

Gerenciamento de configuração: White paper de práticas recomendadas

Contents

[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:

- Reduza os custos de suporte devido a uma diminuição nos problemas de suporte reativo.
- 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. Examinaremos as seguintes etapas em detalhes: [criar padrões](#), [manter a documentação](#) e [validar e auditar 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

A criação de padrões para a consistência da rede ajuda a reduzir a complexidade da rede, o tempo de inatividade não planejado e a exposição a eventos com impacto na rede. Recomendamos os seguintes padrões para a consistência ideal da rede:

- [Controle e gerenciamento de versão de software](#)
- [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](#)
- [Modelos 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. Isso torna o ambiente menos complexo e mais fácil de suportar. Em geral, o controle da versão do software

melhora a disponibilidade da rede e ajuda a diminuir os custos de suporte reagente.

Observação: dispositivos de rede semelhantes são definidos como dispositivos de rede padrão com um chassi comum que fornece 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 de endereçamento IP definem o tamanho da sub-rede, a atribuição de sub-rede, as atribuições de dispositivos de rede e as atribuições de endereços dinâmicos em 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 endereço [RFC 1918](#), que não é endereçável pela Internet, mas pode ser usado para acessar a rede em conjunto com a [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 subdividir ainda mais esses blocos com base no número e tamanho das sub-redes dentro do intervalo definido. 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. Em seguida, a organização define os tamanhos de sub-rede dentro desses blocos e aloca subseções de cada bloco para um tamanho de sub-rede IP específico. Cada bloco principal ou todo o espaço de endereço IP pode

ser documentado em uma planilha que mostra sub-redes alocadas, usadas e disponíveis 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 usuários podem ser sub-redes /24 com 253 atribuições de endereço disponíveis. Os roteadores podem ficar com os endereços .1 e .2, o endereço de HSRP pode ficar com o endereço .3, os Switches com os endereços .5 a .9 e o DHCP com o intervalo de .10 a .253. 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. Eles podem ser uma interface Ethernet dentro ou fora da banda 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. Nos roteadores, é altamente recomendável usar a interface de loopback como a interface de gerenciamento principal, pois ela pode ser acessada de diferentes interfaces. Você também deve configurar interfaces de loopback como o endereço IP origem para interceptações, SNMP e mensagens de syslog. As interfaces individuais podem ter uma convenção de nomenclatura que identifica o dispositivo, o local, a finalidade e a interface.

Também recomendamos a identificação das faixas DHCP e a inclusão das mesmas no DNS, incluindo o local dos usuários. Pode ser uma parte do endereço IP ou um local físico. Um exemplo pode ser "dhcp-bldg-c21-10" a "dhcp-bldg-c21-253", que identifica endereços IP no prédio C, segundo andar, wiring closet 1. Você também pode usar a sub-rede precisa para identificação. Depois que uma convenção de nomenclatura tiver sido criada para dispositivos e DHCP, você precisará de ferramentas para rastrear e gerenciar entradas, 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.

We recommend creating standard configurations for each device classification, such as router, LAN Switch, WAN Switch, or ATM Switch. Cada configuração padrão deve conter os comandos de configuração global, de mídia e de protocolo necessários para manter a consistência da rede. A configuração de mídia inclui configuração ATM, Frame Relay ou 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 pela criação de um formato padrão que se aplica a cada interface. O descritor inclui a finalidade e o local da interface, outros dispositivos ou locais conectados à interface e 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 disso, você deve documentar o arquivo de configuração padrão, incluindo uma explicação de cada parâmetro de configuração global e por que ele é importante. [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 atualização ajudam a garantir que as atualizações de software e hardware ocorram sem problemas, com o mínimo de inatividade. Os procedimentos de atualização incluem verificação do fornecedor, referências de instalação do fornecedor, como notas de versão, metodologias ou etapas de atualização, 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. Individual router or Switch upgrade requirements may be developed and tested within an architecture group and referenced in any change documentation. 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 atualizar procedimentos de atualização em conjunto com qualquer nova implantação de software 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 modelos de solução para todas as implantações de maior risco e soluções que serão implantadas 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. O 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.
- Todas as configurações não padrão, não específicas de dispositivos, incluindo protocolos de roteamento, configurações de mídia, configuração de VLAN, listas de acesso, segurança, caminhos de switching, parâmetros de spanning tree e outros.
- Requisitos de gerenciamento fora da banda.
- Requisitos de cabo.
- Requisitos de instalação incluindo ambiente, energia e locais de rack.

Observe que o modelo de solução não contém muitos requisitos. Requisitos específicos, como endereçamento IP para a solução específica, nomeação, atribuições de DNS, atribuições de DHCP, atribuições de PVC, descritores de interface e outros, devem ser cobertos pelas práticas gerais de gerenciamento de configuração. Requisitos mais gerais, como configurações padrão, planos de gerenciamento de alterações, procedimentos de atualização de documentação ou procedimentos de atualização de gerenciamento de rede, devem ser cobertos pelas práticas gerais de gerenciamento de configuração.

Documentação de manutenção

Recomendamos documentar a rede e as alterações que ocorreram na rede quase em tempo real. 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 atual, link e inventário de usuário final](#)
- [Sistema de controle de versão de configuração](#)

- [Registro da configuração TACACS](#)
- [Documentação de topologia de rede](#)

Dispositivo atual, link e inventário de usuário final

Informações atuais sobre dispositivos, links e inventário de usuários finais permitem que você rastreie o inventário e os recursos da rede, o impacto de problemas e o impacto de alterações na rede. A capacidade de rastrear o inventário e os recursos da rede em relação aos requisitos do usuário ajuda a garantir que os dispositivos de rede gerenciados sejam usados ativamente, fornece as informações necessárias para auditorias e ajuda a gerenciar os recursos do 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 principal desenvolvedor de software de inventário de rede é a [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. Esse carimbo é então copiado com o arquivo de configuração para o 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 autenticação com o servidor TACACS fornecendo uma ID de usuário e senha. O NTP é facilmente habilitado em um dispositivo de rede apontando o dispositivo para um relógio mestre de 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 da topologia possa ocorrer, a importância da documentação deve ser enfatizada e as informações devem estar disponíveis para atualizações. É altamente recomendável atualizar a documentação de topologia sempre que houver alterações na rede.

A documentação da topologia de rede é normalmente mantida usando-se um aplicativo gráfico como o [Microsoft Visio](#) . Outros produtos, como o [Visionael](#) , fornecem recursos superiores para gerenciar informações 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. Implementando um programa de aprimoramento de processo para gerenciamento de configuração, você pode usar os indicadores de desempenho para identificar problemas de consistência e melhorar o gerenciamento da configuração geral.

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](#)
- [Revisão de padrões e documentação](#)

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

Recomendamos auditorias mensais ou trimestrais, caso somente a validação seja necessária. Revise auditorias anteriores para confirmar se os problemas anteriores estão resolvidos. Procure melhorias e metas gerais para demonstrar o progresso e o valor. Crie métricas para mostrar a quantidade de inconsistências de configuração de rede de alto, médio e baixo risco.

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. Essa ferramenta insere todas as configurações do dispositivo e cria um relatório de configuração que identifica problemas atuais, como endereços 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

As auditorias de dispositivo, protocolo e mídia são um indicador de desempenho para consistência em versões de software, dispositivos e módulos de hardware, protocolo e mídia e convenções de nomenclatura. 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.

[O Cisco RME](#) é uma ferramenta de gerenciamento de configuração que pode auditar e gerar relatórios sobre versões de hardware, módulos e 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 trimestralmente: definições de configuração padrão, modelos de solução incluindo configurações de hardware recomendadas, versões de software padrão atuais, procedimentos de atualização para todos os dispositivos e versões de software, documentação de topologia, modelos atuais e gerenciamento de endereço IP.

Informações Relacionadas

- [Suporte Técnico - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.