

Práticas de liderança de Cisco: Operações do Gerenciamento do Cisco IOS

Índice

[Resumo](#)

[Introdução](#)

[Overview](#)

[Objetivos](#)

[Audiência](#)

[Pré-requisitos](#)

[Criando uma estratégia das operações do Gerenciamento do Cisco IOS](#)

[Identificando Deliverables](#)

[Identificando medidas do dispositivo chave](#)

[Definindo papéis e responsabilidades](#)

[Identificando as áreas de especialização exigidas](#)

[Identificando os contribuinte chaves](#)

[Identificando responsabilidades](#)

[Recursos de realização do orçamento](#)

[Depois de um processo das operações do Gerenciamento do Cisco IOS do melhor prática](#)

[Controle de versão de software](#)

[Gerenciamento de falhas](#)

[Gerenciamento de problemas](#)

[Padronização de configuração](#)

[Gerenciamento de disponibilidade](#)

[Lista de verificação das operações do Gerenciamento do Cisco IOS](#)

[Informações Relacionadas](#)

[Serviços da Cisco e apoio](#)

Resumo

As práticas de liderança de Cisco são um grupo de originais codificados que fornecem a orientação relevante e segura em operações de rede de comunicação para o Produtos da Cisco e as soluções. As práticas de liderança são desenvolvidas e apoiadas pelos coordenadores vencedores dum prêmio do tac Cisco e dos Serviços avançados que você pode usar para ajudar a criar seu próprio grupo de práticas de liderança emular. Os clientes Cisco aplicaram estas práticas de liderança em seu ambiente de rede ganhar o desempenho da rede e a Disponibilidade.

É altamente recomendado suplementar estas práticas de liderança com os serviços de Cisco e de seus Parceiros. Para obter mais informações sobre de como aperfeiçoar seus desempenho da rede e Disponibilidade, contactar por favor seu representante de vendas dos serviços sobre o

Web site dos Serviços avançados de Cisco e encontrar mais sobre o apoio da otimização de rede - suporte de engenharia focalizado, disponibilidade da rede do apoio da melhoria (NAIS), avaliação do processo de gerenciamento de software (SMPA), e aplicação NAIS-SMPA.

Introdução

Overview

Os processos operacionais em torno do gerenciamento de software podem ajudar a reduzir a complexidade de rede, questões de suporte reagente da diminuição e a melhorar o tempo de definição de problema. Este original fornece uma estratégia, recomendações da ferramenta, e melhores práticas para o Gerenciamento total do software do [®] do Cisco IOS (Cisco IOS).

[A criação de uma estratégia das operações do Gerenciamento do Cisco IOS](#) e [seguir](#) seções de um [processo das operações do Gerenciamento do Cisco IOS do melhor prática](#) neste original discutem a metodologia recomendada para obter começos e alistem as melhores ferramentas a ser usadas para a fase das operações. A fase das operações inclui os processos da melhor prática para o seguinte:

Processo	Descrição
Controle de versão de software	Seguir, validar, e melhorar a consistência do software dentro do software identificado "seguem".
Gerenciamento de defeito	Dinamicamente monitorando e atuando em cima da prioridade mais alta SNMP e dos mensagens do syslog gerados pelo Cisco IOS.
Gerência de problemas	Rapidamente e eficientemente recolhendo a informação do problema crítico para problemas relacionados do software a fim ajudar a impedir ocorrências futuras.
Padronização de configuração	"Estandarizando" configurações para reduzir o potencial para que o código não experimentado seja exercitado na produção e para estandarizar o protocolo de rede e o comportamento da característica.
Gerenciamento de disponibilidade	Melhorando a Disponibilidade baseada no medidor, nos meta de aperfeiçoamento, e nos projetos da melhoria

Este original supõe que você executou os seguintes processos da melhor prática para o planejamento, o projeto e a aplicação do Cisco IOS:

- Áreas do software manejáveis identificadas (rastreamentos de software) em seu ambiente

baseado na plataforma, no módulo, na característica, no protocolo, e nos requisitos de topologia.

- Versões do Cisco IOS selecionadas, certificadas, e comunicadas por rastreamentos de software.
- Executou consistentemente as versões do Cisco IOS padrão em cada um dos rastreamentos de software.

Objetivos

Esta seção ajuda-lhe em controlar e em manter versões do Cisco IOS standardizadas dentro das trilhas definidas. Você aprenderá como:

- Desenvolva um processo do controle de versão de software para assegurar a consistência da versão de software dentro dos rastreamentos de software identificados.
- Monitore, notifique, e resolva os processos baseados em mensagens de gerenciamento da falha de dispositivo e em alertas (SNMP/syslog) para ajudar dinamicamente a resolver edições potenciais do software e da falha.
- Coleção eficiente da informação do problema crítico para que o software ajude a reduzir o tempo de definição de problema para questões relacionadas ao software.
- Standardize configurações de dispositivo para ajudar a assegurar o protocolo, a característica, o acesso, e a consistência da Segurança para o ambiente.

Audiência

Este original é apropriado para indivíduos e gerentes com uma orientação técnica que são responsáveis para a operação diária da rede. O original descreve como estabelecer processos operacionais para ajudá-lo a reduzir a complexidade de rede, questões de suporte reagente da diminuição e a melhorar o tempo de definição de problema pela consistência de rede de construção e melhorando capacidades para o gerenciamento de falha pró-ativo.

Pré-requisitos

Aqueles envolvidos em operações do Gerenciamento do Cisco IOS devem ter um conhecimento contínuo do projeto da infraestrutura de rede, e a administração, particularmente com equipamento da Cisco, e devem ter o acesso aos detalhes da topologia de rede do alvo, da configuração de dispositivo, do perfil da atividade, do uso do aplicativo, e da política da utilização de recurso. Alcance a, e a experiência com, as ferramentas da informação disponíveis no [Cisco Connection Online](#) (CCO), é exigida igualmente. Se você [não se tem registrado](#) já [com CCO](#), nós sugerimos que você faça assim para o acesso às ferramentas descritas neste original.

Criando uma estratégia das operações do Gerenciamento do Cisco IOS

Muitas estratégias de qualidade e ferramentas existem para ajudar a controlar ambientes do Cisco IOS. Este capítulo centra-se sobre três estratégias chaves para controlar operações do Cisco IOS na disponibilidade mais alta dos ambientes, e inclui-se uma matriz das ferramentas operacionais chaves que são especificamente úteis para controlar edições do Cisco IOS e do Cisco IOS.

A primeira estratégia chave é manter tão simples quanto possível o ambiente, evitando a variação na configuração e nas versões do Cisco IOS tanto quanto possível. A certificação do Cisco IOS tem sido discutida já, porém a consistência da configuração é uma outra área principal. O grupo de arquitetura e engenharia deve ser responsável pela criação dos padrões de configuração. A aplicação e o grupo de operações têm então a responsabilidade configurar os padrões e manter os padrões através do controle de versão do Cisco IOS e dos padrões da configuração do IOS da Cisco/control.

A segunda estratégia chave é a capacidade para identificar e resolver rapidamente defeitos de rede. O grupo de operações deve geralmente identificar problemas de rede antes dos usuários relata-los, e os problemas devem ser resolvidos o mais rapidamente possível sem impacto mais adicional ou mudança do ambiente. Duas melhores práticas chaves nesta área são gerência de problemas e gerenciamento de defeito (ambos são discutidos mais tarde neste original).

Nota: A ferramenta de decodificação de pilha do Cisco IOS pode ser usada para ajudar rapidamente a diagnosticar impactos do Cisco IOS Software.

A terceira estratégia chave é “melhora consistentemente”. O processo preliminar é melhorar uma Disponibilidade qualidade-baseada do programa de melhoria. Executando a análise de causa de raiz em todas as edições, incluindo edições IO-relacionadas de Cisco, uma organização pode melhorar a cobertura do teste, melhorar o tempo de definição de problema, e melhorar os processos que eliminarão ou reduzirão o impacto da indisponibilidade. A organização também pode verificar problemas comuns e construir processos para resolvê-los com mais rapidez.

Identificando Deliverables

Os Deliverables do processo da operação do Gerenciamento do Cisco IOS Software incluem:

- Processos e ferramentas do controle de versão de software
- Monitoração e processos do gerenciamento de defeito
- Processos de gerenciamento de problema
- Padrões de configuração de dispositivo e processos da auditoria
- Disponibilidade da rede da metodologia, o relatório e os processos da revisão

Identificando medidas do dispositivo chave

O medidor deve ser definido como parte do plano de operações e ser usado para determinar se as ferramentas e os processos estão produzindo os resultados desejados. Os seguintes são alguns exemplos do medidor útil do Gerenciamento do Cisco IOS Software:

- Disponibilidade da rede (devido às questões de software)
- % da conformidade da versão do Cisco IOS ao padrão (na pela base da trilha)
- % da consistência da configuração de dispositivo (baseada em padrões)
- Medidor da gerência de problemas (MTTR, # bilhetes, códigos do fechamento)

Definindo papéis e responsabilidades

Identifique, qualifique, e monte um grupo cruz-funcional de gerentes e/ou de ligações da arquitetura de rede, da engenharia da rede, e dos grupos de operações da aplicação para ajudar a assegurar o planejamento, o projeto, a aplicação, e as fases bem sucedidas das operações de

seus projetos da upgrade de IOS.

Identificando as áreas de especialização exigidas

Monte um grupo cruz-funcional de gerentes e/ou de ligações do Gerenciamento de redes, da engenharia da rede, da aplicação e dos grupos de operações para ajudar com a fase das operações de seu projeto do Gerenciamento do Cisco IOS.

Identificando os contribuinte chaves

- Gerente de rede: Os gerentes nomeiam, departamento, informação de contato Nome do backup principal, departamento, informação de contato Nome do backup secundário, departamento, informação de contato se for necessário
- Arquiteto de rede: Os arquitetos nomeiam, departamento, informação de contato Nome do backup principal, departamento, informação de contato Nome do backup secundário, departamento, informação de contato se for necessário
- Engenheiro de rede: Os coordenadores nomeiam, departamento, informação de contato Nome do backup principal, departamento, informação de contato Nome do backup secundário, departamento, informação de contato se for necessário
- Coordenadores das operações de rede (NOC): Os coordenadores nomeiam, departamento, informação de contato Nome do backup principal, departamento, informação de contato Nome do backup secundário, departamento, informação de contato se for necessário

Identificando responsabilidades

- A gerente de rede é responsável para: Mantendo o plano de projeto Atribuição/atribuindo novamente recursos Controlando o controle de alterações Controlando o progresso Controlando o relatório de orçamento
- O arquiteto de rede é responsável para: Analisando padrões de rede e advertências da liberação Mantendo a matriz do upgrade de software Mantendo a matriz do gerenciamento de candidato Mantendo a matriz dos requisitos de memória
- Os coordenadores da rede (NOC) são responsáveis para: Executando e assegurando a conformidade aos padrões de rede Identificando problemas de software e causas de raiz Ação corretiva de recomendação Monitorando a rede

Recursos de realização do orçamento

Os requisitos de recurso devem ser determinados na fase das operações apoiar a estratégia de gerenciamento de software para a organização. Isto incluirá os pessoais exigidos cronometra e as despesas em investimento necessárias apoiar a estratégia do software.

Em muitos casos, um retorno de investimento (ROI) ou o plano orçamental para práticas de gerenciamento do software podem ser gerados com base nos custos de tempo ocioso e nos requisitos de disponibilidade. Se a organização pode determinar o downtime devido aos problemas de software, a seguir uma maioria deste custo pode ser deslocada através das melhores práticas identificadas do gerenciamento de software. Se o custo não pode completamente ser deslocado, a seguir a organização deve considerar mais estratégia de gerenciamento do software básico que ajudará a melhorar a produtividade impedindo o rework adicional em consequência dos problemas de software.

Depois de um processo das operações do Gerenciamento do Cisco IOS do melhor prática

Os melhores prática para seguir um processo das operações do Gerenciamento do Cisco IOS incluem:

Melhor prática	Detalhe
Controle de versão de software	Executando somente versões de software estandardizadas e monitorando a rede para validar ou mudar possivelmente o software devido à conformidade da NON-versão.
Gerenciamento de falhas	O SNMP & a coleção do mensagem do syslog, a monitoração e a análise são processos de gerenciamento de falha recomendados resolver mais problemas de rede específicos do Cisco IOS que são difíceis ou impossíveis identificar toda a outra maneira.
Gerenciamento de problemas	Processos de gerenciamento de problema detalhados que definem a identificação do problema, a coleção de informação, e um trajeto bem-analisado da solução. Estes dados são usados para determinar a causa de raiz.
Padronização de configuração	Os padrões de configuração representam a prática de criar e de manter dispositivos como "globais" padrão e serviços dos parâmetros de configuração transversalmente tendo por resultado a consistência de configuração global larga da empresa.
Gerenciamento de disponibilidade	Melhoria de qualidade usando a disponibilidade da rede como a métrica da melhoria de qualidade.

Controle de versão de software

O controle da versão do software é o processo de implementação apenas das versões de software padronizadas e de monitoramento da rede para validar ou possivelmente alterar o software devido à compatibilidade de não versão. Geralmente, o controle de versão de software é realizado usando um processo de certificação e um controle dos padrões. Muitas organizações publicam padrões de versão em um servidor de Web central. Além, um pessoal da aplicação é treinado para rever que versão está sendo executado e para atualizar a versão se não é em conformidade com padrões. Algumas organizações têm um processo da porta da qualidade onde a validação secundária seja terminada com as auditorias para se assegurar de que o padrão esteja seguido durante a aplicação.

Durante a operação de rede, não é igualmente raro ver versões de software não padronizadas na

rede, especialmente se a rede é grande com um grande pessoal das operações. Isto pode ser devido a um do seguinte:

- Pessoal mais novo inexperiente
- Comandos boot desconfigurados
- Implementações não verificada

Recomenda-se validar periodicamente padrões de versão de software usando ferramentas tais como o Resource Manager Essentials do CiscoWorks2000 (RME) que pode classificar todos os dispositivos pela versão do Cisco IOS. Quando uma versão não padronizada é identificada, deve imediatamente ser embandeirada e uma documentação de problema ou para mudar o bilhete seja iniciada para trazer a versão ao padrão identificado.

Ferramentas disponíveis

O RME Inventory Manager do CiscoWorks2000 simplifica extremamente o Gerenciamento da versão do Cisco IOS dos roteadores Cisco e do Switches através das ferramentas de relatório com base na Web que os dispositivos do relatório e do tipo basearam na versão de software, na plataforma do dispositivo, e no nome de dispositivo.

Gerenciamento de falhas

O gerenciamento de defeito é o processo de recolher, de monitorar e de analisar o SNMP e os mensagens do syslog para resolver mais problemas de rede específicos do Cisco IOS que são difíceis ou impossíveis identificar toda a outra maneira.

Coleção da armadilha de SNMP

A coleção e a notificação da armadilha de SNMP são um processo básico no gerenciamento de defeito usado para identificar eventos do software ou do hardware e/ou causam um crash sem polling snmp em cima ou atraso incorrido dos intervalos de polling. Os mensagens de armadilha são gerados diretamente do dispositivo de rede a um sistema de gerenciamento de rede que proporcione Serviços de notificação. A coleção e a notificação destas armadilhas são essenciais à resolução rápida de muitos eventos de rede que incluem eventos não de impacto tais como a perda de dispositivos principais ou de links em um ambiente redundante.

A fim recolher e monitorar estas armadilhas, as armadilhas devem corretamente ser configuradas no dispositivo assim como nos sistemas de gerenciamento de rede. Os sistemas de gerenciamento de rede devem alertar o grupo de operações de rede quando uma armadilha foi recebida. A notificação pode então ocorrer sob a forma da paginação, do email ou das telas do evento em um ambiente NOC.

Apesar de como os dados são apresentados, estes criticam exemplos, ou as exceções, devem ser analisadas e revisto numa base regular (diário preferivelmente) pelas operações de rede e/ou pelo equipe de suporte de rede. As causas de todas as exceções encontradas devem ser investigadas. Algumas exceções registradas não podem ser críticas bastante para levantar imediatamente um alarme no Network Operations Center. A revisão, a investigação e a definição dinâmicas de exceções menores podem ajudar grupos de suporte da rede a reduzir ou impedir paradas de rede.

Coleção do mensagem do syslog

Os mensagens do syslog são enviados pelo dispositivo a um servidor de levantamento. Estas

mensagens podem ser erro de hardware ou de software ou podem ser informativas (como quando alguém esteve dentro configurar o terminal em um dispositivo).

A monitoração do Syslog exige o apoio ou os scripts da ferramenta de sistema de gerenciamento de rede (NMS) ajudar a analisar gramaticalmente e relatar em dados de SYSLOG. Isto inclui a capacidade de classificar mensagens do syslog na data ou o período de tempo, o dispositivo, o tipo de mensagem do syslog ou a frequência de mensagem. Em redes maiores, as ferramentas ou os scripts podem ser executados para analisar gramaticalmente dados de SYSLOG e enviar alertas ou notificações aos sistemas de gerenciamento de evento ou as operações e os pessoais de engenharia. Se os alertas para uma ampla variedade de dados de SYSLOG não são usados, a organização deve rever uns dados de SYSLOG mais prioritários pelo menos diários e criar documentações de problema para problemas potenciais. A fim detectar dinamicamente os problemas de rede que não podem ser considerados com a monitoração normal, revisão periódica e a análise de dados de SYSLOG históricos deve ser executada para detectar as situações que não podem indicar um problema imediato, mas pode fornecer uma indicação de um problema antes que se transforme impacto do serviço.

Ferramentas disponíveis

Algumas das ferramentas mais populares do receptor de armadilha de SNMP incluem o seguinte:

- HP OpenView Network Node Manager do Hewlett Packard em openview.hp.com
- Integridade do espectro de Aprisma em www.aprisma.com
- Netview de IBM Tivoli em www.tivoli.com

A ferramenta a mais popular do Syslog para o Gerenciamento do Cisco IOS é gerenciador de Syslog de RME do CiscoWorks2000. Outras ferramentas disponíveis incluem o SL4NT, um programa do shareware de www.netal.com que deixa cisco.com e I privado de OpenSystems em www.opensystems.com

Gerenciamento de problemas

A gerência de problemas, um aspecto do gerenciamento de defeito, é a disciplina controlar de problemas da época da ocorrência através da identificação, do Troubleshooting, da definição e do fechamento.

Muitos clientes experimentam o downtime devido adicional a uma falta dos processos na gerência de problemas. O tempo ocioso da máquina adicional pode ocorrer quando os administradores de rede tentam resolver o problema que usa rapidamente uma combinação de comandos ou de alterações de configuração de impacto um pouco do que passando o tempo na identificação do problema, na coleção de informação, e em um trajeto bem-analisado da solução. O comportamento observado nesta área inclui dispositivos de recarregamento ou tabelas de IP Routing de cancelamento antes de investigar um problema e sua causa de raiz. Em alguns casos isto ocorre devido aos objetivos de definição de problema do suporte de primeiro nível. A meta, em todos os problemas relacionados a software, deve ser coletar rapidamente as informações necessárias para a análise da causa principal antes de restaurar a conectividade ou o serviço.

Um processo de gerenciamento de problema é recomendado, e deve incluir um determinado grau de descrições do problema do padrão e de coleções apropriadas do comando " show " antes de escalar o problema a um segundo nível do apoio. O suporte de primeiro nível deve nunca incluir rotas do esclarecimento ou dispositivos de recarregamento. Idealmente, a organização do suporte de primeiro nível deve rapidamente recolher a informação e então escalar o problema ao suporte de segundo nível. Passando um pouco de mais tempo que identifica e que descreve o problema

no apoio do nível um, uma descoberta da causa de raiz é muito mais provável, assim permitindo uma ação alternativa, uma identificação de laboratório, e um relatório do erro. O suporte de segundo nível deve ser bem versado nos tipos de informação que Cisco pode precisar de diagnosticar um problema ou de arquivar uns relatórios de bug, incluindo:

- Dumps de memória
- Saída de informação do roteamento
- Show command output (resultado do comando show) do dispositivo

Padronização de configuração

Os padrões de configuração de dispositivo globais representam a prática de manter dispositivos como “globais” padrão e serviços dos parâmetros de configuração transversalmente tendo por resultado a consistência de configuração global larga da empresa. Os comandos global configuration são os comandos que se aplicam ao dispositivo inteiro e não às portas individuais, aos protocolos ou às relações, e geralmente o acesso de dispositivo do impacto, comportamento geral do dispositivo e segurança do dispositivo. No Cisco IOS, isto inclui os comandos seguintes:

- Serviço
- IP
- VTY
- Porta de Console
- Registro
- AAA/TACACS+
- SNMP:
- Bandeira

Igualmente importante em padrões de configuração de dispositivo globais é uma convenção de nomeação apropriada do dispositivo que permita que os administradores identifiquem o lugar do dispositivo, do tipo de dispositivo e do dispositivo baseado no nome de DNS do dispositivo. A consistência de configuração global é importante para a capacidade de suporte total e a confiança de um ambiente de rede porque ajuda a reduzir a complexidade de rede e aumentar a capacidade de suporte da rede. Geralmente, o usuário passa por problemas no suporte sem padronização de configuração, seja devido a um comportamento incorreto ou indevido do dispositivo, ao acesso SNMP ou, ainda, devido à segurança geral do dispositivo.

Manter padrões de configuração de dispositivo globais é realizada normalmente por um grupo interno da engenharia ou de operações que crie e mantenha parâmetros de configuração globais para dispositivos de rede similares. É igualmente uma boa prática fornecer uma cópia do arquivo de configuração global nos diretórios de TFTP de modo que possam inicialmente ser transferidos toda recentemente aos dispositivos fornecida. Igualmente útil é um arquivo acessível da Web que forneça o arquivo de configuração padrão uma explicação de cada parâmetro de configuração. Algumas organizações configuram tudo dispositivos como em uma base periódica para ajudar a assegurar a consistência de configuração global, ou periodicamente dispositivos da revisão para os padrões corretos da configuração global.

Os padrões da relação ou da configuração de protocolo representam a prática de padrões de manutenção para a relação e a configuração de protocolo, que melhora a disponibilidade da rede reduzindo a complexidade de rede, fornecendo o dispositivo previsto e o comportamento de protocolo e melhorando a capacidade de suporte da rede. A inconsistência da relação ou da configuração de protocolo pode conduzir ao comportamento do dispositivo inesperado, às edições do roteamento de tráfego, aos problemas de conectividade aumentados e ao tempo aumentado

do suporte reagente.

Os padrões da configuração da interface podem incluir:

- CDP (protocolo cisco discovery)
- Descritores da relação
- Configuração de ocultação
- Outros padrões do específico do protocolo

Os padrões de configuração específicos do protocolo podem incluir:

- Configuração de Roteamento IP
- Configuração DLSw
- Configuração de lista de acesso
- Configuração de ATM
- Configuração do Frame Relay
- Configuração de árvore de abrangência
- Atribuição de VLAN & configuração
- VTP (protocolo virtual trunking)
- HSRP (protocolo de roteamento do standby recente)
- Outro segundo o que é configurado dentro da rede

Um exemplo de padrões IP pode incluir o tamanho de sub-rede, o espaço de endereços IP usado, o protocolo de roteamento usado e a configuração de protocolo de roteamento.

Manter padrões do protocolo e da configuração da interface é normalmente a responsabilidade dos grupos da engenharia e da aplicação da rede. O grupo de engenharia deve ser responsável para identificar, testar, validar e documentar os padrões. O grupo da aplicação é então responsável para usar os documentos de engenharia ou os gabaritos de configuração para provisionar serviços novos. O grupo de engenharia deve criar documentação sobre todos os aspectos dos padrões exigidos para garantir consistência. Os gabaritos de configuração devem igualmente ser criados para ajudar a reforçar os padrões de configuração. Os grupos de operação também devem receber treinamento sobre os padrões e devem ser capazes de identificar problemas de configurações que não sejam padrão. A consistência da configuração é do grande ajuda nos testes, na validação, e na fase da certificação. Sem gabaritos de configuração standardizados, é quase impossível testar, validar, ou certificar adequadamente moderadamente uma versão do Cisco IOS para uma rede grande.

Gerenciamento de disponibilidade

O gerenciamento de disponibilidade é o processo de melhoria de qualidade usando a disponibilidade da rede como a métrica da melhoria de qualidade. Muitas organizações estão medindo agora o tipo de Disponibilidade e de indisponibilidade. Os tipos da indisponibilidade podem incluir o seguinte:

- Hardware
- Software
- Link/portador
- Potência/ambiente
- Projeto
- Erro de usuário/processo

Identificando indisponibilidade e executando a análise de causa de raiz imediatamente depois da

recuperação, a organização pode identificar métodos para melhorar a Disponibilidade. Quase todas as redes que conseguiram a Alta disponibilidade têm algum tipo de processo da melhoria de qualidade no lugar.

[Lista de verificação das operações do Gerenciamento do Cisco IOS](#)

- Passo 1: [Defina requisitos de objetivo de negócios](#) (o [clientes registrados somente](#))
- Passo 2: [Avalie o status atual de práticas de gerenciamento do Cisco IOS Software](#) (o [clientes registrados somente](#))
- Passo 3: [Defina papéis e responsabilidades](#) (o [clientes registrados somente](#))
- Passo 4: [Desenvolva um plano de projeto do gerenciamento de software](#) (o [clientes registrados somente](#))
- Passo 5: [Desenvolva uma matriz dos requisitos de software](#) (o [clientes registrados somente](#))

[Informações Relacionadas](#)

Um apêndice foi criado para ajudar ao cliente em obter a outra informação relacionada valiosa do Cisco IOS como: Fundamentos do Cisco IOS, processos internos do Cisco IOS Software de Cisco, análise de confiabilidade de software, programa de qualidade de Cisco metodologias, de teste interno internos de Cisco, e uma análise de campo que mostre práticas atuais da indústria e experiências totais do cliente com Cisco IOS Software

- Gerenciamento do Cisco IOS: A informação adicional no Gerenciamento do Cisco IOS e os melhores prática podem ser encontrados do “no White Paper do gerenciamento de rede de alta disponibilidade Cisco IOS” no seguinte local:
http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a00800a998b.shtml
- Ra obter informações específicas sobre de como executar as pontas de prova da rede, que comandos CLI se usar, como analisar e interpretar dados do tráfego de rede, e como estabelecer políticas de utilização do aplicativo, visita <http://www.cisco.com>. Este local fornece uma escala detalhada do apoio, do treinamento, da referência técnica, e de soluções de consulta.
- O Cisco IOS tem as convenções de nomeação específicas que são definidas aqui:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_tech_note09186a0080101cda.shtml
- A informação sobre a Disponibilidade do Cisco IOS Release é fornecida aqui:
http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html
- As liberações do Cisco IOS eventualmente são removidas do CCO e podem já não ser pedidas. Seja por favor certo ajustar em conformidade expectativas do cliente.
- Os boletins de produto do Cisco IOS são usados para anunciar liberações do Cisco IOS aos clientes. Contêm a breve informação sobre o índice de liberação. Verifique aqui para ver se há a Disponibilidade de liberações

http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html do Novo Cisco IOS

- A Segurança dos punhos do Product Security Incident Response Team para o Produtos da Cisco. Todas as edições relativas à segurança do Cisco IOS devem ser referidas esta equipe. Cisco publica-a publicamente é vulnerabilidades de segurança.

<http://tools.cisco.com/security/center/publicationListing>

- Defeitos do Cisco IOS: Os defeitos sérios do Cisco IOS devem ser recomendados para o adiamento. Qualquer funcionário do Cisco pode fazer a recomendação.
- As edições do campo no Cisco IOS são comunicadas aos clientes com os relatórios formais do Cisco IOS.

http://www.cisco.com/en/US/products/products_security_advisory09186a0080b20ee1.shtml

- Características do Cisco IOS: A ferramenta de recurso de navegador permite clientes de encontrar e vice-versa as liberações que apoiam características específicas.

<http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>

- O conselheiro de software Cisco permite clientes de encontrar o suporte de software para características ou o suporte de software para o hardware.

<http://tools.cisco.com/Support/Fusion/FusionHome.do> (clientes registrados somente)

Serviços da Cisco e apoio

- [Serviços de suporte técnico](#)
- [Serviços específicos às Tecnologias de Rede e às soluções de Cisco](#)