Cisco Best Practices: Cisco IOS-Managementoperationen

Inhalt

Zusammenfassung

Cisco Leading Practices umfassen eine Reihe kodifizierter Dokumente, die wichtige und zuverlässige Anleitungen für den Netzwerkbetrieb von Cisco Produkten und Lösungen liefern. Die Best Practices werden von preisgekrönten Cisco TAC- und Advanced Services-Technikern entwickelt und unterstützt, die Sie bei der Entwicklung Ihrer eigenen Best Practices unterstützen. Cisco Kunden setzen diese Best Practices in ihrer Netzwerkumgebung ein, um Netzwerkleistung und -verfügbarkeit zu verbessern.

Es wird dringend empfohlen, diese Best Practices durch Services von Cisco und seinen Partnern zu ergänzen. Weitere Informationen zur Optimierung von Netzwerkleistung und -verfügbarkeit erhalten Sie von Ihrem Ansprechpartner für Services auf der Cisco Advanced Services-Website. Dort erhalten Sie weitere Informationen zu Network Optimization Support - Focused Engineering

Support, Network Availability Improvement Support (NAIS), Software Management Process Assessment (SMPA) und NAIS-SMPA Implementation.

Einleitung

Überblick

Betriebsprozesse rund um das Software-Management können dazu beitragen, die Netzwerkkomplexität zu reduzieren, reaktive Supportprobleme zu reduzieren und die Problembehebungszeit zu verkürzen. Dieses Dokument enthält eine Strategie, Empfehlungen zu Tools und Best Practices für die allgemeine Verwaltung der Cisco IOS® Software (Cisco IOS).

Die Abschnitte Erstellen einer Cisco IOS Management Operations Strategy und Befolgen eines Best Practice Cisco IOS Management Operations Process in diesem Dokument besprechen die empfohlene Methodik für den Einstieg und enthalten die besten Tools für die Betriebsphase. Die Betriebsphase umfasst Best Practice-Prozesse für:

Prozess	Beschreibung
Software-Versionskontrolle	Verfolgung, Validierung und Verbesserung der Softwarekonsistenz innerhalb der identifizierten Software-Tracks.
Fehlermanagement	Proaktive Überwachung und Reaktion auf von Cisco IOS generierte SNMP- und Syslog-Meldungen höherer Priorität
Problemmanagement	Schnelle und effiziente Erfassung wichtiger Probleminformationen zu softwarebezogenen Problemen, um zu verhindern, dass es in Zukunft zu Vorfällen kommt.
Standardisierung der Konfiguration	"Standardisierung" von Konfigurationen, um das Potenzial für ungetesteten Code in der Produktion zu reduzieren und das Verhalten von Netzwerkprotokollen und -funktionen zu standardisieren.
Verfügbarkeitsmanagement	Verbesserung der Verfügbarkeit anhand von Kennzahlen, Verbesserungszielen und Verbesserungsprojekten

In diesem Dokument wird davon ausgegangen, dass Sie die folgenden Best Practice-Prozesse für die Planung, das Design und die Implementierung von Cisco IOS implementiert haben:

- Auf Plattform-, Modul-, Funktions-, Protokoll- und Topologieanforderungen basierende, verwaltbare Softwarebereiche (Software-Tracks) in Ihrer Umgebung identifiziert.
- Cisco IOS-Versionen pro Software-Programmzweig ausgewählt, zertifiziert und kommuniziert.
- Konsistente Implementierung der Cisco IOS-Standardversionen in die einzelnen Software-Programmzweige

Ziele

Dieser Abschnitt unterstützt Sie bei der Verwaltung und Pflege standardisierter Cisco IOS-Versionen innerhalb definierter Programmzweige. In diesem Kurs erfahren Sie, wie Sie:

- Entwickeln Sie einen Prozess zur Softwareversionskontrolle, um die Konsistenz der Softwareversionen innerhalb der identifizierten Software-Programmzweige sicherzustellen.
- Überwachung, Benachrichtigung und Behebung von Prozessen auf der Grundlage von Fehlermanagement-Meldungen und Warnmeldungen (SNMP/Syslog) für das Gerät, um proaktiv bei der Behebung potenzieller Software- und Fehlerprobleme zu helfen.
- Effiziente Erfassung kritischer Probleminformationen für Software, um die Zeit für die Problembehebung bei softwarebezogenen Problemen zu verkürzen.
- Standardisierung von Gerätekonfigurationen zur Gewährleistung von Protokollen, Funktionen, Zugriff und Sicherheit in der Umgebung

Zielgruppe

Dieses Dokument ist für Personen und Manager mit technischer Ausrichtung geeignet, die für den täglichen Netzwerkbetrieb verantwortlich sind. In diesem Dokument wird beschrieben, wie Sie Betriebsprozesse einrichten, um die Netzwerkkomplexität zu reduzieren, reaktive Support-Probleme zu reduzieren und die Problembehebungszeit zu verkürzen, indem Netzwerkkonsistenz geschaffen und die Funktionen für ein proaktives Fehlermanagement verbessert werden.

Voraussetzungen

Diejenigen, die an den Cisco IOS-Managementvorgängen beteiligt sind, sollten über fundierte Kenntnisse im Design und in der Verwaltung der Netzwerkinfrastruktur verfügen, insbesondere mit Geräten von Cisco. Sie müssen Zugriff auf Details der Topologie, Gerätekonfiguration, dem Aktivitätsprofil, der Anwendungsnutzung und der Ressourcenauslastungsrichtlinie des Zielnetzwerks haben. Der Zugriff auf und die Nutzung der in Cisco Connection Online (CCO) verfügbaren Informationstools ist ebenfalls erforderlich. Falls Sie noch nicht bei CCO registriert sind, empfehlen wir Ihnen, dies für den Zugriff auf die in diesem Dokument beschriebenen Tools zu tun.

Erstellen einer Cisco IOS Management Operations Strategy

Zur Verwaltung von Cisco IOS-Umgebungen stehen zahlreiche Qualitätsstrategien und -tools zur Verfügung. Dieses Kapitel konzentriert sich auf drei wichtige Strategien für das Management von Cisco IOS-Prozessen in Umgebungen mit höherer Verfügbarkeit und enthält eine Matrix von wichtigen Betriebstools, die speziell für die Verwaltung von Cisco IOS- und Cisco IOS-Problemen hilfreich sind.

Die erste wichtige Strategie besteht darin, die Umgebung so einfach wie möglich zu gestalten und so viele Abweichungen bei der Konfiguration und den Cisco IOS-Versionen wie möglich zu vermeiden. Die Cisco IOS-Zertifizierung wurde bereits diskutiert, aber die Konsistenz der Konfiguration ist ein weiterer wichtiger Bereich. Die Architektur-/Engineering-Gruppe sollte für die Erstellung von Konfigurationsstandards zuständig sein. Die Implementierungs- und Betriebsgruppe ist dann für die Konfiguration der Standards und die Einhaltung der Standards durch die Cisco IOS-Versionskontrolle und die Cisco IOS-Konfigurationsstandards/-kontrolle verantwortlich.

Die zweite wichtige Strategie besteht darin, Netzwerkfehler zu erkennen und schnell zu beheben.

Die Betriebsgruppe sollte im Allgemeinen Netzwerkprobleme identifizieren, bevor Benutzer diese melden. Probleme sollten so schnell wie möglich gelöst werden, ohne dass die Umgebung weiter beeinträchtigt oder verändert wird. Zwei wichtige Best Practices in diesem Bereich sind das Problem Management und das Fehlermanagement (beide werden später in diesem Dokument behandelt).

Hinweis: Mit dem Cisco IOS-Stack-Decoder-Tool können Abstürze der Cisco IOS-Software schnell diagnostiziert werden.

Die dritte Schlüsselstrategie ist eine "konsequente Verbesserung". Der primäre Prozess ist die Verbesserung eines qualitätsbasierten Programms zur Verbesserung der Verfügbarkeit. Durch die Durchführung von Ursachenanalysen für alle Probleme, einschließlich Cisco IOS-bezogene Probleme, kann ein Unternehmen die Testabdeckung verbessern, die Problembehebungszeiten verkürzen und Prozesse optimieren, die die Auswirkungen von Ausfällen beseitigen oder reduzieren. Darüber hinaus können allgemeine Probleme analysiert und Prozesse entwickelt werden, um diese Probleme schneller zu beheben.

Identifizierung der Leistungen

Zu den Leistungen des Cisco IOS Software Management-Prozesses gehören:

- Softwareversionskontrollprozesse und -tools
- Fehlermanagement-Überwachung und -Prozesse
- Problemmanagement-Prozesse
- Gerätekonfigurationsstandards und Auditprozesse
- Verfahren zur Netzwerkverfügbarkeit, Berichterstellung und Überprüfung

Identifizierung wichtiger Gerätemessungen

Kennzahlen sollten im Rahmen des Betriebsplans definiert und verwendet werden, um zu bestimmen, ob die Tools und Prozesse die gewünschten Ergebnisse liefern. Im Folgenden finden Sie einige Beispiele für hilfreiche Kennzahlen zur Verwaltung der Cisco IOS-Software:

- Netzwerkverfügbarkeit (aufgrund von Softwareproblemen)
- % Einhaltung von Standards bei Cisco IOS-Versionen (auf Track-Basis)
- Konsistenz der Gerätekonfiguration in % (basierend auf Standards)
- Kennzahlen zum Problem Management (MTTR, Anzahl Tickets, Abschlusscodes)

Definition von Rollen und Verantwortlichkeiten

Identifizieren, qualifizieren und zusammenstellen einer funktionsübergreifenden Gruppe von Managern und/oder Leads aus den Bereichen Netzwerkarchitektur, Netzwerktechnik und Implementierung/Betrieb, um die erfolgreiche Planung, Entwicklung, Implementierung und Betriebsphase von IOS-Upgrades sicherzustellen.

Erforderliche Fachgebiete ermitteln

Stellen Sie eine funktionsübergreifende Gruppe von Managern und/oder Leitern aus den Bereichen Netzwerkmanagement, Netzwerktechnik, Implementierung und Betrieb zusammen, die

Sie bei der Betriebsphase Ihres Cisco IOS-Managementprojekts unterstützen.

Ermittlung der wichtigsten Beitragszahler

- Netzwerkmanager:Name des/der Manager, Abteilung, KontaktinformationenName der primären Sicherung, Abteilung, KontaktinformationenSekundärer Sicherungsname, Abteilung, Kontaktinformationen, falls erforderlich
- Netzwerkarchitekten:Name des/der Architekten, Abteilung, KontaktinformationenName der primären Sicherung, Abteilung, KontaktinformationenSekundärer Sicherungsname, Abteilung, Kontaktinformationen, falls erforderlich
- Netzwerktechniker:Name des/der Techniker, Abteilung, KontaktinformationenName der primären Sicherung, Abteilung, KontaktinformationenSekundärer Sicherungsname, Abteilung, Kontaktinformationen, falls erforderlich
- NOC-Techniker (Network Operations):Name des/der Techniker, Abteilung, KontaktinformationenName der primären Sicherung, Abteilung, KontaktinformationenSekundärer Sicherungsname, Abteilung, Kontaktinformationen, falls erforderlich

Verantwortlichkeiten identifizieren

- Netzwerkmanager sind verantwortlich für:Verwalten des ProjektplansZuweisen/Zuweisen von RessourcenVerwalten der ÄnderungskontrolleVerwaltung des FortschrittsVerwalten der Budgetberichterstattung
- Netzwerkarchitekten sind verantwortlich für:Analyse von Netzwerkstandards und VersionshinweiseWartung der Software-Upgrade-MatrixVerwalten der KandidatenverwaltungsmatrixVerwalten der Matrix der Speicheranforderungen
- Netzwerktechniker (NOC) sind für Folgendes verantwortlich:Implementierung und Sicherstellung der Einhaltung von NetzwerkstandardsIdentifizierung von Softwareproblemen und UrsachenEmpfehlung von KorrekturmaßnahmenÜberwachen des Netzwerks

Budgetierung von Ressourcen

Die Ressourcenanforderungen sollten in der Betriebsphase festgelegt werden, um die Softwaremanagementstrategie für das Unternehmen zu unterstützen. Dazu gehören die für die Softwarestrategie erforderlichen personellen Zeit- und Kapitalausgaben.

In vielen Fällen kann ein Return on Investment (ROI) oder ein Budgetplan für Software-Management-Verfahren basierend auf den Kosten für Ausfallzeiten und Verfügbarkeitsanforderungen erstellt werden. Wenn das Unternehmen Ausfallzeiten aufgrund von Softwareproblemen ermitteln kann, kann der Großteil dieser Kosten über die ermittelten Best Practices für das Softwaremanagement ausgeglichen werden. Wenn die Kosten nicht vollständig ausgeglichen werden können, sollte das Unternehmen eine grundlegendere Strategie für das Softwaremanagement in Betracht ziehen, die dazu beiträgt, die Produktivität zu verbessern, indem zusätzliche Nachbearbeitungen aufgrund von Softwareproblemen vermieden werden.

Best Practice-Verfahren für Cisco IOS-Managementoperationen

Zu den Best Practices für das Befolgen eines Cisco IOS Management Operations-Prozesses

gehören:

Best Practices	Details
Software-Versionskontrolle	Implementieren Sie nur standardisierte Softwareversionen, und überwachen Sie das Netzwerk, um Software aufgrund der Nichtversionskonformität zu validieren oder möglicherweise zu ändern.
Fehlermanagement	Die Erfassung, Überwachung und Analyse von SNMP- und Syslog-Meldungen sind Fehlermanagementprozesse, die zur Behebung von Problemen mit Cisco IOS-spezifischen Netzwerken empfohlen werden, die auf andere Weise schwierig oder unmöglich zu identifizieren sind.
Problemmanagement	Detaillierte Problemmanagement-Prozesse, die Problemerkennung, Informationserfassung und einen gut analysierten Lösungspfad definieren. Diese Daten werden zur Bestimmung der Ursache verwendet.
Standardisierung der Konfiguration	Konfigurationsstandards stellen die gängige Praxis dar, "globale" Standardkonfigurationsparameter für Geräte und Services zu erstellen und beizubehalten. Dies führt zu einer globalen Konsistenz der Konfiguration im gesamten Unternehmen.
Verfügbarkeitsmanagement	Qualitätssteigerung durch Netzwerkverfügbarkeit als Metrik zur Qualitätsverbesserung.

Software-Versionskontrolle

Die Softwareversionskontrolle umfasst die Implementierung nur standardisierter Softwareversionen und die Überwachung des Netzwerks, um Software aufgrund der Nichtversionskonformität zu validieren oder möglicherweise zu ändern. Im Allgemeinen erfolgt die Softwareversionskontrolle mithilfe eines Zertifizierungsprozesses und der Standardkontrolle. Viele Unternehmen veröffentlichen Versionsstandards auf einem zentralen Webserver. Darüber hinaus ist ein Implementierungspersonal darauf geschult, die ausgeführte Version zu überprüfen und die Version zu aktualisieren, wenn sie nicht den Standards entspricht. Einige Unternehmen verfügen über einen Prozess, bei dem eine sekundäre Validierung durch Audits durchgeführt wird, um sicherzustellen, dass der Standard bei der Implementierung eingehalten wird.

Beim Netzwerkbetrieb sind auch nicht standardmäßige Softwareversionen im Netzwerk zu beobachten, insbesondere wenn das Netzwerk groß ist und ein großer Teil der Mitarbeiter im Betrieb beschäftigt. Dies kann auf einen der folgenden Gründe zurückzuführen sein:

- Ungeschultes neueres Personal

- Falsch konfigurierte Boot-Befehle
- Nicht geprüfte Implementierungen

Es wird empfohlen, Softwareversionsstandards regelmäßig mithilfe von Tools wie CiscoWorks200 Resource Manager Essentials (RME) zu validieren, mit denen alle Geräte nach der Cisco IOS-Version sortiert werden können. Wenn eine nicht standardmäßige Version identifiziert wird, sollte diese sofort markiert und ein Trouble Ticket oder ein Change Ticket gestartet werden, um die Version auf den festgelegten Standard zu bringen.

Verfügbare Tools

CiscoWorks2000 RME Inventory Manager vereinfacht die Verwaltung von Cisco IOS-Versionen für Router und Switches mithilfe webbasierter Reporting-Tools, die Geräte anhand von Softwareversion, Geräteplattform und Gerätenamen melden und sortieren.

Fehlermanagement

Beim Fehlermanagement werden SNMP- und Syslog-Meldungen erfasst, überwacht und analysiert, um mehr Cisco IOS-spezifische Netzwerkprobleme zu beheben, die schwer oder unmöglich auf andere Weise zu identifizieren sind.

SNMP-Trap-Sammlung

Die Erfassung und Benachrichtigung von SNMP-Traps ist ein grundlegender Prozess im Fehlermanagement, der verwendet wird, um Software- oder Hardwareereignisse und/oder Abstürze ohne SNMP-Polling-Overhead oder Verzögerungen durch Polling-Intervalle zu identifizieren. Trap-Meldungen werden direkt vom Netzwerkgerät zu einem Netzwerkmanagementsystem generiert, das Benachrichtigungsdienste bereitstellt. Die Erfassung und Benachrichtigung dieser Traps ist für die schnelle Behebung vieler Netzwerkereignisse, einschließlich nicht benutzerrelevanter Ereignisse, wie z. B. Verlust von primären Geräten oder Verbindungen in einer redundanten Umgebung, unerlässlich.

Um diese Traps sammeln und überwachen zu können, müssen die Traps sowohl auf dem Gerät als auch in den Netzwerkmanagementsystemen korrekt konfiguriert sein. Die Netzwerkmanagementsysteme sollten die Netzwerkbetriebsgruppe benachrichtigen, wenn ein Trap empfangen wurde. Die Benachrichtigung kann dann in Form von Paging, E-Mail oder Ereignisbildschirmen in einer NOC-Umgebung erfolgen.

Unabhängig davon, wie die Daten präsentiert werden, müssen diese Fehlerinstanzen oder Ausnahmen regelmäßig (vorzugsweise täglich) vom Netzwerkbetrieb und/oder Netzwerk-Support-Personal analysiert und geprüft werden. Die Ursachen aller gefundenen Ausnahmen sollten untersucht werden. Einige protokollierte Ausnahmen sind möglicherweise nicht wichtig genug, um sofort einen Alarm im Network Operations Center auszulösen. Die proaktive Überprüfung, Untersuchung und Behebung geringfügiger Ausnahmen kann Netzwerk-Support-Gruppen dabei unterstützen, Netzwerkausfälle zu reduzieren oder zu verhindern.

Syslog-Meldungserfassung

Syslog-Meldungen werden vom Gerät an einen Erfassungsserver gesendet. Diese Meldungen können Hardware- oder Softwarefehler sein oder Informationen enthalten (z. B. wenn sich jemand im Terminal eines Geräts befindet).

Die Syslog-Überwachung erfordert Unterstützung für das Network Management System (NMS)-

Tool oder Skripts, die bei der Analyse und dem Reporting von Syslog-Daten helfen. Dazu gehört die Möglichkeit, Syslog-Meldungen nach Datum oder Uhrzeit, Gerät, Syslog-Meldungstyp oder Häufigkeit der Meldungen zu sortieren. In größeren Netzwerken können Tools oder Skripts implementiert werden, um Syslog-Daten zu analysieren und Alarme oder Benachrichtigungen an Ereignismanagementsysteme oder Betriebspersonal zu senden. Wenn Warnungen für eine Vielzahl von Syslog-Daten nicht verwendet werden, sollte die Organisation Syslog-Daten mit höherer Priorität mindestens täglich überprüfen und Support-Tickets für potenzielle Probleme erstellen. Um Netzwerkprobleme proaktiv zu erkennen, die bei der normalen Überwachung möglicherweise nicht sichtbar sind, sollten regelmäßige Überprüfungen und Analysen der historischen Syslog-Daten durchgeführt werden, um Situationen zu erkennen, die nicht auf ein unmittelbares Problem hindeuten können, jedoch ein Anzeichen für ein Problem sein können, bevor es zu Servicebeeinträchtigungen wird.

Verfügbare Tools

Zu den gängigsten SNMP-Trap-Receiver-Tools gehören:

- HP OpenView Network Node Manager von Hewlett Packard unter openview.hp.com
- Spectrum Integrity von Aprisma unter www.aprisma.com
- NetView von IBM Tivoli unter www.tivoli.com

Das beliebteste Syslog-Tool für die Cisco IOS-Verwaltung ist der CiscoWorks2000 RME Syslog Manager. Weitere verfügbare Tools sind SL4NT, ein Shareware-Programm von www.netal.com , das cisco.com verlässt, und Private I von OpenSystems unter www.opensystems.com

Problemmanagement

Problemmanagement, ein Aspekt des Fehlermanagements, ist die Disziplin, Probleme vom Eintreten bis zur Identifizierung, Fehlerbehebung, Behebung und Schließung zu verwalten.

Viele Kunden verzeichnen zusätzliche Ausfallzeiten aufgrund fehlender Prozesse im Problem Management. Weitere Ausfallzeiten können auftreten, wenn Netzwerkadministratoren versuchen, das Problem schnell mithilfe einer Kombination aus servicerelevanten Befehlen oder Konfigurationsänderungen zu beheben, anstatt Zeit für die Problemerkennung, die Erfassung von Informationen und einen gut analysierten Lösungspfad zu verbringen. Das beobachtete Verhalten in diesem Bereich beinhaltet das Neuladen von Geräten oder das Löschen von IP-Routing-Tabellen, bevor ein Problem und dessen Ursache untersucht werden. In einigen Fällen liegt dies an der Problemlösung auf der ersten Support-Ebene. Das Ziel bei allen softwarebezogenen Problemen sollte es sein, schnell die erforderlichen Informationen für die Ursachenanalyse zu sammeln, bevor die Verbindung oder der Service wiederhergestellt wird.

Es wird empfohlen, ein Problem-Management-Verfahren einzuführen, das ein gewisses Maß an Standard-Problembeschreibungen und angemessene "show"-Befehlsauflistungen umfasst, bevor das Problem auf eine zweite Support-Ebene eskaliert wird. Der First-Level-Support sollte niemals das Löschen von Routen oder das Neuladen von Geräten beinhalten. Im Idealfall sollte der erste Support-Mitarbeiter schnell Informationen sammeln und das Problem dann an den zweiten Support eskalieren. Indem Sie etwas mehr Zeit in die Identifizierung und Beschreibung des Problems im Level-1-Support investieren, ist eine Ursachenerkennung viel wahrscheinlicher, was eine Problemumgehung, Laborerkennung und Fehlerberichte ermöglicht. Der Support auf zweiter Ebene sollte gut mit den Informationen vertraut sein, die Cisco möglicherweise benötigt, um ein Problem zu diagnostizieren oder einen Fehlerbericht zu erstellen. Dazu gehören:

- Speicherabbilder

- Ausgabe von Routing-Informationen
- Ausgabe des Befehls "Device show"

Standardisierung der Konfiguration

Globale Gerätekonfigurationsstandards ermöglichen die Beibehaltung "globaler" Standardkonfigurationsparameter für Geräte und Services, was zu einer unternehmensweiten globalen Konsistenz der Konfiguration führt. Globale Konfigurationsbefehle sind Befehle, die auf das gesamte Gerät und nicht auf einzelne Ports, Protokolle oder Schnittstellen angewendet werden und sich im Allgemeinen auf den Gerätezugriff, das allgemeine Geräteverhalten und die Gerätesicherheit auswirken. In Cisco IOS enthält dies die folgenden Befehle:

- Service
- IP
- VTY
- Konsolenport
- Protokollieren
- AAA/TACACS+
- SNMP
- Banner

Wichtig bei globalen Gerätekonfigurationsstandards ist auch eine geeignete Namenskonvention für Geräte, die es Administratoren ermöglicht, das Gerät, den Gerätetyp und den Gerätestandort anhand des DNS-Namens des Geräts zu identifizieren. Die globale Konsistenz der Konfiguration ist für die allgemeine Unterstützung und Zuverlässigkeit einer Netzwerkumgebung wichtig, da sie dazu beiträgt, die Netzwerkkomplexität zu reduzieren und die Netzwerkunterstützung zu verbessern. Probleme bei der Unterstützung treten häufig ohne Standardisierung der Konfiguration auf, da das Geräteverhalten inkorrekt oder inkonsistent ist, der SNMP-Zugriff nicht funktioniert und die allgemeine Gerätesicherheit nicht gewährleistet ist.

Die Einhaltung globaler Gerätekonfigurationsstandards wird in der Regel von einer internen Engineering- oder Betriebsgruppe durchgeführt, die globale Konfigurationsparameter für ähnliche Netzwerkgeräte erstellt und verwaltet. Es empfiehlt sich auch, eine Kopie der globalen Konfigurationsdatei in TFTP-Verzeichnissen bereitzustellen, damit diese zunächst auf alle neu bereitgestellten Geräte heruntergeladen werden können. Außerdem ist eine für das Internet zugängliche Datei hilfreich, die die Standardkonfigurationsdatei mit einer Erläuterung der einzelnen Konfigurationsparameter bereitstellt. Einige Unternehmen konfigurieren alle Geräte regelmäßig, um eine globale Konsistenz der Konfiguration sicherzustellen, oder überprüfen Geräte regelmäßig auf die korrekten globalen Konfigurationsstandards.

Schnittstellen- oder Protokollkonfigurationsstandards sind die Praxis, Standards für die Schnittstellen- und Protokollkonfiguration beizubehalten. Dies verbessert die Netzwerkverfügbarkeit, indem die Netzwerkkomplexität verringert, das erwartete Geräte- und Protokollverhalten bereitgestellt und die Netzwerkunterstützung verbessert wird. Inkonsistente Schnittstellen- oder Protokollkonfigurationen können zu unerwartetem Geräteverhalten, Problemen bei der Datenverkehrsweiterleitung, erhöhten Konnektivitätsproblemen und einer erhöhten Reaktionszeit beim Support führen.

Schnittstellenkonfigurationsstandards können Folgendes umfassen:

- CDP (Cisco Discovery Protocol)
- Schnittstellendeskriptoren

- Caching-Konfiguration
- Weitere protokollspezifische Standards

Protokollspezifische Konfigurationsstandards können Folgendes umfassen:

- IP-Routing-Konfiguration
- DLSW-Konfiguration
- Konfiguration der Zugriffslisten
- ATM-Konfiguration
- Konfiguration von Frame-Relay
- Spanning Tree-Konfiguration
- VLAN-Zuweisung und -Konfiguration
- VTP (Virtual Trunking Protocol)
- HSRP (Hot Standby Routing Protocol)
- Andere, je nachdem, was im Netzwerk konfiguriert wird

Ein Beispiel für IP-Standards kann die Subnetzgröße, der verwendete IP-Adressraum, das verwendete Routing-Protokoll und die Routing-Protokollkonfiguration sein.

Die Einhaltung von Protokoll- und Schnittstellenkonfigurationsstandards liegt normalerweise in der Verantwortung der Netzwerktechniker- und Implementierungsgruppen. Die technische Gruppe sollte für die Identifizierung, das Testen, die Validierung und die Dokumentation der Standards zuständig sein. Die Implementierungsgruppe ist dann für die Bereitstellung neuer Dienste mithilfe der Engineering-Dokumente oder Konfigurationsvorlagen verantwortlich. Die Techniker sollten Dokumentation zu allen Aspekten der geforderten Standards erstellen, um die Konsistenz sicherzustellen. Außerdem sollten Konfigurationsvorlagen erstellt werden, um die Durchsetzung der Konfigurationsstandards zu erleichtern. Die Betriebsgruppen sollten auch für die Standards geschult werden und in der Lage sein, nicht standardmäßige Konfigurationsprobleme zu identifizieren. Die Konsistenz der Konfiguration ist in der Test-, Validierungs- und Zertifizierungsphase von großer Bedeutung. Ohne standardisierte Konfigurationsvorlagen ist es nahezu unmöglich, eine Cisco IOS-Version für ein mäßig großes Netzwerk angemessen zu testen, zu validieren oder zu zertifizieren.

Verfügbarkeitsmanagement

Das Verfügbarkeitsmanagement ist der Prozess der Qualitätsverbesserung, bei dem die Netzwerkverfügbarkeit als Metrik zur Qualitätsverbesserung eingesetzt wird. Viele Unternehmen messen mittlerweile Verfügbarkeit und Ausfallart. Ausfallarten können Folgendes umfassen:

- Hardware
- Software
- Verbindung/Träger
- Stromversorgung/Umgebung
- Design
- Benutzerfehler/Prozess

Indem das Unternehmen Ausfälle identifiziert und unmittelbar nach der Wiederherstellung Ursachenanalysen durchführt, kann es Methoden zur Verbesserung der Verfügbarkeit identifizieren. Fast alle Netzwerke, die eine hohe Verfügbarkeit erreicht haben, verfügen über einen bestimmten Prozess zur Qualitätsverbesserung.

Checkliste für Cisco IOS Management Operations

❑Schritt 1: Definition von Geschäftsanforderungen und -zielen (nur registrierte Kunden)

❑Phase 2: Bewertung des aktuellen Status der Cisco IOS Software Management Practices (nur registrierte Kunden)

❑Schritt 3: Rollen und Verantwortlichkeiten definieren (nur registrierte Kunden)

❑Schritt 4: Entwicklung eines Projektplans für das Softwaremanagement (nur registrierte Kunden)

❑Schritt 5: Entwicklung einer Matrix für Softwareanforderungen (nur registrierte Kunden)

Zugehörige Informationen

Ein Anhang wurde erstellt, um den Kunden beim Erhalt weiterer wichtiger Cisco IOS-Informationen zu unterstützen, z. B.: Cisco IOS-Grundlagen, interne Cisco IOS-Softwareprozesse, Software-Zuverlässigkeitsanalyse, internes Cisco Qualitätsprogramm, interne Testmethoden von Cisco und eine Feldanalyse, die aktuelle Branchenpraktiken und die allgemeine Kundenerfahrung mit der Cisco IOS-Software aufzeigt

- Cisco IOS-Management: Weitere Informationen zum Cisco IOS-Management und zu Best Practices finden Sie im Whitepaper "Cisco IOS Management for High Availability Networking" unter: http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a00800a998b.shtml
- Detaillierte Informationen zum Ausführen von Netzwerkprüfungen, zu verwendenden CLI-Befehlen, zum Analysieren und Interpretieren von Netzwerkverkehrsdaten und zum Festlegen von Anwendungsnutzungsrichtlinien finden Sie unter http://www.cisco.com. Diese Website bietet ein umfassendes Angebot an Support-, Schulungs-, technischen Referenzen und Beratungslösungen.
- Cisco IOS verfügt über spezifische Benennungskonventionen, die hier definiert sind: http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_tech_note09186a0080101cda.shtml
- Informationen zur Verfügbarkeit von Cisco IOS-Versionen finden Sie hier: http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html
- Cisco IOS-Versionen werden schließlich aus CCO entfernt und können nicht mehr bestellt werden. Stellen Sie sicher, dass Sie die Erwartungen des Kunden entsprechend festlegen.
- Cisco IOS-Produktmitteilungen werden verwendet, um Kunden über Cisco IOS-Versionen zu informieren. Sie enthalten kurze Informationen zum Veröffentlichungsinhalt. Informationen zur Verfügbarkeit neuer Cisco IOS-Versionen finden Sie hier http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html
- Das Product Security Incident Response Team ist für die Sicherheit von Cisco Produkten zuständig. Alle Cisco IOS-Sicherheitsprobleme sollten an dieses Team verwiesen werden. Cisco veröffentlicht seine Sicherheitslücken öffentlich. http://tools.cisco.com/security/center/publicationListing
- Cisco IOS-Fehler: Schwerwiegende Cisco IOS-Fehler sollten für einen Aufschub empfohlen

werden. Jeder Mitarbeiter von Cisco kann die Empfehlung abgeben.
- Problemfälle im Cisco IOS werden den Kunden über Cisco IOS-Ratgeber mitgeteilt. http://www.cisco.com/en/US/products/products_security_advisory09186a0080b20ee1.shtml
- Funktionen von Cisco IOS: Mit dem Feature Navigator können Kunden nach Releases suchen, die bestimmte Funktionen unterstützen, und umgekehrt. http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp
- Mit dem Cisco Software Advisor können Kunden Software-Support für Funktionen oder Software-Support für Hardware finden. http://tools.cisco.com/Support/Fusion/FusionHome.do (nur registrierte Kunden)

Cisco Services und Support

- Technische Support-Services
- Spezielle Services für Netzwerktechnologien und -lösungen von Cisco