

# Cisco IOS Management pour la gestion de réseaux à haute disponibilité : Livre blanc sur les pratiques recommandées

## Contenu

[Introduction](#)

[Présentation des meilleures pratiques de Cisco IOS](#)

[Présentation du processus de gestion du cycle de vie des logiciels](#)

[Planification - Création du cadre de gestion Cisco IOS](#)

[Stratégie et outils pour la planification de Cisco IOS](#)

[Définitions du suivi des versions logicielles](#)

[Cycle de mise à niveau et définitions](#)

[Processus de certification](#)

[Conception - Sélection et validation des versions de Cisco IOS](#)

[Stratégie et outils pour la sélection et la validation de Cisco IOS](#)

[Gestion des candidats](#)

[Test et validation](#)

[Mise en oeuvre : déploiement rapide et réussi de Cisco IOS](#)

[Stratégie et outils pour les déploiements Cisco IOS](#)

[Processus pilote](#)

[Mise en oeuvre](#)

[Opérations - Gestion de la mise en oeuvre de Cisco IOS haute disponibilité](#)

[Stratégies et outils pour les opérations Cisco IOS](#)

[Contrôle de version du logiciel](#)

[Gestion proactive des Syslog](#)

[Gestion des problèmes](#)

[Normalisation de la configuration](#)

[Gestion de la disponibilité](#)

[Annexe A - Présentation des versions de Cisco IOS](#)

[Jalons des cycles de vie des versions](#)

[Convention de dénomination de version Cisco IOS](#)

[Annexe B - Fiabilité de Cisco IOS](#)

[Programme de qualité Cisco IOS](#)

[Test de version de Cisco IOS](#)

[MTBF logiciel](#)

[Hypothèses de fiabilité des logiciels](#)

[Informations connexes](#)

## [Introduction](#)

Le déploiement et la maintenance d'un logiciel Cisco IOS® fiable sont une priorité dans l'environnement de réseau stratégique actuel, qui nécessite une attention renouvelée de la part de Cisco et du client pour assurer une disponibilité continue. Bien que Cisco doive se concentrer sur son engagement en faveur de la qualité des logiciels, les groupes de conception et d'assistance réseau doivent également se concentrer sur les meilleures pratiques de gestion des logiciels Cisco IOS. L'objectif est d'améliorer la disponibilité et l'efficacité de la gestion des logiciels. Cette méthode est un partenariat combiné qui permet de partager, d'apprendre et de mettre en oeuvre les meilleures pratiques de gestion des logiciels.

Ce document fournit un cadre opérationnel efficace des pratiques de gestion de Cisco IOS pour les entreprises et les fournisseurs de services qui contribuent à améliorer la fiabilité des logiciels, à réduire la complexité du réseau et à accroître la disponibilité du réseau. Ce cadre permet également d'améliorer l'efficacité de la gestion des logiciels en identifiant les domaines de responsabilité et les chevauchements dans les tests de gestion des logiciels et la validation entre les opérations de version de Cisco et la base de clients de Cisco.

## [Présentation des meilleures pratiques de Cisco IOS](#)

Les tableaux suivants présentent les meilleures pratiques de Cisco IOS. Ces tableaux peuvent être utilisés comme une présentation de la gestion des meilleures pratiques définies, une liste de contrôle d'analyse des écarts pour passer en revue les pratiques de gestion actuelles de Cisco IOS, ou comme cadre pour la création de processus autour de la gestion de Cisco IOS.

Les tableaux définissent les quatre composants du cycle de vie de la gestion de Cisco IOS. Chaque tableau commence par une stratégie et un résumé des outils pour la zone de cycle de vie identifiée. Le résumé de la stratégie et des outils présente les meilleures pratiques spécifiques qui s'appliquent uniquement à la zone de cycle de vie définie.

[Planification - Création du cadre de gestion de Cisco IOS](#) - La planification est la phase initiale de la gestion de Cisco IOS nécessaire pour aider une organisation à déterminer quand mettre à niveau le logiciel, où mettre à niveau et quel processus sera utilisé pour tester et valider les images potentielles.

<b>Meilleure pratique</b>	<b>Détail</b>
<u><a href="#">Stratégie et outils pour la planification de Cisco IOS</a></u>	La planification de la gestion de Cisco IOS commence par une évaluation honnête des pratiques actuelles, le développement d'objectifs réalisables et la planification de projets.
<u><a href="#">Définitions du suivi des versions logiciels</a></u>	Indique où la cohérence des logiciels peut être maintenue. Une piste logicielle peut être définie comme un regroupement de versions logicielles unique, différencié des autres zones par la géographie, les plates-formes, les modules ou les exigences de fonctionnalités uniques.

<a href="#">es</a>	
<a href="#">Cycle de mise à niveau et définitions</a>	Les définitions de cycle de mise à niveau peuvent être définies comme des étapes de qualité de base dans le logiciel et la gestion des modifications utilisées pour déterminer quand un cycle de mise à niveau logicielle doit être lancé.
<a href="#">Processus de certification</a>	Les étapes du processus de certification devraient inclure l'identification des pistes, les définitions de cycle de mise à niveau, la gestion des candidats, les essais/validation et au moins une partie de l'utilisation de la production pilote.

[Conception - Sélection et validation des versions d'IOS](#) - Le fait d'avoir un processus bien défini de sélection et de validation des versions de Cisco IOS aide une organisation à réduire les temps d'arrêt imprévus dus à des tentatives de mise à niveau infructueuses et à des défauts logiciels non planifiés.

<b>Meilleure pratique</b>	<b>Détail</b>
<a href="#">Stratégie et outils pour la sélection et la validation de Cisco IOS</a>	Définir les processus de sélection, de test et de validation des nouvelles versions de Cisco IOS. Ceci inclut un laboratoire de test de réseau qui émule le réseau de production
<a href="#">Gestion des candidats</a>	La gestion des candidats consiste à identifier les exigences de version logicielle et les risques potentiels pour le matériel et les ensembles de fonctionnalités activés spécifiques.
<a href="#">Test et validation</a>	Les tests et la validation sont un aspect essentiel de la gestion des logiciels et de la mise en réseau haute disponibilité. Des tests en laboratoire appropriés peuvent réduire considérablement les temps d'arrêt de la production, aider à former le personnel d'assistance réseau et aider à rationaliser les processus de mise en oeuvre du réseau.

[Mise en oeuvre - Déploiement rapide et réussi de Cisco IOS](#) - Des processus de mise en oeuvre bien définis permettent à une entreprise de déployer rapidement et efficacement de nouvelles versions de Cisco IOS.

<b>Meilleure</b>	<b>Détail</b>

<b>pratique</b>	
<a href="#">Stratégie et outils pour les déploiements Cisco IOS</a>	La stratégie de base pour les déploiements Cisco IOS consiste à effectuer une certification finale via un processus pilote et un déploiement rapide à l'aide d'outils de mise à niveau et d'un processus de mise en oeuvre bien défini.
<a href="#">Processus pilote</a>	Afin de minimiser l'exposition potentielle et de capturer plus en toute sécurité les problèmes de production restants, un pilote logiciel est recommandé. Le plan pilote individuel devrait tenir compte de la sélection des pilotes, de la durée du pilote et de la mesure.
<a href="#">Mise en oeuvre</a>	Une fois la phase pilote terminée, la phase de mise en oeuvre de Cisco IOS doit commencer. La phase de mise en oeuvre peut inclure plusieurs étapes pour assurer la réussite et l'efficacité de la mise à niveau logicielle, notamment le démarrage lent, la certification finale, la préparation de la mise à niveau, l'automatisation de la mise à niveau et la validation finale.

[Opérations - Gestion de la haute disponibilité Mise en oeuvre de Cisco IOS](#) - Les meilleures pratiques pour les opérations de Cisco IOS incluent le contrôle de version logicielle, la gestion Syslog de Cisco IOS, la gestion des problèmes, la standardisation de la configuration et la gestion de la disponibilité.

<b>Meilleure pratique</b>	<b>Détail</b>
<a href="#">Stratégies et outils pour les opérations Cisco IOS</a>	La première stratégie des opérations de Cisco IOS consiste à maintenir l'environnement aussi simple que possible, en évitant les variations de configuration et de versions de Cisco IOS. La deuxième stratégie consiste à identifier et à résoudre rapidement les pannes de réseau.
<a href="#">Contrôle de version du logiciel</a>	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.

<a href="#">Gestion proactive des Syslog</a>	La collecte, la surveillance et l'analyse Syslog sont des processus de gestion des pannes recommandés pour résoudre d'autres problèmes réseau spécifiques à Cisco IOS difficiles ou impossibles à identifier par d'autres moyens.
<a href="#">Gestion des problèmes</a>	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 peuvent être utilisées pour déterminer la cause première.
<a href="#">Normalisation de la configuration</a>	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.
<a href="#">Gestion de la disponibilité</a>	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.

## [Présentation du processus de gestion du cycle de vie des logiciels](#)

La gestion du cycle de vie du logiciel Cisco IOS est définie comme l'ensemble des processus de planification, de conception, de mise en oeuvre et d'exploitation recommandés pour les mises en oeuvre logicielles fiables et la mise en réseau haute disponibilité. Cela inclut les processus de sélection, de validation et de maintenance des versions de Cisco IOS dans le réseau.

L'objectif de la gestion du cycle de vie du logiciel Cisco IOS est d'améliorer la disponibilité du réseau en réduisant la probabilité de défauts de production identifiés ou de modifications/mises à niveau liées au logiciel. Il a été démontré que les meilleures pratiques définies dans cette documentation permettent de réduire ces défauts et de les modifier en fonction de l'expérience pratique de nombreux clients Cisco et de l'équipe des services avancés Cisco. La gestion du cycle de vie des logiciels peut d'abord augmenter les dépenses, mais le coût total d'acquisition peut être réduit en raison d'une diminution des pannes et d'une rationalisation des mécanismes de déploiement et d'assistance.

## [Planification - Création du cadre de gestion Cisco IOS](#)

La planification est la phase initiale de la gestion de Cisco IOS nécessaire pour aider une organisation à déterminer quand mettre à niveau le logiciel, où mettre à niveau et quel processus sera utilisé pour tester et valider les images potentielles.

Les meilleures pratiques comprennent les [définitions de suivi de version logicielle](#), le [cycle de mise à niveau et les définitions](#), et la création d'un [processus interne de certification logicielle](#).

## [Stratégie et outils pour la planification de Cisco IOS](#)

Commencez la planification de la gestion de Cisco IOS par une évaluation honnête des pratiques actuelles, du développement d'objectifs réalisables et de la planification de projets. L'auto-évaluation doit être effectuée en comparant les meilleures pratiques de ce document aux processus de votre organisation. Les questions de base doivent comprendre les suivantes :

- Mon entreprise dispose-t-elle d'un processus de certification logicielle qui inclut les tests/validations logiciels ?
- Mon entreprise dispose-t-elle de normes logicielles Cisco IOS avec un nombre limité de versions de Cisco IOS exécutées sur le réseau ?
- Mon entreprise a-t-elle des difficultés à déterminer quand mettre à niveau le logiciel Cisco IOS ?
- Mon entreprise a-t-elle des difficultés à déployer de nouveaux logiciels Cisco IOS de manière efficace et efficiente ?
- Mon entreprise rencontre-t-elle des problèmes de stabilité de Cisco IOS après le déploiement qui affectent sérieusement le coût des temps d'arrêt ?

Après l'évaluation, votre entreprise doit commencer à définir des objectifs pour la gestion de la plate-forme logicielle Cisco IOS. Commencez par rassembler un groupe interfonctionnel de responsables et/ou de responsables issus de groupes de planification de l'architecture, d'ingénierie, de mise en oeuvre et d'opérations pour aider à définir les objectifs de Cisco IOS et les projets d'amélioration des processus. Les réunions initiales devraient avoir pour but de déterminer les objectifs généraux, les rôles et les responsabilités, d'affecter des éléments d'action et de définir les calendriers initiaux des projets. Définissez également les facteurs de réussite et les mesures critiques pour déterminer les avantages de la gestion des logiciels. Les indicateurs potentiels sont les suivants :

- disponibilité (en raison de problèmes logiciels)
- coût des mises à niveau logicielles
- temps requis pour les mises à niveau
- nombre de versions logicielles exécutées en production
- taux de réussite/d'échec de la mise à niveau logicielle

En plus de la planification globale du cadre de gestion de Cisco IOS, certaines organisations définissent également des réunions de planification logicielle en cours qui doivent avoir lieu tous les mois ou tous les trimestres. L'objectif de ces réunions est de passer en revue le déploiement actuel des logiciels et de commencer à planifier toute nouvelle configuration logicielle requise. La planification peut inclure la révision ou la modification des processus actuels de gestion des logiciels, ou simplement la définition des rôles et des responsabilités pour les différentes phases de gestion des logiciels.

Les outils de la phase de planification se composent uniquement d'outils de gestion de l'inventaire logiciel. CiscoWorks 2000 Resource Manager Essentials (RME) Inventory Manager est le principal outil utilisé dans ce domaine. Le [gestionnaire d'inventaire RME de CiscoWorks2000](#) simplifie considérablement la gestion des versions des routeurs et des commutateurs Cisco grâce à des outils de création de rapports basés sur le Web qui permettent de signaler et de trier les périphériques Cisco IOS en fonction de la version du logiciel, de la plate-forme du périphérique, de la taille de la mémoire et du nom du périphérique.

## [Définitions du suivi des versions logicielles](#)

La première meilleure pratique de planification de la gestion du logiciel Cisco IOS identifie les domaines où la cohérence logicielle peut être maintenue. Une piste logicielle est définie comme

un regroupement de versions logicielles unique, différencié d'autres zones par la géographie, les plates-formes, les modules ou les fonctionnalités spécifiques. Optimalement, un réseau ne doit exécuter qu'une seule version logicielle. Cela réduit considérablement les coûts liés à la gestion des logiciels et fournit un environnement homogène et facile à gérer. Cependant, la plupart des entreprises doivent exécuter plusieurs versions du réseau en raison de problèmes de fonctionnalités, de plate-forme, de migration et de disponibilité dans des domaines spécifiques. Dans de nombreux cas, la même version ne fonctionne pas sur des plates-formes hétérogènes. Dans d'autres cas, l'organisation ne peut pas attendre qu'une version prenne en charge toutes ses exigences. L'objectif est d'identifier le moins de pistes logicielles pour le réseau en tenant compte des exigences de test/validation, de certification et de mise à niveau. Dans de nombreux cas, l'entreprise peut avoir un peu plus de pistes pour réduire les coûts globaux de test/validation, de certification et de mise à niveau.

Le premier fait différenciant est le support des plates-formes. En règle générale, les commutateurs LAN, les commutateurs WAN, les routeurs principaux et les routeurs de périphérie ont chacun des pistes logicielles distinctes. D'autres pistes logicielles peuvent être nécessaires pour des fonctionnalités ou services spécifiques, tels que la commutation de liaison de données (DLSw), la qualité de service (QoS) ou la téléphonie IP, en particulier si cette exigence peut être localisée au sein du réseau.

Un autre critère est la fiabilité. De nombreuses entreprises tentent d'exécuter les logiciels les plus fiables vers le coeur du réseau et le centre de données, tout en offrant des fonctionnalités avancées plus récentes, ou une assistance matérielle, vers la périphérie. D'un autre côté, les fonctions d'évolutivité ou de bande passante sont souvent les plus nécessaires dans les environnements de coeur de réseau ou de data center. D'autres pistes peuvent être nécessaires pour des plates-formes spécifiques, telles que des sites de distribution plus importants qui ont une plate-forme de routeur WAN différente. Le tableau suivant est un exemple de définition de suivi logiciel pour une grande entreprise.

Pi st e	Zone	Plates- formes matérie lles	Fonctionnalités	Versio n de Cisco IOS	État de la certifi cation
1	Commuta tion de coeur de réseau local	6500	QoS	12.1E( A8)	Test
2	Commuta teur d'accès LAN	2924XL 2948XL	UDLD (Unidirectional Link Detection Protocol), STP (Spanning Tree Protocol)	12.0(5 .2)XU	Certifi é 3/1/01
3	Distributio n/accès LAN	5500 6509	Superviseur 3	5.4(4)	Certifi é 7/1/01
4	Module de commutat ion de routage	RSM	Routage OSPF (Open Shortest Path First)	12.0(1 1)	Certifi é 3/4/02

	(RSM) du commutateur de distribution				
5	Distribution de tête de réseau WAN	7505 7507 7204 7206	Frame Relay OSPF	12.0(11)	Certifié 11/1/01
6	Accès WAN	2600	Frame Relay OSPF	12.1(8)	Certifié 01/06/01
7	Connectivité IBM	3600	Tête de réseau SDLC (Synchronous Data Link Control)	11.3(8)T1	Certifié 11/1/00

Les affectations de suivi peuvent également changer au fil du temps. Dans de nombreux cas, les fonctionnalités ou la prise en charge matérielle peuvent s'intégrer dans des versions logicielles plus générales, permettant ainsi à différentes pistes de migrer ensemble. Une fois les définitions de suivi définies, l'organisation peut utiliser d'autres processus définis pour migrer vers la cohérence et la validation des nouvelles versions. Les définitions de suivi sont également un effort continu. Chaque fois qu'une nouvelle fonctionnalité, un nouveau service, un nouveau matériel ou un nouveau module est identifié, une nouvelle piste doit être envisagée.

Les organisations souhaitant lancer un processus de suivi doivent commencer par des exigences de suivi nouvellement définies, ou dans certains cas, par des projets de stabilisation pour les réseaux existants. Une organisation peut également avoir des points communs identifiables avec les versions logicielles existantes qui peuvent rendre possible la définition de la piste actuelle. Dans la plupart des cas, une migration rapide vers des versions identifiées n'est pas nécessaire si le client dispose d'une stabilité réseau suffisante. L'architecture réseau, ou groupe d'ingénierie, est généralement propriétaire du processus de définition de la piste. Dans certains cas, une personne peut être responsable de la définition des voies. Dans d'autres cas, les chefs de projet sont chargés d'élaborer des exigences logicielles et de nouvelles définitions de pistes en fonction de projets individuels. Il est également recommandé d'examiner les définitions des pistes tous les trimestres afin de déterminer si de nouvelles pistes sont nécessaires ou si d'anciennes pistes nécessitent une consolidation ou une mise à niveau.

Les entreprises qui identifient et gèrent des pistes logicielles avec un contrôle strict des versions ont obtenu le plus grand succès avec un nombre décroissant de versions logicielles dans le réseau de production. Cela améliore généralement la stabilité des logiciels et la fiabilité globale du réseau.

### Cycle de mise à niveau et définitions

Les définitions de cycle de mise à niveau sont définies comme des étapes de qualité de base dans le logiciel et la gestion des modifications utilisées pour déterminer quand un cycle de mise à niveau logicielle doit être lancé. Les définitions de cycle de mise à niveau permettent à une organisation de planifier correctement un cycle de mise à niveau logicielle et d'allouer les ressources requises. En l'absence de définitions de cycle de mise à niveau, une entreprise



rencontre généralement une augmentation des problèmes de fiabilité logicielle en raison des exigences de fonctionnalités des versions stables actuelles. Une autre exposition pourrait être le fait que l'organisation n'a pas la possibilité de tester et de valider correctement une nouvelle version avant que l'utilisation de la production ne soit requise.

Un aspect important de cette pratique consiste à déterminer quand et dans quelle mesure les processus de planification des logiciels devraient être amorcés. Ceci est dû au fait que l'une des principales causes de problèmes logiciels est d'activer une fonctionnalité, un service ou une fonctionnalité matérielle en production sans diligence raisonnable, ou de mettre à niveau vers une nouvelle version de Cisco IOS sans considérations de gestion logicielle. Un autre problème est de ne pas mettre à niveau. En ignorant les cycles et les exigences logiciels normaux, de nombreux clients sont confrontés à la tâche difficile de mettre à niveau les logiciels par le biais de plusieurs versions principales différentes. La difficulté est due aux tailles d'image, aux changements de comportement par défaut, aux changements d'interpréteur de niveau de commande (CLI) et aux changements de protocole.

Cisco recommande un cycle de mise à niveau bien défini, basé sur les meilleures pratiques telles que définies dans ce document, à initier chaque fois que de nouvelles fonctionnalités, services ou assistance matérielle majeurs sont nécessaires. Le degré de certification et d'essai/validation doit être analysé (en fonction du risque), afin de déterminer les exigences précises en matière d'essai/validation. L'analyse des risques peut être effectuée en fonction de l'emplacement géographique, de l'emplacement logique (couche principale, couche de distribution ou couche d'accès) ou du nombre estimé de personnes/clients concernés. Si la fonctionnalité principale ou la fonctionnalité matérielle est contenue dans la version actuelle, certains processus de cycle de mise à niveau rationalisés doivent également être initiés. Si la fonctionnalité est relativement mineure, prenez en compte le risque et décidez ensuite quels processus doivent être initiés. En outre, les logiciels doivent être mis à niveau dans deux ans ou moins pour vous assurer que votre entreprise reste relativement à jour et que le processus de mise à niveau n'est pas trop encombrant.

Les clients doivent également tenir compte du fait qu'aucune correction de bogues ne sera apportée aux catégories de logiciels qui ont dépassé le statut de fin de vie (EOL). Il convient également de tenir compte des besoins de l'entreprise, car de nombreux environnements peuvent tolérer, voire accueillir, d'autres ajouts de fonctionnalités avec peu ou pas de processus de test/validation et certains temps d'arrêt qui en résultent. Les clients doivent également tenir compte des données plus récentes collectées dans les opérations de mise à jour Cisco lorsqu'ils examinent leurs exigences de test. Une analyse des bogues et des causes premières a montré que la grande majorité des causes premières des bogues étaient le résultat de développeurs codant dans la zone logicielle affectée. Cela signifie que si une organisation ajoute une fonctionnalité ou un module particulier à son réseau dans une version existante, il y a une probabilité de bogue lié à cette fonctionnalité ou ce module, mais une probabilité beaucoup plus faible que la nouvelle fonctionnalité, le nouveau matériel ou le nouveau module aura un impact sur d'autres domaines. Ces données devraient permettre aux entreprises de réduire les exigences de test, lors de l'ajout de nouvelles fonctionnalités ou de nouveaux modules pris en charge dans les versions existantes, en testant uniquement le nouveau service ou la nouvelle fonctionnalité en conjonction avec d'autres services activés. Les données doivent également être prises en compte lors de la mise à niveau du logiciel en fonction de quelques bogues critiques trouvés dans le réseau.

Le tableau suivant indique les exigences de mise à niveau recommandées pour une grande entreprise à haute disponibilité :

Déclencheur de gestion	Exigences relatives au cycle de
------------------------	---------------------------------

logicielle	vie des logiciels
Nouveau service réseau. Par exemple, un nouveau réseau fédérateur ATM ou un nouveau service VPN.	Terminer la validation du cycle de vie du logiciel, y compris les nouveaux tests de fonctionnalités (en association avec d'autres services activés), les tests de topologie regroupés, l'analyse des performances et les tests de profil d'application.
La nouvelle fonctionnalité réseau n'est pas prise en charge dans la version actuelle du logiciel. Exemples : QoS et MPLS (Multiprotocol Label Switching).	Terminer la validation du cycle de vie du logiciel, y compris les nouveaux tests de fonctionnalités, en association avec d'autres services activés, les tests de topologie regroupés, l'analyse des performances et les tests de profil d'application.
Nouvelle fonction principale ou nouveau module matériel existant dans la version actuelle. Par exemple, ajout d'un nouveau module GigE, prise en charge de la multidiffusion ou DLSW.	Processus de gestion des candidats. Validation complète possible en fonction des exigences de la version. Test/validation limité possible si la direction du candidat identifie la version actuelle comme étant potentiellement acceptable.
Ajout mineur de fonctionnalités. Par exemple, un périphérique TACACS pour le contrôle d'accès.	Tenez compte de la gestion des candidats en fonction du risque de la fonction. Envisagez de tester ou de piloter la nouvelle fonctionnalité en fonction des risques.
Logiciels en production pendant deux ans ou une revue trimestrielle des logiciels.	Les décisions de gestion et d'affaires des candidats en ce qui concerne la gestion du cycle de vie pour identifier la version à prendre en charge.

### Mises à niveau d'urgence

Dans certains cas, les entreprises doivent mettre à niveau leurs logiciels en raison de bogues catastrophiques. Cela peut entraîner des problèmes si l'organisation ne dispose pas d'une méthode de mise à niveau d'urgence. Les problèmes liés aux logiciels peuvent aller des mises à niveau logicielles non gérées, où les logiciels sont mis à niveau sans gestion du cycle de vie des logiciels, aux situations où les périphériques réseau sont continuellement en panne, mais l'entreprise ne procède pas à la mise à niveau puisque la certification/les tests de la prochaine version candidate n'ont pas été terminés. Cisco recommande un processus de mise à niveau d'urgence pour les situations où des tests et des pilotes limités sont effectués dans des zones moins critiques du réseau.

Si des erreurs catastrophiques se produisent sans solution apparente et que le problème est lié à un défaut logiciel, Cisco recommande que l'assistance Cisco soit pleinement sollicitée pour isoler le défaut et déterminer si ou quand une solution est disponible. Lorsque la solution est disponible, Cisco recommande un cycle de mise à niveau d'urgence pour déterminer rapidement si le problème peut être réparé avec des temps d'arrêt limités. Dans la plupart des cas, une organisation exécute une version prise en charge du code et le correctif du problème est disponible dans une nouvelle version provisoire du logiciel.

Les entreprises peuvent également se préparer à des mises à niveau d'urgence. La préparation inclut la migration vers les versions de Cisco IOS prises en charge et l'identification/le développement des versions de remplacement des candidats dans la même catégorie de Cisco IOS que la version certifiée. Les logiciels pris en charge sont importants, car cela signifie que le développement de Cisco continue d'ajouter des corrections de bogues à la série de logiciels identifiés. En conservant les logiciels pris en charge sur le réseau, l'entreprise réduit le temps de validation en raison de la base de code plus familière et stable. En règle générale, un candidat de remplacement est une nouvelle image logicielle provisoire dans la même gamme Cisco IOS sans ajout de fonctionnalités ou de support matériel. Une stratégie de remplacement des candidats est particulièrement importante si l'entreprise est dans la phase d'adoption précoce d'un train de logiciels particulier.

## Processus de certification

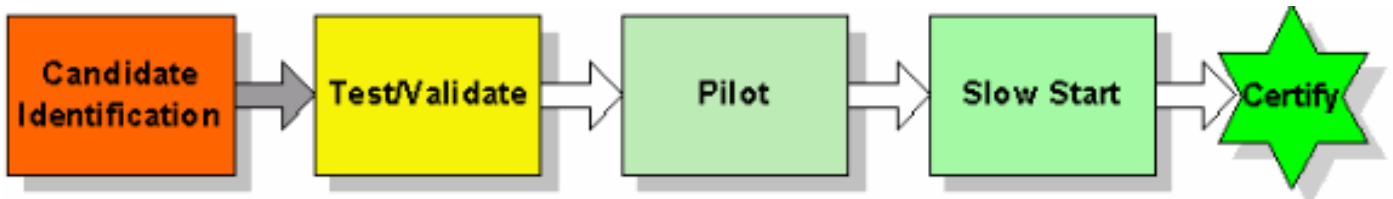
Un processus de certification permet de s'assurer que les logiciels validés sont déployés de manière cohérente dans l'environnement de production de l'entreprise. Les étapes du processus de certification devraient inclure l'identification des pistes, les définitions de cycle de mise à niveau, la gestion des candidats, les essais/validation et certaines utilisations de la production pilote. Cependant, un processus de certification simple permet toujours de s'assurer que des versions logicielles cohérentes sont déployées dans les voies identifiées.

Démarrez un processus de certification en identifiant les personnes issues de l'architecture, de l'ingénierie/déploiement et des opérations pour rédiger et gérer le processus de certification. Le groupe doit d'abord examiner les objectifs commerciaux et les ressources disponibles pour s'assurer que le processus de certification continuera de réussir. Ensuite, confiez à des personnes ou à des groupes la responsabilité générale des principales étapes du processus de certification, y compris la gestion des pistes, les définitions des mises à niveau du cycle de vie, les essais/validation et les pilotes. Chacun de ces domaines devrait être défini, approuvé et communiqué officiellement au sein de l'organisation.

Incluez également des lignes directrices pour la qualité ou l'approbation à chaque étape du processus de certification. On appelle parfois cela un processus de qualité parce que certains critères de qualité doivent être satisfaits avant que le processus puisse passer à l'étape suivante. Cela permet de s'assurer que le processus de certification est efficace et vaut la peine des ressources affectées. En général, lorsque des problèmes de qualité se posent dans un domaine, le processus repousse l'effort d'une étape à l'autre.

Les logiciels candidats ne répondent pas aux critères de certification définis en raison de la qualité du logiciel ou d'un comportement inattendu. Lorsque des problèmes ont une incidence sur l'environnement, l'organisation devrait avoir un processus plus rationalisé pour certifier une libération provisoire ultérieure. Cela contribue à réduire les besoins en ressources et est généralement efficace si l'organisation peut comprendre ce qui a changé et quels défauts ont été résolus. Il n'est pas rare qu'une entreprise rencontre un problème avec un candidat initial et certifie une version intermédiaire ultérieure de Cisco IOS. Les organisations peuvent également

effectuer une certification limitée ou fournir des mises en garde en cas de problème et peuvent effectuer une mise à niveau vers une version certifiée ultérieurement lorsqu'une nouvelle version provisoire a été validée. Le diagramme ci-dessous est un processus de certification de base et comprend des barrières de qualité (examen suivant chaque bloc) :



## Conception - Sélection et validation des versions de Cisco IOS

L'utilisation d'une méthodologie bien définie pour sélectionner et valider les versions de Cisco IOS aide une entreprise à réduire les temps d'arrêt imprévus dus à des tentatives de mise à niveau infructueuses et à des défauts logiciels non planifiés.

La phase de conception comprend la gestion des candidats et les tests/validations. La gestion des candidats est le processus utilisé pour identifier des versions spécifiques pour les pistes logicielles définies. Les tests/validations font partie du processus de certification et garantissent que la version du logiciel identifiée réussit dans le cadre de la piste requise. Les tests/validations doivent être effectués dans un environnement de laboratoire avec une topologie et une configuration réduites qui ressemblent étroitement à l'environnement de production.

### Stratégie et outils pour la sélection et la validation de Cisco IOS

Chaque organisation doit disposer d'un processus de sélection et de validation des versions standard de Cisco IOS pour le réseau, en commençant par un processus de sélection de la version de Cisco IOS. Une équipe interfonctionnelle de l'architecture, de l'ingénierie et des opérations doit définir et documenter le processus de gestion des candidats. Une fois approuvé, le processus doit être remis au groupe de livraison approprié. Il est également recommandé de créer un modèle standard de gestion des candidats qui puisse être mis à jour avec les renseignements sur les candidats au fur et à mesure de leur identification.

Toutes les entreprises ne disposent pas d'un environnement de laboratoire sophistiqué qui peut facilement imiter l'environnement de production. Certaines entreprises ignorent les tests de laboratoire en raison des coûts et de la capacité de piloter une nouvelle version sur le réseau sans impact commercial majeur. Cependant, les organisations à haute disponibilité sont encouragées à créer un laboratoire qui imite le réseau de production et à développer un processus de test/validation pour garantir une couverture de test élevée pour les nouvelles versions de Cisco IOS. Une organisation doit prendre environ six mois pour construire le TP. Au cours de cette période, l'organisation doit travailler à la création de plans et de processus de test spécifiques afin de s'assurer que le TP sera utilisé à son plein avantage. Pour Cisco IOS, cela signifie la création de plans de test Cisco IOS spécifiques pour chaque piste logicielle requise. Ces processus sont essentiels dans les grandes entreprises en raison du fait que de nombreux laboratoires ne sont pas utilisés pour l'introduction de nouveaux produits et logiciels.

Les sections suivantes décrivent brièvement les outils de gestion et de test/validation des candidats à utiliser pour la sélection et la validation de Cisco IOS.

#### **Outils de gestion des candidats**

**Remarque :** Pour utiliser la plupart des outils fournis ci-dessous, vous devez être un utilisateur enregistré et vous devez être connecté.

- [Notes de version](#) : fournit des informations sur la prise en charge matérielle, de module et de fonctionnalité d'une version. Les notes de version doivent être examinées lors de la gestion des candidats afin de s'assurer que toute la prise en charge matérielle et logicielle requise existe dans la version potentielle et de comprendre tous les problèmes de migration, y compris les différents comportements par défaut ou les exigences de mise à niveau.

## Outils de test et de validation

Les outils de test et de validation sont utilisés pour tester et valider les solutions réseau, notamment les nouveaux matériels, logiciels et applications.

- **Générateurs de trafic** - Générer des flux de trafic multiprotocole et des débits de paquets bruts utilisés pour modéliser le débit sur une liaison particulière utilisant des protocoles spécifiques. Les utilisateurs peuvent spécifier les numéros d'adresse MAC source, de destination et de socket. Ces valeurs peuvent être incrémentées à des étapes spécifiées ou configurées pour être statiques/fixes ou par incréments aléatoires. Les générateurs de trafic peuvent générer les paquets pour les protocoles suivants : IP Internet Network Packet Exchange (IPX) DECnet Apple Systèmes de réseau Xerox (XNS) Internet Control Message Protocol (ICMP) Protocole IGMP (Internet Group Management Protocol) Service réseau sans connexion (CLNS) Protocole UDP (User Datagram Protocol) Virtual Integrated Network Service (VINES) Paquets de liaison de données Des outils sont disponibles auprès de [Agilent](#) et [Spirent Communications](#) .
- **Packet Counter/Capture/Decoder (Sniffer)** : permet au client de capturer et de décoder sélectivement des paquets sur toutes les couches de paquets et de liaison de données. L'outil permet à l'utilisateur de spécifier les filtres, ce qui permet de capturer uniquement les données de protocole spécifiées. Les filtres permettent en outre à l'utilisateur de spécifier la capture des paquets correspondant à une adresse IP, un numéro de port ou une adresse MAC spécifique. Des outils sont disponibles auprès de [Sniffer Technologies](#) .
- **Network Simulator/Emulator** - Permet au client de remplir les tables de routage de routeurs spécifiques, en fonction des besoins du réseau de production. Prend en charge la génération de routeurs RIP (IP Routing Information Protocol), OSPF, IS-IS (Intermediate System-to-Intermediate System), IGRP (Interior Gateway Routing Protocol), EIGRP (Enhanced IGRP) et BGP (Border Gateway Protocol). Les outils sont disponibles à partir de [PacketStorm Communications](#) et [Spirent Communications](#).
- **Émulateurs de session** - Génère des flux de trafic multiprotocole de fenêtre glissante et peut envoyer des flux de trafic multiprotocole sur le réseau de test vers le périphérique de réception. Le périphérique récepteur retransmet les paquets vers la source. Le périphérique source vérifie le nombre de paquets envoyés, reçus, hors séquence et d'erreurs. Cet outil offre également la souplesse nécessaire pour définir les paramètres de fenêtre dans le protocole TCP (Transmission Control Protocol), imitant ainsi de près les sessions de trafic client/serveur du réseau de travaux pratiques. Les outils sont disponibles auprès de [Empirix](#) .
- **Émulateurs de réseau à grande échelle** : aide à tester l'évolutivité des environnements plus grands. Ces outils sont capables de créer et d'injecter facilement du trafic de type contrôle dans une topologie de laboratoire afin de mieux imiter un environnement de production. Les fonctionnalités incluent les injecteurs de route, les voisins de protocole et les voisins de protocole de couche 2. Des outils sont disponibles auprès de [Agilent](#) et [Spirent](#)

## Communications .

- **Simulateurs WAN** : idéal pour tester le trafic des applications d'entreprise lorsque la bande passante et le délai sont potentiellement un problème. Ces outils permettent aux entreprises de tester localement une application avec le délai et la bande passante estimés pour voir comment l'application fonctionne sur le WAN. Ces outils sont souvent utilisés pour le développement d'applications et pour les types de tests de profilage d'applications au sein des entreprises. Adtech, une division de [Spirent Communications](#) et [Shunra](#) fournit des outils de simulation WAN.

## Gestion des candidats

La gestion des candidats est le processus d'identification des exigences de version logicielle et des risques potentiels pour le matériel et les ensembles de fonctionnalités activés particuliers. Il est recommandé qu'une organisation passe quatre à huit heures à effectuer des recherches appropriées sur les exigences logicielles, les notes de version, les défauts logiciels et les risques potentiels avant de piloter une version. Les éléments suivants constituent la base de la gestion des candidats :

- Identifier les candidats logiciels via les outils Cisco Connection Online (CCO).
- Maturité du logiciel d'analyse des risques, nouvelle fonctionnalité ou prise en charge du code.
- Identifier et suivre les bogues, problèmes et exigences logiciels connus tout au long du cycle de vie.
- Identifiez le comportement de configuration par défaut de l'image sélectionnée.
- Tenir à jour les candidats reportés et reportés pour les changements éventuels de candidats.
- Les bugs.
- Prise en charge des services avancés Cisco.

L'identification des candidats logiciels est devenue plus complexe avec le nombre croissant de productions et de formations logicielles Cisco. CCO dispose désormais de plusieurs outils, dont le planificateur de mise à niveau Cisco IOS, l'outil de recherche de logiciels, la matrice de compatibilité logicielle-matérielle et l'outil de mise à niveau produit, qui peuvent aider les entreprises à identifier les candidats potentiels à une version. Ces outils sont disponibles à l'adresse <http://www.cisco.com/cisco/software/navigator.html>.

Ensuite, analysez le risque du logiciel candidat potentiel. Il s'agit du processus de compréhension de l'emplacement actuel du logiciel sur la courbe de maturité, puis de l'évaluation des exigences de déploiement avec le risque potentiel du candidat à la version. Par exemple, si une organisation souhaite mettre un logiciel de déploiement précoce (ED) dans un environnement de haute disponibilité critique, il convient de tenir compte des risques et des ressources associés pour obtenir une certification réussie. Une organisation doit au moins ajouter des ressources de gestion logicielle pour les situations à risque plus élevé afin d'assurer le succès. D'un autre côté, si une version de déploiement général (GD) répond aux besoins d'une organisation, alors moins de ressources de gestion logicielle sont nécessaires.

Lorsque des versions et des risques potentiels sont identifiés, exécutez un nettoyage des bogues pour déterminer s'il existe des bogues catastrophiques identifiés qui pourraient empêcher la certification. Les agents Bug Watcher, Bug Navigator et Bug Watcher de Cisco peuvent aider à identifier les problèmes potentiels et doivent être utilisés tout au long du cycle de vie du logiciel pour identifier les problèmes potentiels de sécurité ou de défaut.

Un nouveau logiciel candidat doit également être examiné pour déterminer son comportement de

configuration par défaut potentiel. Pour ce faire, vous pouvez consulter les notes de version de la nouvelle image logicielle et examiner les différences de configuration avec l'image potentielle chargée sur les plates-formes désignées. La gestion des candidats peut également inclure l'identification des versions de retour ou de retour si la version choisie ne satisfait pas aux critères de certification à un moment donné du processus. En observant les bogues liés aux fonctionnalités d'une piste spécifique, une organisation peut conserver les candidats potentiels à la certification.

Les services avancés Cisco constituent également un excellent outil de gestion des candidats. Ce groupe peut fournir des informations complémentaires sur le processus de développement et la collaboration entre un grand nombre d'experts de l'industrie dans de nombreux environnements de marché vertical différents. En règle générale, les meilleures fonctions de nettoyage des bogues ou de gestion des candidats existent au sein de l'assistance Cisco, en raison du niveau d'expertise et de visibilité sur les versions logicielles de production exécutées dans d'autres organisations.

## Test et validation

Les tests et la validation sont un aspect essentiel des meilleures pratiques de gestion et de la mise en réseau haute disponibilité, dans l'ensemble. Des tests en laboratoire appropriés peuvent réduire considérablement les temps d'arrêt de la production, aider à former le personnel d'assistance réseau et aider à rationaliser les processus de mise en oeuvre du réseau. Toutefois, pour être efficace, l'organisation doit allouer les ressources nécessaires pour créer et maintenir l'environnement de laboratoire approprié, utiliser les ressources nécessaires pour effectuer les tests appropriés et utiliser une méthodologie de test recommandée qui inclut la collecte de mesures. Sans ces éléments, un processus de test et de validation peut ne pas répondre aux attentes d'une organisation.

La plupart des entreprises ne disposent pas de l'environnement de laboratoire de test recommandé. Pour cette raison, de nombreuses entreprises ont déployé des solutions incorrectement, ont connu des pannes de modification du réseau ou ont rencontré des problèmes logiciels qui auraient pu être isolés dans un environnement de laboratoire. Dans certains environnements, cela est acceptable, car le coût des temps d'arrêt ne compense pas le coût d'un environnement de laboratoire sophistiqué. Cependant, dans de nombreuses entreprises, les temps d'arrêt ne peuvent être tolérés. Ces organisations sont vivement invitées à développer les laboratoires de test, les types de tests et les méthodologies de test recommandés pour améliorer la qualité du réseau de production.

## **Travaux pratiques et environnement**

Le TP doit être un espace isolé avec suffisamment d'espace pour les bureaux, les bancs de travail, les équipements d'essai et les armoires ou les bâtis d'équipement. La plupart des grandes entreprises auront besoin de quatre à dix racks d'équipement pour imiter l'environnement de production. Une certaine sécurité physique est recommandée pour aider à maintenir un environnement de test pendant que les tests sont en cours. Cela permet d'éviter qu'un test de laboratoire ne soit perturbé en raison d'autres priorités de TP, notamment l'emprunt de matériel, la formation ou les répétitions de mise en oeuvre. La sécurité logique est également recommandée pour empêcher les fausses routes d'entrer dans le réseau de production ou le trafic indésirable de quitter les travaux pratiques. Pour ce faire, vous pouvez utiliser des filtres de routage et des listes d'accès étendues sur un routeur de passerelle de travaux pratiques. La connectivité au réseau de production est utile pour les téléchargements de logiciels et l'accès au réseau de travaux pratiques à partir de l'environnement de production.

La topologie des travaux pratiques doit être capable d'imiter l'environnement de production pour tout plan de test spécifique. Il est recommandé de reproduire le matériel, la topologie du réseau et les configurations des fonctions. Bien sûr, reproduire la topologie réelle est presque impossible, mais ce qui peut être fait est de reproduire la hiérarchie du réseau et l'interaction entre les périphériques de production. Ceci est important pour l'interaction de protocole ou de fonctionnalité entre plusieurs périphériques. Certaines topologies de test seront différentes en fonction des exigences des tests logiciels. Le test de la périphérie WAN Cisco IOS, par exemple, ne doit pas nécessiter de périphériques de type LAN ou de test et peut uniquement nécessiter des routeurs de périphérie WAN et des routeurs de distribution WAN. La clé est d'imiter la fonctionnalité logicielle sans dupliquer la production. Dans certains cas, des outils peuvent même être utilisés pour simuler des comportements à grande échelle, tels que le nombre de voisins de protocole et les tables de routage.

Des outils sont également nécessaires pour aider à certains types de tests en améliorant la capacité à imiter l'environnement de production et à collecter des données de test. Les outils qui permettent de simuler la production incluent les collecteurs de trafic, les générateurs de trafic et les périphériques de simulation WAN. Smartbits est un bon exemple de périphérique capable de collecter et de relayer le trafic réseau ou de générer de grands volumes de trafic. Une entreprise peut également bénéficier de périphériques qui peuvent aider à collecter des données, tels que des analyseurs de protocole.

Le TP nécessite également une certaine gestion. De nombreuses grandes entreprises ont un responsable de laboratoire à temps plein qui est chargé de gérer le réseau des travaux pratiques. D'autres organisations utilisent les équipes d'architecture et d'ingénierie existantes pour la validation des travaux pratiques. Les responsabilités de gestion des travaux pratiques comprennent la commande d'équipements de TP et le suivi des ressources, le câblage, la gestion de l'espace physique, la définition des règles et de l'orientation des travaux pratiques, la planification des travaux pratiques, la documentation des travaux pratiques, la configuration des topologies de TP, la rédaction de plans de test, l'exécution de tests de laboratoire et la gestion des problèmes potentiels identifiés.

## **Types de tests**

Dans l'ensemble, il existe de nombreux types de tests différents qui peuvent être effectués. Avant d'élaborer un laboratoire de test et un plan de test complet capable de tout tester dans une multitude de configurations, une entreprise doit comprendre les différents types de tests, l'objectif des tests et savoir si l'ingénierie, le marketing technique ou la défense des clients de Cisco doivent ou peuvent être responsables de certains des tests. Les plans de test des clients couvrent généralement les types de test les plus exposés. Le tableau suivant permet de comprendre les différents types de tests, le moment où les tests doivent être effectués et les parties responsables.

Parmi les tests ci-dessous, les tests appropriés de l'ensemble de fonctionnalités, de la topologie et de la combinaison d'applications spécifiques d'une organisation sont généralement les plus utiles. Il est important de savoir que Cisco effectue des tests de régression et de fonctionnalités complets. Toutefois, Cisco ne peut pas tester le profil d'application de votre entreprise avec votre combinaison spécifique de topologie, de matériel et de fonctionnalités configurées. En fait, il est impossible de tester l'ensemble des fonctionnalités, du matériel, des modules et des permutations topologiques. En outre, Cisco ne peut pas tester l'interopérabilité avec des équipements tiers. Cisco recommande aux entreprises de tester la combinaison précise de matériel, de modules, de fonctionnalités et de topologie dans leur environnement. Ces tests doivent être effectués dans un laboratoire, avec une topologie réduite représentant l'environnement de production de votre entreprise et d'autres types de tests pris en charge, tels que les performances, l'interopérabilité, les pannes et la mise à feu.



Tester	Présentation du test	Responsabilité du test
Fonctionnalités	<p>Détermine si les fonctions de base de Cisco IOS et les modules matériels Cisco fonctionnent comme annoncé. Les fonctionnalités ou les modules ainsi que les options de configuration des fonctionnalités doivent être testés. La suppression et l'ajout de la configuration doivent être testés. Les tests de base sur les pannes et les tests de combustion sont inclus.</p>	Test des périphériques Cisco
Régression	<p>Détermine si la fonction ou le module fonctionne conjointement avec d'autres modules et fonctions, et si la version de Cisco IOS fonctionne conjointement avec d'autres versions de Cisco IOS par rapport aux fonctionnalités définies. Comprend des tests de mise en mémoire et de panne.</p>	Test de régression Cisco

<p>Performances de base des périphériques</p>	<p>Détermine les performances de base de la fonction ou du module pour déterminer si la fonction Cisco IOS ou les modules matériels répondent aux exigences minimales sous charge.</p>	<p>Test des périphériques Cisco</p>
<p>Combinaison topologique/fonctionnalité/matériel</p>	<p>Détermine si les fonctions et les modules fonctionnent comme prévu dans une topologie spécifique et dans une combinaison module/fonctionnalité/matériel . Ces tests doivent inclure la vérification du protocole, la vérification des fonctions, la vérification de la commande <b>show</b>, les tests de mise en mémoire et les tests de panne.</p>	<p>Cisco teste les topologies standard annoncées dans les laboratoires, telles que l'ingénierie des solutions d'entreprise (ESE) et l'ingénierie des tests d'intégration des solutions en réseau (NSITE). Les clients à haute disponibilité doivent tester les combinaisons de fonctions/modules/topologies selon les besoins, en particulier avec les logiciels les plus utilisés et les topologies non standard.</p>
<p>Panne (What-if)</p>	<p>Inclut les types ou les comportements d'arrêt courants qui peuvent survenir dans un environnement de fonction/module/topologie spécifique et l'impact potentiel sur les</p>	<p>Cisco est responsable des tests de panne de base. Les clients sont en fin de compte responsables des problèmes de performances liés à l'évolutivité de leur environnement individuel. Les tests d'interruption doivent être effectués, si possible, dans</p>

	<p>fonctionnalités. Les tests d'interruption incluent le remplacement de cartes, les basculements de liaison, les pannes de périphériques, les pannes de liaison et les pannes de cartes.</p>	<p>l'environnement de laboratoire du client.</p>
<p>Network Performance (What-if)</p>	<p>Analyse la charge des périphériques par rapport à une combinaison de fonction/matériel/topologie spécifique. L'accent est mis sur la capacité et les performances des périphériques tels que le processeur, la mémoire, l'utilisation de la mémoire tampon et l'utilisation des liaisons par rapport à un type de trafic défini et aux besoins en ressources pour les protocoles, les voisins, le nombre de routes et d'autres fonctionnalités. Le test permet d'assurer l'évolutivité dans les</p>	<p>En fin de compte, les clients sont responsables de la charge et de l'évolutivité des périphériques. Les problèmes de charge et d'évolutivité sont souvent soulevés par les services de vente ou les services avancés de Cisco et sont souvent testés avec des laboratoires Cisco tels que les laboratoires de démonstration de faisabilité du client (CPOC).</p>

	environnements plus grands.	
Correction de bogues	Garantit que les corrections de bogues réparent le défaut identifié.	Cisco teste les corrections de bogues pour s'assurer que le bogue est corrigé. Les clients doivent également tester pour s'assurer que le bogue qu'ils ont connu est corrigé et que le bogue ne casse aucun autre aspect du module ou de la fonctionnalité. Les versions de maintenance sont testées par régression, mais les versions intermédiaires ne le sont généralement pas.
Gestion de réseau CSNA	Analyse les fonctionnalités de gestion SNMP (Simple Network Management Protocol), la précision des variables MIB SNMP, la prise en charge des interruptions et la prise en charge de Syslog.	Cisco est chargé de tester les fonctions SNMP de base, les fonctionnalités et la précision des variables MIB. Les clients doivent valider les résultats de la gestion du réseau et sont en fin de compte responsables de la stratégie et de la méthodologie de gestion des nouveaux déploiements technologiques.
Émulation réseau à grande échelle	L'émulation de réseau à grande échelle utilise des outils tels que le simulateur de routeur Agilent et la suite d'outils de test Spirent	Les clients Cisco sont généralement responsables des aspects des tests de simulation de réseau qui reproduisent leur environnement réseau, qui peuvent inclure le nombre de voisins/contiguïtés

	<p>pour simuler des environnements plus importants. Il peut s'agir des voisins de protocole, du nombre de circuits virtuels permanents (PVC) Frame Relay, des tailles de tables de routage, des entrées de cache et d'autres ressources généralement requises en production qui ne se trouvent pas par défaut dans les travaux pratiques.</p>	<p>de protocole de routage et les tailles de table de routage associées ainsi que d'autres ressources en production.</p>
<p>Interopérabilité</p>	<p>Teste tous les aspects relatifs à la connectivité à un équipement réseau tiers, en particulier si l'interopérabilité du protocole ou de la signalisation est requise.</p>	<p>Les clients Cisco sont généralement responsables de tous les aspects des tests d'interopérabilité.</p>
<p>Gravure</p>	<p>Analyse les ressources du routeur au fil du temps. Les tests de gravure nécessitent généralement qu'un périphérique soit soumis à une certaine charge avec</p>	<p>Cisco effectue des tests de démarrage de base. Il est recommandé de procéder à des tests auprès des clients en fonction de combinaisons uniques de topologie, de périphériques et de fonctionnalités.</p>

	une étude sur l'utilisation des ressources, notamment la mémoire, le processeur et les tampons au fil du temps.	
--	---	--

## Méthodologie de test

Une fois qu'une organisation sait ce qu'elle teste, il faut élaborer une méthodologie pour le processus de test. L'objectif d'une méthodologie d'analyse des meilleures pratiques est de faire en sorte que les tests convenus soient complets, bien documentés, facilement reproductibles et utiles pour trouver des problèmes de production potentiels. La documentation et la recréation de scénarios de travaux pratiques sont particulièrement importantes pour tester les versions ultérieures ou pour tester les corrections de bogues trouvées dans l'environnement de travaux pratiques. Les étapes d'une méthodologie d'essai sont présentées ci-dessous. Certaines étapes de test peuvent également être effectuées simultanément.

1. Créez une topologie de test qui simule l'environnement de production testé. Un environnement de test de périphérie de réseau étendu peut inclure quelques routeurs principaux et un seul routeur de périphérie, tandis qu'un test de réseau local peut inclure davantage de périphériques qui peuvent le mieux représenter l'environnement.
2. Configurez les fonctionnalités qui simulent l'environnement de production. La configuration des équipements de laboratoire doit correspondre étroitement aux configurations matérielles et logicielles attendues des équipements de production.
3. Écrire un plan de test, définir des tests et des objectifs, documenter la topologie et définir des tests fonctionnels. Les tests incluent la validation de protocole de base, la validation de la commande show, les tests de panne et les tests de mise à feu. Le tableau ci-dessous présente un exemple de test spécifique dans un plan de test.
4. Valider le routage et la fonctionnalité de protocole. Document ou ligne de base attendu **show** résultats de commande. Les protocoles doivent inclure à la fois les protocoles de couche 2 tels que ATM, Frame Relay, Cisco Discovery Protocol (CDP), Ethernet et Spanning Tree, ainsi que les protocoles de couche 3 tels que IP, IPX et multidiffusion.
5. Valider la fonctionnalité de la fonction. Document ou ligne de base attendu **show** résultats de commande. Les fonctionnalités peuvent inclure des commandes de configuration globale et toutes les fonctionnalités critiques telles que l'authentification, l'autorisation et la comptabilité (AAA).
6. Simuler la charge, ce qui serait attendu dans l'environnement de production. La simulation de charge peut être faite avec des collecteurs de trafic / générateurs. Validez les variables d'utilisation des périphériques réseau attendues, y compris le processeur, la mémoire, l'utilisation de la mémoire tampon et les statistiques d'interface, en enquêtant sur toute perte de paquets. Document ou ligne de base attendu **show** résultats de commande.
7. Effectuer des tests d'arrêt lorsque le périphérique et le logiciel sont censés traiter ou empêcher une charge insuffisante. Par exemple, retrait de carte, battement de liaison, battement de route et tempêtes de diffusion. Assurez-vous que les interruptions SNMP correctes sont générées en fonction des fonctionnalités utilisées sur le réseau.
8. Les résultats des essais et les mesures des dispositifs doivent être reproductibles.

<b>Nom du test</b>	<b>Basculement du protocole HSRP (Hot Standby Router Protocol)</b>
<b>Configuration des tests requise</b>	Appliquez la charge à l'interface de la passerelle principale. Le trafic doit être d'environ 20 % vers la passerelle du point de vue de la station utilisateur et de 60 % vers celui de la station utilisateur. En outre, augmentez la charge du trafic.
<b>Étapes de test</b>	Surveillez STP et HSRP via les commandes <b>show</b> . Échec de la connexion de l'interface de passerelle principale, puis récupération de la connexion après collecte des informations.
<b>Mesures prévues</b>	Processeur pendant le basculement. Affichez l'interface avant, pendant et après pour la passerelle principale et secondaire. Affichez HSRP avant, pendant et après.
<b>Résultats escomptés</b>	La passerelle principale bascule vers l'autre passerelle du routeur en deux secondes. <b>les</b> commandes <b>show</b> reflètent correctement la modification. Le basculement vers la passerelle principale se produit lorsque la connectivité est restaurée.
<b>Résultats réels</b>	
<b>Réussite ou échec</b>	
<b>Modifications requises pour obtenir la réussite</b>	

## Mesures des périphériques

Au cours de la phase d'essai, effectuez et documentez les mesures suivantes pour vous assurer que le périphérique fonctionne correctement :

- Utilisation de la mémoire
- Charges du processeur
- Utilisation de la mémoire tampon
- Statistiques d'interface
- Tables de routage
- Débogage spécifique

Les informations relatives aux mesures varient en fonction de l'essai particulier mis en oeuvre. Il peut également y avoir des renseignements supplémentaires à mesurer en fonction des questions particulières qui sont abordées.

Pour chaque application testée, mesurez les paramètres afin de s'assurer qu'il n'y a pas d'impact négatif sur les performances de l'application donnée. Pour ce faire, on utilise une base de performances qui permet de comparer les performances avant et après le déploiement. Exemples de tests de mesure d'application :

- Temps moyen nécessaire pour se connecter à un réseau.
- Temps moyen nécessaire à NFS pour copier un groupe de fichiers.
- Temps moyen nécessaire au lancement d'une application et à l'affichage du premier écran.
- Autres paramètres spécifiques à l'application.

## Mise en oeuvre : déploiement rapide et réussi de Cisco IOS

Un processus de mise en oeuvre bien défini permet à une entreprise de déployer efficacement de nouvelles versions de Cisco IOS.

La phase de mise en oeuvre comprend le processus pilote et le processus de mise en oeuvre. Le processus pilote garantit la réussite de la version de Cisco IOS dans l'environnement et le processus de mise en oeuvre permet des déploiements Cisco IOS rapides et réussis à grande échelle.

## Stratégie et outils pour les déploiements Cisco IOS

La stratégie de déploiement de Cisco IOS consiste à effectuer une certification finale via un processus pilote et un déploiement rapide à l'aide d'outils de mise à niveau et d'un processus de mise en oeuvre bien défini.

Avant de lancer un processus pilote de réseau, de nombreuses entreprises élaborent des directives générales pour les projets pilotes. Les lignes directrices du pilote devraient inclure les attentes de tous les pilotes, comme les critères de réussite, les emplacements de pilotes acceptables, la documentation du pilote, les attentes du pilote propriétaire, les exigences de notification des utilisateurs et les durées de pilotes prévues. Une équipe interfonctionnelle d'ingénierie, de mise en oeuvre et d'exploitation participe normalement à l'élaboration de lignes directrices générales et d'un processus pilote. Une fois le processus pilote créé, les groupes de mise en oeuvre individuels peuvent normalement mener des projets pilotes réussis en utilisant les meilleures pratiques identifiées.

Une fois qu'une nouvelle version logicielle a été approuvée pour le déploiement et la certification finale, l'entreprise doit commencer à planifier la mise à niveau de Cisco IOS. La planification commence par l'identification des nouvelles exigences en matière d'image, notamment la plateforme, la mémoire, la mémoire flash et la configuration. Les groupes d'architecture et d'ingénierie définissent généralement de nouvelles exigences en termes d'image logicielle dans la phase de gestion candidate du cycle de vie de la gestion Cisco IOS. Une fois les besoins identifiés, chaque périphérique doit être validé et éventuellement mis à niveau par le groupe de mise en oeuvre. Le module SWIM (Software Image Manager) de CiscoWorks2000 peut également effectuer l'étape de validation en validant les exigences de Cisco IOS par rapport à l'inventaire des périphériques. Lorsque tous les périphériques ont été validés et/ou mis à niveau conformément aux nouvelles normes d'image correctes, le groupe de mise en oeuvre peut commencer un processus de mise en oeuvre lent en utilisant le module SWIM de CiscoWorks2000 comme outil de déploiement logiciel.

Une fois que la nouvelle image a été déployée avec succès plusieurs fois, l'entreprise peut



commencer un déploiement rapide à l'aide de CiscoWorks SWIM.

## Gestion de l'inventaire Cisco IOS

CiscoWorks2000 Resource Manager Essentials (RME) Inventory Manager simplifie considérablement la gestion des versions des routeurs et des commutateurs Cisco grâce à des outils de création de rapports basés sur le Web qui permettent de signaler et de trier les périphériques Cisco IOS en fonction de la version du logiciel, de la plate-forme du périphérique et du nom du périphérique.

## SWIM Cisco IOS

La fonction SWIM de CiscoWorks2000 peut aider à réduire la complexité du processus de mise à niveau sujette aux erreurs. Des liens intégrés vers CCO établissent une corrélation entre les informations en ligne de Cisco sur les correctifs logiciels et les logiciels Cisco IOS et Catalyst déployés sur le réseau, en mettant en évidence les notes techniques associées. Les nouveaux outils de planification détectent les exigences du système et envoient des notifications lorsque des mises à niveau matérielles (ROM de démarrage, mémoire vive flash) sont nécessaires pour prendre en charge les mises à jour d'images logicielles proposées.

Avant le lancement d'une mise à jour, les conditions préalables d'une nouvelle image sont validées par rapport au commutateur cible ou aux données d'inventaire du routeur pour garantir la réussite de la mise à niveau. Lorsque plusieurs périphériques sont mis à jour, SWIM synchronise les tâches de téléchargement et permet à l'utilisateur de surveiller la progression du travail. Les tâches planifiées sont contrôlées par le biais d'un processus de validation, ce qui permet aux responsables d'autoriser les activités d'un technicien avant d'entreprendre chaque tâche de mise à niveau. RME 3.3 inclut la possibilité d'analyser les mises à niveau logicielles des plates-formes Cisco IGX, BPX et MGX, ce qui simplifie et réduit considérablement le temps nécessaire pour déterminer l'impact d'une mise à niveau logicielle.

## [Processus pilote](#)

Afin de minimiser l'exposition potentielle et de capturer plus en toute sécurité les problèmes de production restants, un pilote logiciel est recommandé. Les pilotes sont généralement plus importants pour les déploiements de nouvelles technologies, mais de nombreux nouveaux déploiements de logiciels seront liés à de nouveaux services, fonctionnalités ou matériels, où un pilote est plus critique. Le plan pilote individuel devrait tenir compte de la sélection des pilotes, de la durée du pilote et de la mesure. La sélection des pilotes consiste à déterminer quand et où un pilote doit être effectué. La mesure pilote est le processus de collecte des données nécessaires pour identifier les succès et les échecs ou les problèmes potentiels.

La sélection du pilote indique où et comment un pilote sera effectué. Un pilote peut commencer par un périphérique situé dans une zone à faible impact et s'étendre à plusieurs périphériques situés dans une zone à plus fort impact. Voici quelques éléments à prendre en considération pour la sélection des pilotes où l'impact peut être réduit :

- Installé dans une zone du réseau résiliente à un seul périphérique en raison de la redondance.
- Dans une zone du réseau avec un nombre minimal d'utilisateurs derrière le périphérique sélectionné qui peuvent gérer un impact possible sur la production.
- Songez à séparer le projet pilote en fonction des architectures. Par exemple, pilotez-le dans les couches d'accès, de distribution et/ou coeur de réseau.

La durée de ce pilote doit être fonction du temps nécessaire pour tester et évaluer suffisamment toutes les caractéristiques du périphérique. Cela doit inclure à la fois le système de connexion par câble et le réseau sous des charges de trafic normales. La durée dépend également de l'étape de mise à niveau du code et de la zone du réseau sur laquelle s'exécute Cisco IOS. Si Cisco IOS est une nouvelle version majeure, une période pilote plus longue est préférable. Alors que si la mise à niveau est une version de maintenance avec un minimum de nouvelles fonctionnalités, une période pilote plus courte suffira.

Au cours de la phase pilote, il est important de surveiller et de documenter les résultats de la même manière que les essais initiaux. Cela peut inclure des enquêtes sur les utilisateurs, la collecte de données pilotes, la collecte de problèmes et les critères de réussite/échec. Les personnes devraient être directement responsables du suivi et du suivi des progrès des projets pilotes afin de s'assurer que tous les problèmes sont identifiés et que les utilisateurs et les services qui participent au projet pilote sont satisfaits des résultats des projets pilotes. La plupart des organisations certifieront une version si elle réussit dans un environnement pilote ou de production. Cette étape est un échec critique dans certains environnements en raison d'un succès perçu lorsqu'aucun critère de mesure ou de réussite n'est identifié ou documenté.

## Mise en oeuvre

Une fois la phase pilote terminée au sein du réseau de production, commencez la phase de mise en oeuvre de Cisco IOS. La phase de mise en oeuvre comprend plusieurs étapes pour assurer le succès et l'efficacité de la mise à niveau logicielle, notamment le démarrage lent de la mise en oeuvre, la certification finale, la préparation de la mise à niveau, l'automatisation de la mise à niveau et la validation finale.

La mise en oeuvre lente est le processus de mise en oeuvre lente d'une nouvelle version testée pour s'assurer que l'image est pleinement exposée à l'environnement de production avant la certification finale et la conversion à grande échelle. Certaines entreprises peuvent commencer par un appareil et une journée d'exposition avant de passer à deux mises à niveau le lendemain et peut-être quelques-unes le lendemain. Lorsqu'une dizaine de périphériques ont été mis en production, l'entreprise peut attendre jusqu'à une ou deux semaines avant la certification finale de la version Cisco IOS particulière. Une fois la certification finale obtenue, l'entreprise peut déployer plus rapidement la version identifiée avec un niveau de confiance beaucoup plus élevé.

Après le processus de démarrage lent, tous les périphériques identifiés pour la mise à niveau doivent être examinés et validés à l'aide de l'inventaire des périphériques et d'une matrice des normes minimales de Cisco IOS pour le bootstrap, la DRAM et la mémoire Flash afin de s'assurer que les exigences sont respectées. Les données peuvent être acquises par le biais d'outils internes, d'outils SNMP tiers ou à l'aide de CiscoWorks2000 RME. Le SWIM CiscoWorks2000 examine ou inspecte ces variables avant leur mise en oeuvre. Cependant, il est toujours judicieux de savoir à quoi s'attendre lors des tentatives de mise en oeuvre.

Si plus d'une centaine de périphériques similaires sont prévus pour des mises à niveau, il est fortement recommandé d'utiliser une méthode automatisée. Il a été démontré que l'automatisation améliore l'efficacité de la mise à niveau et améliore le pourcentage de réussite de la mise à niveau des périphériques lors de déploiements de grande envergure, sur la base d'une mise à niveau interne de 1 000 périphériques avec et sans SWIM. Cisco recommande que la fonction SWIM de CiscoWorks 2000 soit utilisée pour les déploiements importants en raison du niveau de vérification effectué lors de la mise à niveau. Si un problème est détecté, SWIM va même quitter une version de Cisco IOS. SWIM fonctionne en créant et en planifiant des tâches de mise à niveau, où une tâche est configurée avec les périphériques, les images de mise à niveau souhaitées et le temps

d'exécution de la tâche. Chaque tâche doit contenir douze mises à niveau de périphérique ou moins et jusqu'à douze tâches peuvent s'exécuter simultanément. SWIM vérifie également que la version de mise à niveau de Cisco IOS planifiée s'exécute correctement après la mise à niveau. Il est recommandé de prévoir environ vingt minutes pour chaque mise à niveau de périphérique (y compris la vérification). Avec cette formule, une entreprise peut mettre à niveau trente-six périphériques par heure. Cisco recommande également de mettre à niveau un maximum de cent périphériques chaque soir afin de réduire l'exposition potentielle aux problèmes.

Après une mise à niveau automatisée, une certaine validation doit être effectuée pour garantir le succès. L'outil SWIM de CiscoWorks2000 peut exécuter des scripts personnalisés après la mise à niveau afin d'effectuer d'autres vérifications. La vérification consiste à vérifier que le routeur dispose du nombre de routes approprié, à s'assurer que les interfaces logiques/physiques sont actives ou à vérifier que le périphérique est accessible. L'exemple de liste de contrôle suivant peut valider entièrement le succès d'un déploiement Cisco IOS :

- Le périphérique a-t-il redémarré correctement ?
- Le périphérique peut-il envoyer une requête ping et être accessible via les plates-formes NMS (Network Management System) ?
- Les interfaces attendues du périphérique sont-elles actives ?
- Le périphérique possède-t-il les contiguïtés de protocole de routage correctes ?
- La table de routage est-elle renseignée ?
- Le périphérique transmet-il le trafic correctement ?

## Opérations - Gestion de la mise en oeuvre de Cisco IOS haute disponibilité

Les meilleures pratiques de haute disponibilité de l'environnement Cisco IOS permettent de réduire la complexité du réseau, d'améliorer le temps de résolution des problèmes et d'améliorer la disponibilité du réseau. La section relative aux opérations de la gestion de Cisco IOS comprend des méthodologies de stratégie, d'outils et de meilleures pratiques recommandées pour la gestion de Cisco IOS.

Les meilleures pratiques pour les opérations de Cisco IOS incluent le contrôle de version logicielle, la gestion de Syslog Cisco IOS, la gestion des problèmes, la standardisation de la configuration et la gestion de la disponibilité. Le contrôle de version logicielle est le processus de suivi, de validation et d'amélioration de la cohérence logicielle dans les pistes logicielles identifiées. La gestion Syslog de Cisco IOS est le processus de surveillance proactive et d'action sur les messages Syslog de priorité supérieure générés par Cisco IOS. La gestion des problèmes consiste à collecter rapidement et efficacement des informations critiques sur les problèmes liés aux logiciels afin d'éviter les événements futurs. La standardisation de la configuration est le processus de normalisation des 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. La gestion de la disponibilité est le processus d'amélioration de la disponibilité basé sur des mesures, des objectifs d'amélioration et des projets d'amélioration.

## Stratégies et outils pour les opérations Cisco IOS

Il existe de nombreuses stratégies et outils de qualité pour aider à gérer les environnements Cisco IOS. La première stratégie clé pour les opérations de Cisco IOS 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 a ensuite la responsabilité de configurer et de maintenir les normes via le contrôle de version et les normes/contrôles de configuration de Cisco IOS.

La deuxième stratégie pour les opérations de Cisco IOS consiste à identifier et résoudre rapidement les pannes de réseau. Les problèmes réseau doivent généralement être identifiés par le groupe d'opérations avant que les utilisateurs ne les appellent. Les problèmes doivent également être résolus le plus rapidement possible sans autre impact ou changement dans l'environnement. Quelques bonnes pratiques dans ce domaine sont la gestion des problèmes et la gestion Syslog de Cisco IOS. Cisco Output Interpreter est un outil permettant de diagnostiquer rapidement les pannes du logiciel Cisco IOS.

La troisième stratégie est une amélioration constante. 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 éliminent ou réduisent l'impact des pannes. L'organisation peut également examiner les problèmes courants et élaborer des processus pour les résoudre plus rapidement.

Les outils pour les opérations Cisco IOS incluent la gestion de l'inventaire pour le contrôle de version logicielle (CiscoWorks2000 RME), la gestion Syslog pour gérer les messages Syslog et les gestionnaires de configuration de périphérique pour gérer la cohérence de la configuration des périphériques.

## **Gestion Syslog**

Les messages Syslog sont des messages envoyés par le périphérique à un serveur de collecte. Ces messages peuvent être des erreurs (par exemple, une liaison s'arrêtant) ou des informations, par exemple lorsqu'une personne est entrée pour configurer un terminal sur un périphérique.

Les outils de gestion Syslog consignent et suivent les messages Syslog reçus par les routeurs et les commutateurs. Certains outils disposent de filtres permettant de supprimer les messages indésirables qui peuvent nuire aux messages importants. Les outils Syslog doivent également permettre la création de rapports en fonction des messages reçus. Les rapports peuvent être affichés par période, périphérique, type de message ou priorité de message.

L'outil Syslog le plus utilisé pour la gestion de Cisco IOS est CiscoWorks2000 RME Syslog Manager. D'autres outils sont disponibles dont SL4NT, un programme shareware de [Netal](#) et Private I d'OpenSystems.

## **Gestionnaire de configuration de périphérique CiscoWorks**

CiscoWorks2000 Device Configuration Manager gère une archive active et fournit un moyen simple de mettre à jour les modifications de configuration sur plusieurs routeurs et commutateurs Cisco. Le gestionnaire de configuration surveille le réseau pour les modifications de configuration, met à jour l'archive lorsqu'une modification est détectée et consigne les informations de modification au service d'audit des modifications. Une interface utilisateur Web vous permet de rechercher dans l'archive des attributs de configuration spécifiques et de comparer le contenu de deux fichiers de configuration pour identifier facilement les différences.

## Interpréteur de sortie Cisco

Cisco Output Interpreter est un outil utilisé pour diagnostiquer les plantages forcés de logiciels. L'outil peut aider à identifier les défauts logiciels sans appeler le centre d'assistance technique Cisco (TAC), ou il peut être utilisé comme informations principales au centre d'assistance technique après un plantage logiciel forcé. Ces informations permettront généralement d'accélérer la résolution du problème, au moins en ce qui concerne la collecte des informations requises.

## 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, il n'est pas rare de voir des versions non standard dans le réseau, en particulier si le personnel du réseau et des opérations est important. Cela peut être dû à une nouvelle équipe non formée, à des commandes de démarrage mal configurées ou à des mises en oeuvre non contrôlées. Il est toujours judicieux de valider périodiquement les normes de version logicielle à l'aide d'outils tels que CiscoWorks 2000 RME qui permettent de trier tous les périphériques par version Cisco IOS. Lorsque des non-normes sont identifiées, elles doivent être immédiatement signalées et un rapport d'incident ou de modification doit être lancé pour amener la version à la norme identifiée.

## Gestion proactive des Syslog

La collecte, la surveillance et l'analyse Syslog sont des processus de gestion des pannes recommandés pour résoudre d'autres problèmes réseau spécifiques à Cisco IOS difficiles ou impossibles à identifier par d'autres moyens. La collecte, la surveillance et l'analyse Syslog permettent d'améliorer le temps de résolution des problèmes en identifiant et en résolvant de nombreuses pannes de manière proactive avant que des problèmes réseau plus graves ne soient rencontrés ou signalés par les utilisateurs. Syslog fournit également une méthode plus efficace de collecte d'une grande variété de problèmes par rapport à l'interrogation SNMP cohérente pour un grand nombre de variables MIB. La collecte, la surveillance et l'analyse Syslog s'effectuent à l'aide de la configuration Cisco IOS correcte, des outils de corrélation Syslog, tels que CiscoWorks2000 RME et/ou de la gestion des événements Syslog. La gestion des événements Syslog est effectuée en analysant les données Syslog collectées pour identifier les messages critiques, puis en transférant une alerte ou un déroutement à un gestionnaire d'événements pour notification et résolution en temps réel.

La surveillance Syslog nécessite la prise en charge d'outils NMS ou de scripts pour aider à analyser et à 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.

## Gestion des problèmes

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 dans les environnements plus grands. Ce processus doit inclure un certain degré de description des problèmes par défaut et des collections de commandes **show** appropriées avant de passer à un second niveau. La prise en charge du premier niveau ne doit jamais consister à supprimer des routes ou à recharger des périphériques. Optimalement, l'organisation de premier niveau doit rapidement collecter des informations et passer à un second niveau. En ne consacrant que quelques minutes de plus à l'identification des problèmes ou à la description des problèmes, une découverte des causes premières est beaucoup plus probable, permettant ainsi une solution de contournement, l'identification des travaux pratiques et la création de rapports de bogues. Le support de deuxième niveau doit être bien informé des types d'informations dont Cisco peut avoir besoin pour diagnostiquer un problème ou pour déposer un rapport de bogue. Cela inclut les vidages de mémoire, la sortie des informations de routage et la sortie de la commande **show** du périphérique.

## Normalisation de la configuration

Les normes de configuration globale des périphériques représentent la pratique consistant à maintenir les 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 à des ports, protocoles ou interfaces individuels. Les commandes de configuration globale affectent généralement l'accès aux périphériques, le comportement général des périphériques et la sécurité des périphériques. Dans Cisco IOS, cela inclut les commandes service, IP, vty, console port, logging, AAA/TACACS+, SNMP et banner. 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 (Domain Name System) 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 entreprises configurent même des périphériques similaires de manière périodique afin d'assurer la cohérence de la configuration globale ou d'examiner périodiquement les périphériques afin de déterminer les normes de configuration globale correctes. Les normes de configuration de protocole et d'interface représentent la pratique consistant à maintenir des normes de configuration d'interface et de protocole.

La cohérence de la configuration des protocoles et des interfaces 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 protocoles ou des interfaces 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 doivent inclure des descripteurs d'interface CDP, la configuration de mise en cache et d'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

**Remarque** : il est possible d'avoir d'autres normes de configuration spécifiques aux protocoles en fonction de ce qui est configuré dans le réseau.

Voici un exemple de normes IP :

- Taille du sous-réseau
- Espace d'adressage IP utilisé
- Protocole de routage utilisé
- 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. En fait, 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 le matériel, les logiciels, les liaisons/opérateurs, l'alimentation/environnement, la conception ou les erreurs/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 un processus d'amélioration de la qualité.

## Annexe A - Présentation des versions de Cisco IOS

La stratégie de mise à jour de la plate-forme logicielle Cisco IOS repose sur le développement de logiciels sains, l'assurance de la qualité et le délai de commercialisation rapide, qui sont essentiels au succès des réseaux des clients de Cisco.

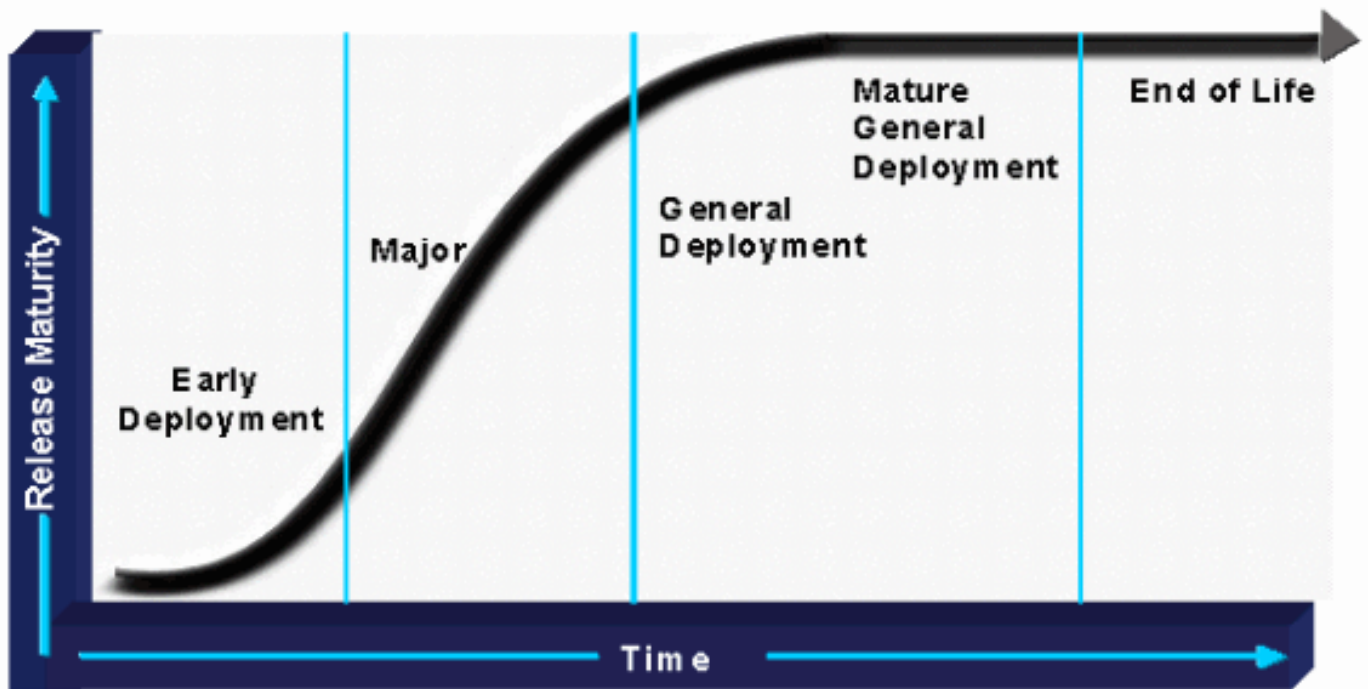
Le processus est défini autour de quatre catégories de versions, qui sont expliquées ci-dessous :

- Version de déploiement anticipé (ED)
- Version majeure
- Version de déploiement limité (LD)
- Version de déploiement général (GD)

Cisco crée et met à jour une [feuille de route IOS](#) qui contient des informations sur les versions individuelles, les marchés cibles, les chemins de migration, les nouvelles descriptions de fonctionnalités, etc.

La figure ci-dessous illustre le cycle de vie des versions du logiciel Cisco IOS :





## Versions ED

Les versions ED de Cisco IOS sont des véhicules qui apportent un nouveau développement sur le marché. Chaque révision de maintenance d'une version ED inclut non seulement des corrections de bogues, mais également un ensemble de nouvelles fonctionnalités, une nouvelle prise en charge de plate-forme et des améliorations générales des protocoles et de l'infrastructure Cisco IOS. Tous les deux ans, les fonctionnalités et les plates-formes des versions ED sont portées à la prochaine version principale de Cisco IOS.

Il existe quatre types de versions ED, chacune avec un modèle de version légèrement différent et des étapes de cycle de vie différents. Les versions ED peuvent être classées comme suit :

- **Versions CTED (Consolidation Technology Early Deployment)** - Le nouveau modèle de version de Cisco IOS utilise la série de versions ED consolidée, également connue sous le nom de série T, pour introduire de nouvelles fonctionnalités, de nouvelles plates-formes matérielles et d'autres améliorations à Cisco IOS. Ils sont appelés technologies consolidées car ils transcendent les définitions internes des unités commerciales (BU) et des divisions (LOB). Cisco IOS 11.3T, 12.0T et 12.1T sont des exemples de versions de technologie consolidée.
- **Versions de déploiement anticipé de technologies spécifiques (STED)** - Les versions de STED ont des caractéristiques d'engagement de fonctionnalités similaires à celles des versions de CTED, sauf qu'elles ciblent une technologie ou une zone de marché spécifique. Ils sont toujours disponibles sur des plates-formes spécifiques et sont uniquement sous la supervision d'une unité commerciale Cisco. Les versions STED sont identifiées à l'aide de deux lettres jointes à la version principale. Cisco IOS 11.3NA, 11.3MA, 11.3WA et 12.0DA sont des exemples de versions de STED.
- **Versions SMED (Specific Market Early Deployment)** - Les SMED Cisco IOS se différencient des STED par le fait qu'ils ciblent un segment de marché vertical spécifique (FAI, entreprises, institutions financières, sociétés Telcom, etc.). Les SMED incluent des caractéristiques technologiques spécifiques uniquement pour des plates-formes spécifiques présentant un intérêt et utilisées par le marché vertical prévu. Ils peuvent être différenciés des TED en

raison du fait qu'ils ne sont conçus que pour des plates-formes spécifiques présentant un intérêt pour le marché vertical, alors que les TED seraient conçues pour un plus grand nombre de plates-formes en fonction d'un besoin technologique plus large. Les versions SMED de Cisco IOS sont identifiées par un caractère alphabétique ajouté à la version de la version principale (comme le CTED). Cisco IOS 12.0S et 12.1E sont des exemples de SMED.

- **Versions de déploiement précoce de courte durée, également appelées versions X (XED)**—Les versions XED de Cisco IOS introduisent de nouveaux matériels et technologies sur le marché. Ils ne fournissent pas de révisions de maintenance logicielle et ne fournissent pas de révisions intermédiaires logicielles régulières. Si un défaut est détecté dans le XED avant sa convergence avec le CTED, une reconstruction logicielle est initiée et un numéro est ajouté au nom. Par exemple, les versions 12.0(2)XB1 et 12.0(2)XB2 de Cisco IOS sont des exemples de reconstructions 12.0(2)XB.

## Versions principales

Les principales versions sont les principaux véhicules de déploiement des produits de la plate-forme logicielle Cisco IOS. Ils sont gérés par la division technologique de Cisco IOS et consolident les fonctionnalités, les plates-formes, les fonctionnalités, la technologie et la prolifération des hôtes des versions ED précédentes. Les principales versions de Cisco IOS recherchent une plus grande stabilité et une meilleure qualité. Pour cette raison, les versions majeures n'acceptent pas l'ajout de fonctionnalités ou de plates-formes. Chaque révision de maintenance fournit uniquement des corrections de bogues. Par exemple, les versions 12.1 et 12.2 du logiciel Cisco IOS sont des versions principales.

Les versions principales ont des mises à jour de maintenance planifiées appelées versions de maintenance qui sont entièrement testées par régression, incorporent les correctifs de bogues les plus récents et ne prennent en charge aucune nouvelle plate-forme ou fonctionnalité. Le numéro de version d'une version principale identifie la version principale et son niveau de maintenance. Dans le logiciel Cisco IOS Version 12.0(7), 12.0 est le numéro de la version principale et 7 est son niveau de maintenance. Le numéro de version complet est 12.0(7). De même, 12.1 est une version majeure et 12.1(3) est la troisième version de maintenance du logiciel Cisco IOS principal version 12.1.

## Versions de déploiement limité (LD)

LD est la phase de maturité de Cisco IOS entre FCS et le déploiement général pour les versions principales. Les versions de la plate-forme logicielle Cisco IOS ED ne vivent que dans la phase de déploiement limitée, car elles n'obtiennent jamais la certification GD.

## Versions de déploiement général (GD)

À un moment ou à un autre du cycle de vie de la version, Cisco déclarera qu'une version majeure est prête pour la certification GD. Seule une version majeure peut atteindre le statut GD. Il respecte le jalon de la certification GD lorsque Cisco est convaincu que la version a été :

- Éprouvé grâce à une large exposition au marché dans divers réseaux.
- Qualifié par des mesures analysées pour la stabilité et les tendances des bogues.
- Qualifié par le biais d'enquêtes de satisfaction client.
- Une réduction de la tendance normalisée des clients a révélé des défauts dans la version par rapport aux quatre versions de maintenance précédentes.

Une équipe interfonctionnelle de certification GD de plaidoyer client composée d'ingénieurs TAC, d'ingénieurs AES (Advanced Engineering Services), d'ingénieurs de test système et d'ingénieurs

Cisco IOS est constituée pour évaluer chaque défaut exceptionnel de la version. Cette équipe donne l'approbation finale pour la certification GD. Une fois qu'une version atteint le statut GD, chaque révision ultérieure de la version est également GD. Par conséquent, une fois qu'un rejet est déclaré GD ; il entre automatiquement dans la phase de maintenance restreinte. Pendant cette phase, la modification technique du code, y compris les corrections de bogues avec refonte majeure du code, est strictement limitée et contrôlée par un responsable de programme. Cela garantit qu'aucun bogue indésirable n'est introduit dans une version certifiée GD du logiciel Cisco IOS. GD est réalisé par une version de maintenance particulière. Les mises à jour de maintenance ultérieures pour cette version sont également des versions de GD. Par exemple, la version 12.0 du logiciel Cisco IOS a obtenu la certification GD à 12.0(8). Ainsi, les versions du logiciel Cisco IOS 12.0(9), 12.0(10), etc. sont des versions GD.

## Images expérimentales ou diagnostiques

Les images expérimentales ou de diagnostic sont parfois appelées spécialisation en ingénierie et ne sont créées que lorsque des problèmes logiciels critiques ont été identifiés. Ces images ne font pas partie du processus de publication normal. Les images de cette catégorie sont des builds spécifiques au client conçues pour aider à diagnostiquer un problème, tester une correction de bogue ou fournir une correction immédiate. Une correction immédiate peut être fournie lorsqu'il n'est pas possible d'attendre la prochaine version intermédiaire ou de maintenance. Les images expérimentales ou de diagnostic peuvent être construites sur toute base logicielle prise en charge, y compris la maintenance ou les versions intermédiaires de tout type de version. Il n'existe pas de convention officielle d'attribution de noms, mais dans de nombreux cas le développeur ajoute des initiales, exp (pour expérimental) ou des chiffres supplémentaires au nom de l'image de base. Ces images ne sont prises en charge que de manière temporaire, en conjonction avec le développement de Cisco, car les opérations du TAC et de la version de Cisco IOS ne tiennent pas à jour la documentation de support, comme les tableaux de symboles ou l'historique des images de base. Ces images ne font l'objet d'aucun test interne de Cisco.

## Jalons des cycles de vie des versions

À un moment donné, les versions GD sont remplacées par les nouvelles versions par les dernières technologies de mise en réseau. Par conséquent, un processus de mise à la retraite a été établi avec les trois principales étapes suivantes :

- **Fin de vente (EOS)** : pour les versions principales, la date EOS est de trois ans après la date de première livraison commerciale (FCS). Cela définit une date finale pour laquelle la version peut être achetée pour de nouveaux systèmes. La version EOS continue d'être téléchargée à partir de Cisco Connection Online (CCO) pour les mises à niveau de maintenance.
- **Fin de l'ingénierie (EOE)** - La version EOE est la dernière version de maintenance de la version GD et suit généralement environ trois mois après la version EOS. Les clients peuvent continuer à bénéficier de l'assistance technique du centre d'assistance technique Cisco et télécharger la version EOE à partir de CCO. Le bulletin d'information sur les produits annonçant les versions et les dates des produits EOS et EOE est publié un an avant la date prévue de l'EOS. À ce stade, les clients doivent commencer à étudier la mise à niveau de leur logiciel Cisco IOS afin de tirer parti des dernières technologies réseau.
- **Fin de vie (EOL)** : à la fin du cycle de vie de la version, la prise en charge de la version du logiciel Cisco IOS est terminée et ne peut plus être téléchargée à la date de fin de vie. En général, la date de fin de vie est de cinq ans après la date de fin de vie. Un bulletin sur les produits en fin de vie est publié environ un an avant la date réelle de fin de vie.

## Convention de dénomination de version Cisco IOS

La convention de dénomination des images Cisco IOS fournit un profil complet de toutes les images publiées. Le nom inclut toujours l'identificateur de la version principale et l'identificateur de la version de maintenance. Le nom peut également inclure un désignateur de train, un désignateur de reconstruction (pour la version de maintenance), des désignateurs de fonctions spécifiques à une unité commerciale (BU) et des identificateurs de reconstruction spécifiques à une unité commerciale. Le format peut être ventilé comme suit :

**[x.y (z[p])] [A] [o [u(v[p])]] 12.1(8a)E6**

Section de la convention de dénomination	Explication
x.y	Une combinaison de deux identificateurs distincts (un ou deux) de chiffres séparés par un '.' qui identifie la valeur de version principale. Cette valeur est déterminée par le marketing Cisco IOS. Exemple : 12.1
z	Un à trois chiffres qui identifie la version de maintenance de x.y. Cela se produit toutes les huit semaines. Les valeurs sont 0 pour la version bêta, 1 pour la version FCS et 2 pour la première version de maintenance. Exemple : 12.1(2)
p	Un caractère alpha qui identifie une reconstruction de x.y(z). La valeur commence par une minuscule « a » pour la première reconstruction, puis « b », et ainsi de suite. Exemple : 12.1(2 bis)
A	<p>Une à trois lettres alpha sont l'indicateur du train de libération et sont obligatoires pour les versions CTED, STED et X. Il identifie également une famille de produits ou de plates-formes. Les versions de technologie ED utilisent deux lettres. La première lettre représente la technologie et la seconde est utilisée pour différencier. Exemple :</p> <ul style="list-style-type: none"> <li>A = Access Server/Dial technology (exemple:11.3AA)</li> <li>B = Broadband (exemple:12.2B)</li> <li>D = xDSL technology (exemple:12.2DA)</li> <li>E = Enterprise feature set (exemple:12.1E)</li> <li>H = SDH/SONET technology (exemple:11.3HA)</li> <li>N = Voice, Multimedia, Conference (exemple:11.3NA)</li> <li>M = Mobile (exemple:12.2MB)</li> <li>S = Service Provider (exemple:12.0S)</li> <li>T = Consolidated Technology (exemple:12.0T)</li> </ul>

	<p>W = ATM/LAN Switching/Layer 3 (example:12.0W5)</p> <p>Un « X » à la première position du nom de la version identifie une version unique basée sur le train « T » de la TED. Par exemple, XA, XB, XC, etc. Un « X » ou « Y » à la deuxième position du nom de la version identifie une version ED de courte durée basée sur une version STED ou associée à une version STED. Par exemple, 11.3NX (basé sur 11.3NA), 11.3WX (basé sur 11.3WA), etc.</p>
o	<p>Indicateur numérique facultatif à un ou deux chiffres qui identifie une reconstruction d'une valeur de libération particulière. Laissez vide si vous ne représentez pas une reconstruction. Commence par 1, puis 2, et ainsi de suite. Exemple : 12.1(2)T1, 12.1(2)XE2</p>
vous	<p>Indicateur numérique à un ou deux chiffres qui identifie la fonctionnalité de la version spécifique à l'unité commerciale. La valeur est déterminée par l'équipe marketing de l'unité commerciale. Exemple : 11.3(6)WA4, 12.0(1)W5</p>
v	<p>Indicateur numérique à un ou deux chiffres qui identifie la version de maintenance du code spécifique à la BU. Les valeurs sont 0 en version bêta, 1 en version FCS et 2 en tant que première version de maintenance. Exemple : 11.3(6)WA4(9), 12.0(1)W5(6)</p>
p	<p>Indicateur de caractères alpha qui identifie une reconstruction d'une version de technologie spécifique. La valeur commence par une minuscule « a » pour la première reconstruction, puis « b », et ainsi de suite. Exemple : 11.3(6)WA4(9a) serait une reconstruction de 11.3(6)WA4(9).</p>

Le graphique suivant indique les différentes sections de la convention d'attribution de noms Cisco IOS :



## Annexe B - Fiabilité de Cisco IOS

La fiabilité de la plate-forme logicielle Cisco IOS est un domaine dans lequel Cisco s'efforce en permanence d'améliorer ses performances. Avant de discuter des meilleures pratiques orientées client, il est nécessaire de comprendre la qualité et la fiabilité de Cisco IOS interne. Ces sections ont principalement pour but de fournir une vue d'ensemble des efforts plus récents de Cisco en matière de qualité logicielle Cisco IOS et des hypothèses que les clients doivent formuler en matière de fiabilité logicielle.

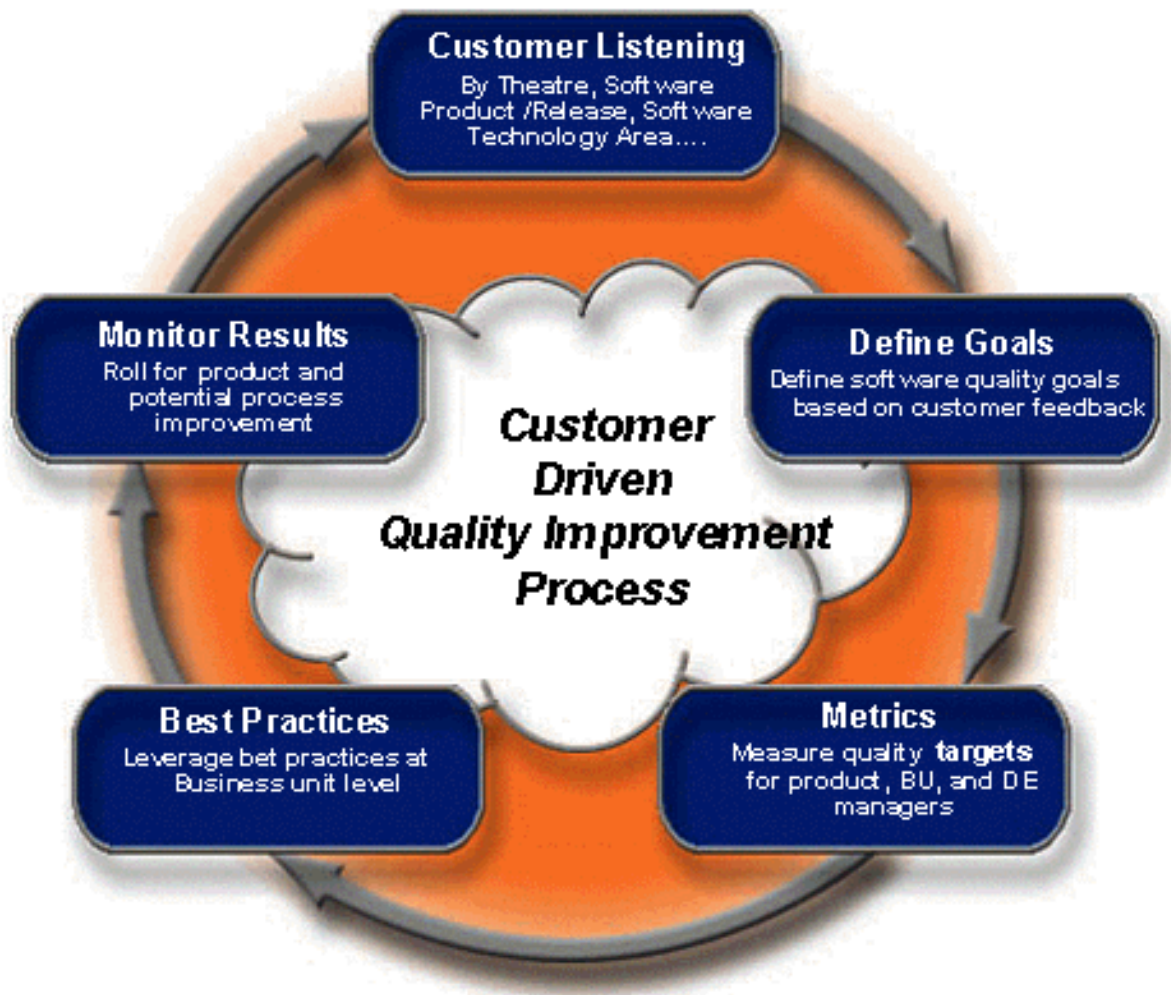
### Programme de qualité Cisco IOS

Cisco a un processus de développement IOS bien défini appelé GEM Great Engineering Methodology (GEM). Ce processus a un cycle de vie en trois phases :

- Stratégie et planification
- Exécution
- Déploiement

Les domaines généraux du cycle de vie incluent la hiérarchisation de l'introduction des fonctionnalités, le développement, le processus de test, les phases d'introduction des logiciels, le premier client expédié (FCS), le GD et l'ingénierie de maintenance. Cisco suit également un certain nombre de directives relatives aux meilleures pratiques en matière de qualité logicielle émanant d'organisations telles que l'Organisation internationale de normalisation (ISO), Telcordia (anciennement Bellcore), l'IEEE et l'Institut d'ingénierie logicielle Carnegie Mellon. Ces directives sont intégrées aux processus GEM de Cisco. Les processus de développement logiciel Cisco sont certifiés ISO 9001 (1994).

Le principal processus d'amélioration de la qualité du logiciel Cisco IOS est un processus piloté par le client, par lequel Cisco écoute les clients, définit les objectifs et les mesures, met en oeuvre les meilleures pratiques et surveille les résultats. Une équipe interorganisationnelle qui s'engage à améliorer la qualité des logiciels est le moteur de ce processus. Un schéma du processus d'amélioration de la qualité de Cisco IOS est présenté ci-dessous :



Le processus d'amélioration de la qualité a des objectifs mesurables distincts pour l'exercice 2002 et au-delà. L'objectif principal de ces objectifs est de réduire les défauts en identifiant les problèmes logiciels plus tôt dans le cycle de test, de réduire l'arriéré de défauts, d'améliorer la cohérence des fonctionnalités et la clarté des versions logicielles, et de fournir des calendriers de publication prévisibles et cohérents ainsi que la qualité des logiciels. Parmi les initiatives prises dans ces domaines figurent de nouveaux outils de couverture de test (identifiant les zones où la couverture de test est plus faible), l'amélioration du processus de correction de test et les améliorations des tests de régression du système Cisco IOS. Des ressources supplémentaires ont été mises en oeuvre pour résoudre ces problèmes et des engagements exécutifs et interfonctionnels ont été pris pour toutes les versions principales du logiciel Cisco IOS.

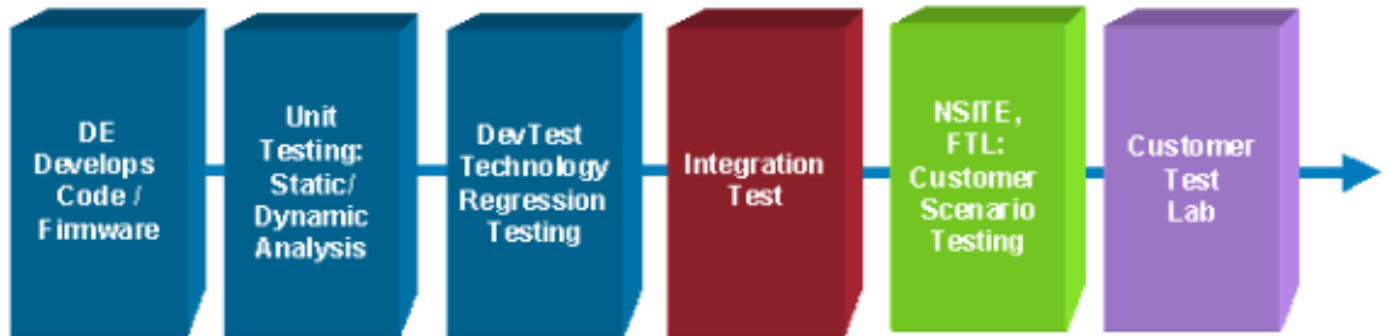
### Test de version de Cisco IOS

La qualité, la portée et la couverture des tests font partie intégrante de l'effort de qualité de la fiabilité des logiciels au sein de Cisco. Globalement, Cisco a les objectifs de qualité IOS suivants :

- Réduisez les défauts de régression interne de Cisco détectés. Cela inclut une meilleure qualité dans le développement et l'identification d'un plus grand nombre de problèmes dans l'analyse statique/dynamique.
- Réduire les défauts détectés par le client
- Réduire le total des défauts en suspens
- Améliorer la clarté et la cohérence des versions logicielles
- Fournir des versions de fonctionnalités et de maintenance avec des calendriers et une qualité

Les tests internes de Cisco peuvent être considérés comme un processus dans lequel différents

défauts sont identifiés à différents stades des tests. L'objectif global est de trouver les bons types de défauts dans le bon laboratoire. C'est important pour plusieurs raisons. Le premier et le plus important est que la couverture adéquate des essais peut ne pas exister au cours des phases ultérieures des essais. Les coûts des tests augmentent également considérablement d'une étape à l'autre en raison de la capacité d'automatisation des phases précédentes et de la complexité et de l'expertise croissantes requises ultérieurement. Le schéma suivant illustre le spectre de test de Cisco IOS.



La première étape est le développement de logiciels. Dans ce domaine, Cisco s'efforce d'améliorer la qualité initiale des logiciels. Les groupes de développement procèdent également à des révisions de code ou même à plusieurs révisions de code pour s'assurer que d'autres développeurs approuvent les modifications logicielles ou le nouveau code de fonction.

L'étape suivante est le test unitaire. Les tests unitaires utilisent des outils qui examinent l'interaction logicielle sans utiliser de travaux pratiques. DevTest sont des tests de laboratoire qui incluent des tests de fonctionnalité et de régression. Les tests de fonctionnalités sont conçus pour examiner la fonctionnalité d'une fonction donnée. Cela inclut la configuration, la déconfiguration et le test de toutes les permutations de fonctionnalités telles que définies dans la spécification de la fonctionnalité. Les tests de régression sont effectués dans une installation de test automatisée conçue pour valider en permanence la fonctionnalité et le comportement des fonctionnalités. Les tests sont principalement axés sur le routage, la commutation et les fonctionnalités dans un certain nombre de topologies de réseau différentes à l'aide de requêtes ping et d'une génération de trafic limitée. Les tests de régression ne sont effectués que sur une combinaison limitée de fonctionnalités, de plates-formes, de versions logicielles et de topologies en raison du nombre extrême de permutations possibles. Cependant, plus de 4 000 scripts de tests de régression sont utilisés aujourd'hui. Les tests d'intégration sont conçus pour développer les capacités de test en laboratoire afin d'obtenir une suite plus complète de produits et d'interopérabilité. Les tests d'intégration augmentent également la couverture du code de test en élargissant les tests pour inclure les tests d'interopérabilité, les tests de résistance et de performances, les tests système et les tests négatifs (tests d'événements inattendus).

La phase de TP suivante fournit des tests de bout en bout pour les environnements clients courants. Ils sont présentés dans le schéma ci-dessus sous les noms de Financial Test Lab (FTL) et NSITE, Customer Scenario Testing. FTL a été conçu pour fournir des tests à la communauté financière critique. NSITE est un groupe qui fournit des tests plus approfondis pour différentes technologies Cisco IOS. Les laboratoires NSITE et FTL se concentrent sur des domaines tels que l'évolutivité et les tests de performances, la mise à niveau, la disponibilité et la résilience, l'interopérabilité et la facilité de maintenance. La facilité de maintenance se concentre sur les problèmes de provisionnement en masse, la gestion/corrélation des événements et le dépannage sous charge. Il existe d'autres laboratoires au sein de Cisco pour différents marchés verticaux afin d'aider à tester ces zones.



Le TP final présenté dans le schéma ci-dessus est identifié comme le TP client. Le test client est une extension de l'effort de qualité et est recommandé pour les environnements à haute disponibilité afin de s'assurer que la combinaison exacte de fonctionnalités, de configuration, de plates-formes, de modules et de topologie a été entièrement testée. La couverture de test doit inclure l'évolutivité et les performances du réseau dans la topologie identifiée, des tests d'application spécifiques, des tests négatifs dans la configuration identifiée, des tests d'interopérabilité pour les périphériques non Cisco et des tests de gravure.

## MTBF logiciel

L'une des mesures les plus courantes de la fiabilité globale est le temps moyen entre les défaillances (MTBF). Le MTBF pour la fiabilité des logiciels est utile en raison des fonctionnalités d'analyse qui ont été développées pour la fiabilité du matériel à l'aide du MTBF. La fiabilité du matériel peut être déterminée plus précisément à l'aide de certaines normes existantes. Cisco utilise la méthode de comptage des pièces basée sur les données MTBF standard de Telcordia Technologies. Toutefois, le logiciel MTBF n'a pas de méthodes d'analyse correspondantes et doit s'appuyer sur la mesure sur le terrain pour l'analyse MTBF.

Au cours des trois dernières années, Cisco a effectué des mesures de fiabilité logicielle sur le terrain pour le réseau informatique interne de Cisco et ce travail est documenté au sein de Cisco. Le travail est basé sur des plantages logiciels forcés pour les périphériques Cisco IOS, qui peuvent être mesurés à l'aide d'informations de dé routement SNMP de gestion de réseau et d'informations de disponibilité. L'étude identifie la fiabilité des logiciels à l'aide d'un modèle de distribution logique statistique pour les versions de logiciels identifiées. Le temps moyen de réparation (MTTR) d'une panne logicielle est basé sur les temps moyens de redémarrage et de récupération du routeur. Un délai de récupération de six minutes est utilisé pour les environnements d'entreprise et de quinze minutes pour les fournisseurs d'accès à Internet de plus grande taille. Le résultat de cette étude en cours est que le logiciel répond généralement à une disponibilité de neuf heures au moment de sa publication, ou après quelques versions de maintenance, et est encore plus élevé au fil du temps, tel que mesuré en utilisant les plantages forcés de logiciels comme seule source de temps d'arrêt. L'étude a identifié des valeurs MTBF potentielles comprises entre 5 000 heures pour les logiciels de déploiement précoce et 50 000 heures pour les logiciels de déploiement général.

La réfutation la plus fréquente à ce travail est que les pannes forcées de logiciels n'incluent pas tous les temps d'arrêt dus à des problèmes de fiabilité du logiciel. Si cette mesure est utilisée dans les efforts d'amélioration de la qualité, elle peut aider à améliorer le taux de plantages forcés de logiciels, mais peut ignorer d'autres domaines critiques de la fiabilité des logiciels. Ce commentaire reste largement sans réponse en raison de la difficulté de prédire avec précision la fiabilité des logiciels à l'aide d'une méthodologie statistique. Les statisticiens de la qualité des logiciels de Cisco ont conclu qu'un plus grand ensemble de données précises serait nécessaire pour prédire de manière fiable le MTBF logiciel en utilisant un plus grand nombre de types de panne. En outre, l'analyse statistique théorique serait difficile en raison de variables telles que la complexité du réseau, l'expertise du personnel pour résoudre les problèmes liés aux logiciels, la conception du réseau, les fonctionnalités activées et les processus de gestion des logiciels.

À l'heure actuelle, aucun travail n'a été effectué dans l'industrie pour prédire plus précisément la fiabilité des logiciels avec des mesures sur le terrain en raison de la difficulté de recueillir précisément ce type de données sensibles. En outre, la plupart des clients ne souhaitent pas que Cisco collecte des informations de disponibilité directement depuis leur réseau en raison de la nature propriétaire des données de disponibilité. Certaines organisations collectent cependant des données sur la fiabilité des logiciels et Cisco encourage les entreprises à collecter des mesures

sur la disponibilité en raison de pannes de logiciels et à effectuer une analyse des causes premières de ces pannes. Les entreprises disposant d'une fiabilité logicielle supérieure ont utilisé cette approche proactive pour améliorer la fiabilité des logiciels grâce à un certain nombre de pratiques qu'elles peuvent contrôler.

## Hypothèses de fiabilité des logiciels

Suite aux commentaires des clients, aux études proactives réalisées par le groupe Cisco IOS Technologies et à l'analyse des causes premières réalisée par l'équipe Cisco Advanced Services, de nouvelles hypothèses et meilleures pratiques ont été élaborées pour améliorer la fiabilité des logiciels. Ces hypothèses sont axées sur les responsabilités de test, la maturité ou l'âge des logiciels, les fonctionnalités activées et le nombre de versions de logiciels déployées.

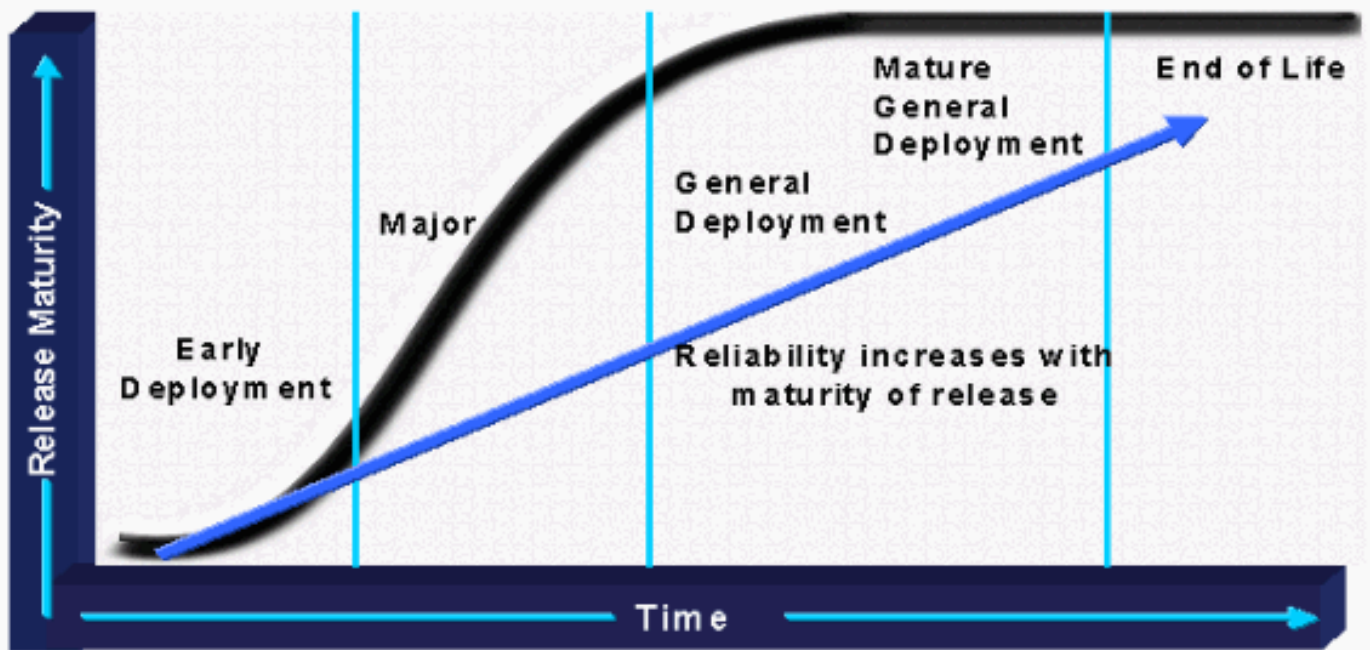
### **Tester la responsabilité**

La première nouvelle hypothèse concerne la responsabilité de test. Cisco est toujours responsable du test/validation des nouvelles fonctionnalités pour s'assurer qu'elles fonctionnent avec de nouveaux produits. Cisco est également responsable des tests de régression pour s'assurer que les nouvelles versions logicielles sont rétrocompatibles. Cependant, Cisco ne peut pas valider toutes les fonctionnalités, topologies et plates-formes par rapport à toutes les contraintes potentielles qu'un environnement client peut apporter (idiosyncrasies de conception, charge et profils de trafic). Les meilleures pratiques en matière de haute disponibilité pour les clients incluent des tests dans une topologie de laboratoire réduite qui imite le réseau de production à l'aide de fonctionnalités, de conception, de services et de trafic d'applications définis par le client.

### **Fiabilité et maturité logicielle**

La fiabilité des logiciels est avant tout un facteur de maturité des logiciels. Le logiciel mûrit au fur et à mesure qu'il est exposé (utilisation) et que les bogues identifiés sont corrigés. Les opérations de mise à jour de Cisco sont passées à une architecture de mise à jour pour s'assurer que les logiciels sont bien à jour sans ajout de nouvelles fonctionnalités. Les clients qui ont besoin d'une haute disponibilité recherchent des logiciels plus matures avec les fonctionnalités dont ils ont besoin aujourd'hui. Il existe alors un compromis entre la maturité du logiciel, les exigences de disponibilité et les facteurs commerciaux pour les nouvelles fonctionnalités. De nombreuses organisations ont des normes ou des lignes directrices pour une maturité acceptable. Certains n'accepteront que la cinquième libération provisoire d'un train en particulier. Pour d'autres, il peut s'agir de la neuvième ou de la certification GD. En fin de compte, l'organisation doit déterminer les niveaux de risque acceptables en termes de maturité logicielle.

## Reliability vs. Software Maturity

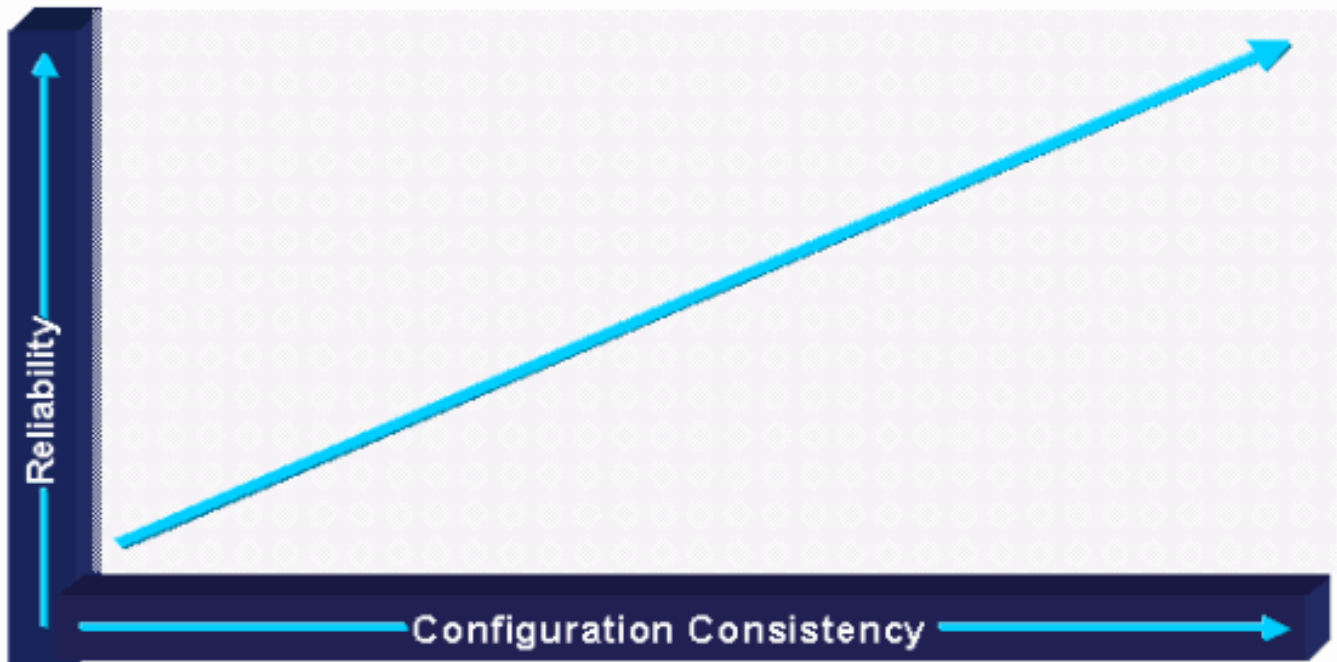


### Fiabilité par rapport au nombre de fonctionnalités et de normes

La fiabilité des logiciels est également un facteur déterminant de la quantité de code qui est testée et exercée dans un environnement de production. À mesure que la quantité de différentes plateformes et modules matériels augmente, la quantité de code exercée augmente également, ce qui augmente généralement l'exposition aux défauts logiciels. Il en va de même pour la quantité de protocoles configurés, la variété des configurations et même la variété de topologie ou de conceptions implémentées. La conception, la configuration, les protocoles et les facteurs de module matériel peuvent contribuer à la quantité de code qui est utilisée et à l'augmentation des risques ou de l'exposition aux défauts logiciels.

Les opérations de mise à jour logicielle ont maintenant des logiciels à usage spécial qui limitent généralement le code disponible dans une zone particulière. Les unités commerciales ont recommandé des conceptions et des configurations qui sont testées de manière plus approfondie au sein de Cisco et sont plus largement utilisées par les clients. Les clients ont également commencé à adopter les meilleures pratiques pour les topologies modulaires normalisées et les configurations standard afin de réduire la quantité d'exposition au code non testé et d'améliorer la fiabilité globale des logiciels. Certains réseaux haute disponibilité ont des directives de configuration standard strictes, des normes de topologie modulaire et un contrôle de version logicielle pour réduire le risque d'exposition au code non testé.

## Reliability vs. Configuration Consistency

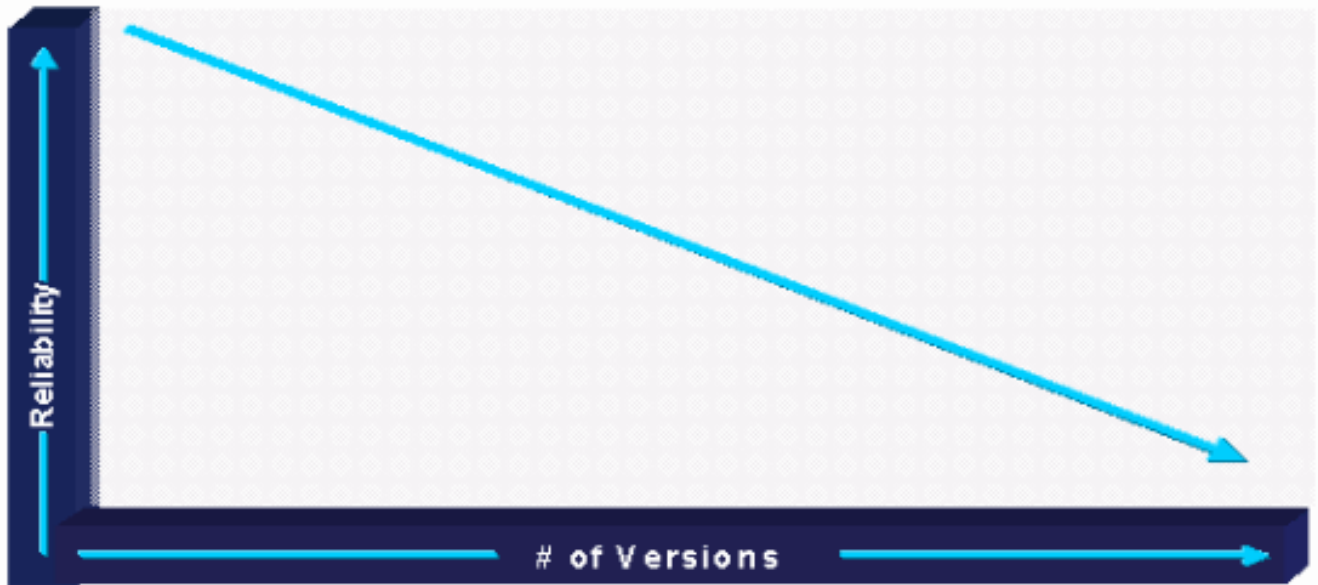


### Fiabilité par rapport au nombre de versions déployées

Un autre facteur de fiabilité du logiciel est l'interopérabilité entre les versions et la quantité de code qui s'exerce avec plusieurs versions. À mesure que la quantité de versions de logiciels augmente, la quantité de code exercé augmente également, ce qui augmente ensuite l'exposition aux défauts logiciels. Le risque de fiabilité augmente presque de façon exponentielle en raison du code supplémentaire appliqué avec plusieurs versions. Il est désormais reconnu que les entreprises doivent exécuter au moins une poignée de versions sur le réseau pour couvrir les besoins spécifiques en matière de fonctionnalités et de plates-formes. Toutefois, le fait de tourner plus de cinquante versions dans un environnement de réseau majoritairement homogène indique généralement des problèmes logiciels dus à l'incapacité d'analyser ou de valider correctement ces nombreuses versions.

Pour améliorer la fiabilité des logiciels, le développement de Cisco effectue des tests de régression logicielle afin de s'assurer que différentes versions de logiciels sont compatibles. En outre, le code logiciel est plus modulaire et les modules principaux sont moins susceptibles de changer significativement d'une version à l'autre au fil du temps. Les opérations de version de Cisco ont également modifié la quantité de logiciels disponibles pour les clients, car les versions présentant des défauts connus ou des problèmes d'interopérabilité sont rapidement supprimées de CCO à mesure que des défauts sont détectés.

## Reliability vs. Number of Deployed Versions



### Informations connexes

- [Systèmes d'exploitation Cisco IOS](#)
- [Support et documentation techniques - Cisco Systems](#)