Konfigurationsverwaltung: Whitepaper zu Best Practices

Inhalt

Einführung

Konfigurationsmanagement ist eine Sammlung von Prozessen und Tools, die die Netzwerkkonsistenz fördern, Netzwerkänderungen nachverfolgen und eine aktuelle Netzwerkdokumentation und -transparenz bereitstellen. Durch den Aufbau und die Beibehaltung von Best Practices für das Konfigurationsmanagement können Sie verschiedene Vorteile wie eine verbesserte Netzwerkverfügbarkeit und geringere Kosten erwarten. Dazu gehören:

- Niedrigere Support-Kosten durch weniger reaktiven Support.
- Geringere Netzwerkkosten durch Tools und Prozesse zur Geräte-, Schaltkreis- und Benutzerverfolgung, die nicht verwendete Netzwerkkomponenten identifizieren
- Verbesserte Netzwerkverfügbarkeit durch niedrigere reaktive Support-Kosten und kürzere Problembehebungszeiten

Die folgenden Probleme sind auf das fehlende Konfigurationsmanagement zurückzuführen:

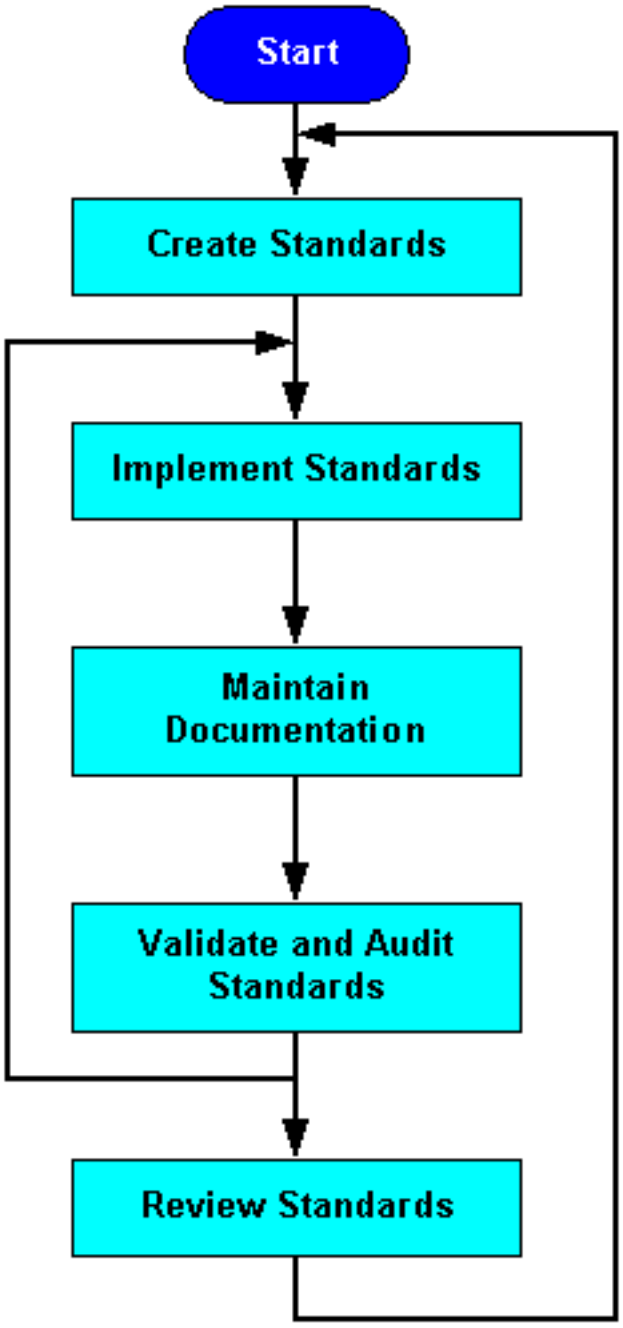
- Die Auswirkungen von Netzwerkänderungen auf die Benutzer können nicht ermittelt werden.
- Erhöhte Reaktionsfähigkeit und Verfügbarkeit

- Schnellere Problembehebung
- Höhere Netzwerkkosten durch nicht verwendete Netzwerkkomponenten

Dieses Best Practice-Dokument enthält ein Ablaufdiagramm für die Implementierung eines erfolgreichen Konfigurationsmanagementplans. Wir werden uns die folgenden Schritte genauer ansehen: Standards erstellen, Dokumentation pflegen, Standards validieren und überprüfen.

Allgemeiner Prozessablauf für das Konfigurationsmanagement

Das nachfolgende Diagramm zeigt, wie Sie mithilfe der entscheidenden Erfolgsfaktoren gefolgt von Leistungsindikatoren einen erfolgreichen Konfigurationsmanagementplan implementieren können.



Standards erstellen

Durch die Festlegung von Standards für Netzwerkkonsistenz wird die Netzwerkkomplexität verringert, die Anzahl ungeplanter Ausfallzeiten reduziert und Netzwerkereignisse in Gefahr gebracht. Die folgenden Standards werden für eine optimale Netzwerkkonsistenz empfohlen:

- Softwareversionskontrolle und -verwaltung
- IP-Adressierungsstandards und -management
- Namenskonventionen und DNS/DHCP-Zuweisungen (Domain Name System/Dynamic Host Configuration Protocol)
- Standardkonfigurationen und Deskriptoren
- Konfigurationsaktualisierungsverfahren
- Lösungsvorlagen

Softwareversions-Kontrolle und -Management

Softwareversionskontrolle ist die Praxis, konsistente Softwareversionen auf ähnlichen Netzwerkgeräten bereitzustellen. Dies erhöht die Chance auf Validierung und Tests der ausgewählten Softwareversionen und schränkt die Anzahl der im Netzwerk festgestellten Softwarefehler und Interoperabilitätsprobleme deutlich ein. Eingeschränkte Softwareversionen reduzieren zudem das Risiko unerwarteter Verhaltensweisen durch Benutzeroberflächen, Befehls- oder Verwaltungsausgaben, Aktualisierungsverhalten und Funktionsverhalten. Dadurch wird die Umgebung weniger komplex und einfacher zu unterstützen. Insgesamt verbessert die Softwareversionskontrolle die Netzwerkverfügbarkeit und senkt reaktive Supportkosten.

Hinweis: Ähnliche Netzwerkgeräte werden als Standard-Netzwerkgeräte mit einem gemeinsamen Chassis definiert, die einen gemeinsamen Dienst bereitstellen.

Führen Sie die folgenden Schritte für die Softwareversionskontrolle durch:

- Bestimmen Sie Geräteklassifizierungen basierend auf Chassis, Stabilität und neuen Funktionsanforderungen.
- Identifizieren Sie einzelne Softwareversionen für ähnliche Geräte.
- Testen, Validieren und Testen ausgewählter Softwareversionen
- Dokumentieren erfolgreicher Versionen als Standard für die Klassifizierung ähnlicher Geräte
- Konsistente Bereitstellung oder Aktualisierung aller ähnlichen Geräte auf die Standard-Softwareversion.

IP-Adressierungsstandards und -management

IP-Adressenverwaltung bezeichnet den Prozess der Zuweisung, Wiederverwendung und Dokumentation von IP-Adressen und Subnetzen in einem Netzwerk. IP-Adressierungsstandards definieren die Subnetzgröße, die Subnetzzuweisung, Netzwerkgerätzuweisungen und dynamische Adressenzuweisungen innerhalb eines Subnetzbereichs. Empfohlene Standards für das IP-Adressmanagement reduzieren die Wahrscheinlichkeit, dass sich die Subnetze überschneiden oder duplizieren, keine Zusammenfassung im Netzwerk erfolgt, doppelte IP-Adressen-Gerätezuweisungen vorgenommen werden, verschwendete IP-Adressbereiche und unnötige Komplexität.

Der erste Schritt zu einer erfolgreichen IP-Adressverwaltung besteht darin, die im Netzwerk verwendeten IP-Adressblöcke zu verstehen. In vielen Fällen müssen sich Netzwerkorganisationen auf den RFC 1918 -Adressbereich verlassen, der nicht über das Internet adressierbar ist, aber für

den Zugriff auf das Netzwerk in Verbindung mit Network Address Translation (NAT) verwendet werden kann. Sobald Sie die Adressblöcke definiert haben, weisen Sie sie Bereichen des Netzwerks so zu, dass eine Zusammenfassung möglich ist. In vielen Fällen müssen Sie diese Blöcke basierend auf der Anzahl und Größe der Subnetze innerhalb des definierten Bereichs weiter unterteilen. Sie sollten Standard-Subnetzgrößen für Standardanwendungen definieren, z. B. für die Erstellung von Subnetzen, WAN-Link-Subnetzgrößen, Loopback-Subnetzgröße oder Subnetzgröße des WAN-Standorts. Sie können dann Subnetze für neue Anwendungen aus einem Subnetzblock innerhalb eines größeren Zusammenfassungsblocks zuweisen.

Nehmen wir zum Beispiel ein großes Unternehmensnetzwerk mit einem Campus an der Ostküste, einem Campus an der Westküste, einem WAN im Inland, einem europäischen WAN und anderen großen internationalen Standorten. Die Organisation weist jedem dieser Bereiche CIDR-Blöcke (Contiguous IP Classless Interdomain Routing) zu, um die IP-Zusammenfassung zu fördern. Die Organisation definiert dann die Subnetzgrößen in diesen Blöcken und weist Unterabschnitte jedes Blocks einer bestimmten IP-Subnetzgröße zu. Jeder Hauptblock oder der gesamte IP-Adressbereich kann in einer Tabelle mit zugewiesenen, verwendeten und verfügbaren Subnetzen für jede verfügbare Subnetzgröße innerhalb des Blocks dokumentiert werden.

Im nächsten Schritt werden Standards für die IP-Adressenzuweisung innerhalb jedes Subnetzbereichs erstellt. Routern und virtuellen Hot Standby Router Protocol (HSRP)-Adressen in einem Subnetz können die ersten verfügbaren Adressen innerhalb des Bereichs zugewiesen werden. Switches und Gateways können die nächsten verfügbaren Adressen zugewiesen werden, gefolgt von anderen festen Adressenzuweisungen und schließlich dynamischen Adressen für DHCP. Beispielsweise können alle Subnetze von Benutzern /24 Subnetze mit 253 verfügbaren Adresszuweisungen sein. Den Routern können die .1- und .2-Adressen zugewiesen werden, und der HSRP-Adresse werden die .3-Adresse, die Switches .5 bis .9 und der DHCP-Bereich von .10 bis .253 zugewiesen. Welche Standards Sie auch entwickeln, sie sollten dokumentiert und in allen Dokumenten des Netzwerkentwicklungsplans referenziert werden, um eine konsistente Bereitstellung zu gewährleisten.

Namenskonventionen und DNS-/DHCP-Zuweisungen

Durch die konsistente, strukturierte Verwendung von Namenskonventionen und DNS für Geräte können Sie das Netzwerk auf folgende Weise verwalten:

- Erstellt einen konsistenten Access Point für Router für alle Netzwerkverwaltungsinformationen, die sich auf ein Gerät beziehen.
- Reduziert die Möglichkeit, IP-Adressen zu duplizieren.
- Erstellt eine einfache Identifizierung eines Geräts, das Standort, Gerätetyp und Zweck anzeigt.
- Verbesserte Bestandsverwaltung durch eine einfachere Methode zur Identifizierung von Netzwerkgeräten

Die meisten Netzwerkgeräte verfügen über eine bis zwei Schnittstellen für das Gerätemanagement. Dabei kann es sich um eine In-Band- oder Out-of-Band-Ethernet-Schnittstelle und eine Konsolenschnittstelle handeln. Sie sollten Namenskonventionen für diese Schnittstellen erstellen, die sich auf Gerätetyp, Standort und Schnittstellentyp beziehen. Für Router wird dringend empfohlen, die Loopback-Schnittstelle als primäre Verwaltungsschnittstelle zu verwenden, da auf sie von verschiedenen Schnittstellen aus zugegriffen werden kann. Sie sollten außerdem Loopback-Schnittstellen als Quell-IP-Adresse für Traps, SNMP und Syslog-Meldungen konfigurieren. Einzelne Schnittstellen können dann über eine Namenskonvention verfügen, die das Gerät, den Standort, den Zweck und die Schnittstelle identifiziert.

Wir empfehlen auch, DHCP-Bereiche zu identifizieren und sie dem DNS hinzuzufügen, einschließlich des Standorts der Benutzer. Dabei kann es sich um einen Teil der IP-Adresse oder einen physischen Standort handeln. Ein Beispiel könnte "dhcp-bldg-c21-10" oder "dhcp-bldg-c21-253" sein, die IP-Adressen in Gebäude C, zweiter Stock, Verteilerschrank 1 identifiziert. Sie können auch das genaue Subnetz zur Identifizierung verwenden. Nach der Erstellung einer Namenskonvention für Geräte und DHCP benötigen Sie Tools zum Nachverfolgen und Verwalten von Einträgen, z. B. Cisco Network Registrar.

Standardkonfiguration und Deskriptoren

Die Standardkonfiguration gilt für Protokoll- und Medienkonfigurationen sowie für globale Konfigurationsbefehle. Bezeichnungen sind Schnittstellenbefehle, die zum Beschreiben einer Schnittstelle verwendet werden.

Wir empfehlen, Standardkonfigurationen für jede Geräteklassifizierung zu erstellen, z. B. Router, LAN-Switch, WAN-Switch oder ATM-Switch. Jede Standardkonfiguration sollte die Befehle für die globale, Medien- und Protokollkonfiguration enthalten, die zur Wahrung der Netzwerkkonsistenz erforderlich sind. Die Medienkonfiguration umfasst die Konfiguration von ATM, Frame Relay oder Fast Ethernet. Die Protokollkonfiguration umfasst standardmäßige Konfigurationsparameter für das IP-Routing-Protokoll, allgemeine Quality of Service (QoS)-Konfigurationen, gemeinsame Zugriffslisten und andere erforderliche Protokollkonfigurationen. Globale Konfigurationsbefehle gelten für alle Geräte und umfassen Parameter wie Dienstbefehle, IP-Befehle, TACACS-Befehle, VTY-Konfiguration, Banner, SNMP-Konfiguration und NTP-Konfiguration (Network Time Protocol).

Deskriptoren werden durch Erstellen eines Standardformats entwickelt, das für jede Schnittstelle gilt. Der Deskriptor enthält den Zweck und die Position der Schnittstelle, andere Geräte oder Standorte, die mit der Schnittstelle verbunden sind, und Schaltkreiskennungen. Deskriptoren helfen Ihrem Support-Unternehmen, den Umfang von Problemen im Zusammenhang mit einer Schnittstelle besser zu verstehen und ermöglichen eine schnellere Problembehebung.

Wir empfehlen, die Standardkonfigurationsparameter in einer Standard-Konfigurationsdatei zu speichern und die Datei vor der Protokoll- und Schnittstellenkonfiguration auf jedes neue Gerät herunterzuladen. Darüber hinaus sollten Sie die Standardkonfigurationsdatei dokumentieren, einschließlich einer Erklärung für jeden globalen Konfigurationsparameter und dessen Bedeutung. Cisco Resource Manager Essentials (RME) kann zur Verwaltung von Standardkonfigurationsdateien, Protokollkonfigurationen und Deskriptoren verwendet werden.

Konfigurationsaktualisierungsverfahren

Aktualisierungsverfahren stellen sicher, dass Software- und Hardware-Upgrades reibungslos und mit minimalen Ausfallzeiten erfolgen. Aktualisierungsverfahren umfassen die Anbieterverifizierung, Anbieterinstallationsreferenzen wie Versionshinweise, Upgrade-Methoden oder -Schritte, Konfigurationsrichtlinien und Testanforderungen.

Upgrade-Verfahren können je nach Netzwerktyp, Gerätetyp oder neuen Softwareanforderungen stark variieren. Individuelle Anforderungen für Router- oder Switch-Upgrades können innerhalb einer Architekturgruppe entwickelt und getestet werden und in jeder Änderungsdokumentation referenziert werden. Andere Upgrades, die ganze Netzwerke umfassen, können nicht so einfach getestet werden. Diese Upgrades erfordern u. U. eine detailliertere Planung, die Einbeziehung des Anbieters und zusätzliche Schritte, um den Erfolg sicherzustellen.

Sie sollten Upgrade-Verfahren in Verbindung mit einer neuen Softwarebereitstellung oder einer

festgelegten Standardversion erstellen oder aktualisieren. Die Verfahren sollten alle Schritte für das Upgrade definieren, die Dokumentation des Anbieters zur Aktualisierung des Geräts referenzieren und Testverfahren für die Validierung des Geräts nach dem Upgrade bereitstellen. Sobald die Aktualisierungsverfahren definiert und validiert sind, sollte in allen für das jeweilige Upgrade geeigneten Änderungsdokumenten auf den Aktualisierungsvorgang verwiesen werden.

Lösungsvorlagen

Sie können Lösungsvorlagen verwenden, um standardmäßige modulare Netzwerklösungen zu definieren. Bei einem Netzwerkmodul kann es sich um einen Verteilerschrank, eine WAN-Außenstelle oder einen Zugriffskonzentrator handeln. In jedem Fall müssen Sie die Lösung definieren, testen und dokumentieren, um sicherzustellen, dass ähnliche Bereitstellungen auf die gleiche Weise durchgeführt werden können. Dadurch wird sichergestellt, dass künftige Änderungen auf einer deutlich geringeren Risikostufe für das Unternehmen vorgenommen werden, da das Verhalten der Lösung genau definiert ist.

Erstellen Sie Lösungsvorlagen für alle Bereitstellungen und Lösungen mit höherem Risiko, die mehrmals bereitgestellt werden. Die Lösungsvorlage enthält alle Standard-Hardware-, Software-, Konfigurations-, Verkabelungs- und Installationsanforderungen für die Netzwerklösung. Spezifische Details der Lösungsvorlage werden wie folgt angezeigt:

- Hardware- und Hardwaremodule, einschließlich Speicher-, Flash-, Stromversorgungs- und Kartenlayouts
- Logische Topologie, einschließlich Portzuweisungen, Anbindung, Geschwindigkeit und Medientyp
- Softwareversionen, einschließlich Modul- oder Firmware-Versionen.
- Alle nicht standardmäßigen, nicht gerätespezifischen Konfigurationen, einschließlich Routing-Protokolle, Medienkonfigurationen, VLAN-Konfiguration, Zugriffslisten, Sicherheit, Switching-Pfade, Spanning Tree-Parameter usw.
- Anforderungen an das Out-of-Band-Management.
- Kabelanforderungen.
- Installationsanforderungen, einschließlich Umgebung, Stromversorgung und Rack-Standorten

Beachten Sie, dass die Projektmappenvorlage nicht viele Anforderungen enthält. Spezifische Anforderungen wie die IP-Adressierung für die spezifische Lösung, Benennung, DNS-Zuweisungen, DHCP-Zuweisungen, PVC-Zuweisungen, Schnittstellenbeschreibungen und andere sollten durch allgemeine Konfigurationsmanagement-Verfahren abgedeckt werden. Allgemeine Anforderungen wie Standardkonfigurationen, Änderungspläne, Dokumentations-Update-Verfahren oder Verfahren für Netzwerkmanagement-Updates sollten durch allgemeine Konfigurationsmanagement-Verfahren abgedeckt werden.

Dokumentation pflegen

Es wird empfohlen, das Netzwerk und die im Netzwerk vorgenommenen Änderungen nahezu in Echtzeit zu dokumentieren. Sie können diese genauen Netzwerkinformationen für die Fehlerbehebung, die Gerätelisten für Netzwerkmanagement-Tools, den Bestand, die Validierung und Audits verwenden. Wir empfehlen die Verwendung der folgenden entscheidenden Erfolgsfaktoren für die Netzwerkdokumentation:

- Aktueller Geräte-, Verbindungs- und Endbenutzerbestand
- Konfigurationsversionskontrollsystem

- TACACS-Konfigurationsprotokoll
- Netzwerktopologie-Dokumentation

Bestand aktueller Geräte, Verbindungen und Endbenutzer

Aktuelle Daten zu Geräten, Verbindungen und Endbenutzerinventaren ermöglichen Ihnen die Nachverfolgung von Netzwerkbestand und -ressourcen, Auswirkungen auf Probleme und Auswirkungen auf Netzwerkänderungen. Die Möglichkeit, Netzwerkinventare und -ressourcen in Bezug auf Benutzeranforderungen nachzuverfolgen, trägt dazu bei, dass verwaltete Netzwerkgeräte aktiv genutzt werden, liefert Informationen, die für Audits benötigt werden, und unterstützt das Management von Geräteressourcen. Die Kundenbeziehungsdaten bieten Informationen zur Definition von Änderungsrisiken und -auswirkungen sowie zur Möglichkeit, Probleme schneller zu beheben und zu beheben. Die Bestandsdatenbanken für Geräte, Verbindungen und Endbenutzer werden in der Regel von zahlreichen führenden Service Provider-Organisationen entwickelt. Der führende Entwickler von Netzwerkinventarsoftware ist die Visionael Corporation . Die Datenbank kann Tabellen für Geräte, Links und Kunden-/Server-Daten enthalten, sodass Sie die Auswirkungen für Endbenutzer verstehen können, wenn ein Gerät ausgefallen ist oder Netzwerkänderungen auftreten.

Konfigurationsversionskontrollsystem

Ein Konfigurationsversionskontrollsystem verwaltet die aktuellen Konfigurationen aller Geräte und eine bestimmte Anzahl von Vorgängerversionen. Diese Informationen können zur Fehlerbehebung und Konfiguration oder zur Änderungsüberprüfung verwendet werden. Bei der Fehlerbehebung können Sie die aktuelle Konfiguration mit vorherigen Arbeitsversionen vergleichen, um festzustellen, ob die Konfiguration in irgendeiner Weise mit dem Problem verknüpft ist. Es wird empfohlen, drei bis fünf frühere Versionen der Konfiguration beizubehalten.

TACACS-Konfigurationsprotokoll

Um zu ermitteln, wer Konfigurationsänderungen vorgenommen hat und wann, können Sie die TACACS-Protokollierung und das NTP verwenden. Wenn diese Services auf Cisco Netzwerkgeräten aktiviert sind, werden die Benutzer-ID und der Zeitstempel der Konfigurationsdatei zum Zeitpunkt der Konfigurationsänderung hinzugefügt. Dieser Stempel wird dann mit der Konfigurationsdatei in das Konfigurationsversionskontrollsystem kopiert. TACACS kann dann als Abschreckung für nicht verwaltete Änderungen dienen und einen Mechanismus zur ordnungsgemäßen Prüfung von Änderungen bereitstellen. TACACS wird mithilfe des Cisco Secure-Produkts aktiviert. Wenn sich der Benutzer beim Gerät anmeldet, muss er sich beim TACACS-Server authentifizieren, indem er eine Benutzer-ID und ein Kennwort eingibt. NTP kann auf einem Netzwerkgerät problemlos aktiviert werden, indem es das Gerät auf eine NTP-Referenzuhr verweist.

Netzwerktopologie-Dokumentation

Die Topologiedokumentation hilft beim Verständnis und der Unterstützung des Netzwerks. Sie können damit Designrichtlinien validieren und ein besseres Verständnis des Netzwerks für zukünftige Design-, Änderungs- oder Fehlerbehebungsmaßnahmen gewinnen. Die Topologiedokumentation sollte logische und physische Dokumentationen umfassen, einschließlich Konnektivität, Adressierung, Medientypen, Geräte, Rack-Layouts, Kartenzuweisungen, Kabelweiterleitung, Kabelerkennung, Terminierungspunkte, Informationen zur Stromversorgung und Informationen zur Schaltkreiserkennung.

Die Pflege der Topologiedokumentation ist der Schlüssel zum erfolgreichen Konfigurationsmanagement. Um eine Umgebung zu schaffen, in der die Pflege der Topologiedokumentation möglich ist, muss auf die Wichtigkeit der Dokumentation hingewiesen werden, und die Informationen müssen für Aktualisierungen verfügbar sein. Es wird dringend empfohlen, die Topologiedokumentation bei jeder Netzwerkänderung zu aktualisieren.

Netzwerktopologiedokumentation wird in der Regel mit einer Grafikanwendung wie Microsoft Visio gepflegt. Andere Produkte wie Visionael bieten erstklassige Funktionen für das Management von Topologieinformationen.

Validierung und Audit-Standards

Leistungsindikatoren für das Konfigurationsmanagement bieten einen Mechanismus zur Validierung und Überprüfung von Netzwerkkonfigurationsstandards und kritischen Erfolgsfaktoren. Durch die Implementierung eines Prozessverbesserungsprogramms für das Konfigurationsmanagement können Sie mithilfe der Leistungsindikatoren Konsistenzprobleme identifizieren und das allgemeine Konfigurationsmanagement verbessern.

Wir empfehlen, ein funktionsübergreifendes Team zu bilden, um den Erfolg des Konfigurationsmanagements zu messen und die Prozesse des Konfigurationsmanagements zu verbessern. Das erste Ziel des Teams ist die Implementierung von Leistungsindikatoren für das Konfigurationsmanagement, um Probleme beim Konfigurationsmanagement zu identifizieren. Wir werden die folgenden Leistungsindikatoren für das Konfigurationsmanagement im Detail besprechen:

- Integritätsprüfungen
- Geräte-, Protokoll- und Medienüberprüfungen
- Überprüfung von Standards und Dokumentation

Nachdem Sie die Ergebnisse dieser Audits bewertet haben, leiten Sie ein Projekt ein, um Inkonsistenzen zu beheben, und ermitteln Sie dann die ursprüngliche Ursache des Problems. Mögliche Ursachen sind z. B. fehlende Dokumentation zu Standards oder ein fehlender konsistenter Prozess. Sie können die Dokumentation von Standards verbessern, Schulungen implementieren oder Prozesse optimieren, um weitere Inkonsistenzen bei der Konfiguration zu vermeiden.

Wir empfehlen monatliche Audits oder ggf. vierteljährliche Prüfungen, wenn nur Validierungen erforderlich sind. Überprüfung vergangener Audits, um sicherzustellen, dass Probleme in der Vergangenheit behoben wurden. Ermitteln Sie anhand der allgemeinen Verbesserungen und Ziele, welche Fortschritte und Wertschöpfung erzielt werden können. Erstellen Sie Kennzahlen, um die Anzahl der Inkonsistenzen bei der Netzwerkkonfiguration mit hohem, mittlerem und niedrigem Risiko aufzuzeigen.

Konfigurationsintegritätsprüfungen

Die Konfigurationsintegritätsprüfung sollte die Gesamtkonfiguration des Netzwerks, seine Komplexität und Konsistenz sowie potenzielle Probleme evaluieren. Für Cisco Netzwerke empfehlen wir die Verwendung des Konfigurationstools von Netsys. Dieses Tool gibt alle Gerätekonfigurationen ein und erstellt einen Konfigurationsbericht, der aktuelle Probleme wie doppelte IP-Adressen, nicht übereinstimmende Protokolle und Inkonsistenzen identifiziert. Das Tool meldet Verbindungs- oder Protokollprobleme, gibt jedoch keine Standardkonfigurationen für die Evaluierung auf den einzelnen Geräten ein. Sie können Konfigurationsstandards manuell

überprüfen oder ein Skript erstellen, das standardmäßige Konfigurationsunterschiede meldet.

Geräte-, Protokoll- und Medien-Audits

Geräte-, Protokoll- und Medienüberprüfungen sind ein Leistungsindikator für die Konsistenz in Softwareversionen, Hardware-Geräten und -Modulen, Protokollen und Medien sowie Namenskonventionen. Bei den Audits sollten zunächst alle nicht standardmäßigen Probleme identifiziert werden, die zu Konfigurationsaktualisierungen führen sollten, um die Probleme zu beheben oder zu verbessern. Evaluieren Sie Gesamtprozesse, um zu ermitteln, wie diese verhindern können, dass suboptimale oder nicht standardmäßige Bereitstellungen stattfinden.

Cisco RME ist ein Konfigurationsverwaltungstool, das Hardware-Versionen, Module und Softwareversionen prüfen und Berichte erstellen kann. Cisco entwickelt außerdem umfassendere Medien- und Protokollprüfungen, die auf Inkonsistenz mit IP, DLSW, Frame Relay und ATM hinweisen. Wenn kein Protokoll oder keine Medienüberwachung entwickelt wurde, können Sie manuelle Audits verwenden, z. B. das Überprüfen von Geräten, Versionen und Konfigurationen für alle Geräte in einem Netzwerk oder das Überprüfen von Geräten, Versionen und Konfigurationen, die vor Ort überprüft werden.

Überprüfung von Standards und Dokumentation

Dieser Leistungsindikator überprüft die Netzwerk- und Standarddokumentation, um sicherzustellen, dass die Informationen korrekt und auf dem neuesten Stand sind. Das Audit sollte die Überprüfung der aktuellen Dokumentation, die Empfehlung von Änderungen oder Ergänzungen und die Genehmigung neuer Standards umfassen.

Sie sollten die folgenden Unterlagen vierteljährlich überprüfen: Standardkonfigurationsdefinitionen, Lösungsvorlagen mit empfohlenen Hardwarekonfigurationen, aktuellen Standard-Softwareversionen, Aktualisierungsverfahren für alle Geräte und Softwareversionen, Topologiedokumentation, aktuelle Vorlagen und IP-Adressverwaltung.

Zugehörige Informationen

- Technischer Support – Cisco Systems