Gerenciamento de rede de alta disponibilidade do Cisco IOS: White Paper de práticas recomendadas

Índice

Introdução

O software seguro de distribuição e de manutenção de Cisco IOS® é uma prioridade no ambiente de rede crítica de hoje do negócio que exige Cisco e o foco do cliente renovados conseguir a Disponibilidade sem parar. 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 disponibilidade mais alta e eficiência no gerenciamento de software. Esse método é uma parceria combinada para compartilhar, aprender e implementar o compartilhamento de práticas ideais.

Este documento fornece um framework operacional efetivo das práticas de gerenciamento do Cisco IOS para a empresa e os clientes de provedor de serviço que ajudam a promover a confiança de software aprimorado, a complexidade de rede reduzida, e o aumento da 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 de ciclo de vida do Gerenciamento do Cisco IOS. Cada tabela começa com uma estratégia e as ferramentas sumárias para a área identificada do ciclo de vida. Depois da estratégia e das ferramentas o sumário é os melhores prática específicos que se aplicam somente à área definida do ciclo de vida.

Planejar - Construindo o framework de gerenciamento do Cisco IOS — O planeamento é a fase inicial de Gerenciamento do Cisco IOS necessária ajudar uma organização a determinar quando ao software de upgrade, onde promover, e que processo será usado para testar e validar imagens potencial.

Melhor prática	Detalhe
Estratégia e Ferramentas para Planejamento de Cisco IOS	Obter começada com planejamento de gerenciamento do Cisco IOS começa com uma avaliação honesta de práticas atuais, do desenvolvimento de metas alcançáveis, e do planejamento de projeto.
Definições de acompanhamento de versão de software	Identifica onde a consistência do software pode ser mantida. Um rastreamento de software pode ser definido como um agrupamento de versão de software exclusivo, diferenciado de outras áreas pela geografia exclusiva, pelas Plataformas, pelo módulo, ou pelos requisitos de recurso.

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 a identificação da trilha, as definições do ciclo de upgrade, o gerenciamento de candidato, o teste/validação, e pelo menos o algum uso da produção piloto.

Projeto - Seleção e validação das Versões do IOS — Ter um processo bem definido para selecionar e validar versões do Cisco IOS ajuda uma organização a reduzir o tempo ocioso não planejado devido às tentativas de upgrade mal sucedidas e aos defeitos do software não programados.

Melhor prática	Detalhe
Estratégia e ferramentas para Seleção e Validação Cisco IOS	Defina processos para selecionar, testar, e validar versões do Novo Cisco IOS. Isso inclui um laboratório de teste de rede que simule a rede de produção
Gerenciamento de candidato	O gerenciamento de candidato é a identificação dos requisitos de versão de software e de riscos potenciais para o hardware particular e os conjuntos de recursos permitidos.
Teste e validação	Testes e validação são aspectos críticos do gerenciamento de software e de redes de alta disponibilidade. Os testes de laboratório apropriados podem significativamente reduzir o tempo de inatividade do produto, ajudá-lo a treinar o equipe de suporte de rede, e ajudá-lo em aerodinamizar processos da implementação de rede.

Aplicação - Desenvolvimento rápido e bem sucedido do Cisco IOS — Os processos de implementação bem definidos permitem uma organização distribuem a rapidamente e com sucesso versões do Novo Cisco IOS.

Melhor prática	Detalhe
Estraté	A estratégia básica das implantações de Cisco

gia e ferramentas para distribuições de Cisco IOS	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	A fim minimizar mais com segurança a exposição potencial e à captação todas as questões de produção restantes, um piloto de software são recomendadas. O plano piloto individual deve considerar a seleção piloto, a duração piloto, e a medida.
Implementação	Após a conclusão da fase piloto, a fase de aplicação 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 - Controlando a Alta disponibilidade da aplicação do Cisco IOS — Os melhores prática para operações do Cisco IOS incluem o controle de versão de software, o Cisco IOS gerenciamento syslog, a gerência de problemas, a padronização de configuração, e o gerenciamento de disponibilidade.

Melhor prática	Detalhe
Estratégias e ferramentas para operações de Cisco IOS	A primeira estratégia de operações do Cisco IOS é manter tão simples quanto possível o ambiente, evitando a variação na configuração e nas versões do Cisco IOS. A segunda estratégia é a capacidade para identificar e resolver rapidamente defeitos 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.
Gerencia	Processos de gerenciamento de problema

mento de problemas	detalhados que definem a identificação do problema, a coleção de informação, e um trajeto bem analisado da solução. Esses dados podem ser usados para determinar a principal causa.
Padronização de configuração	Os padrões de configuração representam a prática de criar e de manter dispositivos como padrão e serviços dos parâmetros de configuração globais transversalmente tendo por resultado a consistência de configuração global larga da empresa.
Gerenciamento de disponibilidade	O gerenciamento de disponibilidade é o processo de melhoria de qualidade usando a disponibilidade da rede como a métrica da melhoria de qualidade.

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

O gerenciamento de ciclo de vida do Cisco IOS Software é definido como o grupo de planeamento, de projeto, de aplicação, e de processos operacionais que são recomendados para aplicações e rede de alta disponibilidade do software confiável. Isso inclui processos de seleção, validação e manutenção das versões do Cisco IOS na rede.

O objetivo do gerenciamento de ciclo de vida do Cisco IOS Software é melhorar a disponibilidade da rede abaixando os defeitos do software identificados probabilidade de produção ou a mudança/falhas de upgrade relativas 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.

Os melhores prática incluem definições de track da versão de software, ciclo de upgrade e definições, e a criação de um processo de certificação do software interno.

Estratégia e Ferramentas para Planejamento de Cisco IOS

Comece o planejamento de gerenciamento do Cisco IOS com uma avaliação honesta de práticas atuais, do desenvolvimento de metas alcançáveis, e do planejamento de projeto. 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 do software que aquela inclua testes/validação do software?
- Minha organização tem padrões do Cisco IOS Software com uma quantidade limitada de versões do Cisco IOS que são executado na rede?
- Minha organização tem a dificuldade que determina quando promover o Cisco IOS Software?
- Minha organização tem o software de distribuição ambos do Novo Cisco IOS da dificuldade de forma eficiente e eficaz?
- Minha organização tem os problemas de estabilidade do Cisco IOS depois do desenvolvimento que impactam seriamente os custos de tempo ocioso?

Depois da avaliação, sua organização deve começar a definir objetivos para o Gerenciamento do Cisco IOS Software. 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. Também, defina fatores e métricas de sucesso críticos para determinar benefícios de gerenciamento de software. A métrica potencial inclui:

- Disponibilidade (devido às questões de software)
- custo de atualizações de software
- Tempo necessário para atualizações
- número de versões do software que são executadas em produção
- sucesso/taxas de falha da upgrade de atualização de software

Além do que o framework de gerenciamento total do Cisco IOS que planeia, algumas organizações igualmente definem reuniões de planejamento em curso do software para ocorrer mensalmente ou trimestralmente. O objetivo destas reuniões é rever o desenvolvimento de software atual e começar a planejar todos os requisitos de software novos. 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 gerente de inventário do Resource Manager Essentials do CiscoWorks2000 (RME) é a ferramenta preliminar usada nesta área. O RME Inventory Manager do CiscoWorks2000 simplifica extremamente o gerenciamento de versão dos roteadores Cisco e do Switches através das ferramentas de relatório com base na Web que os dispositivos IOS Cisco do relatório e do tipo basearam na versão de software, na plataforma do dispositivo, no tamanho de memória, e no nome de dispositivo.

Definições de acompanhamento de versão de software

O primeiro melhor prática do planejamento de gerenciamento do Cisco IOS Software identifica onde a consistência do software pode ser mantida. Um rastreamento de software é definido como um agrupamento de versão de software exclusivo, diferenciado de outras áreas pela geografia exclusiva, pelas Plataformas, pelo módulo, ou pelos requisitos de recurso. Da maneira mais eficiente, uma rede deve executar apenas uma versão de software. Isto abaixa extremamente custos relativos gerenciamento de software e fornece um ambiente consistente e facilmente controlado. Contudo, a realidade é que a maioria de organizações devem executar diversas versões na rede devido à característica, à plataforma, à migração, e aos problemas de

disponibilidade dentro das áreas específicas. Em muitos casos, a mesma versão não trabalha em plataformas heterogênea. Em outros casos, a organização não pode esperar uma versão para apoiar todas suas exigências. 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 organização pode ter levemente mais trilhas para abaixar em geral testes/validação, certificação, e custos da elevação.

O primeiro fator diferenciador é o suporte para plataforma. Tipicamente, os switch LAN, os switch WAN, os roteadores centrais, e os roteadores de ponta cada um têm trilhas do software separado. Outros rastreamentos de software serão necessários para recursos ou serviços específicos, como switching de enlace de dados (DLSw), Qualidade do serviço (QoS) ou telefonia IP, especialmente se esse requisito estiver dentro da rede.

Uns outros critérios são confiança. Muitas organizações tentam executar a maioria de software confiável para o centro de rede e o centro de dados, ao oferecer uns recursos avançados mais novos, ou um suporte a hardware, para a borda. Por outro lado, a escalabilidade ou as características da largura de banda são frequentemente a mais necessário em ambientes do núcleo ou do centro de dados. 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 de certificação
1	Interruptor do núcleo LAN	6500	qos	12.1E (A8)	Testando
2	Interruptor de acesso de LAN	2924XL 2948XL	UDLD (Unidirectional Link Detection Protocol), STP (Spanning Tree Protocol)	12.0(5.2)XU	3/1/01 certificado
3	Distribuição de LAN/acesso	5500 6509	Supervisor 3	5.4(4)	7/1/01 certificado
4	Módulo de switch de rota do switch de distribuição (RS)	RS	Roteamento do OSPF	12.0(11)	3/4/02 certificado
5	Distribuição de fim de cabeçalho WAN	7505 7507 7204 7206	Frame Relay OSPF	12.0(11)	11/1/01 certificado

6	Acesso WAN	2600	Frame Relay OSPF	12.1(8)	6/1/01 certificado
7	Conectividade IBM	3600	Final do cabeçalho do Synchronous Data Link Control (SDLC)	11.3(8)T1	11/1/00 certificado

As atribuições de rastreamento também podem mudar ao longo do tempo. Em muitos casos, as características ou o suporte a hardware podem integrar em mais versões de software do mainline permitindo que as trilhas diferentes migrem eventualmente junto. 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. A qualquer momento uns novos recursos, serviço, hardware, ou o requisito de módulo é identificado, uma trilha nova devem ser considerados.

As organizações que desejam iniciar um processo da trilha devem começar com exigências recentemente definidas da trilha, ou em alguns casos, projetos da estabilização para redes existentes. Uma organização pode igualmente ter algumas comunidades identificáveis com versões de software existentes que podem tornar a definição de track atual possível. Na maioria dos casos, a migração rápida às versões identificadas não é exigida se o cliente tem a suficiente estabilidade de rede. A arquitetura de rede, ou o grupo de engenharia, possuem normalmente o processo da definição de track. Em alguns casos, um indivíduo pode ser responsável para definições de track. Em outros casos, as ligações do projeto são responsáveis para desenvolver os requisitos de software e as definições de track novas baseados em projetos individuais. É igualmente uma boa ideia rever numa base trimestral definições de track para determinar se as trilhas novas estão exigidas, ou se as trilhas velhas exigem a consolidação ou a promovem.

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 upgrade permitem que uma organização planeie corretamente para um ciclo do upgrade de software e atribua recursos requerido. 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. Uma outra exposição poderia ser a organização que falta a oportunidade de testar e validar corretamente uma nova versão antes que o uso de produção esteja exigido.

Um aspecto importante desta prática identificar quando e a que processos de planejamento do grau de software devem ser iniciados. Isto é devido ao fato de que uma causa principal dos problemas de software está girando sobre uma característica, um serviço, ou uma capacidade do

hardware na produção sem a aplicação de dívida, ou a promover ao Novo Cisco IOS uma versão sem considerações sobre gerenciamento de software. Um outro problema não está promovendo. Ignorando ciclos de software e exigências normais, muitos clientes enfrentam as tarefas difíciis do software em upgrade através de um número de versões principal 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.

Cisco recomenda um ciclo de upgrade bem definido, com base nos melhores prática como definido neste papel, ser iniciado sempre que os recursos principais, o serviço, ou o suporte a hardware novo são exigidos. 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 os recursos principais ou a capacidade do hardware são contidos na versão atual, alguns processos de ciclo de upgrade devem igualmente ser iniciados. Se a característica é relativamente menor, considere o risco e decida então que processos devem ser iniciados. Além, o software deve ser promovido em dois anos ou em menos para ajudar a assegurar-se de que sua organização fique relativamente atual e que o processo de upgrade não é demasiado incômodo.

Os clientes devem igualmente considerar o fato de que nenhuma correção de bug estará feita aos trens de software que passaram o fim do estado da vida (EOL). 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 deverem igualmente considerar os dados mais novos recolhidos em operações da versão Cisco quando considerando seus requisitos de teste. Uma análise dos erros e das causas de raiz mostrou que a grande maioria de causas de raiz do erro era o resultado dos colaboradores que codificam dentro da área do software impactada. Isto significa que se uma organização está adicionando uns recursos particulares ou um módulo a sua rede em uma liberação existente, lá é a probabilidade de experimentar um erro relativo a esse característica ou módulo, mas uma probabilidade muito mais baixa que os novos recursos, o hardware, ou o módulo impactem 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
Serviço de rede novo. Por exemplo, um backbone ATM novo ou um serviço novo VPN.	Termine a validação do ciclo de vida do software que inclui testes dos novos recursos (conjuntamente com outro serviços permitidos), teste de topologia compactado, análise de desempenho do What-if, e testes de perfil do aplicativo.
A potencialidade de rede nova não é	Termine a validação do ciclo de vida do software que inclui testes

apoiada na liberação de software atual. Os exemplos incluem QoS e Multiprotocol Label Switching (MPLS).	dos novos recursos, conjuntamente com outro serviços, teste de topologia compactado, análise de desempenho do What-if, e testes de perfil do aplicativo permitidos.
Recursos principais ou módulo de hardware novo que existem na versão atual. Por exemplo, adicionando um módulo, um suporte multicast, ou um DLSW novo do GigE.	Processo de gerenciamento de candidato. Validação completa possível baseada em requisitos de versão. A validação/o teste limitado possível em caso de gerenciamento de candidatos identifica a versão atual como potencialmente aceitável.
Adição de recurso menor. Por exemplo, um dispositivo TACACS para o controle de acesso.	Considere o gerenciamento de candidato baseado no risco da característica. Considere testar ou pilotar os novos recursos baseados no risco.
Software na produção para dois anos ou uma revisão trimestral do software.	Gerenciamento de candidato e decisões de negócio a propósito do gerenciamento de ciclo de vida completo identificar a liberação sustentável atual.

Upgrades de emergência

Em alguns casos, as organizações enfrentam o software de upgrade da necessidade devido aos Bug catastrófico. 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. Cisco recomenda um processo de upgrade de emergência para estas situações onde o teste limitado e os pilotos são executados em menos áreas crítica do negócio da rede.

Se os erros catastróficos ocorrem sem a solução aparente e o problema é defeito do software relativo, Cisco recomenda que Cisco apoia esteja contratado inteiramente para isolar o defeito e para determinar se ou quando um reparo 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 suportada do código e o reparo do problema está disponível em uma versão temporária mais nova existente 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. Mantendo o software suportado na rede, a organização reduz o tempo de

validação devido à base dos mais familiar e códigos estáveis. 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 candidato é especialmente importante se a organização se realiza na fase do early adopter de um trem de software particular.

Processo de certificação

Um processo de certificação ajuda a assegurar-se de que o software validado esteja distribuído consistentemente no ambiente de produção da organização. As etapas do processo de certificação devem incluir a identificação da trilha, as definições do ciclo de upgrade, o gerenciamento de candidato, o teste/validação, e o algum uso da produção piloto. Um processo de certificação simples, contudo, ainda ajuda a assegurar-se de que as versões de software consistente estejam distribuídas 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 primeiramente considerar objetivos do negócio e potencialidades de recurso assegurar-se de que o processo de certificação continue o sucesso. Em seguida, atribua a individual ou em grupo a responsabilidade total para as etapas chaves no processo de certificação que inclui o Gerenciamento da trilha, as definições de upgrade do ciclo de vida, o teste/validação, e os pilotos. Cada um destas áreas deve ser definida, aprovado, e formalmente ser comunicada dentro da organização.

Igualmente inclua diretrizes de qualidade ou aprovação em cada fase do processo de certificação. Isto é chamado às vezes um processo da porta da qualidade porque determinados critérios de qualidade devem ser encontrados antes que o processo possa se mover para a próxima etapa. Isso ajuda a garantir que o processo de certificação é efetivo e vale os recursos atribuídos. Geralmente, quando as edições são encontradas com qualidade em uma área, o processo empurra o esforço para trás uma etapa.

Os candidatos de software não podem encontrar os critérios de certificação definidos devido à qualidade de 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 incomum para que uma organização experimente um problema com um candidato inicial e certifique um Cisco IOS Release provisório mais atrasado. As organizações podem igualmente fazer uma certificação limitada ou fornecer advertências se alguns problemas existem e podem promover a uma liberação inteiramente certificada mais atrasada quando um ínterim novo esteve 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 versões do Cisco IOS ajuda uma organização a reduzir o tempo ocioso não planejado devido às tentativas de upgrade mal sucedidas e aos defeitos do software não programados.

A fase de projeto inclui o gerenciamento de candidato e os testes/validação. O gerenciamento de candidato é o processo usado para identificar versões específicas para os rastreamentos de software definidos. Testar/validação é parte do processo de certificação e assegura-se de que a

versão de software identificada seja bem sucedida dentro da trilha exigida. 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 do Cisco IOS padrão para a rede que começa com um processo para selecionar a versão do Cisco IOS. Uma equipe cruz-funcional da arquitetura, da engenharia, e das operações deve definir e documentar o processo de gerenciamento de candidato. Uma vez que aprovado, o processo deve ser virado ao grupo apropriado da entrega. Igualmente recomenda-se que um molde padrão do gerenciamento de candidato esteja criado que possa ser atualizado com informação sobre candidatos enquanto é identificada.

Não todas as organizações têm um ambiente de laboratório sofisticado que possa facilmente imitar o ambiente de produção. Algumas organizações saltam testes de laboratório devido à despesa e à capacidade pilotar uma nova versão na rede sem impacto de negócios principal. Contudo, as organizações de alta disponibilidade são incentivadas construir um laboratório que imite a rede de produção e desenvolver uns testes/processo de validação para assegurar a teste-cobertura alta para versões do Novo Cisco IOS. Uma organização deve reservar aproximadamente seis meses construir o laboratório. Durante este tempo, a organização deve trabalhar para criar planos de teste e processos específicos assegurar-se de que o laboratório esteja usado a seu benefício completo. Para o Cisco IOS, isto significa a criação de planos de testes específicos do Cisco IOS para cada trilha do software requerido. 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 candidato

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

- Release Note — Fornece informação em relação ao hardware, ao módulo, e ao suporte de recurso de uma liberação. 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** — Gerencia os fluxos de tráfego de multiprotocolos e as taxas de pacote de informação cruas usados para modelar a taxa através de todo o enlace particular que utiliza 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:IPTrocas de Pacote Entre

Redes IPX (IPX)DECNetAppleXerox Network Systems (XNS)Internet Control Message Protocol (ICMP)Internet Group Management Protocol (IGMP)Serviço de rede sem conexão (CLNS)Protocolo de datagrama de usuário (UDP)Serviço de rede integrada virtual (VINES)Pacotes do link de dadosAs ferramentas estão disponíveis de Agilent e de comunicações de Spirent .

- **Contador de pacote de informação/captação/decodificador (sniffer)** — permite que o cliente seletivamente capture e descodifique pacotes em todo o pacote e camadas de link 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 mais adicionais permitem que o usuário especifique a captura dos pacotes que combinam um endereço IP particular, um número de porta ou um MAC address. As ferramentas estão disponíveis com a Sniffer Technologies.
- **Simulador de rede/emulador** — Permite que o cliente povoe as tabelas de roteamento do Roteadores específico, com base nas exigências da 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 das comunicações de Tempestade de Pacote de Informação e das comunicações de Spirent.
- **Emuladores de Sessão** — Os fluxos de tráfego de multiprotocolos do indicador de deslizamento Generate e são capazes de enviar fluxos de tráfego de multiprotocolos através da rede de teste para o 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 da rede em larga escala** — Ajude em 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. As capacidades incluem injetores da rota, vizinhos de protocolo, e mergulham 2 vizinhos de protocolo. As ferramentas estão disponíveis de Agilent e de comunicações de Spirent .
- **Simuladores de WAN** — Ideal para o tráfego de teste do aplicativo corporativo onde a largura de banda e o atraso são potencialmente uma edição. Estas ferramentas permitem que as organizações testem localmente um aplicativo com o atraso e a largura de banda calculados ver como o aplicativo funciona sobre WAN. Essas ferramentas são muito utilizadas para o desenvolvimento de aplicativos e para tipos de teste de perfis de aplicativo em organizações de empreendimento. Adtech, uma divisão da Spirent Communications e Shunra fornecem ferramentas de simulação de WAN.

Gerenciamento de candidato

O gerenciamento de candidato é o processo de identificar requisitos de versão de software e riscos potenciais para o hardware particular e os conjuntos de recursos permitidos. Recomenda-se que uma organização passa quatro a oito horas que pesquisam corretamente requisitos de software, Release Note, defeitos do software, e riscos potenciais antes de pilotar uma liberação. Os seguintes esboços a base para o gerenciamento de candidato:

- Identifique candidatos de software através das ferramentas do Cisco Connection Online (CCO).
- Maturidade de software da análise de risco, novos recursos, ou apoio do código.
- Identifique e siga Bug de Software conhecido, edições, e exigências ao longo do ciclo de vida.
- Identifique o comportamento de configuração padrão da imagem selecionada.
- Maintain back-out e os candidatos rolo-dianteiros para o candidato potencial mudam.
- Erro-esfrega.
- Apoio de Serviços avançados de Cisco.

Identificar candidatos de software tornou-se mais complexa com o número de aumento de produções Cisco e de trens de software. O CCO tem agora diversas ferramentas que incluem o planejador do upgrade do Cisco IOS, a ferramenta de pesquisa de software, a matriz de compatibilidade do software-hardware, e a ferramenta de upgrade de produto que pode ajudar organizações a identificar candidatos de lançamento potencial. Estas ferramentas podem ser encontradas em http://www.cisco.com/cisco/software/navigator.html.

Em seguida, analise o risco do software do candidato potencial. Este é o processo de compreender onde o software reside atualmente na curva da maturidade e então em pesar os requisitos de distribuição com o risco potencial do candidato da liberação. Por exemplo, se uma organização está desejando pôr o software do Early Deployment (ED) em um ambiente crítico de alta disponibilidade, o risco e o requisito de recurso associados para a certificação bem sucedida devem ser considerados. Uma organização deve pelo menos adicionar recursos de gerenciamento de software para que as situações de maior risco assegurem o sucesso. Por outro lado, se uma versão do general deployment (GD) está disponível que encontra as necessidades de uma organização, a seguir menos recursos de gerenciamento de software são precisados.

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. O observador do erro de Cisco, o navegador do erro, e os agentes de vigilância do erro podem ajudar a identificar problemas potenciais e devem ser usados durante todo o ciclo de vida do software para identificar edições da segurança potencial ou do defeito.

Um candidato de software novo deve igualmente ser revisto para o comportamento de configuração padrão potencial. 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 candidato pode igualmente incluir a identificação de back-out versões ou ir-às versões se a versão escolhida não encontra critérios de certificação a dada altura do processo. Olhando os erros relativos às características para uma trilha especificada, uma organização pode manter candidatos potenciais para a certificação.

Os Serviços avançados de Cisco são igualmente uma ferramenta excelente para o gerenciamento de candidato. Este grupo pode fornecer o maior insight no processo de desenvolvimento e na Colaboração entre um grande número especialistas da indústria em muitos ambientes diferentes do mercado vertical. 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

Os testes e a validação são melhores prática e rede de alta disponibilidade de um aspecto crítico

de gerenciamento, totais. 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 qualqueras um áreas, uns testes e um processo de validação não podem encontrar as expectativas de uma organização.

A maioria de organizações de empreendimento não têm o ambiente de laboratório recomendado do teste. Por este motivo, muitas organizações distribuíram soluções incorretamente, experimentaram falhas de alteração de rede, ou são experimentadas os problemas de software que poderiam ter sido isolados em um ambiente de laboratório. Em alguns ambientes, isto é aceitável, porque os custos de tempo ocioso não deslocam o custo de um ambiente de laboratório sofisticado. Em muitas organizações contudo, o tempo ocioso da máquina 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 grandes de organizações precisarão entre quatro aos dez racks de equipamento de imitar o ambiente de produção. Uma certa segurança física é recomendada para ajudar a manter um ambiente de teste enquanto testes estão em andamento. Isto ajuda a impedir que um teste de laboratório seja interrompido devido a outras prioridades de laboratório que incluem o empréstimo, o treinamento, ou os testes de implementação do hardware. A Segurança lógica é recomendada igualmente impedir que as rotas falsas incorporem a rede de produção ou o tráfego indesejável de retirar o laboratório. Isso pode ser feito com filtros de roteamento e listas de acesso estendidas em um Lab Gateway Router. A Conectividade à rede de produção é útil para downloads do software e acesso à rede de laboratório do ambiente de produção.

A topologia de laboratório deve ser capaz de imitar o ambiente de produção para quaisquer planos de teste específicos. O hardware de reprodução, a topologia de rede, e as configurações da característica são recomendados. Naturalmente, reproduzir a topologia real é quase impossível, mas o que pode ser feita é reproduzir a hierarquia de rede e a interação entre os dispositivos da 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 Cisco IOS MACILENTO da borda que testa, por exemplo, não deve exigir o tipo dispositivos ou testes LAN e pode somente exigir roteadores de ponta de WAN e roteadores de distribuição de WAN. A chave é imitar a funcionalidade de software sem produção de duplicação. Em alguns casos, as ferramentas podem mesmo ser usadas para imitar o comportamento em grande escala tal como contagens e tabelas de roteamento do vizinho de protocolo.

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 organização pode igualmente tirar proveito dos dispositivos que podem ajudar a recolher dados, tais como analisadores de protocolo.

O laboratório igualmente exige algum Gerenciamento. Muitas organizações maiores têm uma

gerente de laboratório a tempo completo que tenha a responsabilidade para controlar a rede de laboratório. Outras organizações utilizam equipes de arquitetura e engenharia existentes para validação de laboratório. As responsabilidades de gerenciamento do laboratório incluem o equipamento e ativo pedindo de laboratório gerenciamento de espaço que seguem, da expedição de cabogramas, o físico, definindo regras e sentido do laboratório, programação do laboratório, documentação do laboratório, topologias de lab da fundação, os planos de teste da escrita, executando testes de laboratório, e controlo de edições identificadas potencial.

Tipos de Teste

No geral, há muitos tipos diferentes de testes que podem ser feitos. Antes que construindo um laboratório e um plano de teste completos de teste que possam testar tudo em uma multiplicidade de configurações, uma organização deva compreender os tipos diferentes de testes, a intenção dos testes, e mesmo se o planejamento de Cisco, o marketing técnico, ou a defesa de cliente devem ou poderia ser responsável para alguns dos vários testes. Os planos de teste do cliente cobrem geralmente 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, os testes apropriados do conjunto de recursos específico de uma organização, a topologia, e a mistura de aplicativo são normalmente os mais valiosos. É importante saber que Cisco executa a característica e o teste de regressão completos, porém Cisco não pode testar o perfil do aplicativo da sua organização com seus combinação de topologia, hardware, e recursos configurados específicos. De fato, é inexequível testar a gama completa de características, de hardware, de módulos, e de permutas de topologia. Adicionalmente, Cisco não pode testar a Interoperabilidade com equipamento de terceira parte. Cisco recomenda que as organizações testam a combinação precisa de hardware, de módulos, de características, e de topologia encontrada em seu ambiente. Estes testes devem ser conduzidos em um laboratório, com uma topologia desmoronada que representa o ambiente de produção da sua organização com outros tipos de teste de apoio tais como o desempenho, a Interoperabilidade, a indisponibilidade, e a queima.

Teste	Visão geral do teste	Responsabilidade do Teste
Característica e funcionalidade	Determina se os módulos básicos das características do Cisco IOS e de hardware Cisco funcionam como anunciado. As opções de configuração da característica ou da funcionalidade de módulo assim como da característica devem ser testadas. A remoção de configuração e a adição devem ser	Teste do dispositivo Cisco

	testadas. O teste de interrupção básico e o teste de gravação são incluídos.	
Regressão	Determina se a característica ou o módulo funcionam conjuntamente com outros módulos e características, e se a versão do Cisco IOS funciona conjuntamente com outras versões do Cisco IOS com relação às características definidas. Inclui alguns queima e teste de interrupção.	Teste de regressão de Cisco
Desempenho do dispositivo básico	Determina o desempenho básico da característica ou do módulo determinar se as características do Cisco IOS ou os módulos de hardware cumprem requisitos mínimos sob a carga.	Teste do dispositivo Cisco
Topologia/característica/combinação de hardware	Determina se as características e os módulos funcionam como esperado em uma topologia e em um módulo/característica/combinação de hardware específicos. Este teste deve incluir a verificação de protocolos,	Cisco testa topologias anunciadas padrão nos laboratórios tais como o Enterprise Solutions Engineering (ESE) e a engenharia de teste de integração das soluções de rede

	verificação dos recursos, verificação do comando show, o teste de operação antecipada e o teste de interrupção.	(NSITE). A Alta disponibilidade dos clientes deve testar a característica/módulo/combinações de topologia como necessário, especialmente com software do early adopter e topologias não padronizadas.
Interrupção (E se)	Inclui os tipos ou os comportamentos comuns da indisponibilidade que podem ocorrer em um impacto específico da funcionalidade da característica/módulo/ambiente de topologia e do potencial. O teste de interrupção inclui troca de placas, perda de sincronia do enlace, falhas de dispositivos, falhas de enlaces e falhas de placas.	Cisco é responsável para o teste de interrupção básico. Os clientes são finalmente responsáveis para os problemas de desempenho da indisponibilidade relativos à escalabilidade de seu ambiente individual. O teste de interrupção deve ser feito, se possível, no ambiente do laboratório de cliente.
NetworkPerformance (What-if)	Investiga a carga do dispositivo com relação a uma característica/hardware/combinação de topologia específicos. O foco está na capacidade e no desempenho do dispositivo, como CPU, memória, utilização de buffer e utilização do link em relação	Os clientes são finalmente responsáveis para a carga do dispositivo e a escalabilidade. A carga e os interesses de escalabilidade são levantados frequentemente por vendas Cisco ou por Serviços avançados e testados frequentemente

	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.	com os laboratórios Cisco tais como o Customer Proof-of-Concept Labs (CPOC).
Correção de bug	Assegura-se de que as correções de bug reparem o defeito identificado.	Cisco testa correções de bug para assegurar-se de que o erro seja fixo. Os clientes devem igualmente testar para assegurar-se de que o erro que experimentaram seja fixo e que o erro não quebra nenhum outro aspecto do módulo ou da característica. As versões de manutenção são regressão testada mas as versões temporárias não são geralmente.
Gerenciamento de Rede	Investiga potencialidades de gerenciamento do Simple Network Management Protocol (SNMP), precisão variável do SNMP MIB, suporte armadilha, e suporte de SYSLOG.	Cisco é responsável para testar características SNMP, a funcionalidade, e a precisão básicas do variável MIB. Os clientes devem validar resultados de gerenciamento de rede e são finalmente responsáveis

		para a estratégia de gerenciamento e a metodologia para disposições da nova tecnologia.
Emulation da rede em larga escala	A emulation da rede em larga escala usa ferramentas tais como o simulador de roteador de Agilent e a suite de ferramenta de teste de 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 necessários na produção que não estão no laboratório por padrão.	Os clientes Cisco são geralmente responsáveis para os aspectos dos testes da simulação de rede que reproduzem seu ambiente de rede, que pode incluir o número de vizinhos de protocolo de roteamento/adjacências e os tamanhos de tabela de roteamento associados e os outros recursos que estão na produção.
Interoperabilidade	Testa todos os aspectos relativos à conectividade ao equipamento de rede da terceira, especialmente se a Interoperabilidade do protocolo ou da sinalização é exigida.	Os clientes Cisco são geralmente responsáveis para todos os aspectos de testes da Interoperabilidade.
Queima	Investiga recursos de roteador ao longo do tempo. Os testes da	Cisco executa o teste de gravação básico. O teste de cliente

	queima exigem tipicamente um dispositivo estar sob alguma carga com investigação na utilização de recurso que inclui a memória, o CPU, e os bufferes ao longo do tempo.	é recomendado com relação à topologia exclusiva, ao dispositivo e às combinações de recursos.

Metodologia testando

Uma vez que uma organização conhece o que está testando, uma metodologia deve ser desenvolvida para o processo testando. 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 da recriação são especialmente importantes para versões mais atrasadas de teste ou para correções de bug de teste encontrou no ambiente de laboratório. As etapas de uma metodologia testando são mostradas abaixo. Alguns passos de teste também podem ser executados concomitantemente.

1. Crie uma topologia de teste que simule o ambiente de produção sob o teste. Um ambiente de teste MACILENTO da borda pode incluir alguns roteadores centrais e um roteador de ponta somente, quando um teste LAN puder incluir mais dispositivos que podem melhor representar o ambiente.
2. Configurar as características que simulam o ambiente de produção. A configuração de dispositivos do laboratório deve proximamente combinar as configurações de hardware e de software de dispositivo previstas da produção.
3. Redija um plano de teste, definindo testes e objetivos, 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 dentro de um plano de teste é encontrado na tabela a seguir.
4. Valide o roteamento e a funcionalidade de protocolo. Documento ou resultados previstos linha de base do **comando show**. 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 de recurso. Documento ou resultados previstos linha de base do **comando show**. As características podem incluir comandos global configuration e todos os recursos críticos tais como o Authentication, Authorization, and Accounting (AAA).
6. Simule o carregamento, o qual deve estar previsto no ambiente de produção. A simulação da carga pode ser feita com coletores/geradores do 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. O documento ou a linha de base esperaram resultados do **comando show**.
7. Execute o teste de interrupção onde o dispositivo e o software seriam esperados tratar ou impedir sob a carga. Por exemplo, remoção de placa, não sincronismo de link, não sincronismo de rota, e tempestades de transmissão. Assegure-se de que o SNMP traps correto esteja sendo gerado com base nas características que estão sendo utilizadas dentro

da rede.

8. Documente resultados de teste e medidas do dispositivo como os testes devem ser repetíveis.

Teste o nome	**Failover do Hot Standby Router Protocol (HSRP)**
Teste requisitos de configuração	Aplique a carga à relação 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. Também, aumente o tráfego a uma carga mais alta.
Passos de teste	Monitore o STP e o HSRP através dos **comandos show**. Falhe a conexão de interface do gateway principal e recupere então a conexão depois que a informação é recolhida.
Medidas esperadas	CPU durante o Failover. Mostre a interface antes, durante e depois para o gateway principal e secundário. Mostrar HSRP antes, durante e depois.
Resultados esperados	Gateway principal falhará no outro gateway de roteador em dois segundos. **os comandos show** refletem corretamente a mudança. O Failover ao gateway principal ocorre quando a Conectividade é restaurada.
Resultados reais	
Pass ou Fail (Aprovação ou Falha)	
Alterações exigidas para conseguir a passagem	

Medidas do dispositivo

Durante a fase de teste, realize e documente as seguintes medidas para assegurar-se de que o dispositivo esteja executando corretamente:

- Utilização de memória

- Cargas de CPU
- Uso de buffer
- Estatísticas da relação
- Tabelas de rotas
- Eliminação de erros 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, a medida dos parâmetros assegurar lá não é nenhum impacto no desempenho adverso no aplicativo dado. Isto é terminado utilizando uma linha de base de desempenho que possa ser usada para comparar pre o desempenho e o desenvolvimento do cargo. Os exemplos para testes da medida do aplicativo 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 onde toma para lançar um aplicativo e para o obter alertada com a primeira tela.
- Outros parâmetros específicos dos aplicativos.

Aplicação - Desenvolvimento rápido e bem sucedido do Cisco IOS

Um processo de implementação bem definido permite que uma organização distribua eficientemente versões do Novo Cisco IOS.

A fase de aplicação inclui o processo piloto e o processo de implementação. O processo piloto assegura-se de que a versão do Cisco IOS seja bem sucedida no ambiente e o processo de implementação permita disposições rápidas e bem sucedidas do Cisco IOS da escala maior.

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 da rede, muitas organizações constroem 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 cruz-funcional da engenharia, da aplicação, e das operações é envolvida normalmente em construir diretrizes piloto totais e 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. A arquitetura e os grupos de engenharia definem normalmente exigências novas da

imagem do software na fase do gerenciamento de candidato da duração 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.

Gestão de inventário do Cisco IOS

O gerente de inventário do Resource Manager Essentials do CiscoWorks2000 (RME) simplifica extremamente o gerenciamento de versão dos roteadores Cisco e do Switches através das ferramentas de relatório com base na Web que os dispositivos IOS Cisco do relatório e do tipo basearam na versão de software, na plataforma do dispositivo, e no nome de dispositivo.

NADADA do Cisco IOS

A NADADA do CiscoWorks2000 pode ajudar em reduzir as complexidades sujeitas a erros do processo de upgrade. Os links incorporados ao CCO correlacionam a informações on-line Cisco sobre as correções de software com o Cisco IOS e o Catalyst Software distribuídas na rede, destacando Notas Técnica relacionadas. As ferramentas novas do planeamento encontram requisitos do sistema e enviam notificações quando as upgrades de hardware (ROM da bota, RAM instantâneo) são precisadas de apoiar atualizações propostas da imagem do software.

Antes que uma atualização esteja iniciada, as condições prévias de uma imagem nova estão validadas contra os dados do inventário do interruptor ou do roteador do alvo para ajudar a assegurar uma upgrade bem sucedido. 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

A fim minimizar mais com segurança a exposição potencial e à captação todas as questões de produção restantes, um piloto de software são recomendadas. 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 piloto identifica onde e como um piloto será terminado. Um piloto pode começar com um dispositivo em uma área do baixo-impacto e estender aos dispositivos múltiplos em uma área do alto-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 impacto do dispositivo único devido à Redundância.
- Em uma área da rede com um número mínimo de usuários atrás do dispositivo selecionado que pode tratar algum impacto possível da produção.
- Consider que separa o piloto ao longo das linhas da arquitetura. Por exemplo, pilote-a no acesso, na distribuição, e/ou nas camadas central 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. Isto deve incluir a queima 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 versão principal nova, um período piloto mais longo está preferido. 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 de forma semelhante e documentar resultados como o exame 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 para seguir e o progresso piloto de monitoração para assegurar todas as edições é identificado e que os usuários e os serviços envolvidos no piloto estão satisfeitos com os resultados piloto. A maioria de organizações certificarão uma liberação se é bem sucedida em um piloto ou em um ambiente 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 fase piloto foi terminado dentro da rede de produção, começam a fase de aplicação 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 lento-início da aplicação é o processo lentamente de executar uma liberação recentemente testada para assegurar-se de que a imagem tenha a exposição completa ao ambiente de produção antes da certificação final e da conversão 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 na produção, a organização pode esperar até uma a dois semanas antes da certificação final da versão do Cisco IOS particular. Na certificação final, a organização pode distribuir mais rapidamente a versão identificada com um nível de confiança muito mais elevado.

Depois que o processo lento do começo, todos os dispositivos identificados para a elevação deve ser revisto e validado usando o inventário de dispositivo e uma matriz dos padrões do Cisco IOS mínimo para que a tira de bota, o DRAM, e o flash se assegure de que as exigências estejam cumpridas. 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. Contudo, é sempre uma boa ideia conhecer o que esperar durante a aplicação tenta.

Se mais de cem dispositivos similares são programados para elevações, recomenda-se fortemente que um método automático esteja utilizado. A automatização foi mostrada para

melhorar a eficiência da elevação e para melhorar a porcentagem de sucessos da upgrade de dispositivo durante grandes disposições, com base em uma upgrade interno de 1000 dispositivos com e sem a NADADA. Cisco recomenda que a NADADA do CiscoWorks2000 esteja usada para grande distribuições devido ao grau de verificação que é executado durante a elevação. A NADADA suportará mesmo fora de uma versão do Cisco IOS se um problema é detectado. NADE funções criando e programando os trabalhos de upgrade, onde um trabalho é configurado com os dispositivos, as imagens de upgrade desejadas, e o tempo de execução do trabalho. Cada trabalho deve conter doze ou menos upgrades de dispositivo, e até doze trabalhos podem ser executado simultaneamente. O SWIM também verifica se a versão da atualização de Cisco IOS programada está sendo executada com sucesso após a atualização. Recomenda-se reservar aproximadamente vinte minutos para cada upgrade de dispositivo (que inclui a verificação). Usando esta fórmula, uma organização pode promover trinta e seis dispositivos pela hora. Cisco igualmente recomenda que um máximo de cem dispositivos esteja promovido pela noite para reduzir a exposição do problema potencial.

Depois de uma upgrade automatizado, alguma validação deve ser feita para assegurar 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. A seguinte lista de verificação da amostra pode inteiramente validar o sucesso de um desenvolvimento do Cisco IOS:

- O dispositivo recarregou corretamente?
- São o processo de ping do dispositivo e os alcançáveis através das Plataformas do sistema de gerenciamento de rede (NMS)?
- Estão as relações previstas no dispositivo acima e no active?
- O dispositivo tem as adjacências corretas do protocolo de roteamento?
- A tabela de roteamento é povoada?
- O dispositivo está passando o tráfego corretamente?

Operações - Gerenciamento da implementação de alta disponibilidade do Cisco IOS

A Alta disponibilidade das operações do melhor prática do ambiente do Cisco IOS ajuda a reduzir a complexidade de rede, melhorar o tempo de definição de problema, e a 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.

Os melhores prática para operações do Cisco IOS incluem o controle de versão de software, o Cisco IOS gerenciamento syslog, a gerência de problemas, a padronização de configuração, e o gerenciamento de disponibilidade. O controle de versão de software é o processo de seguir, de validar, e de melhorar a consistência do software dentro dos rastreamentos de software identificados. O gerenciamento syslog do Cisco IOS é o processo dinamicamente de monitoração e de atuação em cima de uns mensagens do syslog mais prioritários gerados 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 de configuração é o processo de estandardizar configurações para reduzir o potencial para que o código não experimentado seja exercitado na produção e para estandardizar o protocolo de rede e o comportamento da característica. O gerenciamento de disponibilidade é o processo de melhorar a Disponibilidade baseado no medidor, nos meta de

aperfeiçoamento, e nos projetos da melhoria.

Estratégias e ferramentas para operações de Cisco IOS

Muitas estratégias de qualidade e ferramentas existem para ajudar a controlar ambientes do 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 tem sido discutida já, porém a consistência do configuração é uma outra área principal. 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 para identificar e resolver rapidamente defeitos de rede. Os problemas de rede devem geralmente ser identificados pelo grupo de operações antes que os usuários os chamem dentro. Problemas também serão resolvidos da forma mais rápida possível sem causar maiores impactos ou alterações no ambiente. Alguns as melhores práticas chaves nesta área são gerência de problemas e gerenciamento syslog do Cisco IOS. Uma ferramenta a ajudar rapidamente a diagnosticar impactos do Cisco IOS Software é o Output Interpreter de Cisco.

A terceira estratégia é aperfeiçoamento consistente. O processo preliminar é melhorar uma Disponibilidade qualidade-baseada do programa de melhoria. Executando a análise de causa de raiz em todas as edições, incluindo problemas relacionados do Cisco IOS, uma organização pode melhorar a cobertura do teste, melhorar o tempo de definição de problema, e melhorar os processos que eliminam ou reduzem o impacto da indisponibilidade. 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 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 syslog registram e os mensagens do syslog da trilha recebidos pelo Roteadores e pelo 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 a mais popular do Syslog para o Gerenciamento do Cisco IOS é gerenciador de Syslog de RME do CiscoWorks2000. Outras ferramentas estão disponíveis incluindo o SL4NT, um programa do shareware de Netal e I privado de OpenSystems.

Gerente da configuração de dispositivo dos CiscoWorks

O gerente da configuração de dispositivo do CiscoWorks2000 mantém um arquivo ativo e fornece uma maneira fácil atualizar alterações de configuração através dos roteadores Cisco e do Switches múltiplos. O gerenciador de configuração monitora a rede para alterações de configuração, atualiza o arquivo quando uma mudança é detectada, e registra a informação de alteração ao serviço do exame de alteração. Uma interface do utilizador baseada Web permite que você procure o arquivo por atributos de configuração específicos e compare os índices de dois arquivos de configuração para a identificação fácil de diferenças.

Output Interpreter de 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. Esta informação ajudará geralmente a expedir uma definição ao problema, pelo menos em termos da coleção de informação requerida.

Controle de versão de software

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

Durante a operação, não é raro ver versões não padronizadas na rede, especialmente se a rede e o pessoal das operações são grandes. 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 padrões de versão de software usando ferramentas tais como o CiscoWorks2000 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 coleção do Syslog, a monitoração, e a ajuda da análise para melhorar o tempo de definição de problema identificando e resolvendo muitas falhas dinamicamente antes que mais problemas de rede graves estejam experientes, ou são relatadas por usuários. O Syslog igualmente fornece um método de mais eficiente de recolher uma ampla variedade de problemas quando comparado ao polling snmp consistente para um grande número variáveis MIB. A coleção, a monitoração, e a análise do Syslog são realizadas utilizando a configuração do IOS da Cisco correta, ferramentas da correlação do Syslog, tais como o Gerenciamento do CiscoWorks2000 RME, e/ou do evento de syslog. O Gerenciamento do evento de syslog é feito analisando gramaticalmente dados de SYSLOG recolhidos para mensagens crítica identificados e então encaminhando um alerta ou armadilha a um gerente do evento para a notificação e a definição do 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, as ferramentas ou os scripts podem ser executados para analisar gramaticalmente dados de SYSLOG e enviar alertas ou notificações aos sistemas de gerenciamento de evento ou as operações e os pessoais de engenharia. Se os alertas para uma ampla variedade de dados de SYSLOG não são usados, a organização deve rever uns dados de SYSLOG mais prioritários pelo menos diários e criar documentações de problema para problemas potenciais. A fim detectar dinamicamente os problemas de rede que não podem ser considerados com a monitoração normal, revisão periódica e a análise de dados de SYSLOG históricos deve ser executada para detectar as situações que não podem indicar um problema imediato, mas pode fornecer uma indicação de um problema antes que se transforme impacto do serviço.

Gerenciamento de problemas

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

Um processo de gerenciamento de problema é recomendado 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 primeiro suporte de alinhamento deve nunca cancelar rotas ou recarregar dispositivos. De forma ideal, a organização de primeiro nível deve coletar rapidamente as informações e ir para uma segunda camada. Passando apenas alguns mais minutos inicialmente na identificação do problema ou na descrição do problema, uma descoberta da causa de raiz é muito mais provável, assim permitindo uma ação alternativa, uma identificação de laboratório, e um relatório do erro. O suporte de segundo nível deve ser bem versado nos tipos de informação que Cisco pode precisar a fim diagnosticar um problema ou arquivar uns relatórios de bug. 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 de configuração de dispositivo globais representam a prática de manter dispositivos como padrão e serviços dos parâmetros de configuração globais transversalmente tendo por resultado a consistência de configuração global larga da empresa. Os comandos global configuration são os comandos que se aplicam ao dispositivo inteiro e não às portas individuais, aos protocolos, ou às relações. Os comandos global configuration impactam geralmente o acesso de dispositivo, o comportamento geral do dispositivo, e a segurança do dispositivo. No Cisco IOS isto inclui comandos service, comandos ip, comandos vty, comandos da porta de Console, comandos logging, comandos AAA/TACACS+, comandos SNMP, e comandos da bandeira. Igualmente importante em padrões de configuração de dispositivo globais é uma convenção de nomeação apropriada do dispositivo que permita que os administradores identifiquem o dispositivo, o tipo de dispositivo, e o lugar do dispositivo baseado no nome do Domain Name System (DNS) do dispositivo. A consistência de configuração global é importante para a

capacidade de suporte total e a confiança de um ambiente de rede porque ajuda a reduzir a complexidade de rede e aumentar a capacidade de suporte da rede. Geralmente, o usuário passa por problemas no suporte sem padronização de configuração, seja devido a um comportamento incorreto ou indevido do dispositivo, ao acesso SNMP ou, ainda, devido à segurança geral do dispositivo.

Manter padrões de configuração de dispositivo globais é realizada normalmente por um grupo interno da engenharia ou de operações que crie e mantenha parâmetros de configuração globais para dispositivos de rede similares. É igualmente uma boa prática fornecer uma cópia do arquivo de configuração global nos diretórios de TFTP de modo que possam inicialmente ser transferidos toda recentemente aos dispositivos fornecida. Igualmente útil é um arquivo acessível da Web que forneça o arquivo de configuração padrão uma explicação de cada parâmetro de configuração. Algumas organizações configuram 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 da configuração da interface devem incluir descritores de interface CDP, configuração de ocultação, e outros padrões do específico do protocolo. Os padrões de configuração específicos do protocolo podem incluir:

- Configuração de Roteamento IP
- Configuração DLSw
- Configuração de lista de acesso
- Configuração de ATM
- Configuração do Frame Relay
- Configuração de árvore de abrangência
- Atribuição de VLAN e configuração
- Protocolo virtual trunking (VTP)
- HSRP

Nota: É possível ter outros padrões de configuração específicos do protocolo segundo o que é configurado dentro da rede.

Um exemplo de padrões IP pode incluir:

- Tamanho de sub-rede
- O espaço de endereços IP usado
- Routing Protocol utilizado
- Configuração do Routing Protocol

Manter padrões do protocolo e da configuração da interface é normalmente a responsabilidade dos grupos da engenharia e da aplicação da rede. O grupo de engenharia deve ser responsável por identificar, testar, validar e documentar o padrões. O grupo da aplicação é então responsável para usar os documentos de engenharia ou os gabaritos de configuração para provision serviços novos. O grupo de engenharia deve criar documentação sobre todos os aspectos dos padrões exigidos para garantir consistência. Os gabaritos de configuração devem igualmente ser criados

para ajudar a reforçar os padrões de configuração. Os grupos de operação também devem receber treinamento sobre os padrões e devem ser capazes de identificar problemas de configurações que não sejam padrão. A consistência do configuração é do grande ajuda nos testes, na validação, e na fase da certificação. De fato, sem gabaritos de configuração estandardizados, é quase impossível testar, validar, ou certificar adequadamente moderadamente uma versão do Cisco IOS para uma rede grande.

Gerenciamento de disponibilidade

O gerenciamento de disponibilidade é o processo de melhoria de qualidade usando a disponibilidade da rede como a métrica da melhoria de qualidade. Muitas organizações estão medindo agora o tipo de Disponibilidade e de indisponibilidade. O tipo de interrupção pode incluir hardware, software, enlace/portadora, energia/ambiente, projeto ou erro de usuário/processo. Identificando indisponibilidade e executando a análise de causa de raiz imediatamente depois da recuperação, a organização pode identificar métodos para melhorar a Disponibilidade. Quase todas as redes que conseguiram a Alta disponibilidade têm algum processo da melhoria de qualidade.

Apêndice A - Liberações da Visão Geral do IOS Cisco

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 distribuição precoce (ED)
- Versão principal
- Liberação limitada da distribuição (LD)
- Versão de distribuição geral (GD)

Cisco cria e mantém um mapa de caminhos de IOS que tenha a informação sobre liberações individuais, mercados de destino, caminhos de migração, descrições dos novos recursos, e assim por diante.

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

Versões da ED

As versões da ED do Cisco IOS são os veículos que trazem a novidade ao mercado. Cada revisão de manutenção de uma versão da ED inclui não somente correções de bug, mas igualmente um grupo de novos recursos, o suporte a plataforma novo, e os aprimoramentos gerais aos protocolos e à infraestrutura Cisco IOS. Cada um a dois anos, as características e as Plataformas das versões da ED são movidos ao Cisco IOS Release seguinte do mainline.

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

- **Liberações do Consolidated Technology Early Deployment (CTED)** — O modelo de versão do Novo Cisco IOS usa o trem de versão ED consolidado, igualmente conhecido como o trem “T”, para introduzir novos recursos, plataformas de hardware novas, e outros realces ao Cisco

IOS. São chamados tecnologia consolidada porque transcendem as definições internas das unidades de negócio (BU) e da linha de negócios (GROSSEIRÃO). Os exemplos das versões tecnológicas consolidadas são Cisco IOS 11.3t, 12.0T, e 12.1T.

- **Liberações do Specific Technology Early Deployment (STED)** — As versões STED têm características similares do comprometimento da característica como versões de cted salvo que visam um teatro específico da tecnologia ou do 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. Os exemplos das versões STED são o Cisco IOS 11.3NA, 11.3MA, 11.3WA, e 12.0DA.
- **Liberações do Specific Market Early Deployment (S ED)** — O Cisco IOS S ED é diferenciado dos STED pelo fato de que visa um segmento de mercado vertical específico (ISP, empresas, instituições financeiras, empresas de Telcom, e assim por diante). Os S ED incluem requisitos de recurso específicos da tecnologia somente para as plataformas de relevância específicas utilizadas pelo mercado vertical pretendido. Podem ser diferenciados dos CTED pelo fato de que estão construídos somente para plataformas de relevância específicas ao mercado vertical, visto que os CTED seriam construídos para mais Plataformas baseadas em um requisito de tecnologia mais largo. As liberações do Cisco IOS S ED são identificadas por um caractere alfabético adicionado ao lançamento de versão principal (apenas como o CTED). Os exemplos dos S ED são Cisco IOS 12.0S e 12.1E.
- **As breves versões de distribuição precoce, igualmente conhecidas como X liberam-se (XED)** — liberações do IOS XED Cisco introduzem o hardware novo e as Tecnologias ao mercado. Elas não fornecem revisões de manutenção de software nem revisões temporárias de software regular. Se um defeito é encontrado no XED antes de sua convergência com o CTED, um software reconstruído está iniciado e um número é adicionado ao nome. Por exemplo, os Cisco IOS Releases 12.0(2)XB1 e 12.0(2)XB2 são exemplos das reconstruções 12.0(2)XB.

Versões principal

As versões principal são os veículos de distribuição principais para o Produtos de Cisco IOS Software. 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 versões principal de IOS Cisco procuram a maiores estabilidade e qualidade. Por essa razão, as versões principal não aceitam a adição de características ou de Plataformas. Cada revisão de manutenção fornece correções de bug somente. Por exemplo, os Cisco IOS Software Releases 12.1 e 12.2 são versões principal.

As versões principal têm as atualizações de manutenção agendada chamadas as versões de manutenção que são inteiramente regressão testada, incorporam as correções de bug as mais recentes, e não apoiam nenhuma Plataformas ou característica nova. 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 são o número da versão principal, e 7 é seu nível da manutenção. O número de versão completo 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.

Liberações da distribuição limitada (LD)

O LD é a fase de maturidade do Cisco IOS entre o FCS e o General Deployment para versões principal. As versões da ED do Cisco IOS vivem somente na fase de distribuição limitada porque nunca alcançam a certificação GD.

Liberações do general deployment (GD)

A dada altura durante o ciclo de vida da versão, Cisco declarará uma versão principal para estar 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 liberação sobre as quatro versões de manutenção precedentes.

Uma equipe cruz-funcional da certificação da defesa de cliente GD composta de coordenadores TAC, de coordenadores do Advanced Engineering Services (AES), de engenharia de teste de sistema, e do planejamento do Cisco IOS é formada para avaliar cada defeito considerável da liberação. 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 uma liberação é GD declarado; incorpora automaticamente a 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. As atualizações da manutenção subsequente para essa liberação são igualmente liberações GD. Por exemplo, o Cisco IOS Software Release 12.0 obteve a certificação GD em 12.0(8). Assim, os Cisco IOS Software Release 12.0(9), 12.0(10), são e assim por diante liberações GD.

Experimental ou imagens de diagnóstico

Experimental ou imagens de diagnóstico estão referidos às vezes como serviços especiais de engenharia e criados somente quando as questões de software críticas foram identificadas. Estas imagens não são parte do processo de liberação normal. As imagens nesta categoria são construções específicas do cliente projetadas ajudar a diagnosticar um problema, para testar uma correção de bug, ou para fornecer um reparo imediato. Um reparo imediato pode ser fornecido quando não é uma opção para esperar o ínterim ou a versão de manutenção seguinte. Experimental ou imagens de diagnóstico pode ser construído em toda a manutenção do software suportado ou versões temporárias incluir baixas de qualquer tipo de versão. Nenhuma convenção de nomenclatura oficial existe, mas em muitos casos o colaborador adicionará iniciais, exp (para experimental), ou dígitos adicionais ao nome da imagem de 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. Estas imagens não se submetem a nenhum teste interno de Cisco.

Marcos de ciclos de vida das versões

Em algum momento, as liberações GD são substituídas por umas liberações mais novas com as Tecnologias de Rede as mais atrasadas. Portanto, um processo de retirada de versão foi estabelecido com os seguintes três marcos principais:

- **Fim das vendas (EOS)** — Para versões principal, a data EOS é três anos após a data do First Commercial Shipment (FCS). Isto ajusta uma data final para que a liberação pode ser comprada para sistemas novos. 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 liberação EOE é a última versão de manutenção para a liberação GD, e segue tipicamente aproximadamente três meses depois que a liberação EOS. Os clientes podem continuar a receber o Suporte técnico do tac Cisco, assim como transferem a liberação 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 tempo, os clientes devem começar a investigar o melhoramento de seu Cisco IOS Software para aproveitar-se das Tecnologias de Rede as mais atrasadas.
- **Fim da vida (EOL)** — Na extremidade do ciclo de vida da versão, todo o apoio para o Cisco IOS Software Release é terminado e já não disponível para transferir na data EOL. Geralmente, a data EOL é cinco anos após a data EOE. Um boletim de produto EOL é publicado aproximadamente um ano antes da data real EOL.

Convenção de nomeação 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 inclui sempre 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 como segue:

Seção da convenção de nomeação	Explicação
x.y	Uma combinação de dois (um ou dois) identificadores de dígito separados separados pelo “.” isso identifica o valor da versão principal. Este valor é determinado pelo mercado do Cisco IOS. Exemplo: 12.1
z	Um a três dígitos que identifica a versão de manutenção de x.y. Isto ocorre 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 reconstrução 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)
A	Uma a três letras alfa são o designador do trem de versão e são imperativas para liberações CTED, STED, e X. Igualmente identifica uma família de produto 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)`"X" na primeira posição do nome de versão identifica uma versão de uma vez baseada no trem CTED "T". Por exemplo, XA, XB, XC, e assim por diante. Um "x" ou "Y" na segunda posição do nome de versão identificam uma versão de ED de vida curta baseada sobre, 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 a placa se não que representa uma reconstrução. Começos com 1, então 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 - Confiança do Cisco IOS

A confiança do Cisco IOS é uma área onde Cisco se esforce continuamente para melhorar. Antes de discutir melhores prática orientado ao cliente, alguma compreensão da qualidade IOS interna Cisco e os esforços de confiabilidade são precisados. 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

Cisco tem um processo de desenvolvimento bem definido IO chamado metodologia da engenharia de GEMA grande (GEMA). Este processo tem um ciclo de vida trifásico:

- Estratégia e planejamento
- Execução
- Desenvolvimento

As áreas gerais dentro do ciclo de vida incluem a prioridade da introdução da característica, o desenvolvimento, o processo testando, as fases da introdução de software, o primeiro cliente enviado (FCS), o GD, e a engenharia de sustentação. Cisco igualmente segue um número de diretrizes de práticas recomendadas da qualidade de software das organizações tais como a organização internacional de padronização (ISO), o Telcordia (anteriormente Bellcore), a IEEE e o instituto da engenharia de Software do Carnegie Mellon. Estas diretrizes são incorporadas em processos da GEMA de Cisco. Os processos de desenvolvimento do software Cisco são ISO 9001 (1994) certificado.

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 cruz-de organização que seja comprometida a melhorar a qualidade de software conduz este processo. Um diagrama do processo da melhoria de qualidade do Cisco IOS é mostrado abaixo:

O processo da melhoria de qualidade tem meta mensuráveis distinta para o FY2002 e além. 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 endereçar estas áreas incluem as ferramentas novas da cobertura do teste (que identificam áreas da cobertura mais fraca do teste), a melhoria de processo da ação corretiva do teste, e do sistema do Cisco IOS realces do teste de regressão. Os recursos adicionais foram aplicados para endereçar estas edições e há um comprometimento executivo e cruz-funcional para todos os Cisco IOS Software Release preliminares.

Teste do Cisco IOS Release

Uma parte integral do esforço de qualidade da confiabilidade de software dentro de Cisco é a qualidade, o espaço, e a cobertura dos testes. Total, Cisco tem os seguintes objetivos de qualidade IO:

- Reduzir defeitos de regressão internos Cisco encontrados. Isto inclui mais de alta qualidade durante o processo de desenvolvimento e a identificação de mais problemas na estática/análise dinâmica.
- Reduza defeitos encontrados cliente
- Reduzir o total de defeitos
- Aumente a claridade do software release e a consistência da característica
- Forneça a característica e as versões de manutenção as programações e a qualidade

O teste interno de Cisco pode ser pensado como de um processo onde os defeitos diferentes sejam identificados em fases diferentes dos testes. O objetivo geral é encontrar os tipos direitos dos defeitos no laboratório direito. 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. Cisco tem diversos esforços nesta área para ajudar a melhorar a qualidade de software inicial. Os grupos do desenvolvimento igualmente executam revisões de código ou mesmo revisões de código múltiplas para assegurar-se de que outros colaboradores aprovem alterações de software ou código dos novos recursos.

A próxima fase é o teste da unidade. Os testes de unidade utilizam as ferramentas que examinam a interação de software sem o uso de um laboratório. DevTest é os testes de laboratório que incluem o teste de recurso/funcionalidade e o teste de regressão. O teste de recurso/funcionalidade é projetado examinar a funcionalidade de uma característica dada. 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 características, de Plataformas, de versões de software, e de topologias devido ao número máximo de trocas possíveis, porém sobre 4000 testes de regressão os scripts são utilizados hoje. O teste de integração é projetado expandir em laboratórios testando potencialidade para mais suite abrangente do Produtos e da Interoperabilidade. O teste de integração igualmente aumenta a cobertura do código de testes expandindo testes para incluir testes de interoperabilidade, esforço e testes de desempenho, testes de sistema, e teste negativo (eventos inesperados de teste).

A próxima fase de laboratório oferece testes ponta-a-ponta para os ambientes comuns do cliente. Estes são mostrados no diagrama acima como o financial test lab (FTL) e o NSITE, testes da encenação do cliente. O FTL foi construído para fornecer testes para a comunidade financeira de missão crítica. O NSITE é um grupo que forneça mais teste em profundidade para Tecnologias Cisco IOS diferentes. 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 utilidade centra-se sobre edições, o gerenciamento de evento/correlação e o Troubleshooting maiorias do abastecimento sob a carga. Outros laboratórios existem dentro de Cisco para que os mercados vertical diferentes ajudem a testar estas áreas.

O laboratório final exibido no diagrama acima é identificado como o laboratório do cliente. O teste de cliente é uma extensão do esforço de qualidade e recomendada para que os ambientes de alta disponibilidade assegurem-se de que a combinação exata de características, a configuração, as Plataformas, os módulos, e a topologia estejam testados inteiramente. 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 da maioria de métrica comum de confiabilidade total é o Mean Time Between Failure (MTBF). O MTBF para a confiabilidade de software é útil devido às potencialidades de análise que foram desenvolvidas para a confiabilidade de hardware usando o MTBF. A confiabilidade de hardware pode mais exatamente ser determinada usando alguns padrões existentes. Cisco utiliza

o método da contagem das peças baseado em dados padrão MTBF de Telcordia Technologies. O software MTBF, contudo, não tem nenhuma metodologia de análise correspondente e deve confiar na medição de campo para a análise de MTBF.

Para últimos três anos, Cisco executou medições de campo da confiabilidade de software para a rede interna de Cisco a TI e este trabalho é documentado dentro de 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 de software usando um modelo lognormal estatístico da distribuição para os software release identificados. O tempo médio ao reparo (MTTR) da falha de software é reinício e tempo de recuperação em média baseados do roteador. Seis tempos de recuperação minutos são usados para ambientes de empreendimento e quinze minutos são usados para os provedores de serviço da Internet maiores (ISP). O resultado deste estudo em curso é que o software encontra geralmente a Disponibilidade fina dos nines quando liberado, ou após algumas versões de manutenção, e é mesmo mais alto ao longo do tempo, como medido usar o software forçado causa um crash como o único origem de tempo ocioso. 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 esta métrica é usada em esforços da melhoria de qualidade, pode ajudar a melhorar a taxa de impactos forçados software mas pode ignorar outras áreas crítica da confiabilidade de software. Esse comentário permanece sem resposta devido à dificuldade em prever de forma precisa a confiança do software utilizando uma metodologia estatística. Os profissionais de estatística qualificados do software Cisco concluíram que um grupo maior da amostra de dados exatos estaria precisado de prever confiantemente o MTBF do software usando uma escala mais larga de tipos da indisponibilidade. Adicionalmente, a análise estatística teórica seria difícil devido às variáveis tais como a complexidade de rede, a experiência do pessoal para resolver problemas relacionados do software, o projeto de rede, as características permitidas, e os processos de gerenciamento de software.

Neste tempo, nenhum trabalho da indústria foi terminado a prevê mais exatamente a confiabilidade de software com as medições de campo devido à dificuldade exatamente de recolher este tipo de dados sensíveis. Também, a maioria de clientes don? t quer a informação de disponibilidade de coleção Cisco diretamente do seu rede devido à natureza proprietária da Disponibilidade dos dados. Algumas organizações contudo recolhem dados na confiabilidade de software e Cisco incentiva organizações recolher o medidor em disponibilidade devido às indisponibilidade do software, e executar a análise de causa de raiz naquelas indisponibilidade. 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

Em consequência do feedback do cliente, os estudos dinâmicos executados pelo grupo de Tecnologias Cisco IOS e a análise da causa raiz executada pelos Serviços avançados de Cisco team, algumas suposições mais novas e os melhores prática foram formados que ajudam a melhorar a confiabilidade de 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. Cisco é sempre responsável para testar/que valida novos recursos e funcionalidade para assegurar-se de que trabalhem nos novos produtos. Cisco é igualmente responsável para que o teste de regressão assegure-se de que as versões de software novas sejam inversas - compatível. Contudo, Cisco não pode validar cada característica, topologia, e plataforma contra cada advertência potencial que um ambiente de cliente pode trazer carregar (idiossincrasias, carga, e perfis de tráfego do projeto). A Alta disponibilidade dos melhores prática para clientes inclui testes em uma topologia de lab desmoronada que imite a rede de produção usando características, o projeto, serviços, e o tráfego de aplicativo definidos cliente.

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 da versão Cisco foram a uma arquitetura da liberação do trem assegurar-se de que o software se amadurecesse sem novos recursos que estão sendo adicionados. Os clientes que exigem a Alta disponibilidade estão procurando um software mais maduro com as características que precisam agora. Umas trocas existem então entre a maturidade do software, requisitos de disponibilidade, e os driveres de negócios para novos recursos ou funcionalidade. Muitas organizações têm padrões ou diretrizes para maturidade aceitável. Algumas apenas aceitarão a quinta versão temporária de um train específico. Para outro, pode ser o nono ou 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 de software é igualmente um fator de quanto do código é testado e exercitado em um ambiente de produção. Enquanto a quantidade de plataformas de hardware e de módulos diferentes aumenta, a quantidade de código exercitada igualmente aumenta, que aumenta geralmente a exposição aos defeitos do 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 projeto, a configuração, os protocolos, e os fatores do módulo de hardware podem contribuir à quantidade de código que é exercitado e ao risco ou à exposição aumentada aos defeitos do 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 negócio recomendaram os projetos e as configurações que são testados mais completamente dentro de Cisco e utilizados mais extensamente por clientes. Os clientes igualmente começaram adotar melhores prática para que topologias e as configurações padrão modulares estandardizadas abaixem a quantidade de exposição não experimentada do código e melhorem a confiabilidade de software total. 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

Um outro fator da confiabilidade de software é Interoperabilidade entre versões e a quantidade completa de código que obtém exercitado com versões múltiplas. Enquanto a quantidade de versões de software aumenta, a quantidade de código exercitada igualmente aumenta, que aumenta então a exposição aos defeitos do software. O risco para confiabilidade aumenta quase

exponencialmente devido ao código adicional exercido com versões múltiplas. Reconhece-se agora que as organizações precisam de executar pelo menos umas diversas versões na rede para cobrir a característica e requisitos de plataforma específicos. 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 de software, o desenvolvimento Cisco executa o teste de regressão do software para assegurar-se de que as versões de software diferentes sejam compatíveis. Além, o código de software é mais modular e os módulos centrais são menos prováveis mudar significativamente ao longo do tempo entre versões. As operações da versão Cisco igualmente mudaram a quantidade de software disponível aos clientes enquanto as versões com defeitos conhecidos ou questões de interoperabilidade estão removidas rapidamente do CCO enquanto os defeitos estão encontrados.

Informações Relacionadas

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