incorrect ou incohérent des périphériques, d'un accès SNMP et de la sécurité générale des périphériques.

La mise à jour des normes de configuration globale des périphériques est normalement assurée par un groupe interne d'ingénierie ou d'exploitation qui crée et gère les paramètres de configuration globale pour des périphériques réseau similaires. Il est également recommandé de fournir une copie du fichier de configuration globale dans les répertoires TFTP afin qu’ils puissent être téléchargés pour la première fois sur tous les périphériques nouvellement provisionnés. Un fichier accessible sur le Web qui fournit au fichier de configuration standard une explication de chaque paramètre de configuration est également utile. Certaines entreprises configurent régulièrement tous les périphériques similaires afin de garantir la cohérence de la configuration globale, ou examinent régulièrement les périphériques pour déterminer les normes de configuration globale appropriées.

Les normes de configuration d’interface ou de protocole représentent la pratique consistant à maintenir des normes pour la configuration d’interface et de protocole, ce qui améliore la disponibilité du réseau en réduisant la complexité du réseau, en fournissant le comportement attendu des périphériques et des protocoles et en améliorant la prise en charge du réseau. L'incohérence de la configuration des interfaces ou des protocoles peut entraîner un comportement inattendu des périphériques, des problèmes de routage du trafic, une augmentation des problèmes de connectivité et une augmentation du temps de prise en charge réactive.

Les normes de configuration d’interface peuvent inclure :

- CDP (Cisco Discovery Protocol)
- Descripteurs d'interface
- Configuration de cache
- Autres normes spécifiques au protocole

Les normes de configuration spécifiques aux protocoles peuvent inclure :

- Configuration du routage IP
- Configuration DLSW
- Configuration de la liste de contrôle d'accès
- configuration ATM
- Configuration Frame Relay
- Configuration Spanning Tree
- Attribution et configuration de VLAN
- Protocole VTP (Virtual Trunking Protocol)
- HSRP (Hot Standby Routing Protocol)
- D'autres selon ce qui est configuré dans le réseau

La taille de sous-réseau, l’espace d’adressage IP utilisé, le protocole de routage utilisé et la configuration du protocole de routage sont des exemples de normes IP.

La mise à jour des normes de configuration des protocoles et des interfaces incombe normalement aux groupes d’ingénierie et de mise en oeuvre du réseau. Le groupe d'ingénierie devrait être responsable de l'identification, de la mise à l'essai, de la validation et de la documentation des normes. Le groupe d'implémentation est alors chargé d'utiliser les documents d'ingénierie ou les modèles de configuration pour provisionner de nouveaux services. Le groupe de l'ingénierie devrait créer de la documentation sur tous les aspects des normes requises pour assurer l'uniformité. Des modèles de configuration doivent également être créés pour faciliter l'application des normes de configuration. Les groupes des opérations doivent également être formés sur les normes et être capables d'identifier les problèmes de configuration non standard. La cohérence de la configuration est très utile lors des phases de test, de validation et de certification. Sans modèles de configuration standardisés, il est presque impossible de tester, valider ou certifier correctement une version de Cisco IOS pour un réseau de taille moyenne.

Gestion de la disponibilité

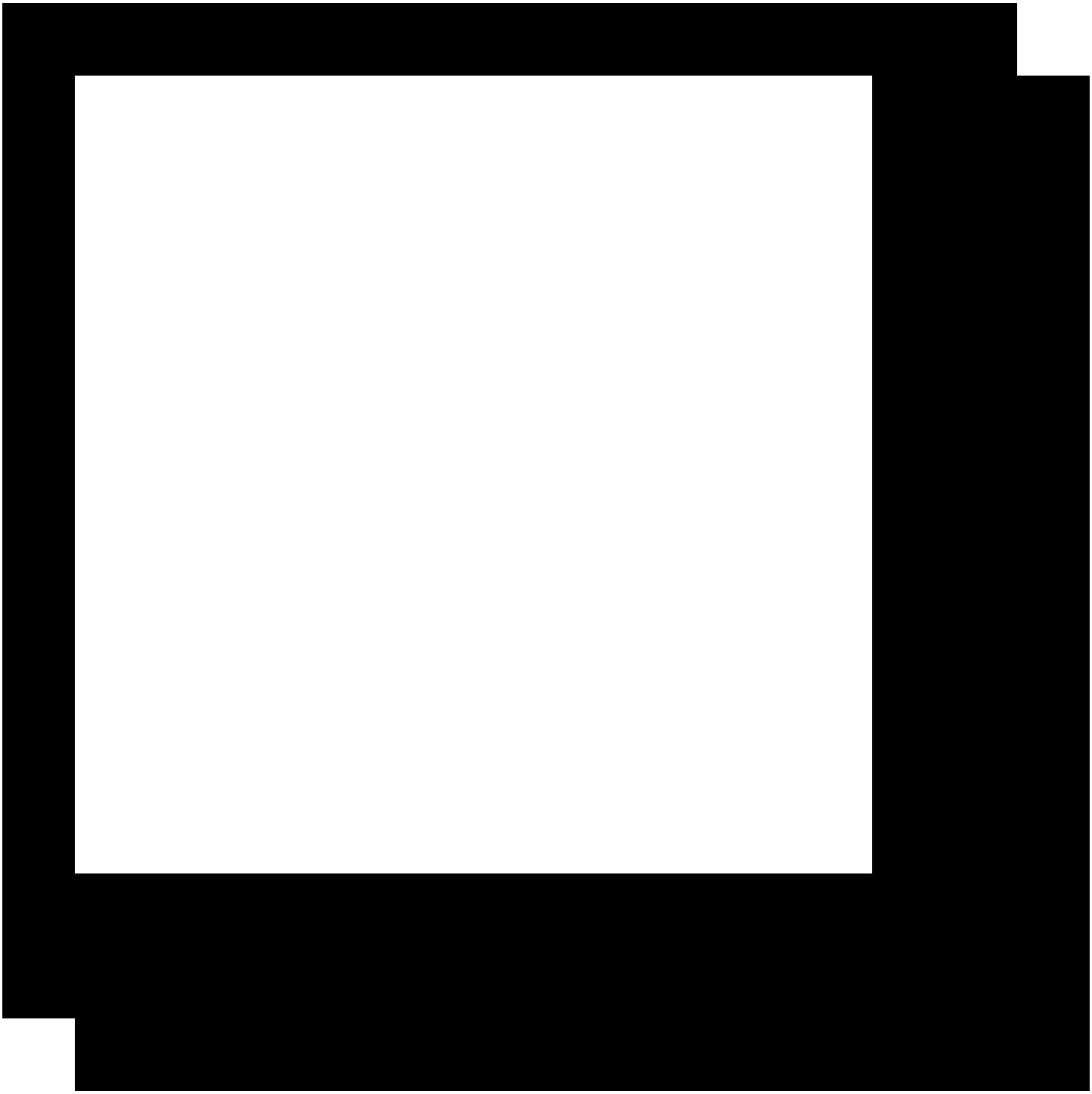
La gestion de la disponibilité est le processus d'amélioration de la qualité utilisant la disponibilité du réseau comme mesure d'amélioration de la qualité. De nombreuses entreprises mesurent

actuellement la disponibilité et le type de panne. Les types de panne peuvent inclure les éléments suivants :

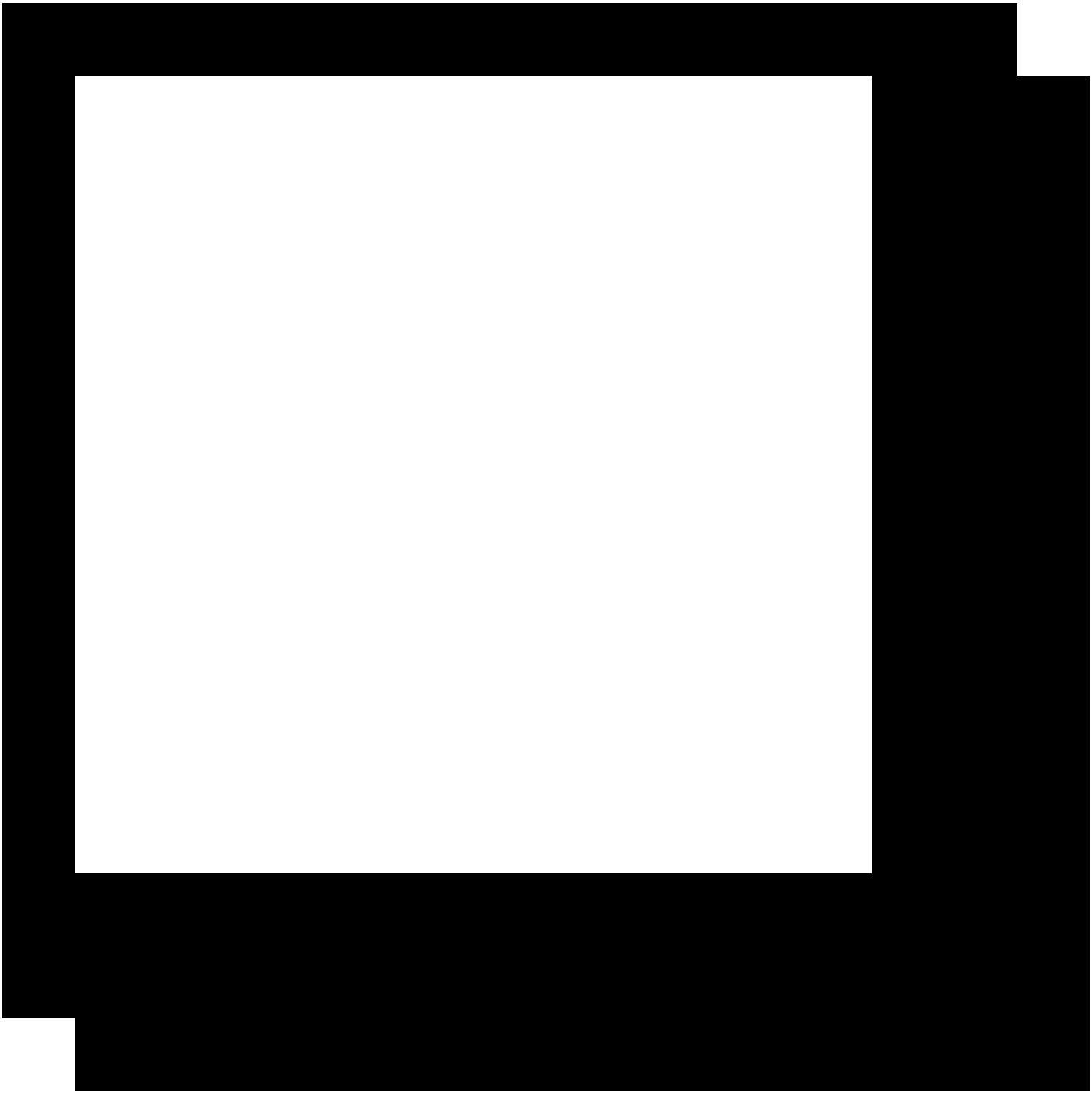
- Matériel
- le logiciel Cisco IOS
- Liaison/porteuse
- Alimentation/environnement
- Conception
- Erreur utilisateur/processus

En identifiant les pannes et en effectuant une analyse de la cause première immédiatement après la reprise, l'entreprise peut identifier des méthodes pour améliorer la disponibilité. Presque tous les réseaux qui ont atteint une haute disponibilité ont mis en place un processus d'amélioration de la qualité.

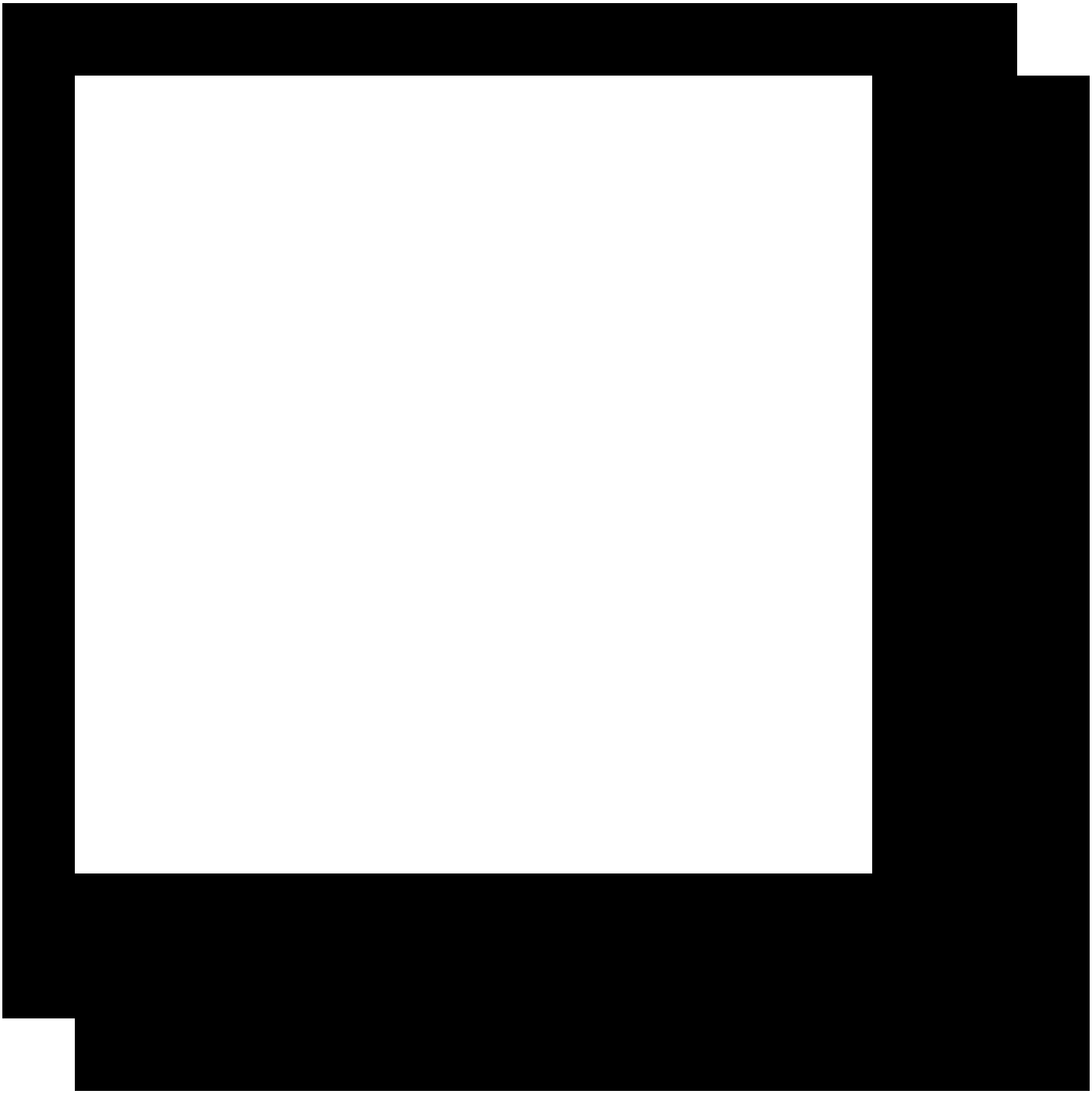
Liste de contrôle des opérations de gestion Cisco IOS



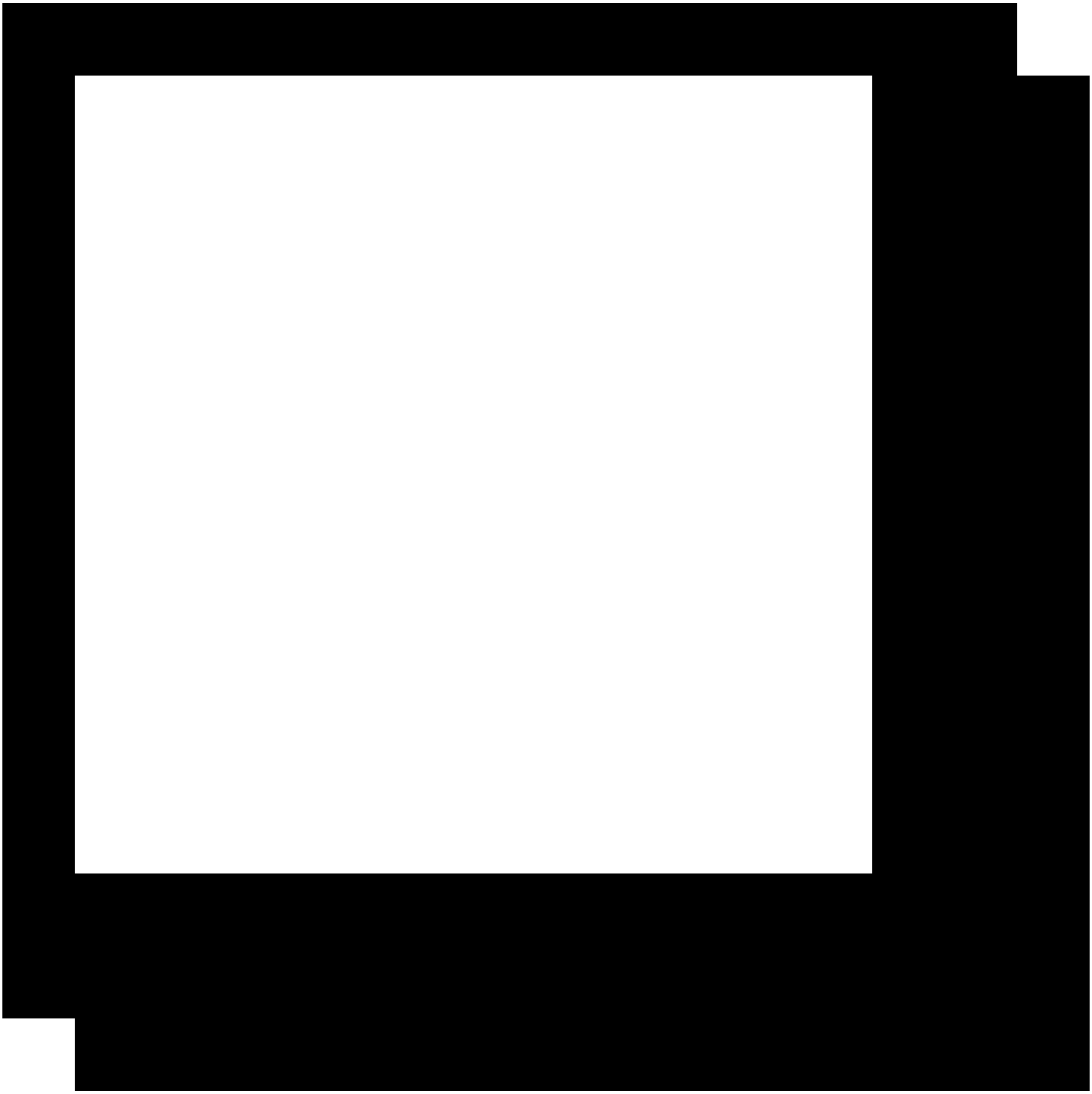
Étape 1 : Définir les exigences et les objectifs commerciaux (clients enregistrés uniquement)



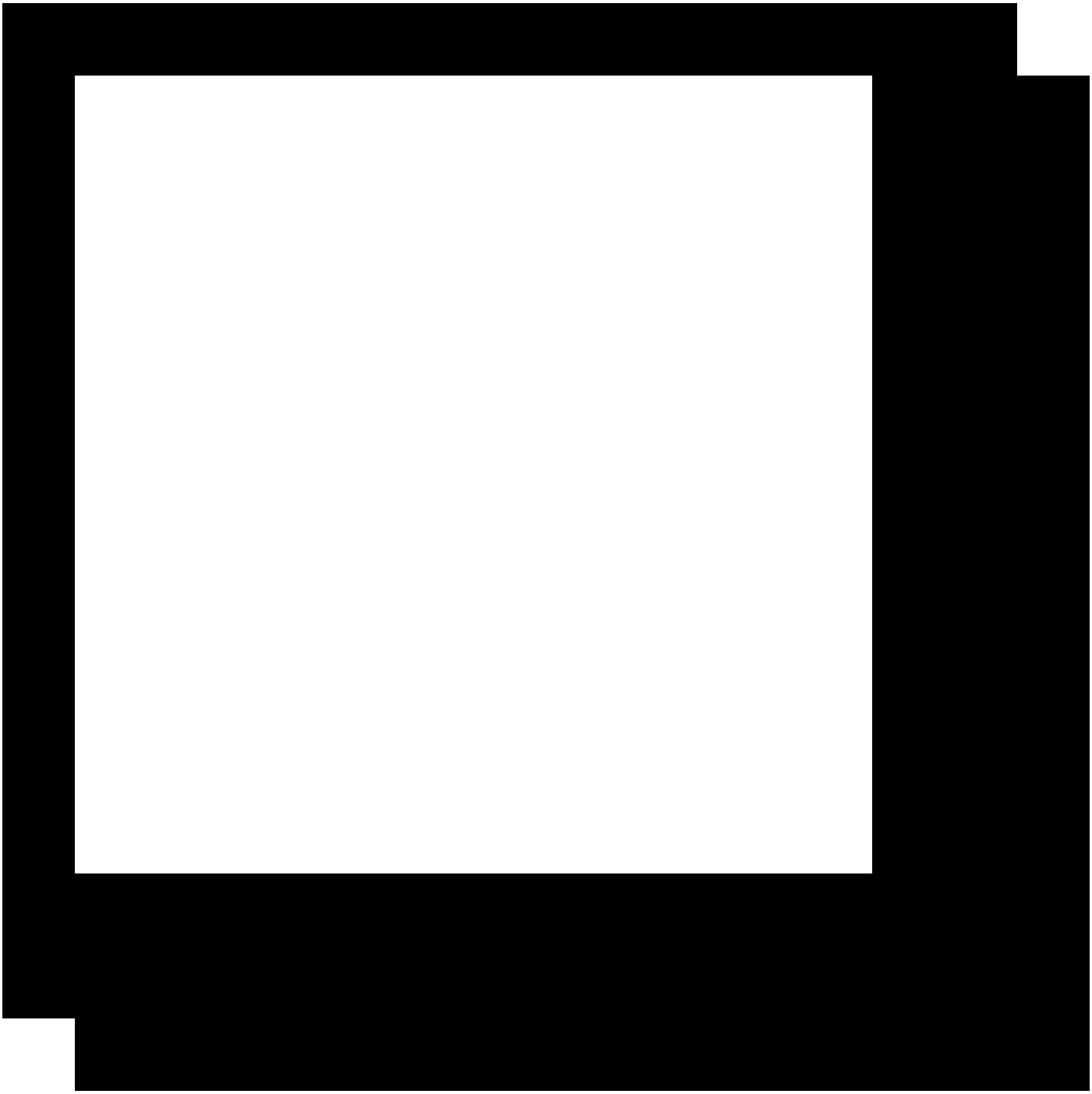
Étape 2 : Évaluation de l'état actuel des pratiques de gestion du logiciel Cisco IOS (clients enregistrés uniquement)



Étape 3 : Définir les rôles et les responsabilités (clients enregistrés uniquement)



Étape 4 : Développement d'un plan de projet de gestion logicielle (clients enregistrés uniquement)



Étape 5 : Développement d'une matrice des exigences logicielles (clients enregistrés uniquement)

Informations connexes

Une annexe a été créée pour aider le client à obtenir d'autres informations utiles relatives à Cisco IOS, telles que : les principes fondamentaux de Cisco IOS, les processus logiciels internes de Cisco IOS, l'analyse de la fiabilité du logiciel, le programme de qualité interne de Cisco, les méthodologies de test internes de Cisco et une analyse de terrain qui montre les pratiques actuelles du secteur et l'expérience globale du client avec le logiciel Cisco IOS

- Cisco IOS Management : des informations supplémentaires sur la gestion et les meilleures

pratiques de Cisco IOS sont disponibles dans le livre blanc « Cisco IOS Management for High Availability Networking » (Gestion Cisco IOS pour la mise en réseau haute disponibilité), disponible à l'adresse suivante : http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a00800a998b.shtml

- Pour obtenir des informations spécifiques sur l'exécution des sondes réseau, les commandes CLI à utiliser, l'analyse et l'interprétation des données de trafic réseau et l'établissement de stratégies d'utilisation des applications, visitez le site http://www.cisco.com. Ce site propose une gamme complète de solutions d'assistance, de formation, de référence technique et de conseil.
- Les conventions d'attribution de noms de Cisco IOS sont définies ici : http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_tech_note09186a0080101cda.s
- Des informations sur la disponibilité de la version de Cisco IOS sont disponibles ici : http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html
- Les versions de Cisco IOS sont finalement supprimées de CCO et ne peuvent plus être commandées. Veillez à définir les attentes du client en conséquence.
- Les bulletins de produits Cisco IOS sont utilisés pour annoncer les versions de Cisco IOS aux clients. Ils contiennent de brèves informations sur le contenu de la version. Cliquez ici pour connaître la disponibilité des nouvelles versions de Cisco IOS http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html
- L'équipe de réponse aux incidents de sécurité des produits gère la sécurité des produits Cisco. Toute question relative à la sécurité de Cisco IOS doit être signalée à cette équipe. Cisco publie publiquement ses vulnérabilités de sécurité. http://tools.cisco.com/security/center/publicationListing
- Défauts de Cisco IOS : les défauts graves de Cisco IOS doivent être recommandés pour le report. Tout employé de Cisco peut faire cette recommandation.
- Les problèmes de terrain sur Cisco IOS sont communiqués aux clients via les conseils Cisco IOS. http://www.cisco.com/en/US/products/products_security_advisory09186a0080b20ee1.shtml
- Fonctionnalités de Cisco IOS : l'outil Feature Navigator permet aux clients de rechercher des versions prenant en charge des fonctionnalités spécifiques, et vice versa. http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp
- Cisco Software Advisor permet aux clients de trouver une assistance logicielle pour les fonctionnalités ou une assistance logicielle pour le matériel. http://tools.cisco.com/Support/Fusion/FusionHome.do (clients enregistrés uniquement)

Services et assistance Cisco

- Services d'assistance technique

- Services spécifiques aux technologies et solutions réseau Cisco

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.