Cisco Leading Practices: Cisco IOS-beheerbewerkingen

Inhoud

Abstract
Inleiding
Overzicht
Doelstellingen
publiek
Voorwaarden
Een Cisco IOS-beheerstrategie maken
Identificatie van te leveren producten
Bepalingen van de belangrijkste voorzieningen
Vaststelling van taken en verantwoordelijkheden
Aanwijzen van de vereiste expertisegebieden
Identificatie van de belangrijkste contribuanten
Verantwoordelijkheden identificeren
Bronnen
Na een optimaal gebruik van Cisco IOS-beheerbewerkingen
Software versie Control
Foutenbeheer
Probleembeheer
Standaardisatie voor configuratie
Beschikbaarheidsbeheer
Cisco IOS-controlelijst voor beheerbewerkingen
Gerelateerde informatie
Cisco-services en -ondersteuning

Abstract

Cisco Leading Practices zijn een reeks gecodificeerde documenten die relevante en betrouwbare richtlijnen voor netwerkbewerkingen voor Cisco-producten en -oplossingen bieden. De leidende praktijken worden ontwikkeld en ondersteund door de prijswinnende Cisco TAC en de Geavanceerd Services engineers die u kunt gebruiken om uw eigen reeks leidende praktijken te creëren om te nabootsen. Cisco-klanten hebben deze leidende praktijken in hun netwerkomgeving toegepast om netwerkprestaties en beschikbaarheid te bereiken.

Het wordt sterk aanbevolen om deze leidende praktijken aan te vullen met de diensten van Cisco en zijn partners. Voor meer informatie over het optimaliseren van uw netwerkprestaties en -beschikbaarheid kunt u contact opnemen met uw servicesvertegenwoordiger over de website van Cisco Advanced Services en meer informatie vinden over de website voor netwerkoptimalisatie -

Gerichte Engineering Support, Network Availability Improvement Support (NAIS), Softwarebeheerevaluatie (SMPA) en de implementatie van NAIS-SMPA.

Inleiding

Overzicht

Operationele processen rond softwarebeheer kunnen netwerkcomplexiteit verminderen, reactieve ondersteuningskwesties verminderen en de tijd voor probleemoplossing verbeteren. Dit document biedt een strategie, aanbevelingen voor gereedschap en best practices voor het algehele beheer van Cisco IOS® software (Cisco IOS).

Het maken van een Cisco IOS Beheersstrategie en Volgend op een secties van het Bewerkingsproces van Cisco IOS van de Beste Handelingen van Bewerkingen in dit document bespreken de aanbevolen methodologie om begonnen te worden en lijsten de beste die voor de exploitatiefase moeten worden gebruikt. De operationele fase omvat de best practice-processen voor:

verwerken	Beschrijving
Softwareversiebeheer	Het traceren, valideren en verbeteren van softwareconsistentie binnen de geïdentificeerde software "sporen".
Foutenbeheer	Proactief toezicht houden op en optreden bij SNMP- en systeemmeldingen die door Cisco IOS gegenereerd zijn.
Probleembeheer	snel en efficiënt kritische probleeminformatie verzamelen voor softwaregerelateerde kwesties om toekomstige voorvallen te helpen voorkomen.
Standaardisatie voor configuratie	"Standaardiserende" configuraties om het potentieel voor niet-geteste code te verminderen om in productie te worden uitgeoefend en netwerkprotocol- en functiegedrag te standaardiseren.
Beschikbaarheidsbeheer	Verbetering van beschikbaarheid op basis van metriek, verbeteringsdoelstellingen, en verbeteringsprojecten

Dit document gaat ervan uit dat u de volgende best practice-processen voor de planning, het ontwerp en de implementatie van Cisco IOS hebt geïmplementeerd:

- Gebleken beheerbare softwaregebieden (softwaresporen) in uw omgeving op basis van platform-, module-, eigenschap-, protocol- en topologievereisten.
- Geselecteerde, gecertificeerd en gecommuniceerd Cisco IOS-versies per softwaresporen.
- Voert consistent de standaard Cisco IOS versies in elk van de software sporen uit.

Doelstellingen

Deze sectie helpt u bij het beheer en het onderhoud van gestandaardiseerde Cisco IOS versies binnen gedefinieerde sporen. U zult leren hoe:

- Ontwikkelen van een softwareversiecontrolesysteem om ervoor te zorgen dat de softwareversie consistent is binnen de vastgestelde softwaresporen.
- Volg processen op basis van meldingen en signaleringen van fouten (SNMP/Syslog) voor het bewaken, melden en oplossen van fouten om potentiële software en foutproblemen proactief op te lossen.
- Efficiënte verzameling van kritische probleeminformatie voor software om de tijd voor het oplossen van problemen voor softwaregerelateerde problemen te verminderen.
- Standaardisatie van apparaatconfiguraties om te helpen zorgen voor protocol-, optie-, toegang- en beveiligingsconsistentie voor de omgeving.

publiek

Dit document is geschikt voor personen en managers met een technische oriëntatie die verantwoordelijk zijn voor de dagelijkse werking van het netwerk. Het document beschrijft hoe u operationele processen kunt opzetten om u te helpen de netwerkcomplexiteit te verminderen, reactieve ondersteuningskwesties te verminderen en de tijd voor probleemoplossing te verbeteren door netwerkconsistentie te bouwen en door mogelijkheden voor proactief foutbeheer te verbeteren.

Voorwaarden

Degenen die betrokken zijn bij Cisco IOS-beheeroperaties moeten een solide kennis hebben van het ontwerp van de netwerkinfrastructuur en het beheer, in het bijzonder met Cisco-apparatuur, en moeten toegang hebben tot details van de topologie, de apparaatconfiguratie, het activiteitenprofiel, het toepassingsgebruik en het beleid voor de benutting van middelen. Toegang tot en ervaring met informatiemiddelen die beschikbaar zijn op Cisco Connection Online (CCO) is ook vereist. Als u zich nog niet bij CCO hebt geregistreerd, raden we u aan dit te doen voor toegang tot de gereedschappen die in dit document worden beschreven.

Een Cisco IOS-beheerstrategie maken

Veel kwaliteitsstrategieën en tools bestaan om Cisco IOS-omgevingen te helpen beheren. Dit hoofdstuk concentreert zich op drie sleutelstrategieën voor het beheer van Cisco IOS operaties in hogere beschikbaarheid omgevingen, en omvat een matrix van belangrijkste operationele tools die specifiek behulpzaam zijn voor het beheer van Cisco IOS en Cisco IOS kwesties.

De eerste belangrijkste strategie is om de omgeving zo eenvoudig mogelijk te houden, waarbij variaties in configuratie en Cisco IOS-versies zoveel mogelijk worden voorkomen. Cisco IOS-certificering is al besproken, maar de configuratie-consistentie is een ander belangrijk gebied. De bouwkundige/technische groep dient verantwoordelijk te zijn voor het opstellen van standaarden voor configuratie. De implementatie en de operaties groep hebben dan de verantwoordelijkheid om de standaarden te configureren en de standaarden te onderhouden via Cisco IOS versiecontrole en Cisco IOS configuratie standaarden/controle.

De tweede belangrijke strategie is de mogelijkheid om netwerkfouten te identificeren en snel op te lossen. De operatiegroep moet netwerkproblemen in het algemeen vaststellen voordat gebruikers ze rapporteren, en problemen moeten zo snel mogelijk worden opgelost zonder dat het milieu

verder wordt beïnvloed of gewijzigd. Twee belangrijke beste praktijken op dit gebied zijn probleembeheer en foutenbeheersing (beide worden later in dit document besproken).

Opmerking: Het Cisco IOS-stapellingdecoder gereedschap kan worden gebruikt om snel te diagnosticeren met Cisco IOS-softwarecrashes.

De derde sleutelstrategie is "consequent verbeteren". Het primaire proces is het verbeteren van een op kwaliteit gebaseerd programma ter verbetering van de beschikbaarheid. Door een analyse van de oorzaak van alle kwesties, inclusief Cisco IOS-gerelateerde kwesties, uit te voeren kan een organisatie testdekking verbeteren, de tijden van probleemoplossing verbeteren en processen verbeteren die outage-impact zullen elimineren of verminderen. De organisatie kan ook naar gemeenschappelijke problemen kijken en processen opbouwen om deze kwesties sneller op te lossen.

Identificatie van te leveren producten

Beschikbaar bij Cisco IOS-softwarebeheerproces:

- Software voor versiecontroleprocessen en -tools
- Toezicht op en processen voor het beheer van fouten
- Problemen beheerprocessen
- Configuratienormen voor apparaten en auditprocessen
- Methodologie voor netwerkbeschikbaarheid, rapportage en beoordelingsprocessen

Bepalingen van de belangrijkste voorzieningen

De metriek moet worden gedefinieerd als deel van het operatieplan en worden gebruikt om te bepalen of de gereedschappen en processen de gewenste resultaten opleveren. Het volgende zijn een paar voorbeelden van nuttige Cisco IOS-softwarebeheermetriek:

- Beschikbaarheid netwerk (vanwege softwareproblemen)
- % conformiteit van Cisco IOS-versie met de standaard (per spoor)
- % Concrete configuratie van het apparaat (gebaseerd op standaarden)
- Problemen beheermethoden (MTTR, # tickets, Closure-codes)

Vaststelling van taken en verantwoordelijkheden

Identificeer, kwalificeer en assembleer een cross-functionele groep van managers en/of lopen van netwerkarchitectuur, netwerkengineering, en implementatie/operaties groepen om de succesvolle planning, ontwerp, implementatie, en exploitatiefase van uw IOS verbeteringsprojecten te verzekeren.

Aanwijzen van de vereiste expertisegebieden

Monteer een cross-functionele groep managers en/of lopen van de groepen van het netwerkbeheer, netwerkengineering, implementatie en bewerkingen om te helpen met de operationele fase van uw Cisco IOS-beheerproject.

Identificatie van de belangrijkste contribuanten

- Netwerkbeheerder(s):Naam, afdeling, contactgegevensNaam primaire back-up, afdeling, contactgegevensSecundaire back-upnaam, afdeling, contactinformatie indien nodig
- Netwerkarchitect(s):Naam van de architect, afdeling, contactgegevensNaam primaire back-up, afdeling, contactgegevensSecundaire back-upnaam, afdeling, contactinformatie indien nodig
- Netwerkingenieur(s):Naam, afdeling, contactgegevensNaam primaire back-up, afdeling, contactgegevensSecundaire back-upnaam, afdeling, contactinformatie indien nodig
- Network Operations (NOC) engineer(en):Naam, afdeling, contactgegevensNaam primaire back-up, afdeling, contactgegevensSecundaire back-upnaam, afdeling, contactinformatie indien nodig

Verantwoordelijkheden identificeren

- Netwerkbeheerder(s) is/zijn verantwoordelijk voor:Behoud van het projectplanToekenning/toewijzing van middelenBesturing van veranderingenVoortgang beherenBeheersende begrotingsrapportage
- Netwerkarchitect(s) is verantwoordelijk voor:Netwerknormen en -releaseDe upgrade-matrix van software onderhoudenDe kandidaat-beheermatrix behoudenDe Memory Requirements Matrix onderhouden
- Network (NOC) engineer(en) is/zijn verantwoordelijk voor:Uitvoering en waarborging van de naleving van netwerknormenProblemen en oorzaken van software identificerenAanbevolen corrigerende maatregelenHet netwerk bewaken

Bronnen

In de exploitatiefase dienen de behoeften aan middelen te worden bepaald ter ondersteuning van de softwarebeheerstrategie voor de organisatie. Dit omvat de vereiste personeelstijd en kapitaaluitgaven die nodig zijn om de softwarestrategie te ondersteunen.

In veel gevallen kan een rendement op investeringen (ROI) of een begrotingsplan voor softwarebeheerspraktijken worden gegenereerd op basis van de kosten van de onderbreking en de beschikbaarheid. Als de organisatie downtime kan bepalen als gevolg van softwareproblemen, kan een meerderheid van deze kosten worden gecompenseerd via de vastgestelde best-practices voor softwarebeheer. Als de kosten niet volledig gecompenseerd kunnen worden, moet de organisatie een meer basale softwarebeheerstrategie overwegen die zal helpen om de productiviteit te verbeteren door te voorkomen dat extra software als gevolg van softwareproblemen opnieuw gaat werken.

Na een optimaal gebruik van Cisco IOS-beheerbewerkingen

De beste praktijken voor het volgen van een Cisco IOS Beheersproces omvatten:

Best Practice	Detail
Software versie Control	Het implementeren van alleen gestandaardiseerde softwareversies en het controleren van het netwerk om software te valideren of mogelijk te veranderen door

	niet-versie-conformiteit.
Foutenbeheer	SNMP & SYS-berichtverzameling, -bewaking en -analyse zijn foutbeheerprocessen die worden aanbevolen om meer Cisco IOS specifieke netwerkproblemen op te lossen die moeilijk of onmogelijk om op een andere manier te identificeren zijn.
Probleembeheer	Gedetailleerde probleembeheerprocessen die probleemidentificatie, informatieverzameling en een goed geanalyseerd oplossingspad definiëren. Deze gegevens worden gebruikt om de oorzaak te bepalen.
Standaardisatie voor configuratie	Configuratienormen vormen de praktijk van het creëren en onderhouden van standaardconfiguratieparameters voor "mondiaal", zoals apparaten en diensten, die resulteren in een globale configuratie voor het gehele bedrijf.
Beschikbaarheidsbeheer	Kwaliteitsverbetering met behulp van netwerkbeschikbaarheid als kwaliteitsverbetering.

Software versie Control

Softwareversiecontrole is het proces van het implementeren van alleen gestandaardiseerde softwareversies en het controleren van het netwerk om software te valideren of mogelijk te wijzigen als gevolg van de niet-versie-conformiteit. In het algemeen wordt de controle van de softwareversie uitgevoerd door middel van een certificeringsproces en een normcontrole. Veel organisaties publiceren versienormen op een centrale webserver. Daarnaast is een implementatiepersoneel opgeleid om te bekijken welke versie wordt uitgevoerd en om de versie bij te werken als deze niet voldoet aan de normen. Sommige organisaties beschikken over een proces van kwaliteitsgate waarbij de secundaire validatie door middel van audits wordt voltooid om ervoor te zorgen dat de norm tijdens de uitvoering wordt nageleefd.

Tijdens de netwerkwerking is het ook niet ongebruikelijk om niet-standaard software versies in het netwerk te zien, vooral als het netwerk groot is met een groot bedrijfspersoneel. Dit kan het gevolg zijn van een van de volgende factoren:

- Onopgeleid nevenpersoneel
- MIS-geconfigureerde laardopdrachten
- Ongecontroleerde implementaties

Het wordt aanbevolen om regelmatig standaarden voor softwareversie te valideren met behulp van gereedschappen zoals CiscoWorks2000 Resource Manager Essentials (RME) die alle apparaten door Cisco IOS-versie kunnen sorteren. Wanneer een niet-standaardversie wordt geïdentificeerd, moet deze onmiddellijk worden gemarkeerd en moet een ticket of een verandering worden geïnitieerd om de versie naar de geïdentificeerde standaard te brengen.

Beschikbare tools

CiscoWorks2000 RME-manager vereenvoudigt zeer het Cisco IOS versiebeheer van Cisco routers en switches door op web-gebaseerde rapportagetools die apparaten rapporteren en sorteren op basis van softwareversie, platform en apparaatnaam.

Foutenbeheer

Foutenbeheer is het proces van het verzamelen, bewaken en analyseren van SNMP- en SYS-berichten om meer Cisco IOS specifieke netwerkproblemen op te lossen die moeilijk of onmogelijk om op een andere manier te identificeren zijn.

SNMP-trap - verzameling

SNMP-trap: verzameling en kennisgeving is een basisproces in foutenbeheersing dat wordt gebruikt om softwaregebeurtenissen of hardwaregebeurtenissen en/of crashes te identificeren zonder SNMP-opiniepeilingen of vertragingen als gevolg van stemintervallen. Trap-berichten worden direct gegenereerd vanaf het netwerkapparaat naar een netwerkbeheersysteem dat aanmeldingsservices biedt. De inzameling en kennisgeving van deze vallen is van essentieel belang voor een snelle oplossing van vele netwerkgebeurtenissen, waaronder gebeurtenissen die geen gevolgen hebben voor de gebruiker, zoals het verlies van primaire apparaten of verbindingen in een redundante omgeving.

Om deze vallen te verzamelen en te bewaken, moeten de vallen op de juiste wijze op het apparaat en de netwerkbeheersystemen worden ingesteld. De netwerkbeheersystemen moeten de netwerkoperatiegroep waarschuwen wanneer een val is ontvangen. Een melding kan vervolgens worden gedaan in de vorm van semafoon-, e-mail- of eventschermen in een NOC-omgeving.

Ongeacht de wijze waarop de gegevens worden gepresenteerd, moeten deze fouten of uitzonderingen regelmatig (bij voorkeur dagelijks) worden geanalyseerd en beoordeeld door de netwerkoperaties en/of het ondersteunend personeel van het netwerk. De oorzaken van alle vastgestelde uitzonderingen moeten worden onderzocht. Sommige geregistreerde uitzonderingen kunnen niet kritiek genoeg zijn om onmiddellijk een alarm in het Centrum van de Verrichtingen van het Netwerk op te heffen. Proactieve beoordeling, onderzoek en oplossing van kleinere uitzonderingen kunnen netwerkondersteuningsgroepen helpen om netwerkstoringen te verminderen of te voorkomen.

Syslog-berichtverzameling

De boodschappen van Syslog worden door het apparaat naar een verzamelserver verzonden. Deze berichten kunnen hardware- of softwarefouten zijn of informatie (zoals wanneer iemand in een configuratieterminal op een apparaat is geweest).

Syslogge-controle vereist ondersteuning voor Network Management System (NMS) of scripts om te helpen bij parsen en rapporteren over Syrische gegevens. Dit omvat de mogelijkheid om Syslog-berichten te sorteren naar datum of tijdsperiode, apparaat, type of frequentie van het Syslog-bericht. In grotere netwerken kunnen tools of scripts worden geïmplementeerd om Syslog-gegevens te parseren en signaleringen of kennisgevingen te verzenden naar beheersystemen voor gebeurtenissen of naar operationele en technische medewerkers. Als er geen signaleringen voor een brede reeks Syrische gegevens worden gebruikt, moet de organisatie ten minste dagelijks hogere prioriteit bieden aan Syslog-gegevens en probleemtickets maken voor mogelijke problemen. Om netwerkproblemen die mogelijk niet door normale bewaking worden gedetecteerd, proactief te detecteren, dienen periodieke review en analyse van historische Syslog-gegevens te

worden uitgevoerd om situaties te detecteren die mogelijk geen onmiddellijk probleem aangeven, maar die wel een indicatie van een probleem kunnen zijn voordat de service een effect heeft.

Beschikbare tools

Enkele van de populairder SNMP Trap ontvangertools omvatten het volgende:

- HP OpenView Network Node Manager van Hewlett Packard op openview.hp.com
- Spectrum Integriteit uit Aprisma op www.aprisma.com
- NetView bij IBM Tivoli op www.tivoli.com

Het populairste gereedschap van de SPRONG voor het beheer van Cisco IOS is CiscoWorks2000 RME Manager. Andere beschikbare gereedschappen zijn onder meer SL4NT, een aandeelhoudersprogramma van www.netal.com , cisco.com en Private I van OpenSystems op www.opensystems.com

Probleembeheer

Probleembeheer, een aspect van foutenbeheer, is de discipline om problemen te beheersen vanaf het moment van voorkomen door identificatie, probleemoplossing, oplossing en sluiting.

Veel klanten ondervinden extra onderbreking door een gebrek aan processen in probleembeheer. Aanvullende downtime kan voorkomen wanneer netwerkbeheerders proberen het probleem snel op te lossen met behulp van een combinatie van opdrachten die de service beïnvloeden of configuratiewijzigingen in plaats van tijd te besteden aan het identificeren van problemen, het verzamelen van informatie en een goed geanalyseerd oplossingspad. Waargenomen gedrag op dit gebied omvat het opnieuw laden van apparaten of het ontruimen van IP-routingtabellen voordat u een probleem en de diepere oorzaak onderzoekt. In sommige gevallen gebeurt dit vanwege de doelstellingen voor probleemoplossing op het eerste niveau. Het doel in alle software-gerelateerde problemen moet zijn om snel de benodigde informatie te verzamelen die nodig is voor de analyse van de oorzaak van de schade voordat de connectiviteit of de service wordt hersteld.

Een probleembeheerproces wordt aanbevolen, waarbij een bepaalde mate van standaardprobleembeschrijvingen en een geschikte 'show'-opdrachtverzameling worden opgenomen voordat het probleem wordt escaleerd naar een tweede ondersteuningsniveau. Ondersteuning op het eerste niveau mag nooit betrekking hebben op clearingroutes of herlaadapparaten. Idealiter zou de ondersteuningsorganisatie op het eerste niveau snel informatie moeten verzamelen en het probleem vervolgens naar ondersteuning op het tweede niveau moeten escaleren. Door wat meer tijd te besteden aan het identificeren en beschrijven van het probleem op niveau één is een ontdekking van de oorzaak veel waarschijnlijker, waardoor een bewerking, lab identificatie en bug rapportage mogelijk is. Ondersteuning op tweede niveau dient goed te zijn verwerkt in de soorten informatie die Cisco mogelijk nodig heeft om een probleem te diagnosticeren of een bug-rapport in te dienen, inclusief:

- Memory dumps
- Routing informatie-uitvoer
- Opdracht uitvoer apparaattonen

Standaardisatie voor configuratie

De mondiale standaarden voor de configuratie van apparaten vormen de praktijk om standaard "mondiale" configuratieparameters voor alle apparaten en diensten te handhaven, wat resulteert in

een globale configuratie voor het gehele bedrijf. Mondiale configuratieopdrachten zijn opdrachten die van toepassing zijn op het gehele apparaat en niet op afzonderlijke poorten, protocollen of interfaces. Over het algemeen worden de toegang tot het apparaat, het algemene gedrag van het apparaat en de beveiliging van het apparaat beïnvloed. In Cisco IOS omvat dit de volgende opdrachten:

- Service
- IP
- VTY
- Console poort
- Vastlegging
- AAA/TACACS+
- SNMP
- Banner

Ook belangrijk in de mondiale standaarden voor apparaatconfiguratie is een geschikte conventie voor het benoemen van apparaten waarmee beheerders het apparaat, het type apparaat en de locatie van het apparaat kunnen identificeren op basis van de DNS naam van het apparaat. Mondiale configuratie consistentie is belangrijk voor de algemene draagbaarheid en betrouwbaarheid van een netwerkomgeving, omdat het de netwerkcomplexiteit helpt verminderen en netwerkondersteuning helpt verbeteren. De moeilijkheid van de ondersteuning wordt vaak ervaren zonder configuratie standaardisatie door incorrect of inconsequent apparaatgedrag, SNMP-toegang en algemene apparaatbeveiliging.

Het handhaven van mondiale normen voor het configureren van apparaten wordt normaal bereikt door een interne engineering of een operationele groep die mondiale configuratieparameters voor gelijksoortige netwerkapparaten creëert en onderhoudt. Het is ook een goede praktijk om een kopie van het globale configuratiebestand in TFTP-telefoongidsen te verstrekken, zodat deze in eerste instantie kunnen worden gedownload naar alle nieuwe voorzieningen. Ook behulpzaam is een web toegankelijk bestand dat het standaard configuratiebestand met een verklaring van elke configuratieparameter bevat. Sommige organisaties configureren allemaal op een periodieke basis als apparaten om te helpen de consistentie van de mondiale configuratie te verzekeren, of bekijken apparaten regelmatig voor de juiste mondiale configuratiestandaarden.

De interface- of protocolconfiguratienormen vormen de praktijk om normen voor interface- en protocolconfiguratie te handhaven, die netwerkbeschikbaarheid verbetert door netwerkcomplexiteit te verminderen, verwacht apparaat- en protocolgedrag te bieden en netwerksupportabiliteit te verbeteren. Inconsistentie van de interface- of protocolconfiguratie kan leiden tot onverwacht gedrag van het apparaat, problemen bij het routeren van verkeer, toegenomen aansluitingsproblemen en toegenomen reactieve ondersteuningstijd.

Interfaceconformatienormen kunnen het volgende omvatten:

- CDP (Cisco Discovery Protocol)
- Interfacebeschrijvers
- Cable-configuratie
- Overige protocolspecifieke normen

Protocol-specifieke configuratienormen kunnen omvatten:

- IP-routeringsconfiguratie
- DLSW-configuratie
- Configuratie van toegangslijsten

- ATM-configuratie
- Frame Relay-configuratie
- Spanning Tree-configuratie
- VLAN-toewijzing en -configuratie
- VTP (Virtual Trunking Protocol)
- HSRP (Hot Standby Routing Protocol)
- Anderen afhankelijk van wat binnen het netwerk wordt geconfigureerd

Een voorbeeld van IP normen kan subnetgrootte, IP adresruimte omvatten die wordt gebruikt, het routeringsprotocol gebruikt en het routeren van protocolconfiguratie.

Het in stand houden van protocol- en interfacestandaarden is normaal de verantwoordelijkheid van de technische en implementatiegroepen van het netwerk. De technische groep moet verantwoordelijk zijn voor het identificeren, testen, valideren en documenteren van de normen. De implementatiegroep is dan verantwoordelijk voor het gebruik van de technische documenten of configuratiesjablonen om nieuwe services te leveren. De technische groep moet documentatie creëren over alle aspecten van de vereiste normen om de consistentie te waarborgen. Configuratiescherm moet ook worden gemaakt om de configuratienormen te helpen handhaven. Operationele groepen moeten ook worden opgeleid op het gebied van de normen en moeten in staat zijn niet-standaardconfiguratie-kwesties te identificeren. De consistentie van de configuratie is van groot belang voor de test-, validatie- en certificeringsfase. Zonder gestandaardiseerde configuratiesjablonen is het vrijwel onmogelijk om een Cisco IOS-versie voor een matig groot netwerk adequaat te testen, valideren of certificeren.

Beschikbaarheidsbeheer

Beschikbaarheidsbeheer is het proces van kwaliteitsverbetering door gebruik te maken van netwerkbeschikbaarheid als de kwaliteitsverbetering. Veel organisaties meten nu de beschikbaarheid en het type stroomuitval. Uitvaltypen kunnen het volgende omvatten:

- Hardware
- in Cisco IOS®-software
- Koppel/drager
- Voeding/omgeving
- Ontwerpen
- Gebruiker-fout/proces

Door stroomstoringen te identificeren en direct na herstel een analyse van de oorzaak uit te voeren kan de organisatie methoden identificeren om de beschikbaarheid te verbeteren. Bijna alle netwerken die een hoge beschikbaarheid hebben bereikt, hebben een of ander proces voor kwaliteitsverbetering.

Cisco IOS-controlelijst voor beheerbewerkingen

❑Stap 1: Bepaal bedrijfsvereisten en -doelstellingen (alleen geregistreerde klanten)

❑Stap 2: Evalueer de huidige status van Cisco IOS-softwarebeheerpraktijken (alleen geregistreerde klanten)

❑Stap 3: Rollen en verantwoordelijkheden definiëren (alleen geregistreerde klanten)

❑Stap 4: Een projectplan voor softwarebeheer ontwikkelen (alleen geregistreerde klanten)

❑Stap 5: Een matrixprinter voor softwarevereisten ontwikkelen (alleen geregistreerde klanten)

Gerelateerde informatie

Er is een bijlage gemaakt om de klant te helpen bij het verkrijgen van andere waardevolle Cisco IOS-gerelateerde informatie, zoals: Cisco IOS fundamentele, Cisco interne Cisco IOS softwareprocessen, analyse van softwarebetrouwbaarheid, Cisco intern kwaliteitsprogramma, Cisco interne testmethodologieën en een veldanalyse die huidige industriepraktijken en algemene klantervaringen met Cisco IOS-software toont

- Cisco IOS-beheer: Aanvullende informatie over Cisco IOS beheer en optimale werkwijzen kan in het "Cisco IOS Management voor High Availability Network" witboek op de volgende website worden gevonden: http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a00800a998b.shtml
- Voor specifieke informatie over hoe te om netwerksondes te lopen, die CLI bevelen te gebruiken, hoe te om netwerkverkeersgegevens te analyseren en te interpreteren, en hoe te om toepassingsgebruiksbeleid in te stellen, bezoek http://www.cisco.com. Deze site biedt een uitgebreide reeks oplossingen voor ondersteuning, training, technische ondersteuning en advies.
- Cisco IOS heeft specifieke naamgevingsconventies die hier worden gedefinieerd: http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_tech_note09186a0080101cda.shtml
- Informatie over de beschikbaarheid van Cisco IOS release wordt hier geleverd: http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html
- Cisco IOS releases wordt uiteindelijk verwijderd van CCO en kan niet langer worden besteld. Zorg ervoor dat u de klant-verwachtingen dienovereenkomstig instelt.
- Cisco IOS-productbulletins worden gebruikt om Cisco IOS-releases aan klanten bekend te maken. Ze bevatten korte informatie over de release-inhoud. Controleer hier op beschikbaarheid van nieuwe Cisco IOS-releases http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html
- Het reactieteam van de productbeveiliging behandelt de beveiliging van Cisco-producten. Alle Cisco IOS-beveiligingsproblemen moeten naar dit team worden verwezen. Cisco publiceert publiekelijk de veiligheidskwetsbaarheden. http://tools.cisco.com/security/center/publicationListing
- Cisco IOS defect: Ernstige Cisco IOS-tekortkomingen moeten worden aanbevolen voor uitstel. Elke Cisco-werknemer kan de aanbeveling doen.
- Veldproblemen op Cisco IOS worden aan de klanten doorgegeven via Cisco IOS-adviseurs. http://www.cisco.com/en/US/products/products_security_advisory09186a0080b20ee1.shtml
- Cisco IOS-functies: Met het Functie Navigator-gereedschap kunnen klanten releases vinden die specifieke functies ondersteunen, en vice versa. http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp
- De Cisco Software Adviseur stelt klanten in staat om softwareondersteuning te vinden voor functies of softwareondersteuning voor hardware.

http://tools.cisco.com/Support/Fusion/FusionHome.do (alleen geregistreerde klanten)

Cisco-services en -ondersteuning

- Technische ondersteuningsservices
- Servicesspecifiek voor Cisco-netwerktechnologieën en -oplossingen