Gerenciamento Cisco IOS para redes de alta disponibilidade: White Paper de práticas recomendadas

Contents

Introduction

A implantação e a manutenção confiáveis do software Cisco IOS® é uma prioridade no ambiente de rede essencial para os negócios de hoje, que exige que a Cisco e o cliente se concentrem novamente para obter disponibilidade ininterrupta. Enquanto a Cisco deve concentrar-se em seu comprometimento com a qualidade de software, os grupos de projeto e suporte de rede devem concentrar-se em melhores práticas para gerenciamento do software Cisco IOS. O objetivo é maior disponibilidade e eficiência de gerenciamento de software. Esse método é uma parceria combinada para compartilhar, aprender e implementar o compartilhamento de práticas ideais.

Este documento fornece uma estrutura operacional eficaz de práticas de gerenciamento do Cisco IOS para clientes corporativos e provedores de serviços que ajudam a promover maior confiabilidade de software, complexidade de rede reduzida e maior disponibilidade de rede. Essa estrutura ajuda também a melhorar a eficiência do gerenciamento de software pela identificação de áreas de responsabilidade e sobreposições nos testes de gerenciamento de software e validação entre operações de versões e a base de clientes Cisco.

Visão geral das práticas recomendadas do Cisco IOS

As tabelas a seguir fornecem uma visão geral de boas práticas do Cisco IOS. Essas tabelas podem ser utilizadas como uma visão geral de gerenciamento das melhores práticas definidas, uma lista de verificação de análise de intervalo para analisar práticas de gerenciamento atuais do Cisco IOS ou como uma estrutura para criar processos em torno do gerenciamento do Cisco IOS.

As tabelas definem os quatro componentes do ciclo de vida do gerenciamento do Cisco IOS. Cada tabela começa com uma estratégia e um resumo de ferramentas para a área de ciclo de vida identificada. Seguindo a estratégia e o resumo de ferramentas, estão as melhores práticas específicas que se aplicam somente à área de ciclo de vida definida.

Planejamento - Criação da estrutura de gerenciamento do Cisco IOS — O planejamento é a fase inicial do gerenciamento do Cisco IOS necessária para ajudar uma organização a determinar quando atualizar o software, onde atualizar e qual processo será usado para testar e validar imagens potenciais.

Prática recomendada	Detalhe
Estratégia e Ferramentas para Planejamento de Cisco IOS	Começar com o planejamento de gerenciamento do Cisco IOS começa com uma avaliação honesta das práticas atuais, o desenvolvimento de metas alcançáveis e o planejamento do projeto.
Definições de acompanhamento de versão de software	Identifica onde a consistência do software pode ser mantida. Uma faixa de software pode ser definida como um agrupamento exclusivo de versões de software, diferenciado de outras áreas por geografia, plataformas, módulos ou requisitos de recursos exclusivos.

Ciclo e definições de atualização	As definições de ciclo de atualização podem ser definidas como passos básicos de qualidade em software e gerenciamento de alteração utilizadas para determinar quando um ciclo de atualização de software deve ser iniciado.
Processo de certificação	As etapas do processo de certificação devem incluir identificação de trilha, definições de ciclo de atualização, gerenciamento de candidatos, teste/validação e pelo menos algum uso de produção piloto.

Design - Seleção e Validação das Versões do IOS —Ter um processo bem definido para selecionar e validar as versões do Cisco IOS ajuda uma organização a reduzir o tempo de inatividade não planejado devido a tentativas de atualização malsucedidas e defeitos de software não planejados.

Prática recomendada	Detalhe
Estratégia e ferramentas para Seleção e Validação Cisco IOS	Definir processos para selecionar, testar e validar novas versões do Cisco IOS. Isso inclui um laboratório de teste de rede que simule a rede de produção
Gerenciamento de candidatos	O gerenciamento de candidatos é a identificação dos requisitos de versão de software e possíveis riscos para o hardware específico e os conjuntos de recursos habilitados.
Teste e validação	Testes e validação são aspectos críticos do gerenciamento de software e de redes de alta disponibilidade. Testes de laboratório adequados podem reduzir significativamente o tempo de inatividade da produção, ajudar a treinar a equipe de suporte da rede e ajudar a otimizar os processos de implementação da rede.

Implementação - Implantação do Cisco IOS rápida e bem-sucedida — Processos de implementação bem definidos permitem que uma organização implante novas versões do Cisco IOS de forma rápida e bem-sucedida.

Prática recome	Detalhe

ndada	
Estratégia e ferramentas para distribuições de Cisco IOS	A estratégia básica das implantações de Cisco IOS é executar a certificação final através de um processo piloto e a implantação rápida usando ferramentas de atualização e um processo de implementação bem definido.
Processo piloto	Para minimizar a exposição potencial e capturar com mais segurança quaisquer problemas de produção restantes, recomenda-se um piloto de software. O plano piloto individual deve considerar a seleção do piloto, a duração do piloto e a medição.
Implementação	Após a conclusão da fase piloto, a fase de implementação do Cisco IOS deve começar. A fase de implementação pode incluir vários passos para garantir o êxito da atualização do software e a eficiência, incluindo o início lento, a certificação final, a preparação para atualização, a automação da atualização e a validação final.

Operações - Gerenciamento da Implementação do Cisco IOS de Alta Disponibilidade — As práticas recomendadas para operações do Cisco IOS incluem controle de versão de software, gerenciamento de syslog do Cisco IOS, gerenciamento de problemas, padronização de configuração e gerenciamento de disponibilidade.

Prática recomendada	Detalhe
Estratégias e ferramentas para operações de Cisco IOS	A primeira estratégia das operações do Cisco IOS é manter o ambiente o mais simples possível, evitando variações na configuração e nas versões do Cisco IOS. A segunda estratégia é a capacidade de identificar e resolver rapidamente falhas de rede.
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.
Gerenciamento de syslog proativo	Coleção, monitoramento e análise de syslog são processos de gerenciamento de falhas recomendados para resolver outros problemas de rede específicos do Cisco IOS

	que são difíceis ou impossíveis de serem identificados por outros meios.
Gerenciamento de problemas	Processos detalhados de gerenciamento de problemas que definem a identificação de problemas, a coleta de informações e um caminho de solução bem analisado. Esses dados podem ser usados para determinar a principal causa.
Padronização de configuração	Os padrões de configuração representam a prática de criar e manter parâmetros de configuração global padrão em dispositivos e serviços semelhantes, resultando em consistência de configuração global em toda a empresa.
Gerenciamento de disponibilidade	O gerenciamento de disponibilidade é o processo de melhoria de qualidade usando a disponibilidade da rede como métrica de melhoria de qualidade.

Visão geral do processo de gerenciamento do ciclo de vida do software

O gerenciamento do ciclo de vida do software Cisco IOS é definido como o conjunto de processos de planejamento, projeto, implementação e operação recomendados para implementações de software confiáveis e redes de alta disponibilidade. Isso inclui processos de seleção, validação e manutenção das versões do Cisco IOS na rede.

O objetivo do gerenciamento do ciclo de vida do software Cisco IOS é melhorar a disponibilidade da rede reduzindo a probabilidade de defeitos de software identificados na produção ou falhas de alteração/atualização relacionadas ao software. As melhores práticas definidas neste documento foram exibidas para reduzir tais defeitos e alterar as falhas, com base na experiência prática de muitos clientes Cisco e da equipe de Serviços avançados da Cisco. O gerenciamento do ciclo de vida do software pode, inicialmente, aumentar as despesas. No entanto, um custo de propriedade global mais baixo pode ser obtido com menos interrupções e mecanismos de distribuição e suporte mais otimizados.

Planejamento - Construção da Cisco IOS Management Framework

O planejamento é a fase inicial do gerenciamento do Cisco IOS necessária para ajudar uma organização a determinar quando e onde o software deve ser atualizado, e qual processo será usado para testar e validar as imagens em potencial.

As práticas recomendadas incluem definições de controle de versão de software, ciclo de atualização e definições, e a criação de um processo interno de certificação de software.

Estratégia e Ferramentas para Planejamento de Cisco IOS

Comece o planejamento de gerenciamento do Cisco IOS com uma avaliação honesta das

práticas atuais, o desenvolvimento de metas alcançáveis e o planejamento de projetos. A auto-avaliação deve ser feita comparando-se as melhores práticas desse documento aos processos da sua organização. As perguntas básicas devem incluir o seguinte:

- Minha organização tem um processo de certificação de software que inclui teste/validação de software?
- Minha organização tem padrões do software Cisco IOS com uma quantidade limitada de versões do Cisco IOS em execução na rede?
- Minha empresa tem dificuldade em determinar quando atualizar o software Cisco IOS?
- Minha empresa tem dificuldade para implantar o novo software Cisco IOS de forma eficiente e eficaz?
- Minha empresa tem problemas de estabilidade do Cisco IOS após a implantação que afetam seriamente o custo do tempo de inatividade?

Após a avaliação, sua empresa deve começar a definir metas para o gerenciamento do software Cisco IOS. Comece por reunir um grupo interfuncional de gerenciadores e/ou clientes em potencial presentes nos grupos de planejamento de arquitetura, engenharia, implementação e operações para auxiliar na definição dos objetivos do Cisco IOS e nos projetos de aprimoramento do processo. A meta das reuniões iniciais deve ser determinar os objetivos, as funções e as responsabilidades gerais, atribuir itens de ação e definir as programações iniciais do projeto. Além disso, defina fatores críticos de sucesso e métricas para determinar os benefícios do gerenciamento de software. As possíveis métricas incluem:

- disponibilidade (devido a problemas de software)
- custo de atualizações de software
- Tempo necessário para atualizações
- número de versões do software que são executadas em produção
- taxa de sucesso/falha de alteração de upgrade de software

Além do planejamento geral da estrutura de gerenciamento do Cisco IOS, algumas organizações também definem reuniões contínuas de planejamento de software a serem realizadas mensalmente ou trimestralmente. O objetivo dessas reuniões é revisar a implantação atual do software e começar a planejar quaisquer novos requisitos de software. O planejamento pode incluir uma nova visita ou a modificação dos processos de gerenciamento de software atuais ou simplesmente a definição de funções e responsabilidades para fases de gerenciamento de software diferentes.

Ferramentas na fase de planejamento consistem simplesmente de ferramentas de gerenciamento de inventário de software. O Gerenciador de inventários do CiscoWorks 2000 Resource Manager Essentials (RME) é a principal ferramenta usada nessa área. O Gerenciador de Inventário do CiscoWorks2000 RME simplifica muito o gerenciamento de versão de roteadores e switches da Cisco por meio de ferramentas de relatório baseadas na Web que relatam e classificam dispositivos do Cisco IOS com base na versão do software, plataforma do dispositivo, tamanho da memória e nome do dispositivo.

Definições de acompanhamento de versão de software

A primeira prática recomendada de planejamento do software Cisco IOS identifica onde a consistência do software pode ser mantida. Uma faixa de software é definida como um agrupamento exclusivo de versões de software, diferenciado de outras áreas por geografia, plataformas, módulos ou requisitos de recursos exclusivos. Da maneira mais eficiente, uma rede deve executar apenas uma versão de software. Isso reduz muito os custos relacionados ao gerenciamento de software e fornece um ambiente consistente e facilmente gerenciado. No

entanto, a realidade é que a maioria das empresas deve executar várias versões na rede devido a problemas de recursos, plataformas, migração e disponibilidade em áreas específicas. Em muitos casos, a mesma versão não funciona em plataformas heterogêneas. Em outros casos, a organização não pode esperar por uma versão para suportar todos os seus requisitos. A meta é identificar a menor quantidade de acompanhamentos de software da rede em consideração a exigências de teste/validação, certificação e atualização. Em muitos casos, a empresa pode ter um pouco mais de trilhas para reduzir os custos gerais de testes/validação, certificação e atualização.

O primeiro fator diferenciador é o suporte para plataforma. Em geral, os Switches de LAN, os Switches de WAN, os roteadores centrais e os roteadores de ponta têm recursos de tracking de Software separados. Outros rastreamentos de software serão necessários para recursos ou serviços específicos, como switching de link de dados (DLSw), Qualidade de serviço (QoS) ou telefonia IP, especialmente se esse requisito estiver dentro da rede.

Outro critério é a fiabilidade. Muitas organizações tentam executar o software mais confiável em direção ao núcleo da rede e ao data center, oferecendo recursos avançados mais novos, ou suporte de hardware, em direção à borda da rede. Por outro lado, os recursos de escalabilidade ou largura de banda são frequentemente mais necessários em ambientes centrais ou de data center. Outros rastreamentos podem ser necessários para plataformas específicas, como instalações de distribuição maiores que possuam uma plataforma de roteadores de WAN diferente. A tabela a seguir é um exemplo de definição de rastreamento de software de uma organização empresarial de grande porte.

Track	Área	Plataformas de hardware	Recursos	Versão do Cisco IOS	Status da certificação
1	LAN core switching	6500	qos	12.1E(A8)	Testando
2	switch de acesso à LAN	2924XL 2948XL	UDLD (Unidirectional Link Detection Protocol), STP (Spanning Tree Protocol)	12.0(5.2)XU	Certificado em 01/03/01
3	distribuição/acesso de LAN	5500 6509	Supervisor 3	5.4(4)	Certificado em 01/07/01
4	Módulo Switch de Rota (RSM - Route Switch Module) do switch de distribuição	RSM	Roteamento do OSPF	12.0(11)	Certificado em 04/03/02

5	distribuição de fim de cabeçalho de WAN	7505 7507 7204 7206	Frame Relay OSPF	12.0(11)	Certificação 11/1/01
6	acesso à WAN	2600	Frame Relay OSPF	12.1(8)	Certificado em 01/06/01
7	conectividade IBM	3600	headend SDLC (Synchronous Data Link Control, Controle de Enlace de Dados Síncrono)	11.3(8)T1	Certificação 11/1/00

As atribuições de rastreamento também podem mudar ao longo do tempo. Em muitos casos, os recursos ou o suporte de hardware podem integrar-se em versões de software mais principais, permitindo que caminhos diferentes eventualmente migrem juntos. Quando as definições de rastreamento estiverem definidas, a organização pode utilizar outros processos definidos para migrar para a consistência e validação de novas versões. As definições de rastreamento também são um esforço contínuo. Sempre que um novo requisito de recurso, serviço, hardware ou módulo for identificado, uma nova faixa deve ser considerada.

As organizações que desejam iniciar um processo de acompanhamento devem começar com novos requisitos de via definidos ou, em alguns casos, projetos de estabilização para redes existentes. Uma empresa também pode ter algumas semelhanças identificáveis com versões de software existentes que podem tornar possível a definição atual do controle. Na maioria dos casos, a migração rápida para versões identificadas não é necessária se o cliente tiver estabilidade de rede suficiente. A arquitetura de rede, ou grupo de engenharia, normalmente possui o processo de definição de controle. Em alguns casos, um indivíduo pode ser responsável pelas definições de controle. Em outros casos, os leads de projeto são responsáveis pelo desenvolvimento de requisitos de software e novas definições de rastreamento com base em projetos individuais. Também é recomendável rever as definições de rastreamento trimestralmente para determinar se novas rotas são necessárias ou se as trilhas antigas exigem consolidação ou atualização.

Organizações que identificam e mantêm acompanhamento de software com controle estrito de versão demonstraram sucesso maior com um número decrescente de versões de software na rede de produção. Geralmente, isso resulta em estabilidade de software aperfeiçoada e confiabilidade geral da rede.

Ciclo e definições de atualização

Definições de ciclos de atualização são identificadas como etapas básicas de qualidade no gerenciamento de softwares e alterações que são usadas para determinar quando um ciclo de atualização de software deve ser iniciado. As definições do ciclo de atualização permitem que uma organização planeje corretamente um ciclo de atualização de software e aloque os recursos necessários. Sem as definições do ciclo de atualizações, uma organização estará sujeita a um número maior de problemas relacionados à confiabilidade do software, normalmente devido às

necessidades de recursos nas versões estáveis atuais. Outra exposição pode ser que a organização não tenha a oportunidade de testar e validar corretamente uma nova versão antes que o uso da produção seja necessário.

Um aspecto importante dessa prática é identificar quando e em que grau os processos de planejamento de software devem ser iniciados. Isso se deve ao fato de que uma das principais causas de problemas de software está ativando um recurso, serviço ou hardware na produção sem a devida diligência ou atualizando para uma nova versão do Cisco IOS sem considerações de gerenciamento de software. Outro problema não é atualizar. Ao ignorar os ciclos e requisitos normais de software, muitos clientes enfrentam a difícil tarefa de atualizar o software por meio de várias versões principais diferentes. A dificuldade se deve a tamanhos de imagem, alterações de comportamento padrão, alterações de Intérprete de nível de comando (CLI) e alterações de protocolo.

A Cisco recomenda um ciclo de atualização bem definido, com base nas melhores práticas definidas neste documento, a ser iniciado sempre que for necessário um novo recurso principal, serviço ou suporte de hardware. O grau de certificação e de teste/validação deve ser analisado (com base no risco) para determinar os requisitos de teste/validação precisos. A análise de risco pode ser feita por local geográfico, local lógico (centro, distribuição ou camadas de acesso) ou pelo número estimado de pessoas/clientes afetados. Se o recurso principal ou de hardware estiver contido na versão atual, alguns processos de ciclo de atualização simplificados também devem ser iniciados. Se o recurso for relativamente pequeno, considere o risco e decida quais processos devem ser iniciados. Além disso, o software deve ser atualizado em dois anos ou menos para ajudar a garantir que sua empresa permaneça relativamente atual e que o processo de atualização não seja muito complicado.

Os clientes também devem considerar o fato de que nenhuma correção de bugs será feita em trilhas de software que passaram o status de EOL (End Of Life [fim da vida útil]). Algumas considerações também devem ser dadas aos requisitos de negócios, uma vez que muitos ambientes podem tolerar, ou mesmo aceitar, mais acréscimos de recursos com pouco ou nenhum processo de teste/validação e algum tempo ocioso resultante. Os clientes também devem considerar os dados mais recentes coletados nas operações de versão da Cisco ao considerar seus requisitos de teste. Uma análise de bugs e causas raiz mostrou que a grande maioria das causas raiz de bugs foi resultado da codificação de desenvolvedores dentro da área de software afetada. Isso significa que se uma organização está adicionando um recurso ou módulo específico à sua rede em uma versão existente, há a probabilidade de ocorrer um bug relacionado a esse recurso ou módulo, mas uma probabilidade muito menor de que o novo recurso, hardware ou módulo afetará outras áreas. Esses dados devem permitir que as organizações diminuam os requisitos de teste, ao adicionar novos recursos ou modelos suportados nas versões existentes, testando apenas o novo serviço ou recurso em conjunto com outros serviços habilitados. Os dados também devem ser considerados durante a atualização do software com base em alguns bugs críticos encontrados na rede.

A seguinte tabela mostra os requisitos de atualização recomendados para uma grande organização empresarial de alta disponibilidade:

Gatilho de gerenciamento de software	Requisito de ciclo de vida de software
Novo serviço de rede. Por exemplo, um novo backbone ATM ou um novo	Validação completa do ciclo de vida do software, incluindo novo teste de recursos (em conjunto com outros serviços habilitados),

serviço VPN.	teste de topologia recolhido, análise de desempenho e teste de perfil de aplicativos.
O novo recurso de rede não é suportado na versão atual do software. Os exemplos incluem QoS e Multiprotocol Label Switching (MPLS).	Validação completa do ciclo de vida do software, incluindo novo teste de recursos, em conjunto com outros serviços habilitados, teste de topologia recolhido, análise de desempenho e teste de perfil de aplicativos.
Novo recurso principal ou módulo de hardware existente na versão atual. Por exemplo, adicionar um novo módulo GigE, suporte a multicast ou DLSW.	Processo de gerenciamento de candidatos. Possível validação completa com base nos requisitos da versão. A validação/o teste limitado possível em caso de gerenciamento de candidatos identifica a versão atual como potencialmente aceitável.
Adição de recursos secundários. Por exemplo, um dispositivo TACACS para controle de acesso.	Considere o gerenciamento de candidatos com base no risco do recurso. Considere testar ou testar o novo recurso com base no risco.
Software em produção por dois anos ou uma revisão trimestral do software.	O gerenciamento de candidatos e as decisões comerciais em relação ao gerenciamento completo do ciclo de vida para identificar a versão suportável atual.

Atualizações de emergência

Em alguns casos, as empresas enfrentam a necessidade de atualizar o software devido a bugs catastróficos. Isso poderá causar problemas se a organização não tiver uma metodologia de atualização de emergências. Problemas com o software podem variar desde atualizações de software não gerenciadas, nas quais o software é atualizado sem gerenciamento de ciclo de vida de software, até situações em que dispositivos de rede travam continuamente, mas a organização não faz atualizações, pois o procedimento de certificação/testes na próxima versão candidata ainda não foi concluído. A Cisco recomenda um processo de atualização de emergência para essas situações em que testes e pilotos limitados são executados em áreas menos críticas da rede.

Se ocorrerem erros catastróficos sem solução aparente e o problema estiver relacionado a defeitos de software, a Cisco recomenda que o suporte da Cisco seja totalmente engajado para isolar o defeito e determinar se ou quando uma correção está disponível. Quando a correção estiver disponível, a Cisco recomenda um ciclo de atualização de emergência para determinar rapidamente se o problema pode ser reparado com tempo de inatividade limitado. Na maioria dos casos, uma organização está executando uma versão compatível do código e a correção do problema está disponível em uma versão mais recente e temporária do software.

As organizações também podem se preparar para possíveis atualizações de emergência. A preparação inclui migração para versões suportadas do Cisco IOS e a identificação/desenvolvimento de versões candidatas à substituição, dentro da mesma versão de treinamento do Cisco IOS da versão certificada. O software suportado é importante porque significa que o desenvolvimento da Cisco ainda está incluindo reparos de erro da versão do software identificado. Ao manter o software suportado na rede, a organização reduz o tempo de validação devido à base de código mais familiar e estável. Em geral, uma substituição de candidatos é um nova imagem intermediária dentro do mesmo Cisco IOS train sem adições de suporte de recursos ou hardware. Uma estratégia de substituição de candidatos é especialmente importante se a empresa estiver na fase de adoção inicial de um treinamento de software específico.

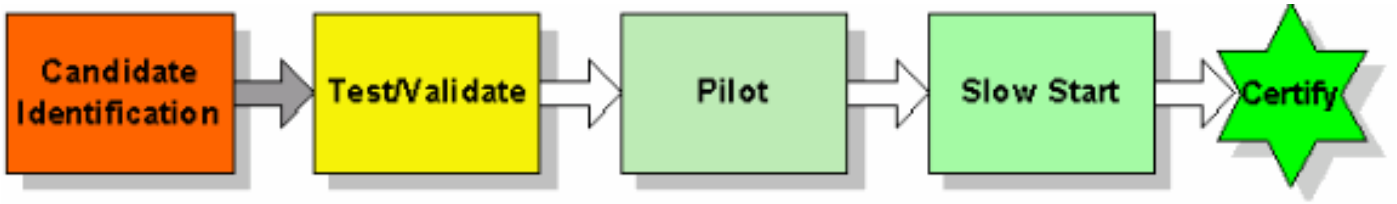
Processo de certificação

Um processo de certificação ajuda a garantir que o software validado seja implantado consistentemente no ambiente de produção da organização. As etapas do processo de certificação devem incluir identificação de trilha, definições de ciclo de atualização, gerenciamento de candidatos, teste/validação e algum uso de produção piloto. Um processo de certificação simples, no entanto, ainda ajuda a garantir que as versões consistentes de software sejam implantadas dentro das trilhas identificadas.

Inicie um processo de certificação identificando indivíduos por arquitetura, engenharia/distribuição e operações para esboçar e gerenciar o processo de certificação. O grupo deve primeiro considerar os objetivos comerciais e os recursos para garantir que o processo de certificação tenha sucesso contínuo. Em seguida, atribua a indivíduos ou grupos a responsabilidade geral pelas etapas principais do processo de certificação, incluindo gerenciamento de rastreamento, definições de atualização do ciclo de vida, teste/validação e pilotos. Cada uma dessas áreas deve ser definida, aprovada e formalmente comunicada dentro da organização.

Inclua também diretrizes para qualidade ou aprovação em cada fase do processo de certificação. Às vezes, isso é chamado de processo de porta de qualidade porque certos critérios de qualidade devem ser atendidos antes que o processo possa passar para a próxima etapa. Isso ajuda a garantir que o processo de certificação é efetivo e vale os recursos atribuídos. Em geral, quando os problemas são encontrados com qualidade em uma área, o processo empurra o esforço para trás um passo.

Os candidatos a software podem não atender aos critérios de certificação definidos devido à qualidade do software ou ao comportamento inesperado. Quando são encontrados problemas que impactam o ambiente, a organização deve adotar um processo mais simplificado para certificar uma versão provisória posterior. Isso ajuda a reduzir os requisitos de recursos e, em geral, é eficiente caso a organização compreenda o que foi alterado e quais são os defeitos a serem solucionados. Não é raro uma organização experimentar um problema com um candidato inicial e certificar uma versão provisória do Cisco IOS posterior. As organizações também podem fazer uma certificação limitada ou fornecer advertências se houver problemas e podem atualizar para uma versão totalmente certificada posteriormente quando um novo intermediário for validado. O fluxograma a seguir representa um processo básico de certificação e inclui portas de qualidade (uma revisão após cada bloco):



Projeto - Seleção e validação das versões do Cisco IOS

Ter uma metodologia bem definida para selecionar e validar as versões do Cisco IOS ajuda a organização a reduzir o tempo de inatividade não planejado devido a tentativas de atualização malsucedidas e defeitos de software não planejados.

A fase de projeto inclui gerenciamento de candidatos e teste/validação. O gerenciamento de candidatos é o processo usado para identificar versões específicas para os softwares definidos. O teste/validação faz parte do processo de certificação e garante que a versão de software identificada seja bem-sucedida dentro da faixa necessária. O teste/validação deve ser realizado em um ambiente de laboratório com topologia comprimida e configuração bastante similar ao ambiente de produção.

Estratégia e ferramentas para Seleção e Validação Cisco IOS

Cada organização deve ter um processo para selecionar e validar versões padrão do Cisco IOS para a rede, iniciando com um processo para selecionar a versão do Cisco IOS. Uma equipe multifuncional de arquitetura, engenharia e operações deve definir e documentar o processo de gerenciamento de candidatos. Depois de aprovado, o processo deve ser transferido para o grupo de entrega apropriado. Também é recomendável criar um modelo padrão de gerenciamento de candidatos que possa ser atualizado com as informações de candidatos conforme elas são identificadas.

Nem todas as organizações têm um ambiente de laboratório sofisticado que pode facilmente imitar o ambiente de produção. Algumas organizações ignoram os testes de laboratório por causa da despesa e da capacidade de pilotar uma nova versão na rede sem grande impacto comercial. No entanto, as organizações de alta disponibilidade são incentivadas a criar um laboratório que imite a rede de produção e a desenvolver um processo de teste/validação para garantir alta cobertura de teste para novas versões do Cisco IOS. Uma organização deve permitir cerca de seis meses para a construção do laboratório. Durante esse período, a organização deve trabalhar para criar planos e processos de teste específicos para garantir que o laboratório seja usado em seu benefício total. Para o Cisco IOS, isso significa a criação de planos de teste específicos do Cisco IOS para cada faixa de software necessária. Esses processos são fundamentais em organizações maiores, devido ao fato de que muitos laboratórios não são usados pra lançamentos de novos produtos e softwares.

As seções seguintes descrevem resumidamente o gerenciamento de candidatos e as ferramentas de teste/validação para uso na seleção e validação do Cisco IOS.

Ferramentas de gerenciamento de candidatos

Observação: para usar a maioria das ferramentas fornecidas abaixo, você deve ser um usuário registrado e estar conectado.

- Notas de versão —Fornece informações sobre o suporte de hardware, módulo e recurso de

uma versão. Notas de versão devem ser revisadas durante o gerenciamento de candidatas para garantir que todo o suporte necessário para hardware e software exista na versão potencial e para compreender todos os problemas de migração, incluindo diferentes requisitos de comportamento padrão ou atualização.

Ferramentas de Validação e Testes

As ferramentas de teste e validação são usadas para soluções de teste e validação de redes que incluem novos hardwares, softwares e aplicativos.

- **Geradores de tráfego**—Gera fluxos de tráfego multiprotocolo e taxas de pacote bruto usadas para modelar a taxa em qualquer link específico utilizando protocolos específicos. Os usuários podem especificar a origem, o destino MAC e os números dos soquetes. Esses valores podem ser incrementados nas etapas especificadas ou podem ser configurados para ser estáticos/fixos ou em incrementos aleatórios. Geradores de tráfego podem gerar os pacotes para os seguintes protocolos:IPInternetwork Packet Exchange (IPX)DECnetAppleXerox Network Systems (XNS)ICMP (Internet Control Message Protocol)Protocolo de Gerenciamento de Grupos Internet (IGMP - Internet Group Management Protocol)Serviço de Rede Sem Conexão (CLNS - Connectionless Network Service)User Datagram Protocol (UDP)Virtual Integrated Network Service (VINES)Pacotes de Enlace de DadosAs ferramentas estão disponíveis na Agilent e na Spirent Communications .
- **Contador/Captura/Decodificador de Pacotes (Sniffer)**—Permite ao cliente capturar e decodificar seletivamente pacotes em todas as camadas de pacote e de enlace de dados. A ferramenta tem a capacidade de permitir que o usuário especifique os filtros, o que permite a captura de dados de protocolo especificados apenas. Os filtros permitem ainda que o usuário especifique a captura dos pacotes que correspondem a um endereço IP, número de porta ou endereço MAC específicos. As ferramentas estão disponíveis com a Sniffer Technologies.
- **Network Simulator/Emulator** —Permite que o cliente preencha as tabelas de roteamento de roteadores específicos, com base nos requisitos de rede de produção. Suporta a geração de roteadores de IP Routing Information Protocol (RIP), OSPF, Intermediate System-To-Intermediate System (IS-IS), Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP) e Border Gateway Protocol (BGP). As ferramentas estão disponíveis em PacketStorm Communications e Spirent Communications.
- **Emuladores de sessão** — Gera fluxos de tráfego multiprotocolo de janela móvel e é capaz de enviar fluxos de tráfego multiprotocolo através da rede de teste em direção ao dispositivo receptor. O dispositivo receptor devolve (eco) os pacotes para a origem. O dispositivo de origem verifica o número de pacotes enviados, recebidos, fora de seqüência e com erro. A ferramenta também oferece a flexibilidade para definir os parâmetros da janela no TCP (Protocolo de Controle da Transmissão), quase imitando, desta forma, as seções de tráfego de cliente/servidor na rede de laboratório. As ferramentas estão disponíveis pela Empirix.
- **Emuladores de rede de grande escala**—Ajudam a testar a escalabilidade de ambientes maiores. Essas ferramentas são capazes de criar e injetar facilmente tráfego de tipo de controle em uma topologia de laboratório de forma a imitar com mais precisão um ambiente de produção. Os recursos incluem injetores de rota, vizinhos de protocolo e vizinhos de protocolo de Camada 2. As ferramentas estão disponíveis na Agilent e na Spirent Communications .
- **Simuladores de WAN** —Ideal para testar o tráfego de aplicativos corporativos onde a largura de banda e o atraso são potencialmente um problema. Essas ferramentas permitem que as organizações testem localmente um aplicativo com o atraso e a largura de banda estimados

para ver como o aplicativo funciona na WAN. Essas ferramentas são muito utilizadas para o desenvolvimento de aplicativos e para tipos de teste de perfis de aplicativo em organizações de empreendimento. A Adtech, uma divisão de Spirent Communications e Shunra fornece ferramentas de simulação de WAN.

Gerenciamento de candidatos

O gerenciamento de candidatos é o processo de identificação dos requisitos de versão de software e possíveis riscos para o hardware específico e conjuntos de recursos habilitados. Recomenda-se que uma empresa passe de quatro a oito horas pesquisando corretamente os requisitos de software, as notas de versão, os defeitos de software e os possíveis riscos antes de testar uma versão. A seguir, é apresentada a base para a gestão dos candidatos:

- Identifique os candidatos de software por meio das ferramentas Cisco Connection Online (CCO).
- Maturidade do software de análise de risco, novo recurso ou suporte a código.
- Identifique e rastreie bugs de software, problemas e requisitos conhecidos durante todo o ciclo de vida.
- Identificar o comportamento de configuração padrão da imagem selecionada.
- Manter candidatos recuados e progressivos para possíveis alterações de candidatos.
- Esfregões de inseto.
- Suporte aos serviços avançados da Cisco.

A identificação de candidatos a software tornou-se mais complexa com o número crescente de produções e trilhas de software da Cisco. O CCO agora tem várias ferramentas, incluindo o planejador de atualização do Cisco IOS, a ferramenta de pesquisa de software, a matriz de compatibilidade de hardware de software e a ferramenta de atualização de produto que pode ajudar as organizações a identificar possíveis candidatos à versão. Essas ferramentas podem ser encontradas em http://www.cisco.com/cisco/software/navigator.html.

Em seguida, analise o risco do software candidato em potencial. Esse é o processo de compreensão de onde o software atualmente reside na curva de maturidade e, em seguida, ponderar os requisitos de implantação com o risco potencial do candidato à versão. Por exemplo, se uma organização deseja colocar o software de implantação precoce (ED) em um ambiente crítico de alta disponibilidade, o risco associado e o requisito de recursos para uma certificação bem-sucedida devem ser considerados. Uma organização deve pelo menos adicionar recursos de gerenciamento de software para situações de risco mais alto para garantir o sucesso. Por outro lado, se uma versão de implantação geral (GD) estiver disponível que atenda às necessidades de uma organização, serão necessários menos recursos de gerenciamento de software.

Quando versões e riscos potenciais forem identificados, realize um apagamento de bug para determinar a existência de algum bug catastrófico identificado que poderia evitar potencialmente a certificação. Os agentes do Cisco Bug Watcher, do Navegador de Erros e do Observador de Erros podem ajudar a identificar possíveis problemas e devem ser usados durante todo o ciclo de vida do software para identificar possíveis problemas de segurança ou defeitos.

Um novo candidato de software também deve ser revisado quanto ao possível comportamento de configuração padrão. Isso pode ser conseguido pela revisão das notas de versão da imagem do novo software e pela revisão das diferenças de configuração com a imagem potencial carregada nas plataformas designadas. O gerenciamento de candidatos também pode incluir a identificação de versões de back-out ou versões de go-to se a versão escolhida não atender aos critérios de certificação em algum ponto do processo. Ao observar bugs relacionados a recursos para uma

faixa especificada, uma organização pode manter candidatos potenciais para certificação.

O Cisco Advanced Services também é uma excelente ferramenta para o gerenciamento de candidatos. Esse grupo pode fornecer mais informações sobre o processo de desenvolvimento e a colaboração entre um grande número de especialistas do setor em vários ambientes de mercado vertical diferentes. Normalmente, os melhores recursos de correção de bug ou de gerenciamento de candidatos estão no suporte da Cisco, devido ao nível de experiência e visibilidade usado nas versões do software de produção executadas em outras empresas.

Teste e validação

O teste e a validação são um aspecto crítico das melhores práticas de gerenciamento e da rede de alta disponibilidade, em geral. Testes de laboratório adequados podem reduzir significativamente o tempo ocioso de produção, ajudar a treinar pessoal de suporte de rede e auxiliar na otimização de processos de implementação de rede. No entanto, para ser eficiente, a organização deve alocar os recursos necessários para criar e manter o ambiente adequado do laboratório, aplicar recursos necessários para executar os testes corretos e usar uma metodologia de testes recomendada que inclua um grupo de medidas. Sem nenhuma dessas áreas, um processo de teste e validação pode não atender às expectativas de uma empresa.

A maioria das organizações corporativas não tem o ambiente de laboratório de teste recomendado. Por esse motivo, muitas organizações implantaram soluções incorretamente, experimentaram falhas na alteração da rede ou experimentaram problemas de software que poderiam ter sido isolados em um ambiente de laboratório. Em alguns ambientes, isso é aceitável, pois o custo do tempo de inatividade não compensa o custo de um ambiente de laboratório sofisticado. Em muitas organizações, no entanto, o tempo de inatividade não pode ser tolerado. É altamente recomendável que essas organizações desenvolvam os laboratórios de testes, os tipos de testes e as metodologias de testes recomendados para aperfeiçoar a qualidade da rede de produção.

Laboratório de teste e ambiente

O laboratório deve estar localizado em uma área isolada, com espaço suficiente para mesas, bancadas, instrumentos de teste e gabinetes ou racks de equipamentos. A maioria das grandes empresas precisará de entre quatro e dez racks de equipamentos para imitar o ambiente de produção. Uma certa segurança física é recomendada para ajudar a manter um ambiente de teste enquanto testes estão em andamento. Isso ajuda a evitar que um teste de laboratório seja interrompido devido a outras prioridades de laboratório, incluindo empréstimos de hardware, treinamento ou ensaios de implementação. A segurança lógica também é recomendada para evitar que rotas falsas entrem na rede de produção ou que tráfego indesejável saia do laboratório. Isso pode ser feito com filtros de roteamento e listas de acesso estendidas em um Lab Gateway Router. A conectividade com a rede de produção é útil para downloads de software e acesso à rede do laboratório a partir do ambiente de produção.

A topologia de laboratório deve ser capaz de imitar o ambiente de produção para quaisquer planos de teste específicos. Recomenda-se a reprodução de hardware, topologia de rede e configurações de recursos. É claro que reproduzir a topologia real é quase impossível, mas o que pode ser feito é reproduzir a hierarquia de rede e a interação entre os dispositivos de produção. Isso é importante para a interação de recurso e protocolo entre vários dispositivos. Algumas topologias de teste serão diferentes com base nos requisitos do teste de software. O teste do Cisco IOS na borda da WAN, por exemplo, não deve exigir dispositivos de tipo LAN ou testes e pode exigir apenas roteadores de borda da WAN e roteadores de distribuição da WAN. O segredo

é mimetizar a funcionalidade do software sem duplicar a produção. Em alguns casos, as ferramentas podem até ser usadas para imitar comportamentos em larga escala, como contagens de vizinhos de protocolo e tabelas de roteamento.

Também são necessárias ferramentas para auxiliar alguns tipos de testes, melhorando a capacidade de reproduzir o ambiente de produção e de coletar os dados dos testes. As ferramentas que ajudam a produção de mímica incluem coletores de tráfego, geradores de tráfego e dispositivos de simulação de WAN. O Smartbits é um bom exemplo de dispositivo que pode coletar e retransmitir tráfego de rede ou gerar grandes volumes de tráfego. Uma empresa também pode se beneficiar de dispositivos que podem ajudar a coletar dados, como analisadores de protocolo.

O laboratório também exige algum gerenciamento. Muitas organizações maiores têm um gerente de laboratório em tempo integral que é responsável pelo gerenciamento da rede do laboratório. Outras organizações utilizam equipes de arquitetura e engenharia existentes para validação de laboratório. As responsabilidades de gerenciamento de laboratório incluem solicitar equipamentos de laboratório e rastreamento de ativos, cabeamento, gerenciamento de espaço físico, definição de regras e direção de laboratório, programação de laboratório, documentação de laboratório, configuração de topologias de laboratório, elaboração de planos de teste, realização de testes de laboratório e gerenciamento de possíveis problemas identificados.

Tipos de Teste

No geral, há muitos tipos diferentes de testes que podem ser feitos. Antes de criar um laboratório de teste completo e um plano de teste que possam testar tudo em uma variedade de configurações, uma organização deve entender os diferentes tipos de testes, a intenção dos testes e se a engenharia, o marketing técnico ou a defesa do cliente da Cisco devem ou podem ser responsáveis por alguns dos vários testes. Os planos de teste do cliente geralmente abrangem os tipos de teste mais expostos. A tabela a seguir ajuda a entender os diferentes tipos de teste, quando devem ser realizados e as partes responsáveis.

Dos testes abaixo, o teste adequado do conjunto de recursos específicos de uma organização, topologia e combinação de aplicativos normalmente é o mais valioso. É importante saber que a Cisco realiza testes completos de recursos e regressão, no entanto, a Cisco não pode testar o perfil de aplicativos da sua organização com sua combinação específica de topologia, hardware e recursos configurados. Na verdade, é inviável testar toda a variedade de recursos, hardware, módulos e permutas de topologia. Além disso, a Cisco não pode testar a interoperabilidade com equipamentos de terceiros. A Cisco recomenda que as organizações testem a combinação precisa de hardware, módulos, recursos e topologia encontrada em seu ambiente. Esse teste deve ser realizado em laboratório, com uma topologia recolhida representando o ambiente de produção da sua empresa com outros tipos de teste de suporte, como desempenho, interoperabilidade, interrupção e burn-in.

Teste	Visão geral do teste	Responsabilidade do Teste
Recurso e funcionalidade	Determina se os recursos básicos do Cisco IOS e os módulos de hardware Cisco	Teste de dispositivos da Cisco

	funcionam como anunciados. A funcionalidade do recurso ou módulo, bem como as opções de configuração do recurso, devem ser testadas. A remoção e a adição da configuração devem ser testadas. O teste básico de interrupção e o teste de burn-in estão incluídos.	
Regressão	Determina se o recurso ou módulo funciona em conjunto com outros módulos e recursos e se a versão do Cisco IOS funciona em conjunto com outras versões do Cisco IOS em relação aos recursos definidos. Inclui alguns testes de burn-in e de paralisação.	Teste de regressão da Cisco
Desempenho básico do dispositivo	Determina o desempenho básico do recurso ou módulo para determinar se o recurso ou os módulos de hardware do	Teste de dispositivos da Cisco

	Cisco IOS atendem aos requisitos mínimos em carga.	
Topologia/Recurso/Combinação de hardware	Determina se os recursos e módulos funcionam conforme esperado em uma topologia específica e em uma combinação módulo/recurso/hardware. Este teste deve incluir a verificação de protocolos, verificação dos recursos, verificação do comando show, o teste de operação antecipada e o teste de interrupção.	A Cisco testa as topologias padrão anunciadas em laboratórios como o Enterprise Solutions Engineering (ESE) e o Networked Solutions Integration Test Engineering (NSITE). Os clientes de alta disponibilidade devem testar as combinações de recursos/módulos/topologia conforme necessário, especialmente com softwares pioneiros e topologias fora do padrão.
Interrupção (Ese)	Inclui tipos de interrupção ou comportamentos comuns que podem ocorrer em um ambiente específico de recurso/módulo/topologia e impacto potencial na funcionalidade. O teste de interrupção inclui troca de placas, perda de sincronia do enlace, falhas de dispositivos, falhas de	A Cisco é responsável por testes básicos de paralisação. Em última análise, os clientes são responsáveis por problemas de desempenho de paralisação relacionados à escalabilidade de seu ambiente individual. Os testes de interrupção devem ser feitos, se possível, no ambiente de laboratório do cliente.

	enlaces e falhas de placas.	
Desempenho da rede (e se)	Investiga a carga do dispositivo em relação a uma combinação específica de recursos/hardware/topologia. O foco está na capacidade e no desempenho do dispositivo, como CPU, memória, utilização de buffer e utilização do link em relação a um tipo de tráfego definido e a requisitos de recursos de protocolos, vizinhos, número de rotas e outros recursos. O teste ajuda a garantir a escalabilidade em ambientes maiores.	Em última análise, os clientes são responsáveis pela carga e escalabilidade do dispositivo. As preocupações com carga e escalabilidade são frequentemente levantadas pelas vendas da Cisco ou pelos Serviços Avançados e são frequentemente testadas com laboratórios da Cisco, como o Customer Proof-of-Concept Labs (CPOC).
Correção de Erros	Garante que os bugs corrigam o defeito identificado.	A Cisco testa correções de bugs para garantir que o bug seja corrigido. Os clientes também devem testar para garantir que o bug que eles experimentaram seja corrigido e que o bug não quebre nenhum outro aspecto do módulo ou recurso. Versões de manutenção são testadas por

		regressão, mas as versões provisórias geralmente não são.
Gerenciamento de Rede	Investiga os recursos de gerenciamento do Protocolo de Gerenciamento de Rede Simples (SNMP - Simple Network Management Protocol), precisão variável SNMP MIB, suporte a interceptação e suporte a Syslog.	A Cisco é responsável por testar os recursos básicos SNMP, a funcionalidade e a precisão das variáveis MIB. Os clientes devem validar os resultados do gerenciamento de rede e, em última análise, são responsáveis pela estratégia e metodologia de gerenciamento para implantações de novas tecnologias.
Emulação de rede em larga escala	A emulação de rede em larga escala usa ferramentas como o simulador de roteador da Agilent e o conjunto de ferramentas de teste da Spirent para simular ambientes maiores. Por exemplo, vizinhos de protocolo, contagens de circuito PVC de Frame Relay, tamanhos de tabelas de roteamento, entradas de cache e outros recursos normalmente	Os clientes da Cisco geralmente são responsáveis pelos aspectos dos testes de simulação de rede que reproduzem seu ambiente de rede, que podem incluir o número de vizinhos/adjacências de protocolo de roteamento e tamanhos de tabela de roteamento associados e outros recursos que estão em produção.

	necessários na produção que não estão no laboratório por padrão.	
Interoperabilidade	Testa todos os aspectos relacionados à conectividade com equipamentos de rede de terceiros, especialmente se a interoperabilidade de protocolo ou sinalização for necessária.	Os clientes da Cisco geralmente são responsáveis por todos os aspectos dos testes de interoperabilidade.
Burn-in	Investiga os recursos do roteador ao longo do tempo. Os testes de burn-in normalmente exigem que um dispositivo esteja sob alguma carga com investigação da utilização de recursos, incluindo memória, CPU e buffers ao longo do tempo.	A Cisco realiza testes básicos de burn-in. O teste do cliente é recomendado em relação à topologia, dispositivo e combinações de recursos exclusivos.

Metodologia de teste

Uma vez que a empresa saiba o que está testando, uma metodologia deve ser desenvolvida para o processo de teste. A finalidade de uma metodologia de teste de prática recomendada é ajudar a garantir que o estabelecido no teste seja abrangente, bem documentado, facilmente reproduzível e valioso, em termos de descoberta de problemas de produção em potencial. A documentação e os cenários de laboratório de recriação são especialmente importantes para testar versões posteriores ou para testar correções de bugs encontradas no ambiente do laboratório. As etapas de uma metodologia de teste são mostradas abaixo. Alguns passos de teste também podem ser executados concomitantemente.

1. Crie uma topologia de teste que simule o ambiente de produção em teste. Um ambiente de teste da borda da WAN pode incluir apenas alguns roteadores centrais e um roteador de borda, enquanto um teste de LAN pode incluir mais dispositivos que possam representar melhor o ambiente.
2. Configurar recursos que simulem o ambiente de produção. A configuração dos dispositivos de laboratório deve corresponder às configurações de hardware e software do dispositivo de produção esperado.
3. Escreva um plano de teste, definindo testes e metas, documentando a topologia e definindo testes funcionais. Os testes incluem validação básica de protocolo,validação do comando show, teste de interrupção e teste de burn-in. Um exemplo de um teste específico em um plano de teste é encontrado na tabela a seguir.
4. Valide o roteamento e a funcionalidade do protocolo. Resultados esperados do **comando show** do documento ou da linha de base. Os protocolos devem incluir os protocolos da Camada 2; por exemplo, ATM, Frame-Relay, CDP (Cisco Discovery Protocol), Ethernet e Spanning-Tree; bem como os protocolos da Camada 3, como IP, IPX e multicast.
5. Valide a funcionalidade do recurso. Resultados esperados do **comando show** do documento ou da linha de base. Os recursos podem incluir comandos de configuração global e quaisquer recursos críticos, como autenticação, autorização e contabilização (AAA).
6. Simule o carregamento, o qual deve estar previsto no ambiente de produção. A simulação de carga pode ser feita com coletores/geradores de tráfego. Validar as variáveis de utilização de dispositivo de rede esperadas, incluindo CPU, memória, utilização de buffer e estatísticas de interface com uma investigação de todas as perdas de pacote. Resultados esperados do **comando show** do documento ou da linha de base.
7. Execute um teste de interrupção no qual o dispositivo e o software devem lidar ou prevenir com carga. Por exemplo, remoção de placa, oscilação de link, oscilação de rota e tempestades de broadcast. Verifique se as interceptações SNMP corretas estão sendo geradas com base nos recursos que estão sendo utilizados na rede.
8. Documentar os resultados dos testes e as medidas dos dispositivos como testes devem ser repetíveis.

Nome do teste	**Failover do Hot Standby Router Protocol (HSRP)**
Testar requisitos de configuração	Aplique a carga à interface do gateway principal. O tráfego deve ser de aproximadamente 20% em direção ao gateway a partir da perspectiva da estação do usuário e de 60% de entrada em direção à perspectiva da estação do usuário. Além disso, aumente o tráfego para uma carga mais alta.
Etapas do teste	Monitore o STP e o HSRP por meio de comandos **show**. Falha na conexão da interface do gateway principal e recupera a conexão depois que as informações são coletadas.
Medições esperadas	CPU durante failover. Mostre a interface antes, durante e depois para o gateway principal e secundário. Mostrar HSRP antes, durante e depois.
Result	Gateway principal falhará no outro gateway de

ados esperados	roteador em dois segundos. **os** comandos **show** refletem corretamente a alteração. O failover para o gateway principal ocorre quando a conectividade é restaurada.
Resultados reais	
Pass ou Fail (Aprovação ou Falha)	
Modificações necessárias para obter aprovação	

Medidas do dispositivo

Durante a fase de ensaio, efetuar e documentar as seguintes medições para assegurar que o dispositivo está a funcionar corretamente:

- Utilização de memória
- Cargas da CPU
- Uso de buffer
- Estatísticas da interface
- Tabelas de rotas
- Depuração específica

As informações de medições variam de acordo com o teste em implementação. Também existem informações adicionais para medição, dependendo das questões específicas que estão sendo abordadas.

Para cada aplicativo que está sendo testado, meça os parâmetros para garantir que não haja impacto negativo no desempenho do aplicativo especificado. Isso é feito utilizando-se uma linha de base de desempenho que pode ser usada para comparar o desempenho antes e depois da implantação. Exemplos de testes de medição de aplicativos incluem:

- O tempo médio necessário para fazer logon em uma rede.
- O tempo médio necessário para que o NFS (Sistema de arquivos de rede) copie um grupo de arquivos.
- O tempo médio necessário para iniciar um aplicativo e ser avisado com a primeira tela.
- Outros parâmetros específicos dos aplicativos.

Implementação - Implantação do Cisco IOS rápida e bem-

sucedida

Um processo de implementação bem definido permite que uma organização implante com eficiência novas versões do Cisco IOS.

A fase de implementação inclui o processo-piloto e o processo de implementação. O processo piloto garante que a versão do Cisco IOS seja bem-sucedida no ambiente e o processo de implementação permite implantações rápidas e bem-sucedidas de maior escala do Cisco IOS.

Estratégia e ferramentas para distribuições de Cisco IOS

A estratégia de distribuição do Cisco IOS é executar a certificação final através de um processo piloto e distribuição rápida, usando ferramentas de atualização e um processo de implementação bem definido.

Antes de iniciar um processo piloto de rede, muitas organizações criam diretrizes piloto gerais. As diretrizes piloto devem incluir expectativas para todos os pilotos, como critério de sucesso, locais aceitáveis do piloto, documentação do piloto, expectativas do proprietário do piloto, solicitações de notificação do usuário e duração esperada do piloto. Uma equipe multifuncional de engenharia, implementação e operações normalmente está envolvida na criação de diretrizes piloto gerais e de um processo piloto. Assim que o processo piloto foi criado, grupos de implementação individuais normalmente podem conduzir pilotos bem sucedidos, utilizando os métodos identificados de melhores práticas.

Após a aprovação de uma nova versão de software para distribuição e certificação final, é necessário que a organização comece a planejar a atualização do Cisco IOS. O planejamento começa com a identificação de novos requisitos de imagem como plataforma, memória, flash e configuração. Os grupos de arquitetura e engenharia normalmente definem novos requisitos de imagem de software na fase de gerenciamento de candidatos do ciclo de vida de gerenciamento do Cisco IOS. Depois de identificados os requisitos, cada dispositivo deverá ser validado e possivelmente atualizado pelo grupo de implementação. O módulo SWIM (Software Image Manager) do CiscoWorks2000 também pode executar a etapa de validação, através da validação dos requisitos do Cisco IOS em relação ao inventário do dispositivo. Quando todos os dispositivos forem validados e/ou atualizados para os padrões corretos da imagem nova, o grupo de implementação poderá iniciar um processo de implementação de início lento, usando o módulo CiscoWorks2000 SWIM como uma ferramenta de implementação de software.

Apenas a distribuição bem-sucedida da nova imagem várias vezes, a organização poderá iniciar uma rápida distribuição usando o CiscoWorks SWIM.

Gerenciamento de inventário do Cisco IOS

O Gerenciador CiscoWorks2000 Resource Manager Essentials (RME) Inventory simplifica bastante o gerenciamento de versão de roteadores e Switches Cisco por meio de ferramentas de relatório baseadas na Web que reportam e classificam dispositivos Cisco IOS, com base na versão do Software, plataforma e nome do dispositivo.

SWIM do Cisco IOS

O CiscoWorks2000 SWIM pode ajudar a reduzir as complexidades propensas a erros do processo de atualização. Os links incorporados ao CCO correlacionam as informações on-line da Cisco sobre patches de software com o software Cisco IOS e Catalyst implantado na rede,

destacando notas técnicas relacionadas. Novas ferramentas de planejamento encontram requisitos do sistema e enviam notificações quando atualizações de hardware (Boot ROM, Flash RAM) são necessárias para suportar as atualizações de imagem de software propostas.

Antes de iniciar uma atualização, os pré-requisitos de uma nova imagem são validados em relação aos dados de inventário do switch ou roteador de destino para ajudar a garantir uma atualização bem-sucedida. Quando vários dispositivos estão sendo atualizados, o SWIM sincroniza tarefas de download e permite que o usuário monitore o progresso do trabalho. Os trabalhos programados são controlados através de um processo de liberação, permitindo que os gerentes autorizem as atividades de um técnico antes de iniciar cada tarefa de atualização. O RME 3.3 inclui a capacidade de analisar atualizações de software para plataformas Cisco IGX, BPX e MGX, simplificando e reduzindo enormemente o tempo necessário para determinar o impacto de uma atualização de software.

Processo piloto

Para minimizar a exposição potencial e capturar com mais segurança quaisquer problemas de produção restantes, recomenda-se um piloto de software. Pilotos são geralmente mais importantes para distribuições de nova tecnologia; entretanto, diversas distribuições de novos softwares serão vinculadas a novos serviços, recursos ou hardwares, onde um piloto é mais crítico. O plano piloto individual deverá considerar a medida, a duração e a seleção de piloto. A seleção de piloto é o processo de identificar quando e onde um piloto deve ser feito. Medição piloto é o processo de coletar os dados necessários para identificar êxito e falha ou problemas em potencial.

A seleção do piloto identifica onde e como um piloto será concluído. Um piloto pode começar com um dispositivo em uma área de baixo impacto e estender-se a vários dispositivos em uma área de maior impacto. Algumas considerações para seleção piloto em que o impacto pode ser reduzido incluem o seguinte:

- Instalado em uma área da rede resiliente a um único dispositivo devido à redundância.
- Em uma área da rede com um número mínimo de usuários atrás do dispositivo selecionado que podem lidar com algum possível impacto na produção.
- Considere separar o piloto em linhas de arquitetura. Por exemplo, teste-o nas camadas de acesso, distribuição e/ou núcleo da rede.

A duração desse piloto deverá se basear no tempo que ele leva para testar e avaliar de forma satisfatória todos os recursos do dispositivo. Isso deve incluir o burn-in e a rede sob cargas de tráfego normais. A duração também depende do passo de atualização do código e da área da rede em que o software Cisco IOS está em execução. Se o Cisco IOS é uma nova versão principal, é preferível um período piloto mais longo. Considerando que a atualização é uma versão de manutenção com o mínimo de recursos novos, um período piloto mais curto será suficiente.

Durante a fase piloto, é importante monitorar e documentar os resultados de forma semelhante ao teste inicial. Isso pode incluir análises de usuário, coleta de dados piloto, coleta de problemas e critérios de êxito/falha. Os indivíduos devem ser diretamente responsáveis pelo acompanhamento e acompanhamento dos progressos dos pilotos, a fim de assegurar que todos os problemas sejam identificados e que os utilizadores e serviços envolvidos no piloto estejam satisfeitos com os resultados dos pilotos. A maioria das organizações certificará uma versão se ela for bem-sucedida em um ambiente piloto ou de produção. Esta etapa é uma falha crítica em alguns ambientes devido ao sucesso observado quando não é identificado nem documentado qualquer critério de sucesso ou medição.

Implementação

Após a conclusão da fase piloto na rede de produção, inicie a fase de implementação do Cisco IOS. A fase de implementação inclui vários passos para assegurar o sucesso da atualização do software e a eficiência de implementação, incluindo o início lento de implementação, certificação final, preparação de atualização, automação de atualização e validação final.

O início lento da implementação é o processo de implementação lenta de uma versão testada recentemente para garantir que a imagem tenha exposição total ao ambiente de produção antes da certificação final e conversão em escala completa. Algumas organizações podem ser iniciadas com um dispositivo e um dia de exposição antes de atualizarem para dois dispositivos no dia seguinte e, talvez, um número maior de dispositivos no terceiro dia. Quando aproximadamente dez dispositivos foram colocados em produção, a organização pode esperar de uma a duas semanas antes da certificação final da versão específica do Cisco IOS. Na certificação final, a organização pode distribuir mais rapidamente a versão identificada com um nível de confiança muito mais elevado.

Após o processo de início lento, todos os dispositivos identificados para atualização devem ser revisados e validados usando o inventário de dispositivos e uma matriz dos padrões mínimos do Cisco IOS para bootstrap, DRAM e flash para garantir que os requisitos sejam atendidos. Os dados podem ser adquiridos por meio de ferramentas próprias, ferramentas SNMP de terceiros ou por meio do uso do CiscoWorks2000 RME. O CiscoWorks2000 SWIM não analisa nem inspeciona essas variáveis antes da implementação. No entanto, é sempre uma boa ideia saber o que esperar durante as tentativas de implementação.

Se mais de uma centena de dispositivos semelhantes estiverem programados para atualizações, é altamente recomendável utilizar um método automatizado. A automação mostrou que melhora a eficiência da atualização e melhora a porcentagem de sucessos na atualização de dispositivos durante grandes implantações, com base em uma atualização interna de 1.000 dispositivos com e sem o SWIM. A Cisco recomenda que o CiscoWorks 2000 SWIM seja usado para implantações grandes devido ao grau de verificação que é realizado durante a atualização. O SWIM ainda sai de uma versão do Cisco IOS se um problema for detectado. O SWIM funciona criando e agendando trabalhos de atualização, onde um trabalho é configurado com os dispositivos, imagens de atualização desejadas e tempo de execução do trabalho. Cada trabalho deve conter doze ou menos atualizações de dispositivo e até doze trabalhos podem ser executados simultaneamente. O SWIM também verifica se a versão da atualização de Cisco IOS programada está sendo executada com sucesso após a atualização. É recomendável permitir aproximadamente vinte minutos para cada atualização de dispositivo (incluindo verificação). Usando essa fórmula, uma empresa pode atualizar trinta e seis dispositivos por hora. A Cisco também recomenda que no máximo cem dispositivos sejam atualizados por noite para reduzir a exposição a problemas em potencial.

Após uma atualização automática, deve ser feita alguma validação para garantir o sucesso. A ferramenta CiscoWorks2000 SWIM pode executar scripts personalizados após a atualização, para executar mais verificações de sucesso. A verificação inclui validar o roteador quanto à quantidade apropriada de rotas, de modo a garantir que as interfaces lógicas/físicas estejam ativas ou seja, que o dispositivo esteja acessível. O exemplo de checklist a seguir pode validar completamente o sucesso de uma implantação do Cisco IOS:

- O dispositivo foi recarregado corretamente?
- O dispositivo pode ser conectado e acessado por meio das plataformas do sistema de gerenciamento de rede (NMS)?

- As interfaces esperadas no dispositivo estão ativas?
- O dispositivo tem as adjacências corretas do protocolo de roteamento?
- A tabela de roteamento está preenchida?
- O dispositivo está transmitindo o tráfego corretamente?

Operações - Gerenciamento da implementação de alta disponibilidade do Cisco IOS

As operações de práticas recomendadas de alta disponibilidade do ambiente Cisco IOS ajudam a reduzir a complexidade da rede, melhorar o tempo de resolução de problemas e melhorar a disponibilidade da rede. A seção de operações de gerenciamento do IOS Cisco inclui estratégia, ferramentas e metodologias de melhores práticas recomendadas para gerenciamento do IOS Cisco.

As práticas recomendadas para operações do Cisco IOS incluem controle de versão de software, gerenciamento de Syslog do Cisco IOS, gerenciamento de problemas, padronização de configuração e gerenciamento de disponibilidade. O controle de versão de software é o processo de rastreamento, validação e melhoria da consistência de software nos controles de software identificados. O gerenciamento de syslog do Cisco IOS é o processo de monitoramento pró-ativo e de atuação sobre mensagens de Syslog de prioridade mais alta geradas pelo Cisco IOS. O gerenciamento de problemas é a prática de coletar informações sobre problemas críticos relacionados a software de modo rápido e eficiente para auxiliar na prevenção de futuras ocorrências. A padronização da configuração é o processo de padronização das configurações para reduzir a possibilidade de que códigos não testados sejam exercidos na produção e para padronizar o comportamento do protocolo e dos recursos da rede. O gerenciamento de disponibilidade é o processo de melhorar a disponibilidade com base em métricas, metas de melhoria e projetos de melhoria.

Estratégias e ferramentas para operações de Cisco IOS

Existem muitas estratégias e ferramentas de qualidade para ajudar a gerenciar os ambientes Cisco IOS. A primeira estratégia fundamental para as operações do Cisco IOS é manter o ambiente o mais simples possível, evitando ao máximo variações na configuração e nas versões Cisco IOS. A certificação do Cisco IOS já foi discutida, mas a consistência da configuração é outra área importante. O grupo de arquitetura e engenharia deve ser responsável pela criação dos padrões de configuração. O grupo de implementação e operações tem a responsabilidade de configurar e manter os padrões por meio do controle de versões e do controle/padrões de configuração do Cisco IOS.

A segunda estratégia para operações do Cisco IOS é a capacidade de identificar e resolver rapidamente falhas de rede. Os problemas de rede geralmente devem ser identificados pelo grupo de operações antes de os usuários ligarem para eles. Problemas também serão resolvidos da forma mais rápida possível sem causar maiores impactos ou alterações no ambiente. Algumas das principais práticas recomendadas nessa área são o gerenciamento de problemas e o gerenciamento de Syslog do Cisco IOS. Uma ferramenta para ajudar a diagnosticar rapidamente falhas do software Cisco IOS é o Cisco Output Interpreter.

A terceira estratégia é uma melhoria consistente. O processo principal é melhorar um programa de melhoria da disponibilidade baseado em qualidade. Executando uma análise da causa básica de todos os problemas, incluindo os relacionados ao Cisco IOS, uma organização pode melhorar

a cobertura do teste, melhorar os tempos de resolução de problemas e melhorar os processos que eliminam ou reduzem o impacto da paralisação. A organização também pode verificar problemas comuns e construir processos para resolvê-los com mais rapidez.

As ferramentas para as operações do Cisco IOS incluem o gerenciamento de inventário para controlar a versão do software (CiscoWorks2000 RME), o gerenciamento de Syslog para gerenciar as mensagens de Syslog e os gerenciadores de configuração de dispositivos para gerenciar a consistência da configuração de dispositivos.

Gerenciamento de syslog

Mensagens do SYSLOG são aquelas enviadas pelo dispositivo para um servidor de coleções. Essas mensagens podem ser erros (por exemplo, um link inativo) ou mensagens informativas, como o momento em que alguém se conecta para configurar um terminal em um dispositivo.

As ferramentas de gerenciamento de syslog registram e rastreiam as mensagens de syslog recebidas por roteadores e switches. Algumas ferramentas são equipadas com filtros para permitir a remoção de mensagens indesejáveis que possam prejudicar as importantes. As ferramentas syslog também devem permitir que o relatório seja criado com base nas mensagens recebidas. O relatório pode ser exibido por período de tempo, dispositivo, tipo de mensagem ou prioridade de mensagem.

A ferramenta de Syslog mais popular para o gerenciamento do Cisco IOS é o gerenciador de Syslog do CiscoWorks2000 RME. Outras ferramentas estão disponíveis, incluindo o SL4NT, um programa shareware da Netal e Private I da OpenSystems.

Gerenciador de configuração de dispositivos CiscoWorks

O Gerenciador de Configuração de Dispositivos do CiscoWorks2000 mantém um arquivo ativo e fornece uma maneira fácil de atualizar as alterações de configuração em vários roteadores e switches da Cisco. O gerenciador de configuração monitora a rede em busca de alterações na configuração, atualiza o arquivo quando uma alteração é detectada e registra as informações de alteração no serviço de auditoria de alterações. Uma interface de usuário baseada na Web permite que você pesquise no arquivo para obter atributos de configuração específicos e compare o conteúdo de dois arquivos de configuração para uma identificação fácil das diferenças.

Intérprete de saída Cisco

O Cisco Output Interpreter é uma ferramenta usada no diagnóstico de travamentos forçados de software. A ferramenta pode ajudar a identificar os defeitos do software sem ligar para o Centro de assistência técnica (TAC) a Cisco ou pode ser usada como informações primárias para o TAC depois de um travamento forçado por software. Essas informações geralmente ajudarão a agilizar a resolução do problema, pelo menos em termos da coleta de informações necessária.

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. Em geral, o controle de versão do software é realizado usando um processo de certificação e controle de padrões. Muitas organizações publicam padrões de versão em um servidor Web central. Além disso, a equipe de implementação é treinada para revisar qual versão está sendo executada e para atualizar a

versão se ela não for compatível com padrões. Algumas organizações têm um processo de porta de qualidade em que a validação secundária é concluída por meio de auditorias para garantir que o padrão seja seguido durante a implementação.

Durante a operação, não é raro ver versões fora do padrão na rede, especialmente se a equipe de rede e de operações for grande. Isso pode ocorrer devido a uma equipe nova e sem treinamento, a comandos de inicialização configurados inadequadamente ou a implementações não verificadas. É sempre uma boa ideia validar periodicamente os padrões de versão de software usando ferramentas como o CiscoWorks 2000 RME que pode classificar todos os dispositivos pela versão do Cisco IOS. Quando versões sem padrão são identificadas, elas devem ser imediatamente sinalizadas e um bilhete de problema ou de alteração deve ser iniciado para trazer a versão para o padrão identificado.

Gerenciamento de syslog proativo

Coleção, monitoramento e análise de syslog são processos de gerenciamento de falhas recomendados para resolver outros problemas de rede específicos do Cisco IOS que são difíceis ou impossíveis de serem identificados por outros meios. A coleta, o monitoramento e a análise de syslog ajudam a melhorar o tempo de resolução de problemas identificando e resolvendo muitas falhas de forma proativa antes que problemas de rede mais graves sejam detectados ou relatados pelos usuários. O syslog também fornece um método mais eficiente de coleta de uma grande variedade de problemas quando comparado à interrogação SNMP consistente para um grande número de variáveis MIB. A coleta, o monitoramento e a análise de syslog são realizados utilizando a configuração correta do Cisco IOS, as ferramentas de correlação de Syslog, como o CiscoWorks2000 RME e/ou o gerenciamento de eventos de Syslog. O gerenciamento de eventos de syslog é feito analisando os dados coletados do Syslog para mensagens críticas identificadas e encaminhando um alerta ou uma armadilha para um gerente de eventos para notificação e resolução em tempo real.

O monitoramento do Syslog requer o suporte da ferramenta NMS ou de scripts para analisar e relatar os dados do Syslog. Isso inclui a capacidade de classificar mensagens Syslog por data ou período, dispositivo, tipo de mensagem Syslog ou freqüência da mensagem. Em redes maiores, ferramentas ou scripts podem ser implementados para analisar dados de Syslog e enviar alertas ou notificações para sistemas de gerenciamento de eventos ou para o pessoal de operações e engenharia. Se os alertas para uma grande variedade de dados de Syslog não forem usados, a organização deve revisar dados de Syslog de prioridade mais alta pelo menos diariamente e criar tíquetes de problemas para possíveis problemas. Para detectar proativamente problemas de rede que podem não ser vistos através de monitoramento normal, deve-se realizar uma revisão periódica e uma análise dos dados históricos do Syslog para detectar situações que podem não indicar um problema imediato, mas podem fornecer uma indicação de um problema antes que ele se torne um serviço impactante.

Gerenciamento de problemas

Muitos clientes sofrem tempo de inatividade adicional devido à falta de processos no gerenciamento de problemas. Pode ocorrer um tempo de inatividade adicional quando os administradores de rede tentam resolver o problema rapidamente usando uma combinação de comandos com impacto no serviço ou alterações de configuração, em vez de gastar tempo na identificação de problemas, na coleta de informações e em um caminho de solução bem analisado. O comportamento observado nessa área inclui recarregar dispositivos ou limpar tabelas de roteamento IP antes de investigar um problema e sua causa raiz. Em alguns casos, isso ocorre devido às metas de primeiro nível de solução de problemas de suporte. 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 problemas é recomendado em ambientes maiores. Esse processo deve incluir um certo grau de descrições de problemas padrão e coletas adequadas do comando show, antes da escalada para uma segundo camada. O suporte de primeiro nível nunca deve estar limpando rotas ou recarregando dispositivos. De forma ideal, a organização de primeiro nível deve coletar rapidamente as informações e ir para uma segunda camada. Ao gastar apenas mais alguns minutos inicialmente na identificação de problemas ou na descrição de problemas, é muito mais provável uma descoberta de causa básica, permitindo, assim, uma solução alternativa, identificação de laboratório e relatório de erros. O suporte de segundo nível deve ser bem informado sobre os tipos de informações que a Cisco pode precisar para diagnosticar um problema ou arquivar um relatório de erro. Isso inclui os dumps de memória, a saída das informações de roteamento e a saída do comando de exibição do dispositivo.

Padronização de configuração

Os padrões globais de configuração de dispositivos representam a prática de manter parâmetros de configuração global padrão em dispositivos e serviços semelhantes, resultando em consistência de configuração global em toda a empresa. Os comandos de configuração global são comandos que se aplicam a todo o dispositivo e não a portas, protocolos ou interfaces individuais. Os comandos de configuração global geralmente afetam o acesso ao dispositivo, o comportamento geral do dispositivo e a segurança do dispositivo. No Cisco IOS, isso inclui comandos de serviço, comandos IP, comandos vty, comandos de porta de console, comandos de registro, comandos AAA/TACACS+, comandos SNMP e comandos de banner. Também importante nos padrões globais de configuração de dispositivos é uma convenção de nomes de dispositivos apropriada que permite aos administradores identificar o dispositivo, o tipo de dispositivo e a localização do dispositivo com base no nome do Sistema de Nomes de Domínio (DNS) do dispositivo. A consistência da configuração global é importante para a capacidade de suporte e confiabilidade gerais de um ambiente de rede, pois ajuda a reduzir a complexidade da rede e a 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.

A manutenção dos padrões globais de configuração de dispositivos é normalmente realizada por um grupo interno de engenharia ou operações que cria e mantém parâmetros de configuração global para dispositivos de rede semelhantes. Também é uma boa prática fornecer uma cópia do arquivo de configuração global em diretórios TFTP para que eles possam ser baixados inicialmente para todos os dispositivos recém-provisionados. Também é útil um arquivo acessível pela Web que fornece ao arquivo de configuração padrão uma explicação de cada parâmetro de configuração. Algumas organizações configuram dispositivos semelhantes em uma base periódica, até mesmo globalmente, para ajudar a assegurar a consistência de configuração global ou revisam dispositivos periodicamente para obter padrões de configuração global corretos. Os padrões de configuração de protocolo e de interface representam a prática de manutenção de padrões para configuração de interface e de protocolo.

A consistência de configuração de protocolo e interface melhora a disponibilidade da rede, ao reduzir a complexidade da rede, fornecer comportamento esperado de dispositivo e protocolo e melhorar a capacidade de suporte da rede. A inconsistência na configuração de interface ou protocolo pode resultar em comportamento inesperado do dispositivo, questões de roteamento de tráfego, problemas de aumento na conectividade e maior tempo de suporte reativo. Os padrões de configuração de interface devem incluir descritores de interface CDP, configuração de cache e

outros padrões específicos de protocolo. Os padrões de configuração específicos de protocolo podem incluir:

- configuração de roteamento IP
- configuração DLSW
- Configuração da lista de acesso
- configuração ATM
- configuração do Frame Relay
- Configuração de árvore de abrangência
- Atribuição e configuração de VLAN
- Virtual Trunking Protocol (VTP)
- HSRP

Observação: é possível ter outros padrões de configuração específicos de protocolo dependendo do que está configurado na rede.

Um exemplo de padrões IP pode incluir:

- Tamanho da sub-rede
- Espaço de endereço IP usado
- Routing Protocol utilizado
- Configuração do Routing Protocol

A manutenção dos padrões de configuração de protocolo e interface é normalmente da responsabilidade dos grupos de engenharia e implementação de rede. O grupo de engenharia deve ser responsável por identificar, testar, validar e documentar o padrões. O grupo de implementação é responsável por usar os documentos de engenharia ou modelos de configuração para provisionar novos serviços. O grupo de engenharia deve criar documentação sobre todos os aspectos dos padrões exigidos para garantir consistência. Os modelos de configuração também devem ser criados para ajudar a aplicar 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 de grande ajuda na fase de teste, validação e certificação. Na verdade, sem modelos de configuração padronizados, é quase impossível testar, validar ou certificar adequadamente uma versão do IOS da Cisco para uma rede moderadamente grande.

Gerenciamento de disponibilidade

O gerenciamento de disponibilidade é o processo de melhoria de qualidade usando a disponibilidade da rede como métrica de melhoria de qualidade. Muitas organizações estão medindo a disponibilidade e o tipo de interrupção. O tipo de interrupção pode incluir hardware, software, enlace/portadora, energia/ambiente, projeto ou erro de usuário/processo. Ao identificar interrupções e executar a análise de causa básica imediatamente após a recuperação, a empresa pode identificar métodos para melhorar a disponibilidade. Quase todas as redes que alcançaram alta disponibilidade têm algum processo de melhoria de qualidade.

Apêndice A - Visão geral das versões do Cisco IOS

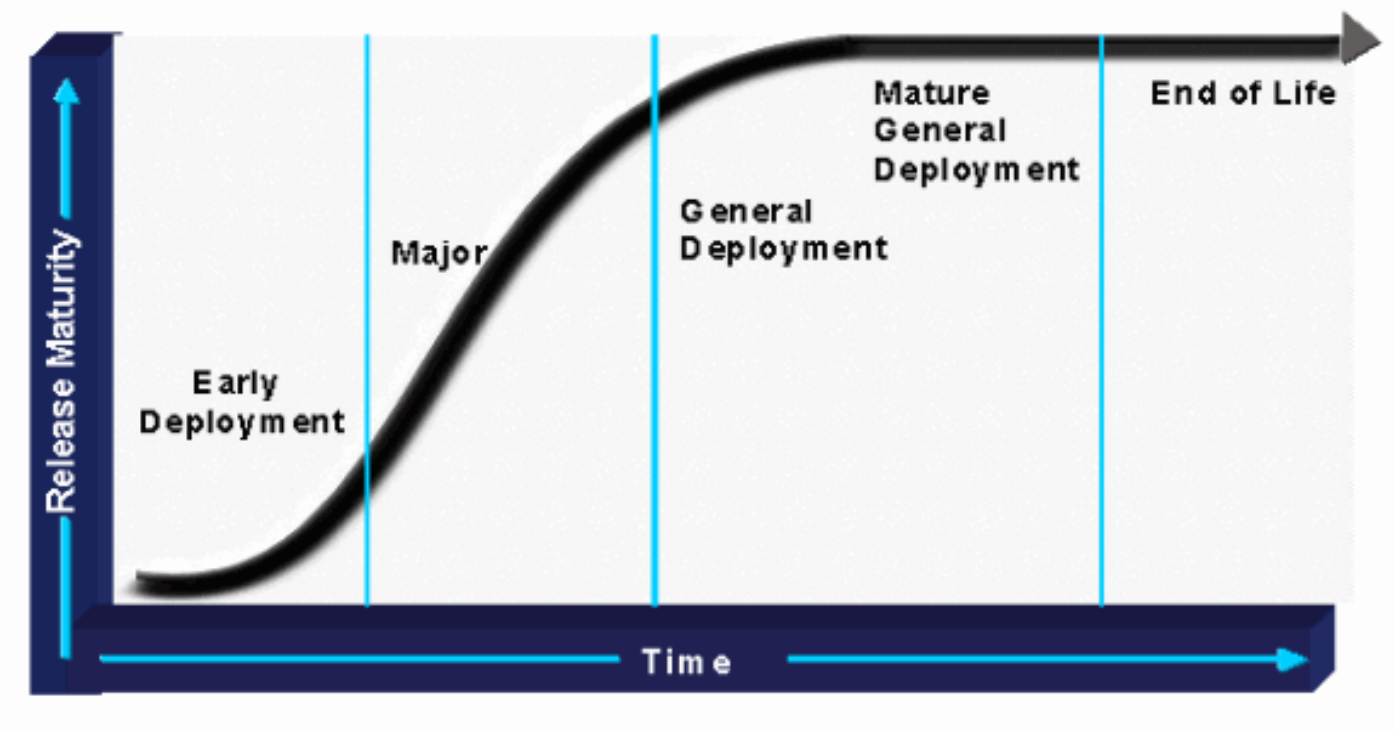
A estratégia dos Cisco IOS Software Releases é criada em torno do desenvolvimento de software eficiente, garantia de qualidade e rapidez no tempo de comercialização, os quais são fundamentais para o sucesso das redes dos clientes da Cisco.

O processo é definido em quatro categorias de versões, as quais estão explicadas abaixo.

- Versão de implantação inicial (ED)
- Versão principal
- LD (Limited Deployment Release, versão de implantação limitada)
- GD (General Deployment Release, versão de implantação geral)

A Cisco cria e mantém um roteiro do IOS que tem informações sobre versões individuais, mercados-alvo, caminhos de migração, descrições de novos recursos e assim por diante.

A figura abaixo ilustra o ciclo de vida da versão do Cisco IOS Software:



Versões ED

As versões ED do Cisco IOS são veículos que trazem novo desenvolvimento ao mercado. Cada revisão de manutenção de uma versão ED inclui não apenas correções de bugs, mas também um conjunto de novos recursos, suporte a novas plataformas e melhorias gerais em protocolos e na infraestrutura do Cisco IOS. De um a dois anos, os recursos e as plataformas das versões ED são portados para a próxima versão principal do Cisco IOS.

Há quatro tipos de verões ED, cada uma com um modelo de versão e marcos de ciclo de vida ligeiramente diferentes. As versões ED podem ser classificadas como:

- **Versões CTED (Consolidated Technology Early Deployment)** —O novo modelo de versão do Cisco IOS usa a versão consolidada ED train, também conhecida como "T" train, para introduzir novos recursos, novas plataformas de hardware e outros aprimoramentos no Cisco IOS. Elas são chamadas de tecnologia consolidada porque transcendem as definições de Unidades de Negócios (BU) internas e de Linha de Negócios (LOB). Exemplos de versões de tecnologia consolidadas são o Cisco IOS 11.3T, 12.0T e 12.1T.
- **Versões STED (Specific Technology Early Deployment, distribuição avançada de tecnologia específica)** —as versões STED têm características de compromisso de recursos semelhantes às versões CTED, exceto que têm como alvo uma tecnologia específica ou uma área de

mercado. Elas sempre são lançadas em plataformas específicas e estão sob a supervisão exclusiva de uma BU da Cisco. Versões STED são identificadas utilizando duas letras anexadas ao lançamento de versão principal. Exemplos de versões STED são Cisco IOS 11.3NA, 11.3MA, 11.3WA e 12.0DA.

- **Versões específicas de implantação antecipada do mercado (SMED**) — Os Cisco IOS SMEDs são diferenciados dos STEDs pelo fato de que eles têm como alvo um segmento de mercado vertical específico (ISPs, empresas, instituições financeiras, empresas Telcom, etc.). Os SMEDs incluem requisitos específicos de recursos de tecnologia apenas para plataformas específicas de relevância utilizadas pelo mercado vertical desejado. Eles podem ser diferenciados dos TEDS pelo fato de serem construídos apenas para plataformas específicas de relevância para o mercado vertical, enquanto os TEDS seriam construídos para mais plataformas baseadas em um requisito de tecnologia mais amplo. As versões SMED do Cisco IOS são identificadas por um caractere alfabético anexado à versão principal (assim como o CTED). Exemplos de SMEDs são o Cisco IOS 12.0S e 12.1E.
- **Versões de implantação antecipada de vida curta, também conhecidas como X Releases (XED)** — as versões XED do Cisco IOS apresentam novo hardware e tecnologias para o mercado. Elas não fornecem revisões de manutenção de software nem revisões temporárias de software regular. Se um defeito for encontrado no XED antes de sua convergência com o CTED, uma recriação de software será iniciada e um número será anexado ao nome. Por exemplo, as versões 12.0(2)XB1 e 12.0(2)XB2 do Cisco IOS são exemplos de recriações de 12.0(2)XB.

Versões principais

As principais versões são os principais veículos de implantação de produtos do software Cisco IOS. Eles são gerenciados pela divisão de tecnologia do Cisco IOS e consolidam a proliferação de recursos, plataformas, funcionalidades, tecnologias e hosts das versões anteriores de ED. As principais versões do Cisco IOS buscam maior estabilidade e qualidade. Por esse motivo, as versões principais não aceitam a adição de recursos ou plataformas. Cada revisão de manutenção fornece apenas correções de bugs. Por exemplo, as versões 12.1 e 12.2 do software Cisco IOS são versões principais.

As versões principais têm atualizações de manutenção programadas, chamadas versões de manutenção totalmente testadas para regressão, incorporam as correções de bugs mais recentes e não oferecem suporte a novas plataformas ou recursos. O número de uma versão importante identifica a própria versão e seu nível de manutenção. No Cisco IOS Software Release 12.0(7), 12.0 é o número da versão principal e 7 é seu nível de manutenção. O número da versão completa é 12.0(7). Da mesma forma, 12.1 é uma versão principal e 12.1(3) é a terceira versão de manutenção da versão principal do Cisco IOS Software Release 12.1.

Versões de implantação limitada (LD)

O LD é a fase de maturidade do Cisco IOS entre o FCS e a implantação geral para as principais versões. As versões ED do Cisco IOS vivem apenas na fase de implantação limitada porque nunca obtêm a certificação GD.

Versões de Implementação Geral (GD - General Deployment)

Em algum momento durante o ciclo de vida da versão, a Cisco declarará uma versão principal pronta para a certificação GD. Apenas uma versão principal pode atingir o status GD. Isto atinge o marco de certificação de GD quando a Cisco está satisfeita com a versão que foi:

- Testado em extensas exposições de mercado em diversas redes.
- Qualificado pela métrica analisada de tendências de estabilidade e de bug.
- Qualificado por meio de pesquisas de satisfação dos clientes.
- Uma redução na tendência normalizada do cliente encontrou defeitos na versão em relação às quatro versões de manutenção anteriores.

Uma equipe multifuncional de certificação GD de defesa do cliente composta por engenheiros TAC, engenheiros de Serviços Avançados de Engenharia (AES), Engenharia de Teste do Sistema e Engenharia do Cisco IOS é formada para avaliar cada defeito notável da versão. Essa equipe fornece a aprovação final para a certificação GD. Quando uma versão alcançar o status GD, cada revisão subseqüente da versão também será GD. Consequentemente, uma vez declarada a libertação GD; entra automaticamente na fase de manutenção restrita. Enquanto estiver nessa fase, a modificação de engenharia do código, incluindo correções de bugs com retrabalho do código principal, é estritamente limitada e controlada por um gerente de programa. Isto assegura que nenhum bug adverso seja introduzido em uma versão de software Cisco IOS certificada por GD. GD é alcançado por uma versão de manutenção específica. Atualizações de manutenção subsequentes para essa versão também são versões GD. Por exemplo, o Cisco IOS Software Release 12.0 recebeu a certificação GD em 12.0(8). Assim, as versões 12.0(9), 12.0(10) e outras do software Cisco IOS são versões GD.

Imagens experimentais ou de diagnóstico

As imagens experimentais ou de diagnóstico às vezes são chamadas de especiais de engenharia e são criadas somente quando problemas críticos de software são identificados. Essas imagens não fazem parte do processo normal de liberação. As imagens nesta categoria são compilações específicas do cliente projetadas para ajudar a diagnosticar um problema, testar uma correção de bug ou fornecer uma correção imediata. Uma correção imediata pode ser fornecida quando não for uma opção de esperar pela próxima versão temporária ou de manutenção. As imagens experimentais ou de diagnóstico podem ser criadas em qualquer base de software suportada, incluindo a manutenção ou versões provisórias de qualquer tipo de versão. Não existem convenções de nomenclatura oficiais, mas em muitos casos o desenvolvedor adicionará iniciais, exp (para experimental) ou dígitos adicionais ao nome da imagem base. Essas imagens são suportadas apenas temporariamente, junto com o desenvolvimento Cisco, pois as operações das versões Cisco TAC e Cisco IOS não mantêm a documentação de suporte como tabelas de símbolo ou histórico de imagem base. Essas imagens não passam por testes internos da Cisco.

Marcos de ciclos de vida das versões

Em algum momento, as versões GD são substituídas por versões mais novas com as mais recentes tecnologias de rede. Portanto, um processo de retirada de versão foi estabelecido com os seguintes três marcos principais:

- **Fim das vendas (EOS)** — Para as principais versões, a data do EOS é três anos após a data da primeira remessa comercial (FCS). Isso define uma data final para a qual a versão pode ser adquirida para novos sistemas. A versão do EOS continua a estar disponível para download a partir do Cisco Connection Online (CCO) para atualizações de manutenção.
- **Fim da Engenharia (EOE)**—A versão EOE é a última versão de manutenção para a versão GD e geralmente segue cerca de três meses após a versão EOS. Os clientes podem continuar a receber suporte técnico do Cisco TAC, bem como baixar a versão EOE do CCO. O boletim de produtos com o anúncio de versões e datas do EOS e EOE é publicado um ano antes da data planejada do EOS. Neste momento, os clientes devem começar a investigar a atualização do software Cisco IOS para aproveitar as tecnologias de rede mais recentes.

- **Fim da vida útil (EOL)** — No fim do ciclo de vida da versão, todo o suporte para a versão do software Cisco IOS é encerrado e não está mais disponível para download na data de EOL. Em geral, a data de EOL é cinco anos após a data de EOE. Um boletim de produto EOL é publicado aproximadamente um ano antes da data real de EOL.

Convenção de nomenclatura da versão do Cisco IOS

A convenção de nomeação da imagem do Cisco IOS oferece um perfil completo de todas as imagens liberadas. O nome sempre inclui o identificador da versão principal e o identificador da versão de manutenção. O nome também pode inclui um designador de treinamento, um designador de recriação (para a versão de manutenção), designadores de recursos específicos de unidade de negócios (BU) e identificadores de recriação do designador de recurso. O formato pode ser dividido da seguinte forma:

Seção Convenção de Nomenclatura	Explicação
x.y	Uma combinação de dois identificadores separados (um ou dois) de dígitos separados por um '.' que identifica o valor da versão principal. Esse valor é determinado pelo marketing do Cisco IOS. Exemplo: 12.1
z	Um a três dígitos que identificam a versão de manutenção de x.y. Isso ocorre a cada oito semanas. Os valores são 0 em beta, 1 em FCS e 2 para a primeira versão de manutenção. Exemplo: 12.1(2)
p	Um caractere alfa que identifica uma recriação de x.y(z). O valor inicia com um "a" minúsculo para a primeira recompilação e, em seguida, "b" e assim por diante. Exemplo: 12.1(2a)

R	Uma a três letras alfa são o designador da versão do treinamento e são obrigatórias para versões CTED, STED e X. Também identifica uma família de produtos ou plataformas. Versões da tecnologia ED utilizam duas letras. A primeira letra representa a tecnologia e a segunda letra é usada para diferenciação. Por exemplo:
	`A = Access Server/Dial technology (example:11.3AA)`
	`B = Broadband (example:12.2B)`
	`D = xDSL technology (example:12.2DA)`
	`E = Enterprise feature set (example:12.1E)`
	`H = SDH/SONET technology (example:11.3HA)`
	`N = Voice, Multimedia, Conference (example:11.3NA)`

	M = Mobile (example:12.2MB) S = Service Provider (example:12.0S) T = Consolidated Technology (example:12.0T) W = ATM/LAN Switching/Layer 3 (example:12.0W5) Um "X" na primeira posição do nome da versão identifica uma versão única com base na trilha "T" do CTED. Por exemplo, XA, XB, XC e assim por diante. Um "X" ou "Y" na segunda posição do nome da versão identifica uma versão ED de vida curta com base em, ou afiliada a, uma versão STED. Por exemplo, 11.3NX (baseado em 11.3NA), 11.3WX (baseado em 11.3WA) e assim por diante.
o	Designador numérico opcional de um ou dois dígitos que identifica a reconstrução de um certo valor de versão. Deixe em branco se não representar uma reconstrução. Começa com 1, depois 2 e assim por diante. Exemplo: 12.1(2)T1, 12.1(2)XE2
u	Designador numérico de um ou dois dígitos que identifica a funcionalidade da versão específica de BU. O valor é definido pela equipe de marketing da BU. Exemplo: 11.3(6)WA4, 12.0(1)W5
v	Designador numérico de um a dois dígitos que identifica a versão de manutenção do código específico de BU. Os valores são 0 em beta, 1 no FCS e 2 como a primeira versão de manutenção. Exemplo: 11.3(6)WA4(9), 12.0(1)W5(6)
p	Um designador de caracteres alfa que identifica a reconstrução de uma versão de tecnologia específica. O valor começa com um "a" minúsculo para a primeira reconstrução, seguido por "b" e assim por diante. Exemplo: 11.3(6)WA4(9a) seria uma reconstrução de 11.3(6)WA4(9).

Os seguintes gráficos rotulam as diferentes seções da convenção de atribuição de nomes do Cisco IOS:

Apêndice B - Confiabilidade do Cisco IOS

A confiabilidade do Cisco IOS é uma área em que a Cisco se esforça continuamente para melhorar. Antes de discutir as melhores práticas orientadas ao cliente, é necessário entender a qualidade interna do Cisco IOS e os esforços de confiabilidade. A finalidade principal destas seções é fornecer uma visão geral dos esforços mais recentes da Cisco na qualidade do software Cisco IOS e definir qual é a concepção do cliente com relação à confiabilidade do software.

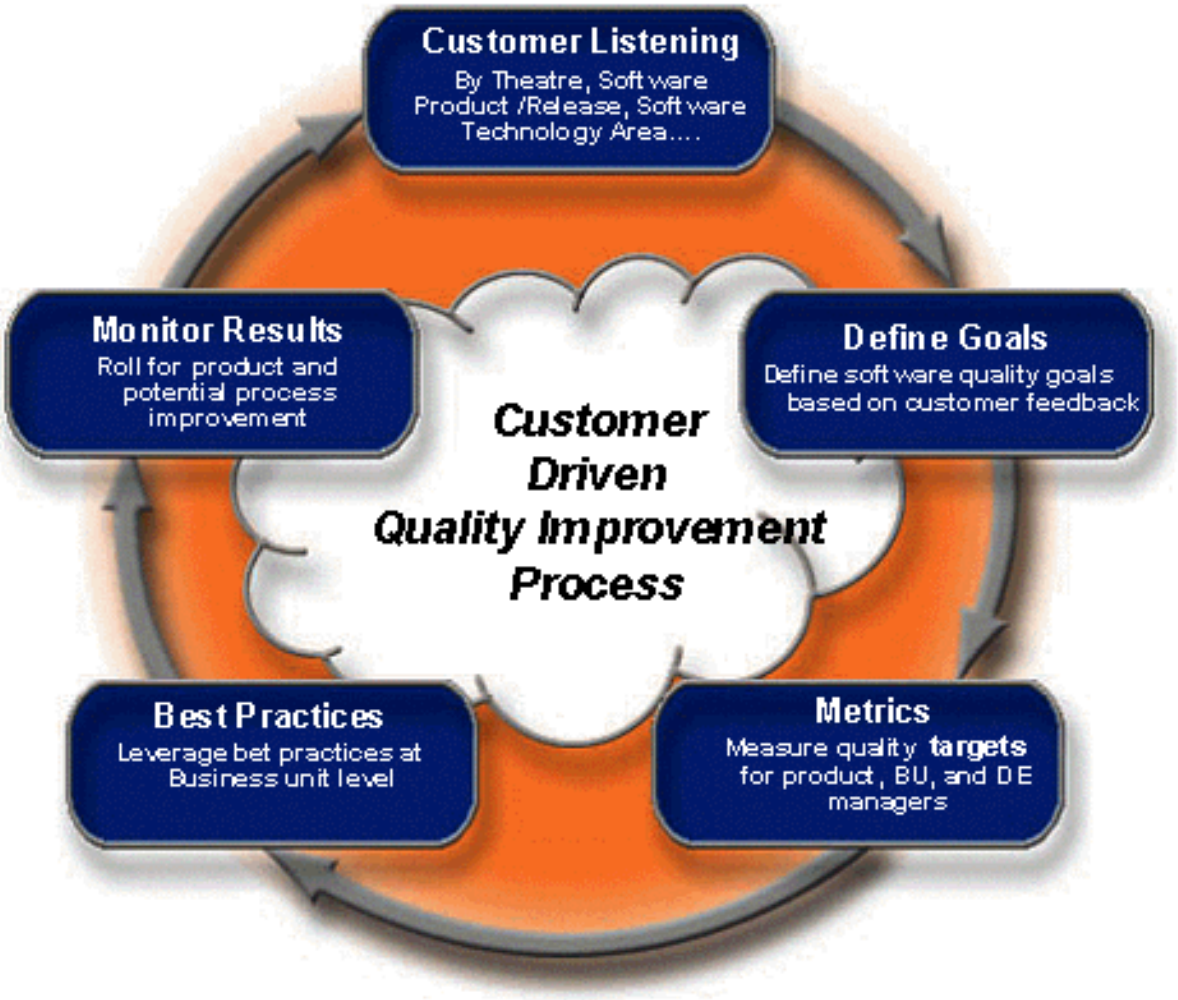
Programa de qualidade do Cisco IOS

A Cisco tem um processo de desenvolvimento do IOS bem definido chamado GEM Great Engineering Methodology (GEM). Esse processo tem um ciclo de vida em três fases:

- Estratégia e planejamento
- Execução
- Implantação

As áreas gerais dentro do ciclo de vida incluem priorização de introdução de recursos, desenvolvimento, processo de teste, fases de introdução de software, First Customer Shipped (FCS), GD e engenharia de sustentação. A Cisco também segue uma série de diretrizes de práticas recomendadas de qualidade de software de organizações como International Standards Organization (ISO), Telcordia (anteriormente Bellcore), IEEE e Carnegie Mellon Software Engineering Institute. Essas diretrizes são incorporadas aos processos GEM da Cisco. Os processos de desenvolvimento de software da Cisco são certificados pela ISO 9001 (1994).

O principal processo para a melhoria de qualidade do Cisco IOS Software é um processo direcionado ao cliente, no qual a Cisco ouve os clientes, define objetivos e métricas, implementa as melhores práticas e monitora os resultados. Uma equipe interorganizacional comprometida com a melhoria da qualidade do software impulsiona esse processo. Um diagrama do processo de melhoria da qualidade do Cisco IOS é mostrado abaixo:



O processo de melhoria da qualidade tem objetivos mensuráveis distintos para o ano fiscal de 2002 e seguintes. O foco principal desses objetivos é reduzir defeitos identificando problemas de software com antecedência no ciclo de testes, diminuir o backlog de defeitos, melhorar a consistência dos recursos e a clareza das versões de software, além de fornecer agendas de versões previsíveis e qualidade de software. As iniciativas para lidar com essas áreas incluem novas ferramentas de cobertura de teste (identificando áreas de cobertura de teste mais fraca), melhoria do processo de ação corretiva de teste e melhorias no teste de regressão do sistema Cisco IOS. Foram aplicados recursos adicionais para lidar com esses problemas e há comprometimento executivo e multifuncional para todas as principais versões do software Cisco IOS.

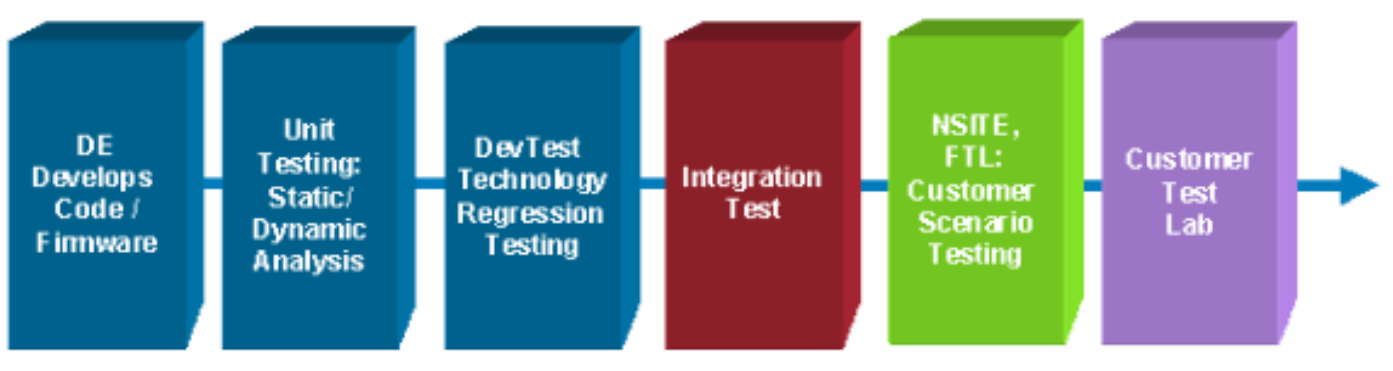
Teste de versão do Cisco IOS

Uma parte integrante do esforço de qualidade de confiabilidade do software na Cisco é a qualidade, o escopo e a cobertura dos testes. Em geral, a Cisco tem os seguintes objetivos de qualidade do IOS:

- Reduzir defeitos de regressão internos Cisco encontrados. Isso inclui maior qualidade no desenvolvimento e identificação de mais problemas na análise estática/dinâmica.
- Reduzir defeitos encontrados pelo cliente
- Reduzir o total de defeitos
- Aumentar a clareza da versão do software e a consistência dos recursos
- Fornece versões de recursos e manutenção com cronogramas e qualidade

Os testes internos da Cisco podem ser considerados como um processo em que defeitos

diferentes são identificados em diferentes estágios de testes. O objetivo geral é encontrar os tipos certos de defeitos no laboratório certo. Isso é importante por diversas razões. A primeira e mais importante é que uma cobertura de teste adequada pode não existir em estágios de teste posteriores. Os custos de teste também aumentam dramaticamente de estágio para estágio, devido à capacidade de automação em estágios iniciais e à complexidade crescente e experiência necessária posteriormente. O diagrama a seguir mostra o espectro de teste para o Cisco IOS.



O primeiro estágio é o desenvolvimento de software. A Cisco tem vários esforços nessa área para ajudar a melhorar a qualidade inicial do software. Os grupos de desenvolvimento também realizam revisões de código ou até mesmo revisões de código múltiplas para garantir que outros desenvolvedores aprovem alterações de software ou um novo código de recurso.

A próxima fase é o teste da unidade. O teste de unidade utiliza ferramentas que examinam a interação do software sem o uso de um laboratório. DevTest são testes de laboratório que incluem teste de recurso/funcionalidade e teste de regressão. O teste de recurso/funcionalidade foi projetado para examinar a funcionalidade de um determinado recurso. Isso inclui configuração, desconfiguração e teste de todas as permutas de recursos, conforme definido na especificação do recurso. O teste de regressão é feito em uma instalação de teste automatizada, projetada para validar comportamento e funcionalidade de recursos continuamente. Os testes concentram-se principalmente no roteamento, na switching e na funcionalidade de recursos de diversas topologias de rede diferentes, usando pings e geração de tráfego limitado. O teste de regressão é feito somente em uma combinação limitada de recursos, plataformas, versões de software e topologias devido ao número extremo de possíveis permutações, no entanto, mais de 4.000 scripts de teste de regressão são são utilizados atualmente. O teste de integração foi projetado para expandir os recursos de teste de laboratório para um conjunto mais abrangente de produtos e interoperabilidade. O teste de integração também aumenta a cobertura do código de teste, expandindo os testes de interoperabilidade, testes de estresse e desempenho, testes de sistema e testes negativos (teste de eventos inesperados).

A próxima fase de laboratório oferece testes ponta-a-ponta para os ambientes comuns do cliente. Eles são mostrados no diagrama acima como Financial Test Lab (FTL) e NSITE, Customer Scenario Testing. A FTL foi criada para fornecer testes para a comunidade financeira de missão crítica. O NSITE é um grupo que oferece testes mais aprofundados para diferentes tecnologias Cisco IOS. Os laboratórios NSITE e FTL se concentram em áreas como, por exemplo, escalabilidade e avaliação de desempenho, capacidade de atualização, disponibilidade e elasticidade, interoperabilidade e operacionalidade. A facilidade de manutenção se concentra em problemas de provisionamento em massa, gerenciamento/correlação de eventos e solução de problemas em carga. Existem outros laboratórios na Cisco para diferentes mercados verticais para ajudar a testar essas áreas.

O laboratório final exibido no diagrama acima é identificado como o laboratório do cliente. O teste

do cliente é uma extensão do esforço de qualidade e recomendado para ambientes de alta disponibilidade para garantir que a combinação exata de recursos, configuração, plataformas, módulos e topologia tenha sido totalmente testada. A abrangência do teste deve incluir a escalabilidade e o desempenho da rede na topologia identificada, testes de aplicativos específicos, testes negativos na configuração identificada, testes de interoperabilidade para dispositivos não-Cisco e testes de operação antecipada.

MTBF de software

Uma das métricas mais comuns de confiabilidade geral é o tempo médio entre falhas (MTBF). O MTBF para a confiabilidade do software é útil devido aos recursos de análise que foram desenvolvidos para a confiabilidade do hardware usando o MTBF. A confiabilidade do hardware pode ser determinada com mais precisão usando alguns padrões existentes. A Cisco utiliza o método de contagem de peças com base nos dados MTBF padrão da Telcordia Technologies. O software MTBF, no entanto, não tem metodologias de análise correspondentes e deve depender da medição de campo para a análise de MTBF.

Nos últimos três anos, a Cisco realizou medições de campo de confiabilidade de software para a rede interna de TI da Cisco e esse trabalho está documentado na Cisco. O trabalho consiste em travamentos forçados por software dos dispositivos do Cisco IOS, que podem ser medidos usando informações de desvios de SNMP de gerenciamento de rede e informações de período operacional. O estudo identifica a confiabilidade do software usando um modelo de distribuição normal de registro estatístico para as versões de software identificadas. O tempo médio para reparo (MTTR) de falha de software é baseado nos tempos médios de reinicialização e recuperação do roteador. Um tempo de recuperação de seis minutos é usado para ambientes empresariais e quinze minutos é usado para provedores de serviços de Internet (ISPs) maiores. O resultado desse estudo contínuo é que o software geralmente atende à disponibilidade de noves finos quando lançado, ou após algumas versões de manutenção, e é ainda mais alto com o tempo, conforme medido usando travamentos forçados de software como a única fonte de tempo de inatividade. O estudo identificou possíveis valores MTBF, como um intervalo entre 5.000 horas para a implantação da versão de desenvolvimento do software e 50.000 horas para a implantação geral do software.

A réplica mais comum a esse trabalho é que o software que forçou os travamentos não inclui todos os tempos de parada ocorridos devido a problemas de confiabilidade do software. Se essa métrica for usada em esforços de melhoria de qualidade, pode ajudar a melhorar a taxa de travamentos forçados do software, mas pode ignorar outras áreas críticas de confiabilidade do software. Esse comentário permanece sem resposta devido à dificuldade em prever de forma precisa a confiança do software utilizando uma metodologia estatística. Os estatísticos de qualidade do software da Cisco concluíram que um conjunto maior de dados precisos seria necessário para prever com segurança o MTBF do software usando uma variedade maior de tipos de interrupção. Além disso, a análise estatística teórica seria difícil devido a variáveis como complexidade de rede, experiência da equipe para resolver problemas relacionados a software, projeto de rede, recursos habilitados e processos de gerenciamento de software.

No momento, nenhum trabalho do setor foi concluído para prever com mais precisão a confiabilidade do software com medições de campo devido à dificuldade de coletar com precisão esse tipo de dados confidenciais. Além disso, a maioria dos clientes não quer que a Cisco colete informações de disponibilidade diretamente de sua rede devido à natureza proprietária dos dados de disponibilidade. No entanto, algumas organizações coletam dados sobre a confiabilidade do software e a Cisco incentiva as organizações a coletar métricas sobre a disponibilidade devido a interrupções do software e a realizar análises de causa básica dessas interrupções. As

organizações com confiabilidade mais alta de software têm usado essa instância pró-ativa para melhorar a confiabilidade do software por meio de várias práticas controláveis.

Suposições de confiabilidade de software

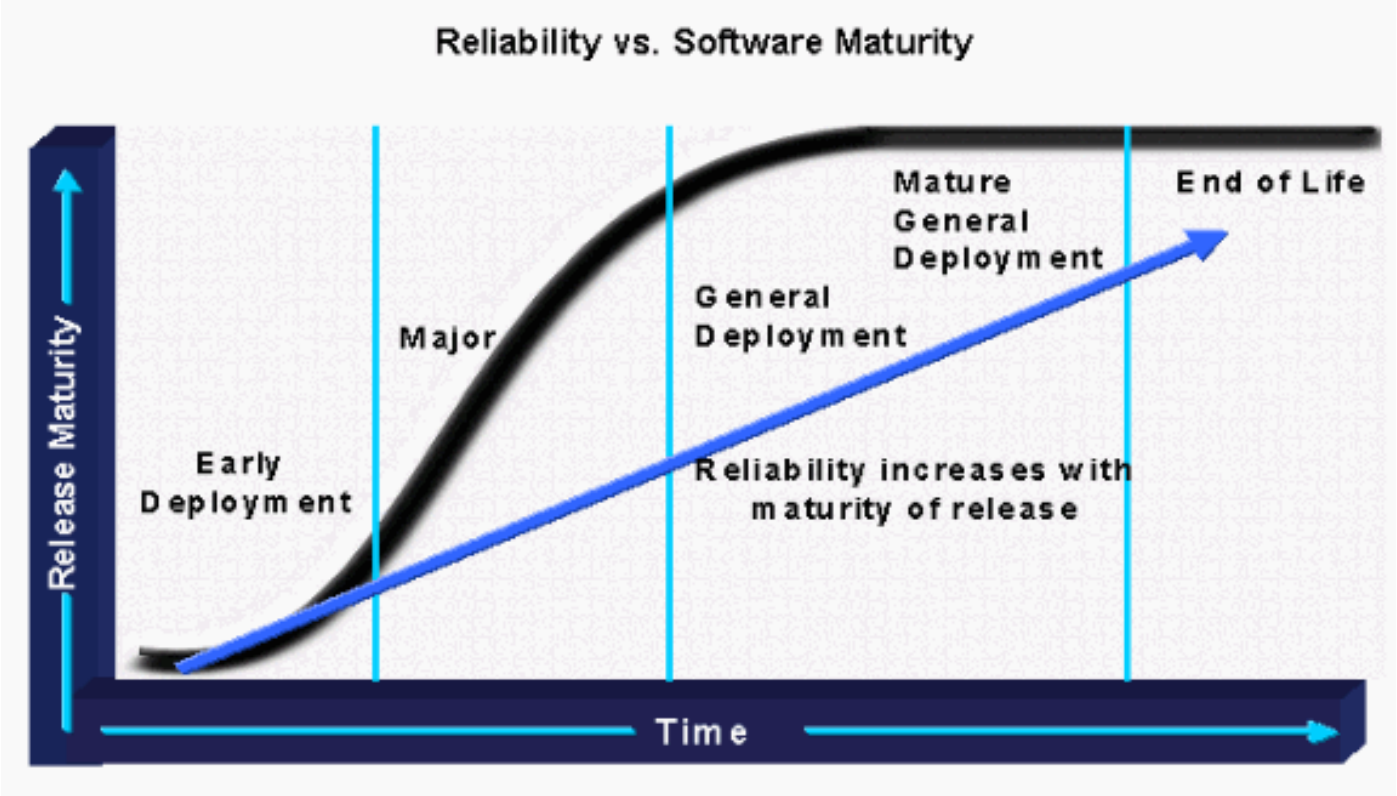
Como resultado do feedback do cliente, estudos proativos realizados pelo grupo de Tecnologias do Cisco IOS e análise da causa básica realizada pela equipe de Serviços Avançados da Cisco, algumas suposições mais recentes e práticas recomendadas foram formadas para ajudar a melhorar a confiabilidade do software. Essas suposições concentram-se em testar as responsabilidades, a maturidade ou idade do software, os recursos ativados e o número das versões de software implementadas.

Responsabilidade pelos testes

A primeira nova hipótese lida com a responsabilidade dos testes. A Cisco é sempre responsável por testar/validar novos recursos e funcionalidades para garantir que eles funcionem em novos produtos. A Cisco também é responsável pelo teste de regressão para garantir que as novas versões de software sejam compatíveis com versões anteriores. No entanto, a Cisco não pode validar todos os recursos, topologias e plataformas em relação a todas as advertências potenciais que um ambiente do cliente possa trazer (idiossincrasias de design, carga e perfis de tráfego). As melhores práticas de alta disponibilidade para os clientes incluem testes em uma topologia de laboratório recolhida que imita a rede de produção usando recursos definidos pelo cliente, design, serviços e tráfego de aplicativos.

Confiabilidade vs. Maturidade do software

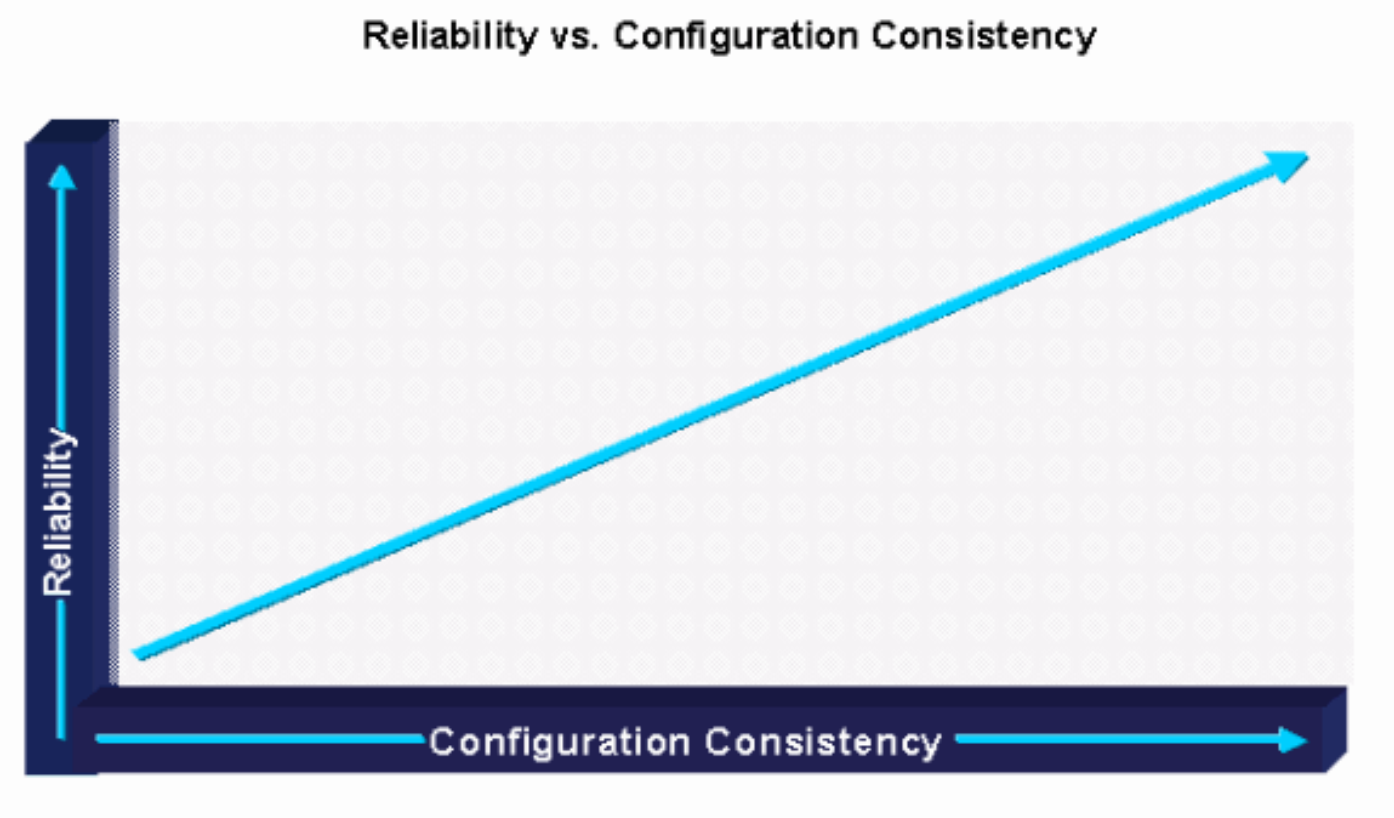
A confiabilidade do software é principalmente um fator de maturidade de software. O software amadurece quando recebe uma exposição (uso) e quando os bugs identificados são corrigidos. As operações de versão da Cisco foram para uma arquitetura de versão de treinamento para garantir que o software amadureça sem que novos recursos sejam adicionados. Os clientes que exigem alta disponibilidade estão procurando por software mais desenvolvido com os recursos de que precisam agora. Existe então uma troca entre a maturidade do software, os requisitos de disponibilidade e os fatores determinantes da empresa para novos recursos ou funcionalidades. Muitas organizações têm padrões ou diretrizes para maturidade aceitável. Algumas apenas aceitarão a quinta versão temporária de um train específico. Para outros, pode ser a nona ou a certificação GD. Enfim, a organização precisa decidir seus níveis aceitáveis de risco em termos de desenvolvimento total de software.



Confiabilidade versus quantidade de recursos e padrões

A confiabilidade do software também é um fator de quanto do código é testado e exercido em um ambiente de produção. À medida que a quantidade de diferentes plataformas de hardware e módulos aumenta, a quantidade de código exercido também aumenta, o que geralmente aumenta a exposição a defeitos de software. Pode-se dizer o mesmo sobre a quantidade de protocolos configurados, a variedade de configurações e até a variedade de topologia ou de designs implementados. O design, a configuração, os protocolos e os fatores do módulo de hardware podem contribuir para a quantidade de código que é exercido e para o aumento do risco ou da exposição a defeitos de software.

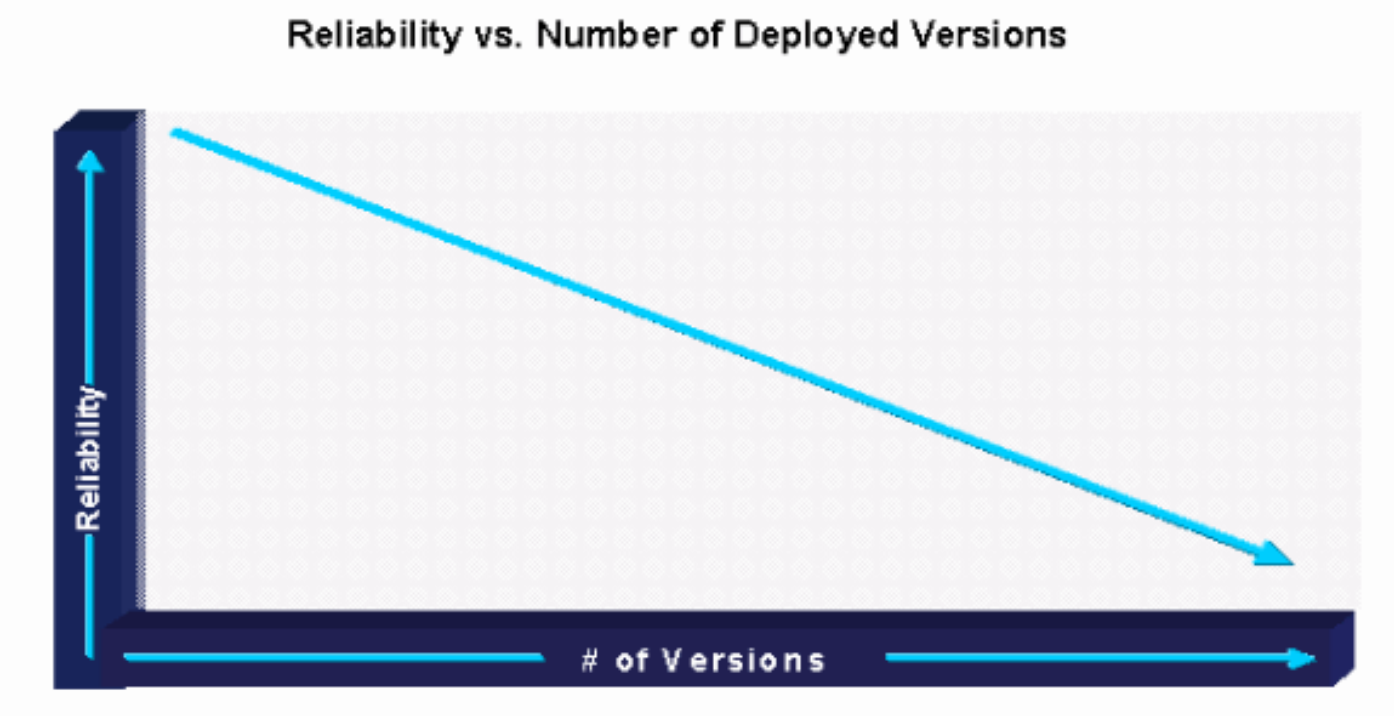
As operações de versão de software agora terão um software para fim específico que limita de maneira geral o código disponível em uma área específica. As unidades de negócios recomendaram projetos e configurações que são testados com mais detalhes na Cisco e mais amplamente utilizados pelos clientes. Os clientes também começaram a adotar as melhores práticas para topologias modulares padronizadas e configurações padrão para reduzir a exposição de código não testada e melhorar a confiabilidade geral do software. Algumas redes de alta disponibilidade têm diretrizes de configuração padrão estritas, padrões de topologia modular e controle de versão de software para ajudar a reduzir o risco de exposição a códigos não testados.



Confiabilidade x número de versões implantadas

Outro fator de confiabilidade do software é a interoperabilidade entre versões e a quantidade total de código que é negociada com várias versões. À medida que a quantidade de versões de software aumenta, também aumenta a quantidade de código exercido, o que aumenta a exposição a defeitos de software. O risco para confiabilidade aumenta quase exponencialmente devido ao código adicional exercido com versões múltiplas. Agora, é reconhecido que as empresas precisam executar pelo menos algumas versões na rede para cobrir requisitos específicos de recursos e plataformas. Executar mais de cinqüenta versões em um ambiente de rede bastante homogêneo, normalmente, é uma indicação de problemas de software devido a incapacidade de análise adequada ou de validação de muitas versões.

Para melhorar a confiabilidade do software, o desenvolvimento da Cisco executa o teste de regressão do software para garantir que diferentes versões de software sejam compatíveis. Além disso, o código de software é mais modular e os módulos de núcleo têm menos probabilidade de mudar significativamente entre versões ao longo do tempo. As operações de lançamento da Cisco também mudaram a quantidade de software disponível para os clientes, já que versões com defeitos conhecidos ou problemas de interoperabilidade são rapidamente removidas do CCO à medida que ocorrem defeitos.



Informações Relacionadas

- Sistemas Operacionais de Interligação de Redes Cisco (IOS)
- Suporte Técnico e Documentação - Cisco Systems