

Gerenciamento de configuração: White Paper de práticas recomendadas

Índice

[Introdução](#)

[Fluxo de processo de alto nível para gerenciamento de configuração](#)

[Criar padrões](#)

[Controle e gerenciamento de versão de software](#)

[Padrões e gerenciamento de endereçamento de IP.](#)

[Convenções de nomenclatura e atribuições DNS/DHCP](#)

[Configuração padrão e descritores](#)

[Procedimentos de atualização da configuração](#)

[Modelos de solução](#)

[Documentação de manutenção](#)

[Dispositivo atual, link e inventário de usuário final](#)

[Sistema de controle de versão de configuração](#)

[Registro da configuração TACACS](#)

[Documentação de topologia de rede](#)

[Validação e auditoria de padrões](#)

[Verificações de integridade de configuração](#)

[Auditorias de dispositivo, protocolo e mídia](#)

[Revisão de padrões e documentação](#)

[Informações Relacionadas](#)

Introdução

O gerenciamento da configuração é um conjunto de processos e ferramentas que promovem a consistência da rede e controlam alterações na rede, além de fornecer documentação e visibilidades sempre atualizadas para a rede. Ao desenvolver e manter as práticas recomendadas de gerenciamento de configurações, pode-se esperar diversos benefícios, como uma disponibilidade de rede melhorada e custos mais baixos. Eles incluem:

- Abaixa os custos de suporte devido a uma diminuição nas questões de suporte reagente.
- Reduza custos de rede devido a ferramentas de controle de dispositivos, circuitos e usuários que identificam componentes de rede não usados.
- Melhoria na disponibilidade da rede devido à diminuição nos custos de suporte reativo e à melhoria no tempo para resolver problemas.

Temos observado os seguintes problemas resultantes da falta do gerenciamento de configurações:

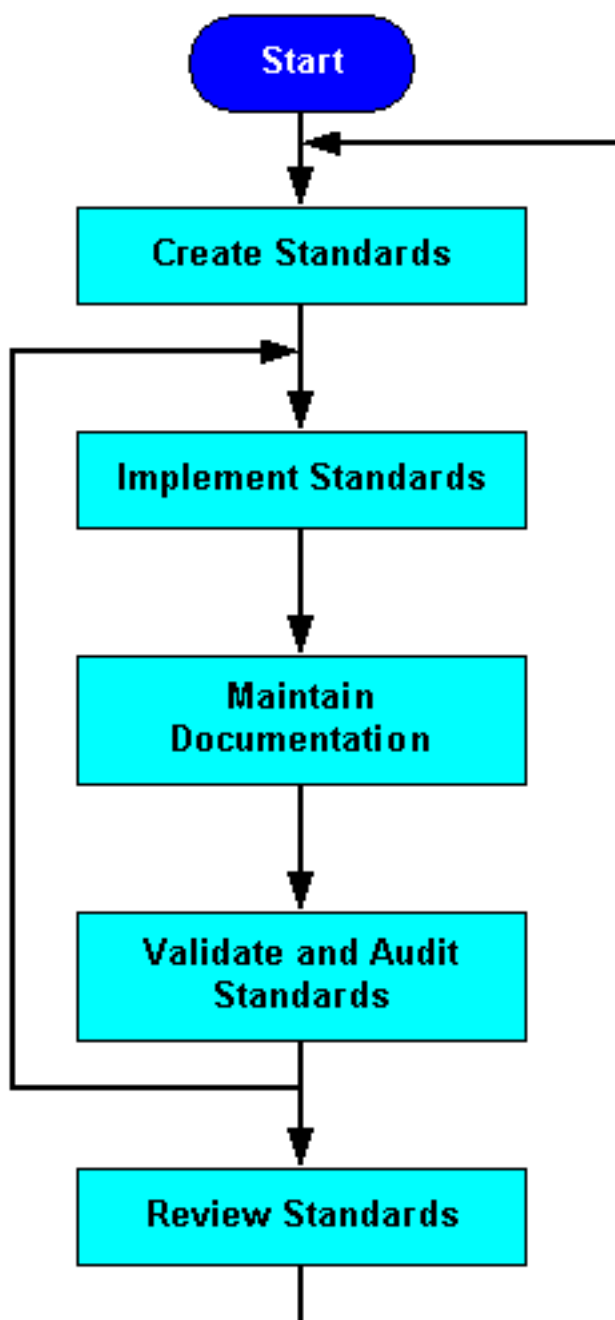
- Impossibilidade de determinar o impacto de usuários devido às alterações em rede

- Problemas de suporte reagente aumentados e disponibilidade mais baixa
- Tempo maior para solucionar problemas
- Custos de rede mais elevados devido aos componentes de rede não utilizados

Este documento da melhor prática fornece um fluxograma do processo de implementação de um plano de gerenciamento de configuração bem-sucedido. Analisaremos as seguintes etapas em detalhes: [Cria padrões](#), [mantém documentação](#) e valida e faz auditoria de padrões.

Fluxo de processo de alto nível para gerenciamento de configuração

O diagrama a seguir mostra como você pode usar os fatores críticos de sucesso seguidos pelos indicadores de desempenho para implementar um plano de gerenciamento de configuração bem-sucedido.



Criar padrões

Criando padrões para ajudas da consistência de rede reduza a complexidade de rede, a quantidade de tempo ocioso não planejado, e a exposição aos eventos de impacto da rede. Nós recomendamos os seguintes padrões para a consistência de rede ótima:

- [Controle de versão de software e Gerenciamento](#)
- [Padrões e gerenciamento de endereçamento de IP.](#)
- [Convenções de nomeação e atribuições de Domain Name System/Dynamic Host Configuration Protocol \(DNS/DHCP\)](#)
- [Configurações e descritores padrão](#)
- [Procedimentos de atualização da configuração](#)
- [Moldes de solução](#)

Controle e gerenciamento de versão de software

O controle das versões do software é a prática da implementação de versões de software consistentes em dispositivos de rede similares. Isso aumenta a chance de validação e testes nas versões de software escolhida e limita amplamente a quantidade de defeitos de software e problemas de interoperabilidade encontrados na rede. As versões de software limitadas também reduzem o risco de comportamento inesperado com interfaces de usuário, comando ou saída de gerenciamento, comportamento de atualização e comportamento de recurso. Isto faz o ambiente menos complexo e mais fácil apoiar. Em geral, o controle da versão do software melhora a disponibilidade da rede e ajuda a diminuir os custos de suporte reagente.

Nota: Os dispositivos de rede similares são definidos como dispositivos da rede padrão com um chassi comum que proporciona um serviço comum.

Siga os seguintes passos para controlar a versão do software:

- Determine as classificações do dispositivo com base nos requisitos de chassi, estabilidade e novos recursos.
- Versões de software individual de destino de dispositivos semelhantes.
- Teste, valide e pilote as versões de software escolhidas.
- As versões bem-sucedidas de documentos como padrão para classificação de dispositivos semelhantes.
- Implemente ou atualize consistentemente todos os dispositivos similares para a versão de software padrão.

Padrões e gerenciamento de endereçamento de IP.

O gerenciamento de endereço IP é o processo de alocação, reciclagem e documentação de endereços IP e sub-redes em uma rede. Os padrões do endereçamento de IP definem o tamanho de sub-rede, a atribuição de subrede, as atribuições de dispositivo de rede e as atribuições de endereço dinâmico dentro de um intervalo de sub-rede. Os padrões de gerenciamento de endereço IP recomendados reduzem a oportunidade de sobreposição ou duplicação de sub-redes, não resumo na rede, atribuição de endereço IP duplicado a dispositivos, desperdício de espaço de endereço IP e complexidade desnecessária.

A primeira etapa para um gerenciamento bem-sucedido do endereço IP é compreender os blocos de endereços IP usados na rede. Em muitos casos, as organizações de rede têm que confiar no espaço de endereços do [RFC 1918](#), que não é Internet endereçável, mas podem ser usadas para alcançar a rede conjuntamente com o [Network Address Translation \(NAT\)](#). Depois que os blocos de endereço tiverem sido definidos, aloque-os para áreas da rede de uma maneira que promova a sumarização. Em muitos casos, você terá que mais subdividir estes blocos baseados no número e no tamanho das sub-redes dentro da escala definida. Você deve definir os tamanhos de sub-rede padrão para aplicações padrão, como tamanhos de sub-rede de edifícios, tamanhos de sub-rede de link WAN, tamanhos de sub-rede de loopback ou tamanhos de sub-rede de site WAN. Você pode então alocar sub-redes para novos aplicativos fora de um bloco de sub-redes dentro de um bloco de resumo maior.

Por exemplo, vamos considerar uma rede empresarial de grande porte com um campus na costa leste, um campus na costa oeste, uma WAN doméstica, uma WAN européia e outros locais internacionais importantes. A organização aloca Contiguous IP Classless Interdomain Routing (CIDR) Blocks a cada uma dessas áreas para promover o resumo IP. A organização então define os tamanhos de sub-rede dentro daqueles blocos e atribui subseções de cada bloco a um tamanho de sub-rede particular IP. Cada bloco principal ou o espaço de endereços IP inteiro podem ser documentados em sub-redes atribuídas, usadas, e disponíveis de uma exibição da planilha para cada tamanho de sub-rede disponível dentro do bloco.

O próximo passo é criar padrões para as atribuições de endereço IP dentro de cada faixa de sub-rede. Aos roteadores e endereços virtuais Hot Standby Router Protocol (HSRP) dentro de uma sub-rede podem ser atribuídos aos primeiros endereços disponíveis dentro da faixa. É possível atribuir aos Switches e gateways os próximos endereços disponíveis, seguidos por outros endereços fixos e, por fim, por endereços dinâmicos para DHCP. Por exemplo, todas as sub-redes de usuário podem ser sub-redes de /24 com 253 atribuições de endereço disponível. O Roteadores pode ser atribuído o .1 e .2 endereço, e o endereço hsrp atribuiu o .3 endereço, o Switches .5 a .9, e a escala de .10 a .253 DHCP. Todos os padrões que você desenvolver deverão ser documentados e citados em todos os documentos do plano de engenharia de rede para ajudar a garantir uma implantação consistente.

Convenções de nomenclatura e atribuições DNS/DHCP

O uso consistente e estruturado de convenções de nomenclatura e do DNS para dispositivos o ajuda a gerenciar a rede das seguintes maneiras:

- Cria um ponto de acesso consistente para roteadores de todas as informações de gerenciamento de rede relacionadas a um dispositivo.
- Reduz a oportunidade para endereços IP duplicados.
- Cria identificação simples de um dispositivo mostrando localização, tipo de dispositivo e finalidade.
- Melhora o gerenciamento de inventários fornecendo um método simplificado de identificação de dispositivos de rede.

A maioria dos dispositivos de rede tem uma ou duas interfaces para o gerenciamento do dispositivo. Estas podem ser uma em-faixa ou os Ethernet out-of-band conectam e uma interface de console. Você deve criar convenções de nomenclatura para essas interfaces relacionadas ao tipo de dispositivo, ao local e ao tipo de interface. No Roteadores, nós recomendamos fortemente usar a interface de loopback como a interface de gerenciamento principal porque pode ser alcançada das relações diferentes. Você deve igualmente configurar interfaces de loopback como o endereço IP de origem para armadilhas, SNMP e mensagens do syslog. As interfaces

individuais podem então ter uma convenção de nomeação que identifique o dispositivo, o lugar, a finalidade, e a relação.

Também recomendamos a identificação das faixas DHCP e a inclusão das mesmas no DNS, incluindo o local dos usuários. Esta pode ser uma parcela do endereço IP de Um ou Mais Servidores Cisco ICM NT ou de um local físico. Um exemplo pôde ser "dhcp-bldg-c21-10" ao "dhcp-bldg-c21-253", que identifica endereços IP de Um ou Mais Servidores Cisco ICM NT no C da construção, segundo andar, o armário de fiação 1. Você também pode usar a sub-rede precisa para identificação. Uma vez que uma convenção de nomeação foi criada para dispositivos e DHCP, você precisa ferramentas de seguir e controlar entradas, tais como o [Cisco Network Registrar](#).

Configuração padrão e descritores

A configuração padrão aplica-se às configurações de protocolo e mídia, além dos comandos de configuração global. Os descritores são os comandos de uma interface usados para descrevê-la.

Nós recomendamos criar configurações padrão para cada classificação do dispositivo, tal como o roteador, o switch LAN, o switch WAN, ou o switch ATM. Cada configuração padrão deve conter o global, os media, e os comandos de configuração de protocolo necessários manter a consistência de rede. A configuração de mídia inclui a configuração ATM, de Frame Relay, ou de Fast Ethernet. A configuração do protocolo inclui os parâmetros de configuração do IP Routing Protocol, configurações de QoS, listas de acesso comuns e outras configurações de protocolo necessárias. Os comandos de configuração global são aplicáveis a todos os dispositivos semelhantes e incluem parâmetros como, por exemplo, comandos de serviços, comandos de IP, comandos TACACS, configuração vty, banners, configuração de SNMP e configuração de NTP (Network Time Protocol).

Os descritores são desenvolvidos criando um formato padrão que se aplique a cada relação. O descritor inclui a finalidade e o lugar da relação, os outros dispositivos ou os lugar conectados à relação, e os identificadores de circuito. Os descritores ajudam sua organização de suporte a compreender melhor o escopo dos problemas relacionados a uma interface e permitem uma solução de problemas mais rápida.

Recomendamos manter os parâmetros da configuração padrão em um arquivo de configuração padrão e fazer o download do arquivo para cada novo dispositivo antes da configuração de protocolo e interface. Além, você deve documentar o arquivo de configuração padrão, incluindo uma explicação de cada parâmetro de configuração global e porque é importante. [O Cisco Resource Manager Essentials \(RME\) pode ser usado para gerenciar arquivos de configuração padrão, configuração de protocolo e descritores.](#)

Procedimentos de atualização da configuração

Os procedimentos de upgrade ajudam a assegurar-se de que as upgrades de software e de hardware ocorram lisamente com tempo ocioso mínimo. Os procedimentos de upgrade incluem a verificação de fornecedor, referências da instalação do vendedor tais como Release Note, metodologias ou etapas da elevação, diretrizes de configuração, e requisitos de teste.

Procedimentos de atualização podem variar consideravelmente dependendo dos tipos de rede, tipos de dispositivo ou novos requisitos de software. Os requisitos de upgrade do roteador individual ou do interruptor podem ser desenvolvidos e testado dentro de um grupo da arquitetura e ser providos em toda a documentação da mudança. Outras atualizações envolvendo redes

inteiras não podem ser testadas tão facilmente. Essas atualizações podem exigir um planejamento mais profundo, envolvimento do fornecedor e etapas adicionais para garantir o sucesso.

Você deve criar ou procedimentos de upgrade da atualização conjuntamente com toda a distribuição de software nova ou versão padrão identificada. Os procedimentos devem definir todos os passos para a atualização, consultar a documentação do fornecedor relacionado à atualização do dispositivo e fornecer procedimentos de teste para validar o dispositivo após a atualização. Uma vez definidos e validados os procedimentos de atualização, o procedimento de atualização deve ser mencionado em toda a documentação de alteração adequada à atualização específica.

Modelos de solução

É possível usar modelos de solução para definir soluções de rede modulares padrão. Um módulo de rede pode ser um Wiring Closet, um escritório de campo de WAN ou um concentrador de acessos. Em cada caso, é necessário definir, testar e documentar a solução para ajudar a garantir que distribuições semelhantes possam ser realizadas exatamente da mesma maneira. Assim você garante que futuras alterações ocorram em um nível muito menor de risco para a organização já que o comportamento da solução é bem definido.

Crie moldes de solução para todas as disposições e soluções mais de alto risco que serão distribuídas mais de uma vez. O modelo de solução contém todos os requisitos padrão de hardware, software, configuração, cabeamento e instalação para a solução de rede. Os detalhes específicos do molde da solução são mostrados a seguir:

- Hardware e módulos de hardware, incluindo memória, flash, energia e layouts de placas.
- Topologia lógica incluindo atribuições de porta, conectividade, velocidade e tipo de mídia.
- Versões de software que incluem versões de módulo ou firmware.
- Toda a configuração não padronizada, não dispositivo-específica que inclui protocolos de roteamento, configurações de mídia, configuração de VLAN, Listas de acesso, Segurança, trajetos de switching, medindo - parâmetros da árvore, e outro.
- Requisitos de gerenciamento out-of-band.
- Requisitos de cabo.
- Requisitos de instalação que incluem environmentais, potência, e lugar da cremalheira.

Observe que o modelo de solução não contém muitos requisitos. As exigências específicas tais como o endereçamento de IP para a solução, a nomeação, as atribuições DNS, as atribuições de DHCP, as atribuições PVC, os descritores da relação, e os outros específicos devem ser cobertos por práticas de gerenciamento da configuração total. Mais requisitos gerais, tais como configurações padrão, planos de gerenciamento de alteração, procedimentos de atualização de documentação, ou procedimentos da atualização de gerenciamento de rede, devem ser cobertos por práticas de gerenciamento da configuração geral.

Documentação de manutenção

Nós recomendamos documentar a rede e as mudanças que ocorreram na rede no tempo real próximo. É possível utilizar essas informações de rede precisas no Troubleshooting, listas de dispositivos de ferramentas de gerenciamento de rede, inventário, validação e auditorias. Recomendamos o uso dos seguintes fatores de sucesso críticos da documentação de rede:

- [Dispositivo, link, e inventário de usuário final atuais](#)

- [Sistema de controle de versão de configuração](#)
- [Log da configuração de TACACS](#)
- [Documentação de topologia de rede](#)

[Dispositivo atual, link e inventário de usuário final](#)

O dispositivo, o link, e a informação atuais do inventário de usuário final permitem-no de seguir o Inventário de redes e os recursos, o impacto do problema, e o impacto da alteração de rede. A capacidade para seguir o Inventário de redes e os recursos com relação às ajudas das requisições de usuário asseguram-se de que os dispositivos da rede gerenciada estejam usados ativamente, fornecem-se a informação necessária para auditorias, e ajudam-se a controlar recursos de dispositivo. Os dados de relacionamento do usuário final fornecem informações que definem o risco da alteração e o impacto, assim como a capacidade de solucionar problemas mais rapidamente. Os bancos de dados de dispositivo, enlace e inventário de usuário final são normalmente desenvolvidos por muitas organizações provedoras de serviço líderes. O desenvolvedor líder do software do Inventário de redes é [Visionael corporation](#) . [O banco de dados pode conter tabelas de dispositivos, links e dados de usuário/servidor de clientes de modo que, quando um dispositivo estiver inativo ou ocorrer alteração na rede, você poderá entender facilmente o impacto no usuário final.](#)

[Sistema de controle de versão de configuração](#)

Um sistema de controle de versões de configuração mantém as atuais configurações em execução de todos os dispositivos e um número definido de versões anteriores em execução. Essas informações podem ser usadas para Troubleshooting e em auditorias de configuração ou alteração. Ao Troubleshoot, você pode comparar a configuração atualmente em execução com as versões de trabalho anteriores para entender se a configuração está vinculada ao problema de algum modo. Recomendamos a manutenção de três a cinco versões de trabalho anteriores da configuração.

[Registro da configuração TACACS](#)

Para identificar quem fez alterações de configuração e quando, é possível utilizar o registro de TACACS e o NTP. Quando esses serviços estão habilitados nos dispositivos de rede Cisco, a identificação de usuário e o rótulo de tempo são adicionados ao arquivo de configuração no momento em que a alteração de configuração é feita. Este selo é copiado então com o arquivo de configuração ao sistema de controle de versão de configuração. TACACS pode então atuar como um dissuasor de alterações não gerenciadas e fornece um mecanismo para executar uma auditoria adequada das alterações ocorridas. O TACACS é habilitado com o produto Cisco Secure. Quando o usuário se registra no dispositivo, ele/ela deve fazer autenticar com o servidor TACACS fornecendo uma ID de usuário e senha. O NTP é permitido facilmente em um dispositivo de rede apontando o dispositivo a um relógio mestre NTP.

[Documentação de topologia de rede](#)

A documentação da topologia ajuda na compreensão e suporte da rede. Você pode usá-la para validar orientações de design e compreender melhor a rede para design, alterações ou Troubleshooting futuros. A documentação de topologia deve abranger a documentação lógica e física, incluindo conectividade, endereçamento, tipos de mídia, dispositivos, disposição de racks, atribuição de placas, roteamento de cabos, identificação de cabos, pontos de terminação, informações sobre energia e informações de identificação de circuito.

A manutenção da documentação da topologia é a chave para um gerenciamento de configuração bem-sucedido. Para criar um ambiente onde a manutenção da documentação de topologia possa ocorrer, a importância da documentação deve ser forçada e a informação deve estar disponível para atualizações. É altamente recomendável atualizar a documentação de topologia sempre que houver alterações na rede.

A documentação de topologia de rede é mantida tipicamente usando um aplicativo gráfico como [Microsoft Visio](#). [O outro Produtos como Visionael](#) fornece capacidades superiores controlando a informação de topologia.

Validação e auditoria de padrões

Os indicadores de desempenho do gerenciamento de configuração oferecem um mecanismo para validar e analisar os padrões de configuração de rede e os principais fatores de sucesso. Executando um programa de melhoria de processo para o gerenciamento de configuração, você pode usar os indicadores de desempenho para identificar edições da consistência e para melhorar o Gerenciamento de configuração total.

É recomendável criar uma equipe funcional para avaliar o êxito do gerenciamento de configuração e melhorar os processos de gerenciamento de configuração. O primeiro objetivo da equipe é implementar indicadores de desempenho de gerenciamento a fim de identificar os problemas de gerenciamento de configuração. Iremos discutir detalhadamente os seguintes indicadores de desempenho do gerenciamento de configuração:

- [Verificações de integridade de configuração](#)
- [Auditorias de dispositivo, protocolo e mídia](#)
- [Padrões e revisão de documentação](#)

Após avaliar os resultados dessas auditorias, inicie um projeto para corrigir inconsistências e, em seguida, determine a causa inicial do problema. As causas potenciais incluem uma falta da documentação de padrões ou uma falta de um processo consistente. Você pode melhorar a documentação de padrões, executar o treinamento, ou melhorar processos para impedir uma inconsistência de configuração mais adicional.

Recomendamos auditorias mensais ou trimestrais, caso somente a validação seja necessária. Revise auditorias anteriores para confirmar se os problemas anteriores estão resolvidos. Procure melhorias total e objetivos para demonstrar o progresso e o valor. Crie o medidor para mostrar a quantidade de alto risco, de media-risco, e de inconsistências de baixo-risco da configuração de rede.

Verificações de integridade de configuração

A verificação de integridade da configuração deverá avaliar a configuração geral da rede, sua complexidade e consistência e problemas potenciais. [Para redes Cisco, recomendamos o uso da ferramenta de validação de configuração Netsys](#). Esta ferramenta entra todas as configurações de dispositivo e cria uns relatórios de configuração que identifiquem problemas atual tais como endereços de IP duplicados, incompatibilidades de protocolo, e inconsistência. A ferramenta relata qualquer tipo de problema de conectividade ou protocolo, mas não introduz configurações padrão para avaliação em cada dispositivo. É possível revisar manualmente os padrões de configuração ou criar um script que relate diferenças na configuração padrão.

Auditorias de dispositivo, protocolo e mídia

O dispositivo, o protocolo, e as auditorias dos media são um indicador de desempenho para a consistência nas versões de software, dispositivos de hardware e módulos, protocolo e media, e convenções de nomeação. Os exames devem primeiramente identificar questões não-padrão, o que deve levar a atualizações de configuração para reparar ou melhorar essas questões. Avalie os processos gerais para determinar como eles devem impedir a ocorrência de implantações otimizadas sem se preocupar com o objetivo geral e de implantações não padrão.

[Cisco RME](#) é uma ferramenta de gerenciamento de configuração que possa examinar e relatar em versões de hardware, em módulos e em versões de software. A Cisco também está desenvolvendo auditorias de mídia e protocolos abrangentes que relatarão a inconsistência com o IP, DLSW, Frame Relay e ATM. Se um protocolo ou auditoria de mídia não for desenvolvido, você pode usar as auditorias manuais, como dispositivos de revisão, versões e configurações de todos os dispositivos semelhantes de uma rede, ou detectar dispositivos de verificação, versões e configurações.

[Revisão de padrões e documentação](#)

Esse indicador de desempenho examina a documentação sobre a rede e sobre os padrões para garantir que as informações estejam precisas e atualizadas. A auditoria pode incluir a revisão da documentação atual, a recomendação de alterações ou adições e a aprovação de novos padrões.

Você deve revisar a seguinte documentação a cada três meses: definições padrão de configuração, moldes de soluções, incluindo configurações recomendadas de hardware, versões atuais de software padrão, procedimentos de atualização para todos os dispositivos e versões de software, documentação de topologia, moldes atuais e gerenciamento de endereços IP.

[Informações Relacionadas](#)

- [Suporte Técnico - Cisco Systems](#)