Meilleures pratiques Cisco : Opérations de gestion Cisco IOS

Contenu

Résumé

Les meilleures pratiques de Cisco sont un ensemble de documents codifiés qui fournissent des conseils pertinents et fiables sur les opérations réseau pour les produits et solutions Cisco. Les meilleures pratiques sont développées et prises en charge par des ingénieurs Cisco TAC et Advanced Services primés que vous pouvez utiliser pour créer votre propre ensemble de meilleures pratiques à imiter. Les clients de Cisco ont appliqué ces meilleures pratiques dans leur environnement réseau pour améliorer les performances et la disponibilité du réseau.

Il est vivement recommandé de compléter ces meilleures pratiques avec les 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 de 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 de support réactif et à améliorer le temps de 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'exploitation de gestion Cisco IOS et Suivi d'une meilleure pratique Processus d'exploitation de gestion Cisco IOS dans ce document présentent la méthodologie recommandée pour démarrer et répertorient les meilleurs outils à utiliser pour la phase d'exploitation. La phase opérationnelle comprend les meilleures pratiques pour les éléments suivants :

Process	Description
Contrôle de version du logiciel	Suivi, validation et amélioration de la cohérence logicielle au sein du logiciel identifié “ suivi ”.
Gestion des pannes	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 liés aux logiciels afin d'éviter les événements futurs.
Normalisation de la configuration	“ standardiser les configurations ” afin de réduire le risque d'utilisation de code non testé en production et de standardiser le comportement des protocoles et des fonctionnalités réseau.
Gestion de la disponibilité	Améliorer 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 :

- Les zones logicielles gérables (pistes logicielles) identifiées dans votre environnement en fonction des besoins de la plate-forme, du module, des fonctionnalités, du protocole et de la topologie.
- Versions de Cisco IOS sélectionnées, certifiées et communiquées par voie logicielle.

- Implémentation constante des versions standard de Cisco IOS dans chacune des pistes logicielles.

Objectifs

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

- Développer un processus de contrôle des versions logicielles pour assurer la cohérence des versions logicielles dans les pistes logicielles identifiées.
- Surveillez, notifiez et résolvez les processus en fonction des messages et des 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 liés aux logiciels.
- Normaliser les configurations des périphériques pour garantir la cohérence des protocoles, des fonctionnalités, de l'accès et de la sécurité de l'environnement.

Public

Ce document s'adresse aux personnes et aux gestionnaires 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 réduire les problèmes de support réactif et à améliorer le temps de résolution des problèmes en améliorant la cohérence du réseau et en améliorant les capacités de gestion proactive des pannes.

Conditions préalables

Les personnes impliquées dans les opérations de gestion de Cisco IOS doivent posséder une solide connaissance de la conception et de l'administration de l'infrastructure réseau, en particulier avec l'équipement Cisco, et 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'utilisation de ces outils sont également requis. Si vous n'êtes pas déjà inscrit auprès de CCO, nous vous suggérons de le faire pour accéder aux outils décrits dans ce document.

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

Il existe de nombreuses stratégies et outils de qualité pour aider à gérer les environnements Cisco IOS. Ce chapitre porte sur trois stratégies clés de gestion des opérations Cisco IOS dans les 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 discutée, mais la cohérence de la configuration est un autre domaine clé. Le groupe architecture/ingénierie doit être chargé de créer des normes de configuration. Le groupe de mise en oeuvre et d'exploitation est alors chargé de configurer les

normes et de les mettre à jour via le contrôle de version de Cisco IOS et les normes/contrôles de configuration de Cisco IOS.

La deuxième stratégie clé consiste à identifier et à résoudre rapidement les pannes de réseau. Le groupe opérationnel doit généralement identifier les problèmes réseau avant que les utilisateurs ne les signalent et les problèmes doivent être résolus le plus rapidement possible sans avoir d'autre impact ou modification sur l'environnement. Deux meilleures pratiques clés dans ce domaine sont la gestion des problèmes et des pannes (les deux sont abordées plus loin dans ce document).

Remarque : L'outil décodeur de pile Cisco IOS peut être utilisé pour diagnostiquer rapidement les pannes du logiciel Cisco IOS.

La troisième stratégie clé consiste à “ constamment améliorer les ”. Le processus principal consiste à améliorer un programme d'amélioration de la disponibilité basé sur la qualité. En effectuant une analyse des causes profondes de tous les problèmes, y compris les problèmes liés à Cisco IOS, une entreprise peut améliorer la couverture des tests, améliorer les temps de résolution des problèmes et améliorer les processus qui élimineront ou réduiront l'impact des pannes. L'organisation peut également examiner les problèmes courants et élaborer des processus pour les résoudre plus rapidement.

Identification des livrables

Les éléments livrables du processus de 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, rapports et processus d'examen de la disponibilité du réseau

Identification des mesures de périphérique clé

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

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

Définition des rôles et des responsabilités

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

Identification des domaines d'expertise requis

Réunissez un groupe interfonctionnel de responsables et/ou de responsables des groupes de gestion du réseau, d'ingénierie réseau, de mise en oeuvre et d'exploitation afin d'aider à la phase opérationnelle de votre projet de gestion Cisco IOS.

Identification des principaux contributeurs

- Responsables réseau :Nom du ou des gestionnaires, service, coordonnéesNom de la sauvegarde principale, service, coordonnéesNom de sauvegarde secondaire, service, coordonnées, le cas échéant
- Architecte(s) réseau :Nom de l'architecte, service, coordonnéesNom de la sauvegarde principale, service, coordonnéesNom de sauvegarde secondaire, service, coordonnées, le cas échéant
- Ingénieur(s) réseau :Nom de l'ingénieur, service, coordonnéesNom de la sauvegarde principale, service, coordonnéesNom de sauvegarde secondaire, service, coordonnées, le cas échéant
- Ingénieur(s) des opérations réseau (NOC) :Nom de l'ingénieur, service, coordonnéesNom de la sauvegarde principale, service, coordonnéesNom de sauvegarde secondaire, service, coordonnées, le cas échéant

Identification des responsabilités

- Les gestionnaires de réseau sont chargés des tâches suivantes :Tenir à jour le plan de projetAffectation/réaffectation de ressourcesGestion du contrôle des modificationsGestion des progrèsGestion des rapports budgétaires
- Les architectes réseau sont responsables des tâches suivantes :Analyse des normes réseau et des mises en garde relatives aux versionsMise à jour de la matrice de mise à niveau logicielleMise à jour de la matrice de gestion des candidatsMise à jour de la matrice des besoins en mémoire
- Le ou les ingénieurs de réseau (NOC) sont responsables des tâches suivantes :Mise en oeuvre et conformité aux normes réseauIdentification des problèmes logiciels et des causes premièresRecommandation de mesures correctivesSurveillance du réseau

Ressources budgétaires

Les besoins en ressources devraient être déterminés à l'étape des opérations pour appuyer la stratégie de gestion des logiciels de l'organisation. Cela comprendra le temps de travail et les dépenses en capital nécessaires pour appuyer la stratégie logicielle.

Dans de nombreux cas, un retour sur investissement (ROI) ou un plan budgétaire pour les pratiques de gestion des logiciels peuvent être générés 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, une grande partie de ce coût peut être compensée par les meilleures pratiques de gestion des logiciels identifiées. Si le coût ne peut pas être entièrement compensé, l'entreprise doit alors envisager une stratégie de gestion logicielle plus basique qui permettra d'améliorer la productivité en évitant les retouches supplémentaires dues à des problèmes logiciels.

Suivre le processus d’exploitation de la gestion de Cisco IOS

selon les meilleures pratiques

Les meilleures pratiques pour suivre un processus de gestion des opérations Cisco IOS sont les suivantes :

Meilleure pratique	Détail
Contrôle de version du logiciel	Mise en oeuvre de versions logicielles normalisées et surveillance du réseau pour valider ou éventuellement modifier les logiciels en raison de la non-conformité des versions.
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 d'autres 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 maintenir des paramètres de configuration ” globale standard “ sur des périphériques et des services similaires, ce qui assure une cohérence de 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 du logiciel

Le contrôle de version logicielle est le processus de mise en oeuvre de versions logicielles normalisées et de surveillance du réseau pour valider ou éventuellement modifier le logiciel en raison d'une non-conformité de version. En règle générale, le contrôle de la version du logiciel s'effectue au moyen 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 quelle version est en cours d'exécution et pour mettre à jour la version si elle n'est pas conforme aux normes. Certaines organisations ont un processus de validation de la qualité qui permet d'effectuer une validation secondaire au moyen de vérifications pour s'assurer que la norme est respectée pendant la mise en oeuvre.

Pendant le fonctionnement du réseau, il n'est pas rare de voir des versions logicielles non standard dans le réseau, en particulier si le réseau est important avec un personnel d'exploitation

important. Cela peut être dû à l'une des raisons suivantes :

- Personnel nouvellement formé
- Commandes de démarrage Mis-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 Cisco IOS. Lorsqu'une version non standard est identifiée, elle doit être immédiatement signalée et un rapport d'incident ou de modification doit être lancé pour amener la version à la norme identifiée.

Outils disponibles

CiscoWorks2000 RME Inventory Manager simplifie considérablement la gestion des versions de Cisco IOS des routeurs et commutateurs Cisco grâce à des outils de création de rapports basés sur le Web qui permettent de signaler et de trier 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 des problèmes réseau spécifiques à Cisco IOS difficiles ou impossibles à identifier autrement.

Collection de déroutements SNMP

La collecte et la notification des déroutements SNMP sont un processus de base dans la gestion des pannes utilisé pour identifier les événements logiciels ou matériels et/ou les pannes sans surcharge d'interrogation SNMP ou délai dû aux intervalles d'interrogation SNMP. Les messages de déroutement 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 interruptions sont essentielles à la résolution rapide de nombreux événements réseau, y compris les événements sans impact sur l'utilisateur, tels que la perte de périphériques ou de liaisons principaux dans un environnement redondant.

Pour collecter et surveiller ces interruptions, elles doivent être correctement configurées sur le périphérique ainsi que sur les systèmes de gestion de réseau. Les systèmes de gestion du réseau doivent avertir le groupe d'opérations du réseau lorsqu'un déroutement a été reçu. La notification peut alors se produire sous forme d'écrans de pagination, de courriels ou d'événements dans un environnement NOC.

Quelle que soit la manière dont les données sont présentées, ces cas de panne, ou exceptions, doivent être analysés et examinés régulièrement (quotidiennement de préférence) par le personnel d'exploitation et/ou d'assistance réseau. Les causes de toutes les exceptions trouvées doivent être examinées. Certaines exceptions consignées peuvent ne pas être suffisamment critiques pour déclencher immédiatement une alarme dans le Centre des opérations 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.

Collection de messages Syslog

Les messages Syslog sont envoyés par le périphérique à un serveur de collecte. Ces messages

peuvent être des erreurs matérielles ou logicielles ou des erreurs d'information (par exemple lorsqu'une personne est en cours de configuration sur un périphérique).

La surveillance Syslog nécessite la prise en charge d'outils ou de scripts NMS (Network Management System) pour analyser et générer des rapports sur les données Syslog. Cela inclut la possibilité de trier les messages Syslog par date ou période, périphérique, type de message Syslog ou fréquence de message. Dans les réseaux plus importants, 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 une grande variété de données Syslog ne sont pas utilisées, l'entreprise doit passer en revue les données Syslog de priorité supérieure au moins tous les jours et créer des dossiers d'incidents pour les problèmes potentiels. Afin de détecter de manière proactive les problèmes réseau qui ne peuvent pas être détectés par une surveillance normale, une révision et une analyse périodiques des données Syslog historiques doivent être effectuées pour détecter des situations qui peuvent ne pas indiquer un problème immédiat, mais fournir une indication d'un problème avant qu'il ne devienne un impact sur le service.

Outils disponibles

Parmi les outils de récepteur de déroutement SNMP les plus répandus, citons les suivants :

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

L'outil Syslog le plus utilisé 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 d'OpenSystems à www.opensystems.com

Gestion des problèmes

La gestion des problèmes, un aspect de la gestion des pannes, est la discipline de la gestion des problèmes depuis le moment où ils surviennent, 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 à l'aide d'une combinaison de commandes ayant un impact sur le service ou de modifications de configuration 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 l’effacement 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 de support de premier niveau. L'objectif de tous les problèmes liés aux 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. Il doit inclure un certain niveau de description des problèmes par défaut et les collections de commandes “ show ” appropriées avant de passer à un second niveau de support. La prise en charge de premier niveau ne doit jamais inclure la suppression de routes ou le rechargement de périphériques. Dans l'idéal, l'organisation d'assistance de premier niveau devrait rapidement recueillir des informations, puis transmettre le problème au support 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 des travaux pratiques et la création de rapports de bogues. L'assistance de deuxième niveau doit être bien informée sur les types d'informations dont Cisco peut avoir besoin pour diagnostiquer un problème ou déposer un rapport de bogue, notamment :

- Décharges de mémoire
- Sortie des informations de routage
- Sortie de commande show du périphérique

Normalisation de la configuration

Les normes de configuration globale des périphériques représentent la pratique consistant à maintenir “ paramètres de configuration globale ” standard sur les périphériques et services similaires, ce qui assure une cohérence de configuration globale à l'échelle de l'entreprise. Les commandes de configuration globale sont des commandes qui s'appliquent à l'ensemble du périphérique et non aux ports, protocoles ou interfaces individuels, et qui affectent généralement l'accès aux périphériques, le comportement général des périphériques et la sécurité des périphériques. Dans Cisco IOS, ceci inclut les commandes suivantes :

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

Il est également important, dans les normes de configuration globale des périphériques, d'utiliser une convention de noms de périphériques appropriée qui permet aux administrateurs d'identifier le périphérique, le type de périphérique et l'emplacement du périphérique en fonction du nom DNS du périphérique. La cohérence de la configuration globale est importante pour la prise en charge et la fiabilité globales d'un environnement réseau, car elle contribue à réduire la complexité du réseau et à améliorer la prise en charge du réseau. Les difficultés de prise en charge sont souvent rencontrées sans standardisation de la configuration en raison d'un comportement incorrect ou incohérent des périphériques, de l'accès SNMP et de la sécurité générale des périphériques.

La maintenance des normes de configuration globale des périphériques est normalement assurée par un groupe d'ingénierie ou d'exploitation interne qui crée et gère des 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 de pouvoir les télécharger initialement sur tous les périphériques nouvellement provisionnés. Il est également utile de disposer d'un fichier accessible sur le Web qui fournit au fichier de configuration standard une explication de chaque paramètre de configuration. Certaines organisations configurent périodiquement tous les périphériques similaires pour garantir la cohérence de la configuration globale, ou examinent périodiquement les périphériques afin de déterminer les normes de configuration globale correctes.

Les normes de configuration d’interface ou de protocole représentent la pratique consistant à maintenir des normes de configuration d’interface et de protocole, ce qui améliore la disponibilité du réseau en réduisant la complexité du réseau, en fournissant le comportement prévu 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, des problèmes de connectivité accrus et une augmentation du temps de support réactif.

Les normes de configuration d'interface peuvent inclure :

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

Les normes de configuration spécifiques au protocole peuvent inclure :

- Configuration du routage IP
- Configuration DLSW
- Configuration de liste d'accès
- configuration ATM
- Configuration Frame Relay
- Configuration Spanning Tree
- Affectation et configuration des VLAN
- VTP (Virtual Trunking Protocol)
- HSRP (Hot Standby Routing Protocol)
- D'autres selon la configuration du réseau

Un exemple de normes IP peut inclure la taille des sous-réseaux, l'espace d'adresses IP utilisé, le protocole de routage utilisé et la configuration du protocole de routage.

La maintenance des normes de configuration de protocole et d'interface relève normalement des groupes d'ingénierie et de mise en oeuvre du réseau. Le groupe d'ingénieurs devrait être chargé d'identifier, de tester, de valider et de documenter les normes. Le groupe de mise en oeuvre est ensuite chargé d'utiliser les documents d'ingénierie ou les modèles de configuration pour fournir de nouveaux services. Le groupe d'ingénieurs devrait créer de la documentation sur tous les aspects des normes requises afin d'assurer l'uniformité. Des modèles de configuration doivent également être créés pour aider à appliquer les normes de configuration. Les groupes opérationnels doivent également recevoir une formation sur les normes et être en mesure d'identifier les problèmes de configuration non standard. La cohérence de la configuration est d'une grande aide dans la phase 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 qui utilise la disponibilité du réseau comme mesure d'amélioration de la qualité. De nombreuses entreprises mesurent maintenant la disponibilité et les types de panne. Les types de panne peuvent inclure les éléments suivants :

- Matériel
- le logiciel Cisco IOS
- Liaison/opérateur
- Alimentation/environnement

- Conception
- Erreur/processus utilisateur

En identifiant les pannes et en effectuant une analyse des causes premières 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 besoins et les objectifs commerciaux (clients enregistrés uniquement)**

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

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

❑**Étape 4 : Élaborer un plan de projet de gestion des logiciels (clients enregistrés uniquement)**

❑**Étape 5 : Développer une matrice des besoins logiciels (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 : Notions de base de Cisco IOS, processus internes de Cisco IOS, analyse de la fiabilité des logiciels, programme de qualité interne de Cisco, méthodologies de test interne de Cisco et analyse sur site qui présente les pratiques actuelles du secteur et l'expérience globale du client avec le logiciel Cisco IOS

- Gestion de Cisco IOS : Vous trouverez des informations supplémentaires sur la gestion de Cisco IOS et les meilleures pratiques dans le livre blanc “ Cisco IOS Management for High Availability Networking ”, disponible sur le site suivant : http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a00800a998b.shtml
- Pour plus d'informations sur l'exécution des sondes réseau, sur les commandes CLI à utiliser, sur l'analyse et l'interprétation des données de trafic réseau et sur l'établissement de politiques 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.
- Cisco IOS a des conventions d'attribution de noms spécifiques définies ici : http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_tech_note09186a0080101cda.shtml
- 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 des clients en conséquence.
- Les bulletins produits Cisco IOS servent à annoncer les versions de Cisco IOS aux clients. Ils contiennent de brèves informations sur le contenu de la version. Consultez 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 Cisco gère la sécurité des produits Cisco. Tout problème lié à la sécurité de Cisco IOS doit être renvoyé à cette équipe. Cisco publie publiquement ses vulnérabilités en matière de sécurité. http://tools.cisco.com/security/center/publicationListing
- Défaillances de Cisco IOS : Il est recommandé de reporter les défauts graves de Cisco IOS. Tout employé de Cisco peut faire cette recommandation.
- Les problèmes de terrain sur Cisco IOS sont communiqués aux clients par le biais des avis 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 de mise en réseau Cisco