Gestion de la configuration : livre blanc sur les meilleures pratiques

Table des matières

Introduction

La gestion de la configuration est une collection de processus et d'outils qui favorisent la cohérence de réseau, dépistent la modification de réseau, et fournissent la documentation réseau et la visibilité à jour. En établissant et en mettant à jour des meilleures pratiques de gestion de la configuration, vous pouvez vous attendre à plusieurs avantages tels que la disponibilité améliorée du réseau et des coûts inférieurs. Ceux-ci incluent :

- Coûts d'assistance réduits en raison d'une diminution des problèmes d'assistance réactive.
- Coûts réseau réduits grâce aux outils et processus de suivi des périphériques, des circuits et des utilisateurs qui identifient les composants réseau inutilisés.
- Meilleure disponibilité du réseau grâce à la réduction des coûts d'assistance réactive et à l'amélioration du délai de résolution des problèmes.

Nous avons constaté les problèmes suivants dus à un manque de gestion de la configuration :

- Incapacité à déterminer l'impact des modifications apportées au réseau sur les utilisateurs
- Problèmes d'assistance réactifs accrus et disponibilité réduite
- Temps accru pour résoudre les problèmes
- Coûts réseau plus élevés en raison de composants réseau inutilisés

Ce document de meilleures pratiques fournit un organigramme de processus pour la mise en oeuvre d'un plan de gestion de la configuration réussi. Nous étudierons en détail les étapes suivantes : création de normes, gestion de la documentation, validation et audit des normes.

Flux de processus de haut niveau pour la gestion de la configuration

Le schéma ci-dessous montre comment utiliser les facteurs de réussite critiques suivis d'indicateurs de performance pour mettre en oeuvre un plan de gestion de la configuration réussi.

Créer des normes

La création de normes pour la cohérence du réseau permet de réduire la complexité du réseau, le nombre d'interruptions non planifiées et l'exposition aux événements ayant un impact sur le réseau. Nous recommandons les normes suivantes pour une cohérence optimale du réseau :

- Contrôle et gestion des versions logicielles
- Normes et gestion d'adressage IP
- Conventions de noms et affectations DNS/DHCP (Domain Name System/Dynamic Host Configuration Protocol)
- Configurations et descripteurs standard
- Procédures de mise à niveau de configuration
- Modèles de solution

Contrôle et gestion des versions logicielles

Le contrôle de version logicielle consiste à déployer des versions logicielles cohérentes sur des périphériques réseau similaires. Cela améliore les chances de validation et de test sur les versions logicielles choisies et limite considérablement le nombre de défauts logiciels et de problèmes d'interopérabilité détectés sur le réseau. Les versions logicielles limitées réduisent également le risque de comportement inattendu avec les interfaces utilisateur, les résultats de commande ou de gestion, le comportement de mise à niveau et le comportement des fonctionnalités. Cela rend l'environnement moins complexe et plus facile à prendre en charge. Dans l'ensemble, le contrôle des versions logicielles améliore la disponibilité du réseau et

contribue à réduire les coûts d'assistance réactive.

Remarque : les périphériques réseau similaires sont définis comme des périphériques réseau standard avec un châssis commun fournissant un service commun.

Pour contrôler la version du logiciel, procédez comme suit :

- Déterminer les classifications des périphériques en fonction des exigences du châssis, de la stabilité et des nouvelles fonctionnalités.
- Ciblez des versions logicielles individuelles pour des périphériques similaires.
- Testez, validez et pilotez les versions logicielles choisies.
- Documentez les versions réussies en tant que norme pour la classification de périphériques similaires.
- Déployez ou mettez à niveau de manière cohérente tous les périphériques similaires vers la version logicielle standard.

Normes et gestion d'adressage IP

La gestion des adresses IP est le processus d’allocation, de recyclage et de documentation des adresses IP et des sous-réseaux dans un réseau. Les normes d’adressage IP définissent la taille de sous-réseau, l’affectation de sous-réseau, les affectations de périphériques réseau et les affectations d’adresses dynamiques dans une plage de sous-réseaux. Les normes de gestion d’adresses IP recommandées réduisent les risques de chevauchement ou de duplication des sous-réseaux, de non-récapitulation sur le réseau, d’affectation de périphériques d’adresses IP en double, de gaspillage d’espace d’adressage IP et de complexité inutile.

La première étape d’une gestion réussie des adresses IP consiste à comprendre les blocs d’adresses IP utilisés dans le réseau. Dans de nombreux cas, les organisations réseau doivent s'appuyer sur l'espace d'adressage RFC 1918, qui n'est pas adressable par Internet, mais qui peut être utilisé pour accéder au réseau en conjonction avec la traduction d'adresses de réseau (NAT). Une fois que vous avez défini les blocs d’adresses, attribuez-les à des zones du réseau d’une manière qui favorise la récapitulation. Dans de nombreux cas, vous devrez subdiviser davantage ces blocs en fonction du nombre et de la taille des sous-réseaux dans la plage définie. Vous devez définir des tailles de sous-réseau standard pour les applications standard, telles que les tailles de sous-réseau de construction, les tailles de sous-réseau de liaison WAN, la taille de sous-réseau de bouclage ou la taille de sous-réseau de site WAN. Vous pouvez ensuite allouer des sous-réseaux pour de nouvelles applications à partir d'un bloc de sous-réseau au sein d'un bloc récapitulatif plus grand.

Prenons l'exemple d'un grand réseau d'entreprise avec un campus de la côte Est, un campus de la côte Ouest, un WAN domestique, un WAN européen et d'autres sites internationaux majeurs. L'entreprise attribue des blocs CIDR (Classless Interdomain Routing) IP contigus à chacune de ces zones afin de promouvoir la récapitulation IP. L’organisation définit ensuite les tailles de sous-réseau dans ces blocs et attribue des sous-sections de chaque bloc à une taille de sous-réseau IP

particulière. Chaque bloc principal ou l'espace d'adressage IP complet peut être documenté dans une feuille de calcul montrant les sous-réseaux alloués, utilisés et disponibles pour chaque taille de sous-réseau disponible dans le bloc.

L’étape suivante consiste à créer des normes pour l’attribution des adresses IP dans chaque plage de sous-réseaux. Les adresses virtuelles des routeurs et du protocole HSRP (Hot Standby Router Protocol) au sein d'un sous-réseau peuvent se voir attribuer les premières adresses disponibles dans la plage. Les commutateurs et les passerelles peuvent se voir attribuer les adresses disponibles suivantes, suivies par d’autres affectations d’adresses fixes, et enfin des adresses dynamiques pour DHCP. Par exemple, tous les sous-réseaux utilisateur peuvent être des sous-réseaux /24 avec 253 affectations d’adresses disponibles. Les adresses .1 et .2 peuvent être attribuées aux routeurs, et l'adresse HSRP peut être attribuée à l'adresse .3, aux commutateurs .5 à .9 et à la plage DHCP de .10 à .253. Quelles que soient les normes que vous développez, elles doivent être documentées et référencées dans tous les documents du plan d'ingénierie réseau afin de garantir un déploiement cohérent.

Conventions de noms et affectations DNS/DHCP

L'utilisation cohérente et structurée des conventions d'attribution de noms et du DNS pour les périphériques vous aide à gérer le réseau de la manière suivante :

- Crée un point d'accès cohérent aux routeurs pour toutes les informations de gestion du réseau relatives à un périphérique.
- Réduit les possibilités de duplication des adresses IP.
- Crée une identification simple d'un périphérique indiquant son emplacement, son type et sa fonction.
- Améliore la gestion de l'inventaire en fournissant une méthode plus simple pour identifier les périphériques réseau.

La plupart des périphériques réseau disposent d'une ou deux interfaces pour gérer le périphérique. Il peut s’agir d’une interface Ethernet intrabande ou hors bande et d’une interface de console. Vous devez créer des conventions d'attribution de noms pour ces interfaces en fonction du type de périphérique, de l'emplacement et du type d'interface. Sur les routeurs, nous vous recommandons vivement d’utiliser l’interface de bouclage comme interface de gestion principale, car elle est accessible à partir de différentes interfaces. Vous devez également configurer les interfaces de bouclage comme adresse IP source pour les messages déroutés, SNMP et syslog. Chaque interface peut alors avoir une convention d'attribution de noms qui identifie le périphérique, l'emplacement, la fonction et l'interface.

Nous vous recommandons également d'identifier les plages DHCP et de les ajouter au DNS, y compris l'emplacement des utilisateurs. Il peut s'agir d'une partie de l'adresse IP ou d'un emplacement physique. Par exemple, « dhcp-bldg-c21-10 » à « dhcp-bldg-c21-253 » identifie les adresses IP du bâtiment C, deuxième étage, local technique 1. Vous pouvez également utiliser le sous-réseau précis pour l'identification. Une fois qu'une convention d'attribution de noms a été créée pour les périphériques et DHCP, vous aurez besoin d'outils pour suivre et gérer les entrées,

tels que Cisco Network Registrar.

Configuration et descripteurs standard

La configuration standard s'applique aux configurations de protocole et de support, ainsi qu'aux commandes de configuration globale. Les descripteurs sont des commandes d'interface utilisées pour décrire une interface.

Nous vous recommandons de créer des configurations standard pour chaque classification de périphérique, comme un routeur, un commutateur LAN, un commutateur WAN ou un commutateur ATM. Chaque configuration standard doit contenir les commandes de configuration globale, de média et de protocole nécessaires pour maintenir la cohérence du réseau. La configuration des supports inclut la configuration ATM, Frame Relay ou Fast Ethernet. La configuration de protocole inclut des paramètres de configuration de protocole de routage IP standard, des configurations de qualité de service (QoS) communes, des listes d'accès communes et d'autres configurations de protocole requises. Les commandes de configuration globale s'appliquent à tous les périphériques similaires et incluent des paramètres tels que les commandes de service, les commandes IP, les commandes TACACS, la configuration vty, les bannières, la configuration SNMP et la configuration NTP (Network Time Protocol).

Les descripteurs sont développés en créant un format standard qui s'applique à chaque interface. Le descripteur comprend l'objectif et l'emplacement de l'interface, d'autres périphériques ou emplacements connectés à l'interface, et des identificateurs de circuit. Les descripteurs aident votre service d'assistance à mieux comprendre l'étendue des problèmes liés à une interface et permettent une résolution plus rapide des problèmes.

Nous vous recommandons de conserver les paramètres de configuration standard dans un fichier de configuration standard et de télécharger le fichier sur chaque nouveau périphérique avant de procéder à la configuration du protocole et de l'interface. En outre, vous devez documenter le fichier de configuration standard, y compris une explication de chaque paramètre de configuration globale et pourquoi il est important. Cisco Resource Manager Essentials (RME) peut être utilisé pour gérer les fichiers de configuration standard, la configuration de protocole et les descripteurs.

Procédures de mise à niveau de configuration

Les procédures de mise à niveau permettent de garantir une mise à niveau logicielle et matérielle fluide avec un temps d'arrêt minimal. Les procédures de mise à niveau incluent la vérification du fournisseur, les références d'installation du fournisseur telles que les notes de version, les méthodologies ou étapes de mise à niveau, les directives de configuration et les exigences de test.

Les procédures de mise à niveau peuvent varier considérablement en fonction des types de réseau, des types de périphériques ou des nouvelles exigences logicielles. Les exigences de mise à niveau d'un routeur ou d'un commutateur peuvent être développées et testées au sein d'un groupe d'architecture et référencées dans toute documentation de modification. Les autres mises à niveau, impliquant des réseaux entiers, ne peuvent pas être testées aussi facilement. Ces mises à niveau peuvent nécessiter une planification plus approfondie, l'intervention du fournisseur et des

étapes supplémentaires pour garantir la réussite.

Vous devez créer ou mettre à jour des procédures de mise à niveau en conjonction avec tout nouveau déploiement de logiciel ou toute version standard identifiée. Les procédures doivent définir toutes les étapes de la mise à niveau, faire référence à la documentation du fournisseur relative à la mise à jour du périphérique et fournir des procédures de test pour la validation du périphérique après la mise à niveau. Une fois que les procédures de mise à niveau ont été définies et validées, elles doivent être référencées dans toute la documentation de modification appropriée à la mise à niveau concernée.

Modèles de solution

Vous pouvez utiliser des modèles de solution pour définir des solutions réseau modulaires standard. Un module de réseau peut être un local technique, un bureau extérieur WAN ou un concentrateur d'accès. Dans chaque cas, vous devez définir, tester et documenter la solution pour vous assurer que des déploiements similaires peuvent être effectués exactement de la même manière. Cela permet de garantir que les modifications futures se produiront à un niveau de risque beaucoup plus faible pour l'organisation, puisque le comportement de la solution est bien défini.

Créez des modèles de solution pour tous les déploiements et solutions à haut risque qui seront déployés plusieurs fois. Le modèle de solution contient toutes les exigences standard en matière de matériel, de logiciels, de configuration, de câblage et d'installation pour la solution réseau. Les détails spécifiques du modèle de solution sont indiqués comme suit :

- Modules matériels et matériels, y compris la mémoire, la mémoire flash, l'alimentation et les configurations de carte.
- Topologie logique incluant les affectations de ports, la connectivité, la vitesse et le type de support.
- Versions logicielles, y compris les versions de module ou de microprogramme.
- Toutes les configurations non standard et non spécifiques au périphérique, y compris les protocoles de routage, les configurations de support, la configuration VLAN, les listes d'accès, la sécurité, les chemins de commutation, les paramètres Spanning Tree, etc.
- Exigences de gestion hors bande.
- Configuration des câbles.
- Exigences d'installation, notamment les environnements, l'alimentation et les emplacements des racks.

Notez que le modèle de solution ne contient pas beaucoup d'exigences. Les exigences spécifiques telles que l'adressage IP pour la solution spécifique, l'attribution de noms, les attributions DNS, les attributions DHCP, les attributions PVC, les descripteurs d'interface, etc., doivent être couvertes par les pratiques de gestion de la configuration globale. Les exigences plus générales, telles que les configurations standard, les plans de gestion des modifications, les procédures de mise à jour de la documentation ou les procédures de mise à jour de la gestion du

réseau, doivent être couvertes par les pratiques générales de gestion de la configuration.

Conserver la documentation

Nous vous recommandons de documenter le réseau et les modifications qui y ont été apportées en temps quasi réel. Vous pouvez utiliser ces informations réseau précises pour le dépannage, les listes de périphériques de l'outil de gestion du réseau, l'inventaire, la validation et les audits. Nous vous recommandons d'utiliser la documentation réseau suivante pour les facteurs de réussite critiques :

- Inventaire actuel des périphériques, des liaisons et des utilisateurs finaux
- Système de contrôle de version de configuration
- Journal de configuration TACACS
- Documentation topologique du réseau

Inventaire actuel des périphériques, des liaisons et des utilisateurs finaux

Les informations actuelles sur les périphériques, les liaisons et les utilisateurs finaux vous permettent de suivre l'inventaire et les ressources du réseau, l'impact des problèmes et l'impact des modifications apportées au réseau. La possibilité de suivre l'inventaire et les ressources du réseau en fonction des besoins des utilisateurs permet de s'assurer que les périphériques réseau gérés sont activement utilisés, fournit les informations nécessaires aux audits et aide à gérer les ressources des périphériques. Les données relatives aux relations avec l'utilisateur final fournissent des informations permettant de définir les risques et l'impact des modifications, ainsi que la capacité à résoudre et à dépanner plus rapidement les problèmes. Les bases de données d'inventaire des périphériques, des liaisons et des utilisateurs finaux sont généralement développées par de nombreuses entreprises de fournisseurs de services de premier plan. Visionael Corporation est le principal développeur de logiciels d’inventaire réseau . La base de données peut contenir des tables pour des périphériques similaires, des liens et des données utilisateur/serveur client, de sorte que lorsqu'un périphérique est en panne ou que des modifications du réseau se produisent, vous pouvez facilement comprendre l'impact sur l'utilisateur final.

Configuration Version Control System

Un système de contrôle de version de configuration conserve les configurations en cours de tous les dispositifs et un nombre défini de versions en cours d'exécution précédentes. Ces informations peuvent être utilisées pour le dépannage, la configuration ou les audits des modifications. Lors du dépannage, vous pouvez comparer la configuration en cours aux versions de travail précédentes pour mieux comprendre si la configuration est liée au problème de quelque manière que ce soit. Nous vous recommandons de conserver trois à cinq versions de travail précédentes de la configuration.

Journal de configuration TACACS

Pour identifier les personnes qui ont apporté des modifications de configuration et quand, vous pouvez utiliser la journalisation TACACS et NTP. Lorsque ces services sont activés sur des périphériques réseau Cisco, l'ID utilisateur et l'horodatage sont ajoutés au fichier de configuration au moment de la modification de la configuration. Ce tampon est ensuite copié avec le fichier de configuration dans le système de contrôle de version de configuration. TACACS peut alors agir comme un élément dissuasif pour les changements non gérés et fournir un mécanisme permettant d'auditer correctement les changements qui se produisent. TACACS est activé à l'aide du produit Cisco Secure. Lorsque l'utilisateur se connecte au périphérique, il doit s'authentifier auprès du serveur TACACS en fournissant un ID utilisateur et un mot de passe. Le protocole NTP est facilement activé sur un périphérique réseau en le dirigeant vers une horloge principale NTP.

Documentation de topologie réseau

La documentation topologique aide à comprendre et à prendre en charge le réseau. Vous pouvez l'utiliser pour valider les directives de conception et pour mieux comprendre le réseau en vue d'une conception, d'une modification ou d'un dépannage futurs. La documentation topologique doit inclure la documentation logique et physique, notamment la connectivité, l'adressage, les types de supports, les périphériques, les dispositions de rack, les affectations de cartes, le routage des câbles, l'identification des câbles, les points de terminaison, les informations d'alimentation et les informations d'identification des circuits.

La tenue à jour de la documentation topologique est la clé d'une gestion réussie de la configuration. Pour créer un environnement dans lequel la maintenance de la documentation topologique peut avoir lieu, il convient de souligner l'importance de la documentation et de mettre les informations à disposition pour les mises à jour. Nous vous recommandons vivement de mettre à jour la documentation topologique en cas de modification du réseau.

La documentation de topologie réseau est généralement gérée à l'aide d'une application graphique telle que Microsoft Visio . D'autres produits tels que Visionael offrent des capacités supérieures de gestion des informations de topologie.

Normes de validation et d'audit

Les indicateurs de performance de gestion de la configuration fournissent un mécanisme de validation et d'audit des normes de configuration du réseau et des facteurs de réussite critiques. En mettant en oeuvre un programme d'amélioration des processus pour la gestion de la configuration, vous pouvez utiliser les indicateurs de performance pour identifier les problèmes de cohérence et améliorer la gestion globale de la configuration.

Nous vous recommandons de créer une équipe interfonctionnelle pour mesurer la réussite de la gestion des configurations et améliorer les processus de gestion des configurations. Le premier objectif de l'équipe est de mettre en oeuvre des indicateurs de performance de gestion de la configuration afin d'identifier les problèmes de gestion de la configuration. Nous aborderons en détail les indicateurs de performance suivants relatifs à la gestion de la configuration :

- Contrôles d'intégrité de configuration

- Audits des périphériques, des protocoles et des supports
- Examen des normes et de la documentation

Après avoir évalué les résultats de ces audits, lancez un projet pour corriger les incohérences, puis déterminez la cause initiale du problème. Parmi les causes possibles, mentionnons l'absence de documentation sur les normes ou l'absence d'un processus cohérent. Vous pouvez améliorer la documentation des normes, mettre en oeuvre la formation ou améliorer les processus pour éviter d'autres incohérences de configuration.

Nous recommandons des audits mensuels, voire trimestriels si seule la validation est nécessaire. Examiner les audits précédents pour confirmer que les problèmes passés sont résolus. Recherchez des améliorations et des objectifs généraux pour démontrer les progrès et la valeur. Créez des mesures pour indiquer le nombre d'incohérences de configuration réseau à haut risque, à risque moyen et à faible risque.

Contrôles d'intégrité de configuration

Le contrôle d'intégrité de la configuration doit évaluer la configuration globale du réseau, sa complexité et sa cohérence, ainsi que les problèmes potentiels. Pour les réseaux Cisco, nous vous recommandons d'utiliser l'outil de validation de configuration Netsys. Cet outil entre toutes les configurations de périphériques et crée un rapport de configuration qui identifie les problèmes actuels tels que les adresses IP en double, les incohérences et les incohérences de protocole. L'outil signale tout problème de connectivité ou de protocole, mais n'entre pas de configurations standard pour l'évaluation de chaque périphérique. Vous pouvez revoir manuellement les normes de configuration ou créer un script qui signale les différences de configuration standard.

Audits des périphériques, des protocoles et des supports

Les audits des périphériques, des protocoles et des supports sont un indicateur de performance pour la cohérence des versions logicielles, des modules et des périphériques matériels, des protocoles et des supports, ainsi que des conventions d'attribution de noms. Les audits doivent d'abord identifier les problèmes non standard, ce qui doit conduire à des mises à jour de la configuration pour les corriger ou les améliorer. Évaluer l'ensemble des processus pour déterminer comment ils pourraient empêcher les déploiements non optimaux ou non standard de se produire.

Cisco RME est un outil de gestion de la configuration qui permet d'auditer et de générer des rapports sur les versions matérielles, les modules et les versions logicielles. Cisco développe également des audits plus complets des médias et des protocoles qui signaleront les incohérences avec IP, DLSW, Frame Relay et ATM. Si aucun protocole ou audit de support n'est développé, vous pouvez utiliser des audits manuels, comme la vérification des périphériques, des versions et des configurations pour tous les périphériques similaires d'un réseau, ou en contrôlant les périphériques, les versions et les configurations.

Révision des normes et de la documentation

Cet indicateur de performance examine la documentation relative au réseau et aux normes pour s'assurer que les informations sont exactes et à jour. La vérification devrait comprendre l'examen de la documentation actuelle, la recommandation de changements ou d'ajouts et l'approbation de nouvelles normes.

Vous devez consulter la documentation suivante tous les trimestres : définitions de configuration standard, modèles de solution incluant les configurations matérielles recommandées, versions logicielles standard actuelles, procédures de mise à niveau pour tous les périphériques et versions logicielles, documentation de topologie, modèles actuels et gestion des adresses IP.

Informations connexes

- Support technique - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.