

컨피그레이션 관리:모범 사례 백서

목차

[소개](#)

[구성 관리를 위한 상위 레벨 프로세스 흐름](#)

[표준 생성](#)

[소프트웨어 버전 제어 및 관리](#)

[IP 주소 지정 표준 및 관리](#)

[명명 규칙 및 DNS/DHCP 할당](#)

[표준 구성 및 설명자](#)

[구성 업그레이드 절차](#)

[솔루션 템플릿](#)

[문서 유지 관리](#)

[현재 디바이스, 링크 및 최종 사용자 인벤토리](#)

[구성 버전 제어 시스템](#)

[TACACS 컨피그레이션 로그](#)

[네트워크 토폴로지 문서](#)

[표준 검증 및 감사](#)

[구성 무결성 검사](#)

[장치, 프로토콜 및 미디어 감사](#)

[표준 및 문서 검토](#)

[관련 정보](#)

소개

구성 관리는 네트워크 일관성을 높이고 네트워크 변경을 추적하고 최신 네트워크 문서와 가시성을 제공하는 프로세스와 툴의 모음입니다. 컨피그레이션 관리 모범 사례를 구축하고 유지하면 네트워크 가용성 향상 및 비용 절감과 같은 여러 이점을 얻을 수 있습니다. 여기에는 다음이 포함됩니다.

- 사후 대응적 지원 문제 감소로 지원 비용 절감
- 사용하지 않는 네트워크 구성 요소를 식별하는 장치, 회로 및 사용자 추적 도구 및 프로세스로 인해 네트워크 비용이 절감됩니다.
- 사후 대응적 지원 비용이 감소하고 문제 해결 시간이 단축되어 네트워크 가용성이 향상되었습니다.

컨피그레이션 관리 부족으로 인해 다음과 같은 문제가 발생했습니다.

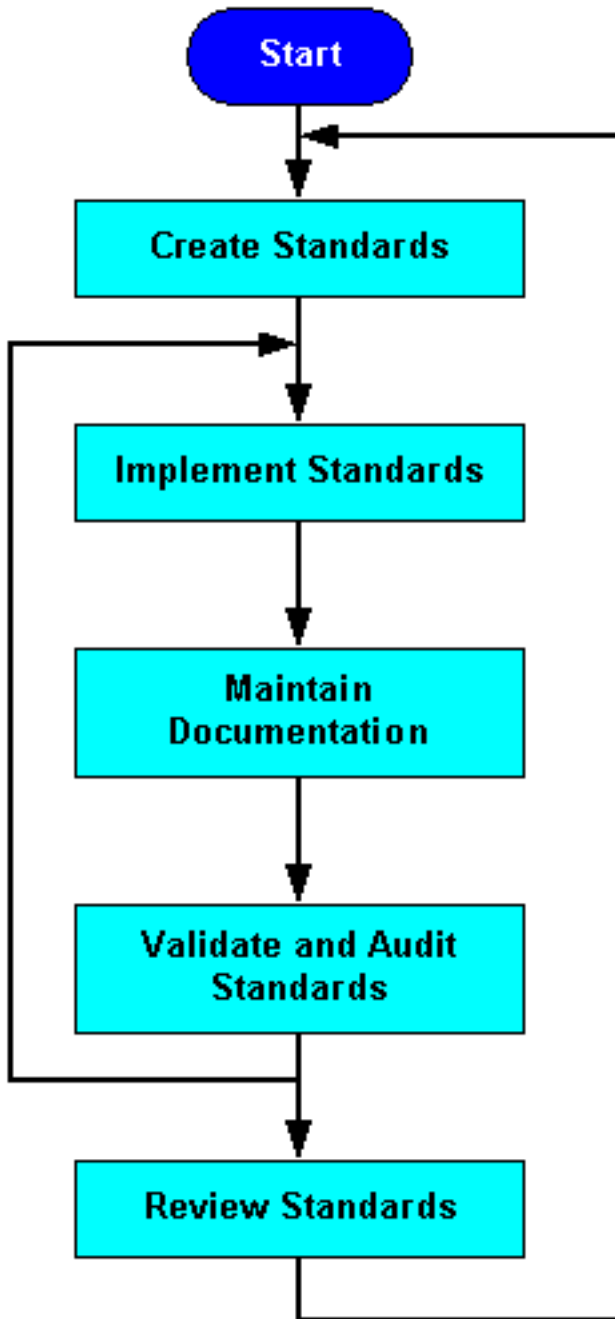
- 네트워크 변경으로 인한 사용자 영향을 확인할 수 없음
- 사후 대응적 지원 문제 증가 및 가용성 감소
- 문제 해결 시간 증가
- 사용하지 않는 네트워크 구성 요소로 인해 네트워크 비용 증가

이 모범 사례 문서에서는 성공적인 컨피그레이션 관리 계획을 구현하는 프로세스 흐름도를 제공합

니다. 다음 단계를 자세히 살펴보겠습니다. [표준 생성](#), 문서 [유지](#), [표준 검증 및 감사](#).

구성 관리를 위한 상위 레벨 프로세스 흐름

아래 다이어그램은 성공적인 컨피그레이션 관리 계획을 구현하기 위해 중요한 성공 요인을 사용하고 성과 지표를 사용하는 방법을 보여줍니다.



표준 생성

네트워크 일관성에 대한 표준을 만들면 네트워크 복잡성, 계획되지 않은 다운타임의 양, 네트워크에 영향을 미치는 이벤트에 대한 노출을 줄일 수 있습니다. 최적의 네트워크 일관성을 위해 다음 표준을 권장합니다.

- [소프트웨어 버전 제어 및 관리](#)
- [IP 주소 지정 표준 및 관리](#)
- [명명 규칙 및 DNS/DHCP\(Domain Name System/Dynamic Host Configuration Protocol\) 할당](#)
- [표준 구성 및 설명자](#)
- [구성 업그레이드 절차](#)
- [솔루션 템플릿](#)

[소프트웨어 버전 제어 및 관리](#)

소프트웨어 버전 제어는 유사한 네트워크 디바이스에 일관된 소프트웨어 버전을 구축하는 방식입니다. 이렇게 하면 선택한 소프트웨어 버전에 대한 검증 및 테스트 기회가 향상되고 네트워크에서 발견되는 소프트웨어 결함 및 상호 운용성 문제의 양이 크게 제한됩니다. 제한된 소프트웨어 버전은 사용자 인터페이스, 명령 또는 관리 출력, 업그레이드 동작 및 기능 동작으로 예기치 않은 동작의 위험을 줄입니다. 따라서 환경이 덜 복잡하고 지원하기가 쉬워집니다. 전반적으로 소프트웨어 버전 제어는 네트워크 가용성을 향상시키고 사후 대응적 지원 비용을 절감합니다.

참고: 유사한 네트워크 디바이스는 공통 서비스를 제공하는 공통 새시를 사용하는 표준 네트워크 디바이스로 정의됩니다.

소프트웨어 버전 제어를 위해 다음 단계를 구현합니다.

- 새시, 안정성 및 새로운 기능 요구 사항을 기준으로 장치 분류를 결정합니다.
- 유사한 디바이스의 개별 소프트웨어 버전을 대상으로 지정합니다.
- 선택한 소프트웨어 버전을 테스트, 검증 및 파일럿
- 유사 디바이스 분류를 위한 표준으로 성공적인 버전을 문서화합니다.
- 모든 유사한 디바이스를 표준 소프트웨어 버전으로 일관성 있게 구축 또는 업그레이드

[IP 주소 지정 표준 및 관리](#)

IP 주소 관리는 네트워크에서 IP 주소와 서브넷을 할당, 재활용 및 문서화하는 프로세스입니다. IP 주소 지정 표준은 서브넷 범위 내에서 서브넷 크기, 서브넷 할당, 네트워크 디바이스 할당 및 동적 주소 할당을 정의합니다. 권장 IP 주소 관리 표준은 중복 서브넷, 네트워크 비효율, 중복 IP 주소 디바이스 할당, IP 주소 공간 낭비, 불필요한 복잡성 등의 문제를 줄일 수 있습니다.

성공적인 IP 주소 관리를 위한 첫 번째 단계는 네트워크에서 사용되는 IP 주소 블록을 이해하는 것입니다. 대부분의 경우 네트워크 조직은 인터넷 주소를 지정할 수 없지만 [NAT\(Network Address Translation\)](#)와 함께 네트워크에 액세스하는 데 사용할 수 있는 [RFC 1918](#) 주소 공간을 사용해야 합니다. 주소 블록을 정의한 후에는 요약할 수 있는 방법으로 네트워크 영역에 해당 블록을 할당합니다. 대부분의 경우 정의된 범위 내의 서브넷 수와 크기에 따라 이러한 블록을 더 세분화해야 합니다. 표준 애플리케이션에 대한 표준 서브넷 크기를 정의해야 합니다. 예를 들어 서브넷 크기, WAN 링크 서브넷 크기, 루프백 서브넷 크기 또는 WAN 사이트 서브넷 크기 등이 있습니다. 그런 다음 더 큰 요약 블록 내의 서브넷 블록에서 새 애플리케이션에 대한 서브넷을 할당할 수 있습니다.

예를 들어, 동부 해안 캠퍼스, 서부 해안 캠퍼스, 국내 WAN, 유럽 WAN 및 기타 주요 국제 사이트가 있는 대규모 엔터프라이즈 네트워크를 예로 들어보겠습니다. 조직은 IP 요약을 촉진하기 위해 이러한 각 영역에 연속 IP CIDR(Classless Interdomain Routing) 블록을 할당합니다. 그런 다음 해당 블록 내의 서브넷 크기를 정의하고 각 블록의 하위 섹션을 특정 IP 서브넷 크기에 할당합니다. 각 주요 블록 또는 전체 IP 주소 공간은 블록 내에서 사용 가능한 각 서브넷 크기에 대해 할당, 사용 및 사용 가능한 서브넷을 보여 주는 스프레드시트에 문서화할 수 있습니다.

다음 단계는 각 서브넷 범위 내에서 IP 주소 할당에 대한 표준을 만드는 것입니다. 서브넷 내의 라우

터 및 HSRP(Hot Standby Router Protocol) 가상 주소에 범위 내에서 사용 가능한 첫 번째 주소가 할당될 수 있습니다.스위치와 게이트웨이에 사용 가능한 다음 주소를 할당할 수 있으며, 그 다음에 다른 고정 주소 할당, 마지막으로 DHCP를 위한 동적 주소가 할당됩니다.예를 들어, 모든 사용자 서브넷은 253개의 사용 가능한 주소 할당이 있는 /24 서브넷일 수 있습니다.라우터에는 .1 및 .2 주소가 할당될 수 있으며 HSRP 주소에는 .3 주소, 스위치 .5 ~ .9, DHCP 범위는 .10 ~ .253이 할당됩니다.어떤 표준을 개발하든 모든 네트워크 엔지니어링 계획 문서에서 이를 문서화하고 참조하여 일관성 있는 구축을 보장해야 합니다.

명명 규칙 및 DNS/DHCP 할당

명명 규칙 및 디바이스에 대한 DNS를 일관되고 구조적으로 사용하면 다음과 같은 방법으로 네트워크를 관리할 수 있습니다.

- 디바이스와 관련된 모든 네트워크 관리 정보에 대해 라우터에 대한 일관된 액세스 포인트를 생성합니다.
- 중복 IP 주소의 기회를 줄입니다.
- 위치, 디바이스 유형 및 용도를 표시하는 디바이스를 간단하게 식별합니다.
- 네트워크 장치를 식별하는 더 간단한 방법을 제공하여 인벤토리 관리를 향상시킵니다.

대부분의 네트워크 디바이스에는 디바이스를 관리하기 위한 인터페이스가 1개에서 2개 있습니다. 이는 대역 내 또는 대역 외 이더넷 인터페이스와 콘솔 인터페이스일 수 있습니다.디바이스 유형, 위치 및 인터페이스 유형과 관련된 이러한 인터페이스에 대한 명명 규칙을 작성해야 합니다.라우터에서는 루프백 인터페이스를 기본 관리 인터페이스로 사용하는 것이 좋습니다. 루프백 인터페이스는 다른 인터페이스에서 액세스할 수 있기 때문입니다.또한 트랩, SNMP 및 syslog 메시지에 대한 소스 IP 주소로 루프백 인터페이스를 구성해야 합니다.그러면 개별 인터페이스에는 디바이스, 위치, 용도 및 인터페이스를 식별하는 명명 규칙이 있을 수 있습니다.

또한 DHCP 범위를 식별하고 사용자 위치를 포함하여 DNS에 추가하는 것이 좋습니다.이는 IP 주소 또는 물리적 위치의 일부일 수 있습니다.예를 들어 "dhcp-bldg-c21-10"에서 "dhcp-bldg-c21-253"으로 지정할 수 있습니다. 이는 건물 C, 2층, 와이어링 클로짓 1에서 IP 주소를 식별합니다. 정확한 서브넷을 사용하여 식별할 수도 있습니다.디바이스 및 DHCP에 대한 명명 규칙이 생성되면 [Cisco Network Registrar](#)과 같은 항목을 추적하고 관리하는 툴이 필요합니다.

표준 구성 및 설명자

표준 컨피그레이션은 프로토콜 및 미디어 컨피그레이션과 전역 컨피그레이션 명령에 적용됩니다. 설명자는 인터페이스를 설명하는 데 사용되는 인터페이스 명령입니다.

라우터, LAN 스위치, WAN 스위치 또는 ATM 스위치와 같은 각 디바이스 분류에 대한 표준 구성을 생성하는 것이 좋습니다.각 표준 컨피그레이션에는 네트워크 일관성을 유지하는 데 필요한 전역, 미디어 및 프로토콜 컨피그레이션 명령이 포함되어야 합니다.미디어 구성에는 ATM, 프레임 릴레이 또는 고속 이더넷 구성이 포함됩니다.프로토콜 컨피그레이션에는 표준 IP 라우팅 프로토콜 컨피그레이션 매개변수, 공통 QoS(Quality of Service) 컨피그레이션, 공통 액세스 목록 및 기타 필수 프로토콜 컨피그레이션이 포함됩니다.전역 컨피그레이션 명령은 모든 유사 디바이스에 적용되며 service 명령, IP 명령, TACACS 명령, vty 컨피그레이션, 배너, SNMP 컨피그레이션, NTP(Network Time Protocol) 컨피그레이션과 같은 매개변수를 포함합니다.

설명자는 각 인터페이스에 적용되는 표준 형식을 생성하여 개발됩니다.설명자에는 인터페이스의 목적 및 위치, 인터페이스에 연결된 다른 디바이스 또는 위치, 회선 식별자가 포함됩니다.설명자는 지원 조직이 인터페이스와 관련된 문제의 범위를 더 잘 이해하고 문제를 더 신속하게 해결할 수 있도록 지원합니다.

표준 컨피그레이션 매개변수를 표준 컨피그레이션 파일에 유지하고 프로토콜 및 인터페이스 컨피그레이션에 앞서 각 새 디바이스에 파일을 다운로드하는 것이 좋습니다. 또한 각 글로벌 컨피그레이션 매개변수에 대한 설명 및 중요한 이유를 포함하여 표준 컨피그레이션 파일을 문서화해야 합니다. [Cisco RME\(Resource Manager Essentials\)](#)를 사용하여 표준 구성 파일, 프로토콜 구성 및 설명자를 관리할 수 있습니다.

구성 업그레이드 절차

업그레이드 절차를 통해 다운타임을 최소화하면서 소프트웨어 및 하드웨어 업그레이드가 원활하게 이루어지도록 할 수 있습니다. 업그레이드 절차에는 공급업체 검증, 릴리스 정보 등의 공급업체 설치 참조, 업그레이드 방법론 또는 단계, 구성 지침, 테스트 요구 사항이 포함됩니다.

업그레이드 절차는 네트워크 유형, 디바이스 유형 또는 새로운 소프트웨어 요구 사항에 따라 크게 달라질 수 있습니다. 개별 라우터 또는 스위치 업그레이드 요구 사항은 아키텍처 그룹 내에서 개발 및 테스트될 수 있으며 변경 문서에서 참조할 수 있습니다. 전체 네트워크를 포함한 다른 업그레이드는 이처럼 쉽게 테스트할 수 없습니다. 이러한 업그레이드는 더 심층적인 계획, 공급업체 참여, 성공을 보장하기 위한 추가 단계를 필요로 할 수 있습니다.

새로운 소프트웨어 구축 또는 식별된 표준 릴리스와 함께 업그레이드 절차를 생성하거나 업데이트해야 합니다. 이 절차에서는 업그레이드에 대한 모든 단계를 정의하고, 디바이스 업데이트와 관련된 공급업체 설명서를 참조하며, 업그레이드 후 디바이스의 유효성을 검사하는 테스트 절차를 제공해야 합니다. 업그레이드 절차를 정의하고 검증한 후에는 특정 업그레이드에 적합한 모든 변경 문서에서 업그레이드 절차를 참조해야 합니다.

솔루션 템플릿

솔루션 템플릿을 사용하여 표준 모듈형 네트워크 솔루션을 정의할 수 있습니다. 네트워크 모듈은 와이어링 클로짓, WAN 현장 사무실 또는 액세스 집선 장치일 수 있습니다. 각각의 경우 유사한 구축을 정확히 동일한 방식으로 수행할 수 있도록 솔루션을 정의, 테스트 및 문서화해야 합니다. 따라서 솔루션의 행동이 잘 정의되어 있으므로 조직이 앞으로 훨씬 더 낮은 위험 수준에서 변화가 일어날 수 있습니다.

위험이 높은 모든 구축 및 두 번 이상 배포될 솔루션에 대한 솔루션 템플릿을 생성합니다. 솔루션 템플릿에는 네트워크 솔루션에 대한 모든 표준 하드웨어, 소프트웨어, 구성, 케이블 연결 및 설치 요구 사항이 포함되어 있습니다. 솔루션 템플릿의 구체적인 세부 정보는 다음과 같습니다.

- 메모리, 플래시, 전원 및 카드 레이아웃을 포함한 하드웨어 및 하드웨어 모듈
- 포트 할당, 연결, 속도 및 미디어 유형을 포함한 논리적 토폴로지
- 모듈 또는 펌웨어 버전을 포함한 소프트웨어 버전
- 라우팅 프로토콜, 미디어 구성, VLAN 컨피그레이션, 액세스 목록, 보안, 스위칭 경로, 스페닝 트리 매개변수 등을 포함한 모든 비표준, 디바이스별 컨피그레이션
- 대역 외 관리 요구 사항.
- 케이블 요구 사항
- 환경, 전원, 랙 위치 등의 설치 요구 사항

솔루션 템플릿에는 많은 요구 사항이 포함되어 있지 않습니다. 특정 솔루션에 대한 IP 주소 지정, 이름 지정, DNS 할당, DHCP 할당, PVC 할당, 인터페이스 설명자 등의 특정 요구 사항은 전반적인 구성 관리 관행에 따라 다루어져야 합니다. 표준 구성, 변경 관리 계획, 문서 업데이트 절차, 네트워크 관리 업데이트 절차 등 일반적인 요구 사항은 일반적인 구성 관리 방식으로 처리해야 합니다.

문서 유지 관리

네트워크에서 거의 실시간으로 발생한 네트워크 및 변경 사항을 문서화하는 것이 좋습니다. 문제 해결, 네트워크 관리 툴 디바이스 목록, 인벤토리, 검증 및 감사에 이 정밀한 네트워크 정보를 사용할 수 있습니다. 다음 네트워크 문서의 주요 성공 요인을 사용하는 것이 좋습니다.

- [현재 디바이스, 링크 및 최종 사용자 인벤토리](#)
- [구성 버전 제어 시스템](#)
- [TACACS 컨피그레이션 로그](#)
- [네트워크 토폴로지 문서](#)

[현재 디바이스, 링크 및 최종 사용자 인벤토리](#)

현재 디바이스, 링크 및 최종 사용자 인벤토리 정보를 통해 네트워크 인벤토리 및 리소스, 문제 영향, 네트워크 변경 영향을 추적할 수 있습니다. 사용자 요구 사항과 관련하여 네트워크 인벤토리 및 리소스를 추적하는 기능은 관리되는 네트워크 장치가 적극적으로 사용되고 감사에 필요한 정보를 제공하며 장치 리소스를 관리하는 데 도움이 됩니다. 최종 사용자 관계 데이터는 변경 위험과 영향을 정의하는 정보와 더 신속하게 문제를 해결하고 해결할 수 있는 기능을 제공합니다. 장치, 링크 및 최종 사용자 인벤토리 데이터베이스는 일반적으로 대표적인 서비스 공급자 조직이 개발합니다. 네트워크 인벤토리 소프트웨어의 주요 개발자는 [Visionael Corporation](#)입니다. 데이터베이스에는 디바이스, 링크, 고객 사용자/서버 데이터와 같은 디바이스, 사용자/서버 데이터에 대한 테이블이 포함될 수 있으므로, 디바이스가 다운되거나 네트워크가 변경될 때 최종 사용자의 영향을 쉽게 파악할 수 있습니다.

[구성 버전 제어 시스템](#)

컨피그레이션 버전 제어 시스템은 모든 디바이스의 현재 실행 중인 컨피그레이션 및 이전 실행 버전의 집합 수를 유지 관리합니다. 이 정보는 문제 해결 및 구성 또는 변경 감사에 사용할 수 있습니다. 문제 해결 시 현재 실행 중인 컨피그레이션을 이전 작업 버전과 비교하여 컨피그레이션이 어떤 식으로든 문제에 연결되어 있는지 파악할 수 있습니다. 컨피그레이션의 이전 작동 버전을 3~5개 유지하는 것이 좋습니다.

[TACACS 컨피그레이션 로그](#)

누가 컨피그레이션을 변경했는지 그리고 언제 변경했는지 식별하려면 TACACS 로깅 및 NTP를 사용할 수 있습니다. 이러한 서비스가 Cisco 네트워크 디바이스에서 활성화되면 컨피그레이션 변경 시 사용자 ID 및 타임스탬프가 컨피그레이션 파일에 추가됩니다. 그런 다음 컨피그레이션 파일과 함께 컨피그레이션 버전 제어 시스템에 이 스탬프가 복사됩니다. 그런 다음 TACACS는 관리되지 않는 변경을 억제하고 발생하는 변경 사항을 올바르게 감사하는 메커니즘을 제공할 수 있습니다. TACACS는 Cisco Secure 제품을 사용하여 활성화됩니다. 사용자가 디바이스에 로그인할 때 사용자 ID와 비밀번호를 입력하여 TACACS 서버를 인증해야 합니다. NTP는 디바이스를 NTP 마스터 클럭으로 가리키면 네트워크 디바이스에서 쉽게 활성화됩니다.

[네트워크 토폴로지 문서](#)

토폴로지 문서는 네트워크를 이해하고 지원하는 데 도움이 됩니다. 이를 사용하여 설계 지침을 검증하고 향후 설계, 변경 또는 문제 해결을 위해 네트워크를 더 잘 이해할 수 있습니다. 토폴로지 문서에는 연결, 주소 지정, 미디어 유형, 장치, 랙 레이아웃, 카드 할당, 케이블 라우팅, 케이블 식별, 종단 점, 전원 정보, 회선 식별 정보 등 논리적 및 물리적 문서가 모두 포함되어야 합니다.

성공적인 컨피그레이션 관리를 위해서는 토폴로지 설명서를 유지하는 것이 중요합니다. 토폴로지 문서 유지 관리를 수행할 수 있는 환경을 만들려면 문서의 중요도를 강조해야 하며 정보를 업데이트할 수 있어야 합니다. 네트워크 변경이 발생할 때마다 토폴로지 문서를 업데이트하는 것이 좋습니다.

다.

네트워크 토폴로지 설명서는 일반적으로 [Microsoft Visio](#)와 같은 그래픽 응용 프로그램을 사용하여 유지됩니다. [Visionael](#)과 같은 다른 제품은 토폴로지 정보 관리를 위한 탁월한 기능을 제공합니다.

[표준 검증 및 감사](#)

구성 관리 성능 지표는 네트워크 구성 표준 및 주요 성공 요인을 검증하고 감사하는 메커니즘을 제공합니다. 구성 관리를 위한 프로세스 개선 프로그램을 구현하면 성능 지표를 사용하여 일관성 문제를 파악하고 전반적인 구성 관리를 개선할 수 있습니다.

구성 관리의 성공을 측정하고 구성 관리 프로세스를 개선하기 위해 여러 부서의 팀을 구성하는 것이 좋습니다. 팀의 첫 번째 목표는 구성 관리 문제를 식별하기 위해 구성 관리 성능 지표를 구현하는 것입니다. 다음 컨피그레이션 관리 성능 지표를 자세히 살펴보겠습니다.

- [구성 무결성 검사](#)
- [장치, 프로토콜 및 미디어 감사](#)
- [표준 및 문서 검토](#)

이러한 감사의 결과를 평가한 후 불일치를 수정하는 프로젝트를 시작한 다음 문제의 초기 원인을 파악합니다. 표준 문서의 부족 또는 일관성 있는 프로세스의 부재가 발생할 수 있습니다. 더 이상 컨피그레이션 불일치를 방지하기 위해 표준 문서를 개선하고 교육을 구현하거나 프로세스를 개선할 수 있습니다.

월별 감사 또는 검증만 필요한 경우 분기별 감사를 권장합니다. 과거 감사를 검토하여 이전 문제가 해결되었는지 확인합니다. 전반적인 개선 및 목표를 통해 진도와 가치를 입증하십시오. 고위험, 중간 위험 및 저위험 네트워크 컨피그레이션 불일치의 수량을 표시하는 메트릭을 생성합니다.

[구성 무결성 검사](#)

컨피그레이션 무결성 검사는 네트워크의 전체 컨피그레이션, 복잡성 및 일관성, 잠재적 문제를 평가해야 합니다. Cisco 네트워크의 경우 Netsys 컨피그레이션 검증 툴을 사용하는 것이 좋습니다. 이 툴은 모든 디바이스 컨피그레이션을 입력하고 중복 IP 주소, 프로토콜 불일치, 불일치와 같은 현재 문제를 식별하는 컨피그레이션 보고서를 생성합니다. 이 툴은 모든 연결 또는 프로토콜 문제를 보고하지만, 각 디바이스에서 평가를 위한 표준 컨피그레이션을 입력하지 않습니다. 구성 표준을 수동으로 검토하거나 표준 구성 차이를 보고하는 스크립트를 작성할 수 있습니다.

[장치, 프로토콜 및 미디어 감사](#)

디바이스, 프로토콜 및 미디어 감사는 소프트웨어 버전, 하드웨어 디바이스 및 모듈, 프로토콜 및 미디어, 이름 지정 규칙의 일관성을 유지하기 위한 성능 지표입니다. 먼저 감사에서 비표준 문제를 식별해야 합니다. 그러면 컨피그레이션 업데이트를 통해 문제를 수정하거나 개선할 수 있습니다. 전체 프로세스를 평가하여 차선 또는 비표준 구축이 발생하지 않도록 방지하는 방법을 결정합니다.

[Cisco RME](#)는 하드웨어 버전, 모듈 및 소프트웨어 버전에 대해 감사하고 보고할 수 있는 구성 관리 툴입니다. Cisco는 또한 IP, DLSW, Frame Relay 및 ATM과 불일치를 보고할 보다 포괄적인 미디어 및 프로토콜 감사를 개발하고 있습니다. 프로토콜 또는 미디어 감사가 개발되지 않은 경우, 네트워크의 모든 유사 디바이스에 대한 디바이스, 버전 및 컨피그레이션을 검토하거나 디바이스, 버전 및 컨피그레이션을 스팟 검사하여 수동 감사를 사용할 수 있습니다.

[표준 및 문서 검토](#)

이 성능 지표에서는 네트워크 및 표준 문서를 검토하여 정보가 정확한지 확인합니다.감사에는 현재 문서 검토, 변경 사항 또는 추가 사항 권고, 새 표준 승인 등이 포함되어야 합니다.

분기별로 다음 문서를 검토해야 합니다.표준 구성 정의, 권장 하드웨어 구성, 현재 표준 소프트웨어 버전, 모든 장치 및 소프트웨어 버전에 대한 업그레이드 절차, 토폴로지 문서, 현재 템플릿, IP 주소 관리를 포함한 솔루션 템플릿.

관련 정보

- [Technical Support - Cisco Systems](#)