構成管理： ベスト プラクティスのホワイト ペーパー

目次

概要

構成管理とは、ネットワークの一貫性の確保、ネットワーク変更の追跡、最新ネットワークに関する文書の閲覧、およびネットワークの最新状態の表示を可能にするプロセスとツールを集めたものです。 構成管理の最適な方法を確立し、維持することによって、ネットワーク アベイラビリティの向上やコストの削減などの利点を期待できます。 これには次のものがあります。

- 事後対処的なサポート問題の減少によるサポート コストの削減
- 未使用のネットワーク コンポーネントを特定するデバイス、回線、およびユーザ追跡ツールとプロセスによる、ネットワーク コストの削減
- 事後対処的なサポート コストの削減と問題解決時間の短縮によるネットワーク アベイラビリティの向上

構成管理が欠けていると、結果的に次のような問題が生じます。

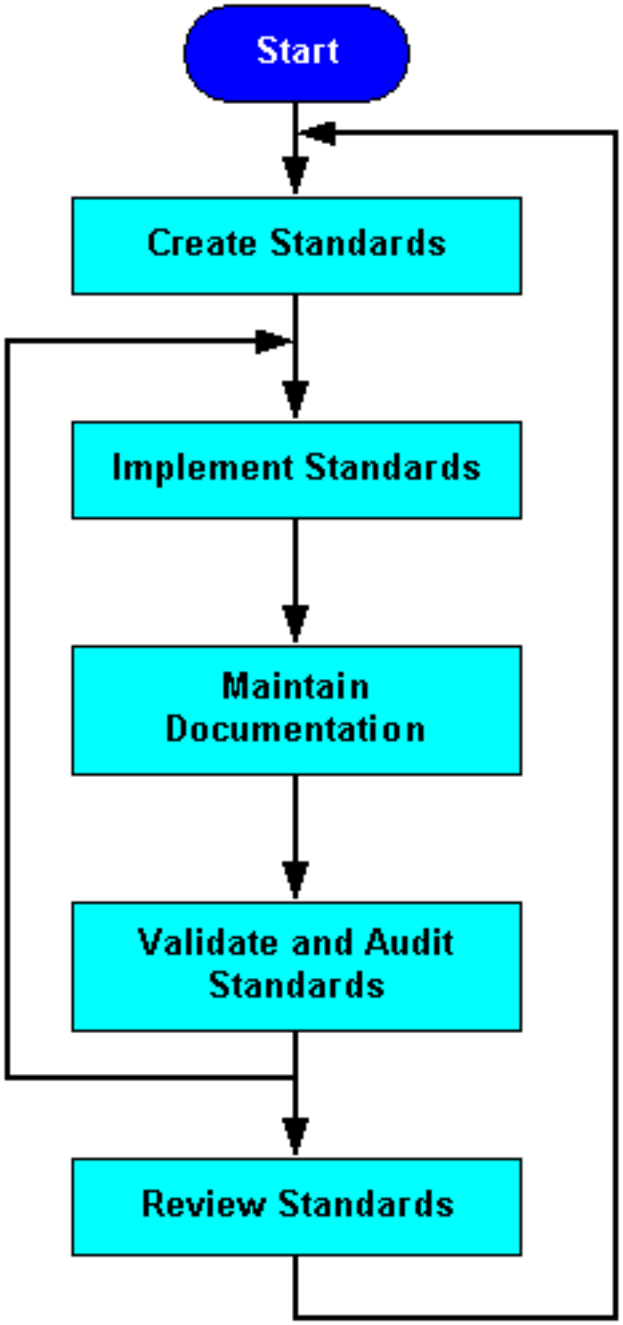
- ネットワーク変更に伴うユーザへの影響を判断できない
- 事後対処的なサポート問題の増加とアベイラビリティの低下
- 問題解決時間の増加

- 未使用のネットワーク コンポーネントによるネットワーク コストの増加

この最適な方法についての文書には、構成管理計画を成功させるためのプロセス フローチャートが含まれています。 各ステップについて詳細に説明します 標準規定の作成、文書の保守、<t

構成管理の高レベル プロセス フロー

次の図は、構成管理計画を成功させるために、重要な成功要因とパフォーマンス インジケータをどのように使用すればよいかを示しています。



標準規定の作成

ネットワークの一貫性を確保するための標準規定を作成すれば、ネットワークの複雑さが軽減され、予期しないダウンタイムを短縮できるほか、ネットワークに影響を与えるイベントからネッ

トワークを保護できます。 最適なネットワークの一貫性を確保するために、次の標準規定を作成することを推奨します。

- ソフトウェア バージョン管理
- IP アドレッシング標準規定と管理
- 命名規則と Domain Name System/Dynamic Host Configuration Protocol（DNS/DHCP）の割り当て
- 標準規定コンフィギュレーションと記述子
- 設定のアップグレード手順
- ソリューション テンプレート

ソフトウェア バージョン管理

ソフトウェア バージョン管理は、同類ネットワーク デバイスに一貫したソフトウェア バージョンを導入するための方法です。 これにより、選択したソフトウェア バージョンの検証およびテストを実施する機会が増え、ソフトウェア不良とネットワーク内で見られる相互運用性の問題を大幅に制限できます。 また、ソフトウェア バージョンを限定することにより、ユーザ インターフェイス、コマンド、または管理出力に関する予期しない動作、アップグレード動作、および各種機能の動作についてのリスクが小さくなります。 さらに、環境の複雑さも軽減され、サポートが容易になります。 全体的に見ると、ソフトウェア バージョン管理はネットワーク アベイラビリティを向上させ、事後対処的なサポート コストの削減に役立ちます。

注:「同類ネットワーク デバイス」は、共通のサービスを提供する共通のシャーシを備えた、標準規定的なネットワーク デバイスとして定義されます。

ソフトウェア バージョン管理を行うには、次の手順を実行します。

- シャーシ、安定性、および新機能要件に基づいて、デバイスの分類を決定します。
- 同類デバイス用の、対象となる個々のソフトウェア バージョンを決定します。
- 選択したソフトウェア バージョンをテスト、検証し、試験的に使用します。
- 合格したバージョンを同類デバイス分類の標準規定として文書に記述します。
- 既存の同類デバイスすべてを標準規定ソフトウェア バージョンにアップグレードします。

IP アドレッシング標準規定と管理

IP アドレス管理は、ネットワーク内の IP アドレスおよびサブネットの割り当て、再利用、および文書への記述を行うプロセスです。 IP アドレッシング標準規定では、サブネット範囲内でのサブネットのサイズ、サブネットの割り当て、ネットワーク デバイスの割り当て、およびダイナミック アドレスの割り当てを定義します。 IP アドレス管理標準規定を作成すると、サブネットの一部または完全な重複、ネットワーク内での非集約、デバイスへの重複した IP アドレスの割り当て、IP アドレス空間の浪費、および不必要な複雑さが起こる可能性が低くなります。

IP アドレス管理を成功させるための最初のステップは、ネットワークで使用される IP アドレス ブロックを把握することです。 多くの場合、ネットワーク組織は RFC 1918 アドレス スペースに アドレス指定可能なインターネットではない頼らなければなりませんでしたりしかしネットワーク アドレス変換（NAT）と共にネットワークにアクセスするのに使用することができます。 アドレス ブロックの定義が終わったら、それらのアドレス ブロックを、集約が促進されるようにネットワークのエリアに割り当てます。 多くの場合、これらのブロックは、定義された範囲内のサブネットの数とサイズに基づいてさらに分割する必要があります。 標準規定的な用途に対する標準規定のサブネット サイズ、たとえば建物のサブネット サイズ、WAN リンクのサブネット サイズ、ループバックのサブネット サイズ、WAN サイトのサブネット サイズなどを定義します。 新

しい用途については、より大きいサマリー ブロック内のサブネット ブロックからサブネットを割り当てることができます。

たとえば、東海岸地域キャンパス、西海岸地域キャンパス、国内 WAN、ヨーロッパ WAN、およびその他の主要海外サイトを持つ大きな企業ネットワークについて考えてみます。 この場合は、IP 集約を促進するために、隣接した IP Classless Interdomain Routing (CIDR) ブロックを各エリアに割り当てます。 続いて各ブロック内のサブネット サイズを定義し、各ブロックのサブセクションを特定の IP サブネット サイズに割り当てます。 ブロック内の使用可能なサブネット サイズごとに割り当て済み、使用済み、および使用可能なサブネットを記録するスプレッドシートを作成し、それぞれの主要ブロックまたは IP アドレス空間全体をそのスプレッドシートに記入します。

次のステップは、各サブネット範囲内の IP アドレス割り当ての標準規定を作成することです。 サブネット内のルータおよび Hot Standby Router Protocol (HSRP; ホットスタンバイ ルータ プロトコル) の仮想アドレスには、その範囲内で最初に使用可能なアドレスを割り当てます。 スイッチとゲートウェイにはその次に使用可能なアドレスを割り当て、次に固定アドレス、最後に DHCP 用のダイナミック アドレスを割り当てます。 たとえば、すべてのユーザサブネットは 253 の利用可能なアドレス 割り当てを用いる /24 サブネットであるかもしれません。 ルータには .1 と .2 のアドレスを割り当て、HSRP アドレスには .3 アドレスを、スイッチには .5 ～ .9 のアドレスを割り当て、DHCP の範囲には .10 ～ .253 のアドレスを割り当てることができます。 どのような標準規定を策定した場合でも、導入の一貫性を確保するために、すべてのネットワーク技術計画文書に記述し、それらの文書を常に参照する必要があります。

命名規則と DNS/DHCP 割り当て

命名規則と DNS を構造化された方法で一貫してデバイスに適用すると、次のような形でネットワークを管理できます。

- デバイスに関連するすべてのネットワーク管理情報について、ルータへの一貫したアクセス ポイントを作成する。
- IP アドレスが重複する可能性を減らす。
- ロケーション、デバイス タイプ、および用途を示す、デバイスの簡単な識別情報を作成する。
- ネットワーク デバイスを容易に特定する方法を提供することにより、インベントリ管理を改善する。

ほとんどのネットワーク デバイスには、デバイスを管理するためのインターフェイスが 1 ~ 2 個あります。 これらは、インバンドまたはアウトバンドのイーサネット インターフェイスとコンソール インターフェイスです。 これらのインターフェイスには、デバイス タイプ、ロケーション、およびインターフェイス タイプに関連する命名規則を定めます。 ルータでは、一次管理インターフェイスとしてできるだけループバック インターフェイスを使用することが推奨されます。ループバック インターフェイスはさまざまなインターフェイスからアクセスできるからです。 また、トラップ、SNMP、および syslog メッセージの送信元 IP アドレスとしても、ループバック インターフェイスを使用します。 個々のインターフェイスには、デバイス、ロケーション、用途、およびインターフェイスを明示する命名規則を定めます。

また、DHCP 範囲を明示し、その範囲やユーザのロケーションなどを DNS に追加することも推奨されます。 これには、IP アドレスの一部や物理的な場所を使用できます。 例は、二階、ワイヤリング クローゼット 1.ビルディング C の IP アドレスを識別する"dhcp bldg へ"dhcp bldgc21 10" であるかもしれません。 識別のために、正確なサブネットを使用することもできます。 デバイスと DHCP の命名規則を定めたら、エントリを追跡および管理するツール (Cisco Network Registrar など) が必要になります。

標準の設定と記述子

標準規定コンフィギュレーションには、プロトコル設定とメディア設定、およびグローバル設定コマンドを利用します。 記述子は、インターフェイスの記述に使用するインターフェイス コマンドです。

標準規定コンフィギュレーションは、ルータ、LAN スイッチ、WAN スイッチ、ATM スイッチなどのデバイス分類ごとに作成することが推奨されます。 それぞれの標準規定コンフィギュレーションには、ネットワークの一貫性を確保するために必要なグローバル設定、メディア設定、およびプロトコル設定コマンドを含めます。 メディア設定には、ATM、フレームリレー、ファーストイーサネットの設定などが含まれます。 プロトコル設定には、標準規定 IP ルーティング プロトコル設定パラメータ、共通の Quality of Service (QoS) 設定、共通のアクセス リスト、その他の必要なプロトコル設定などが含まれます。 グローバル設定コマンドはすべての同類デバイスに適用され、サービス コマンド、IP コマンド、TACACS コマンド、vty 設定、バナー、SNMP 設定、Network Time Protocol (NTP) 設定などのパラメータが含まれます。

記述子は、各インターフェイスに適用される標準規定フォーマットを作成することによって定義されます。 記述子には、インターフェイスの用途と口ケーション、インターフェイスに接続される他のデバイスまたは口ケーション、回線識別情報などが含まれます。 記述子を使用すると、サポート部門で特定のインターフェイスに関連する問題の適用範囲を的確に把握できるため、迅速な問題解決が可能になります。

標準規定コンフィギュレーション パラメータは標準規定コンフィギュレーション ファイル内に保存しておき、各新規デバイスでプロトコルおよびインターフェイスの設定を行う前に、標準規定コンフィギュレーション ファイルを新規デバイスにダウンロードすることを推奨します。 また、標準規定コンフィギュレーション ファイル内の各グローバル設定パラメータの説明やその重要性の理由などを文書に記述します。 標準規定コンフィギュレーション ファイル、プロトコル設定、および記述子の管理には、Cisco Resource Manager Essentials (RME) を使用できます。

設定のアップグレード手順

アップグレード手順を利用すると、ソフトウェアおよびハードウェアのアップグレードを最小のダウンタイムで円滑に実行できます。 アップグレード手順には、ベンダーの確認、ベンダーのインストール用リファレンス (リリース ノートなど)、アップグレード方法またはステップ、設定のガイドライン、テスト要件などが含まれます。

アップグレード手順は、ネットワーク タイプ、デバイス タイプ、または新規ソフトウェアの要件によって大きく異なる場合があります。 個々のルータまたはスイッチのアップグレード要件はアーキテクチャ グループ内で作成およびテストし、変更文書に参照として記載しても構いません。 その他のアップグレードはネットワーク全体にかかわるため、容易にテストできません。 このようなアップグレードでは、確実に成功させるために、より詳細な計画の立案、ベンダーの介入、および追加ステップが必要となる場合があります。

アップグレード手順は、新規ソフトウェアの導入または決定済みの標準規定リリースにあわせて作成または更新します。 アップグレード手順では、アップグレードに必要なすべてのステップを定義し、デバイスのアップデートに関連するベンダーの文書を参照として記載し、アップグレード後にデバイスを検証するためのテスト手順を含めてください。 アップグレード手順の定義と検証が終わったら、特定のアップグレードに対応するすべての変更文書にアップグレード手順を参照として記載します。

ソリューション テンプレート

標準規定のモジュラ式ネットワーク ソリューションを定義するために、ソリューション テンプレートを使用できます。 ネットワーク モジュールには、ワイヤリング クローゼット、WAN フィールド オフィス、アクセス コンセントレータなどを選択できます。 どの場合でも、ソリューションを定義、テスト、および文書化して、同じような導入作業をまったく同じ方法で実行できる必要があります。 これにより、ソリューションの動作が明確に規定されるため、将来変更が起こったときも、組織に対するリスク レベルはかなり低くなります。

ソリューション テンプレートは、繰り返し行われるリスクの高い導入作業とソリューションすべてについて作成します。 ソリューション テンプレートには、ネットワーク ソリューションの標準規定ハードウェア、ソフトウェア、設定、ケーブル接続、およびインストール要件がすべて含まれます。 ソリューション テンプレートの具体的な詳細は次のとおりです。

- ハードウェアおよびハードウェア モジュール。メモリ、フラッシュ、電源、カードのレイアウトなど。
- 論理的トポロジ。ポート割り当て、接続性、速度、メディア タイプなど。
- ソフトウェア バージョン。モジュールやファームウェアのバージョンなど。
- 非標準規定で、デバイスに固有でないすべての設定。ルーティング プロトコル、メディア設定、VLAN 設定、アクセス リスト、セキュリティ、スイッチング パス、スパニングツリー パラメータなど。
- 帯域外管理要件。
- ケーブル要件。
- インストール要件。環境、電源、ラックの位置など。

ソリューション テンプレートにはそれほど多くの要件は含まれません。 特定のソリューションにおける IP アドレッシング、ネーミング、DNS 割り当て、DHCP 割り当て、PVC 割り当て、インターフェイス記述子などの個別要件は、全体的な構成管理方法の対象範囲です。 標準規定コンフィギュレーション、変更管理計画、文書更新手順、ネットワーク管理更新手順などの一般的な要件は、一般的な構成管理方法の対象範囲です。

文書の保守

ネットワークに関する情報とネットワーク内に起こった変更をほぼリアルタイムで文書に記述することを推奨します。 この正確なネットワーク情報は、トラブルシューティング、ネットワーク管理ツール デバイス リスト、インベントリ、検証、および監査に使用できます。 ネットワーク文書にとって重要な、次の成功要因を使用することを推奨します。

- 現在のデバイス、リンク、およびエンドユーザ インベントリ
- コンフィギュレーション バージョン管理システム
- TACACS 設定ログ
- ネットワークトポロジドキュメンテーション

現在のデバイス、リンク、およびエンドユーザ インベントリ

現在のデバイス、リンク、およびエンドユーザ インベントリ情報を使用すると、ネットワークのインベントリとリソース、問題の影響、およびネットワーク変更の影響を追跡できます。 ネットワークのインベントリとリソースをユーザ要件と関連付けて追跡することにより、管理対象のネットワーク デバイスが実際に使用されていて、監査に必要な情報を提供し、データ リソースの管理に活用されていることを確認できます。 エンドユーザ関係データは、迅速なトラブルシューティングと問題解決を可能にするだけでなく、変更によるリスクと影響を規定するための情報を提供します。 一般に、デバイス、リンク、およびエンドユーザ インベントリ データベースは、多くの主要サービス プロバイダー組織によって開発されています。 ネットワークインベントリ ソ

フトウェアの代表的 ディベロッパは Visionael Corporation です 。 データベースには同類デバイス、リンク、およびカスタマーのユーザ/サーバ データ用のテーブルが格納されているため、デバイスの障害やネットワークの変更が発生した場合に、エンドユーザへの影響を容易に把握できます。

コンフィギュレーション バージョン管理システム

コンフィギュレーション バージョン管理システムは、全デバイスの現在の実行コンフィギュレーションと、以前の実行バージョンのセット番号を保持しています。 この情報はトラブルシューティングと設定または変更の監査に使用できます。 トラブルシューティングを行うときは、現在の実行コンフィギュレーションと以前使用していたバージョンを比較して、設定がなんらかの点で問題と関係しているかどうかを判断できます。 以前使用していた設定のバージョンは 3 ~ 5 世代前まで保持することを推奨します。

TACACS 設定ログ

だれがいつ設定を変更したかを特定するために、TACACS ロギングと NTP を使用できます。 Cisco ネットワーク デバイスでこれらのサービスが有効になっていると、設定が変更されたときにコンフィギュレーション ファイルにユーザ ID とタイムスタンプが追加されます。 このタイムスタンプはコンフィギュレーション ファイルとともにコンフィギュレーション バージョン管理システムにコピーされます。 TACACS は管理されていない変更が発生しないようにする役割を果たし、発生した変更を正しく監査するためのメカニズムを提供します。 TACACS を有効にするには、Cisco Secure 製品を使用します。 ユーザはデバイスにログインするときにユーザ ID とパスワードを入力して、TACACS サーバによる認証を受ける必要があります。 NTP はネットワーク デバイス上で NTP マスター クロックを設定することにより、容易に有効にできます。

ネットワーク トポロジ文書

トポロジ 文書はネットワークを理解し、サポートする上で役立ちます。 トポロジ 文書を使用することで、設計ガイドラインを検証し、将来の設計、変更、またはトラブルシューティングに際してネットワークを十分理解できます。 トポロジ 文書には、論理的な情報と物理的な情報が必要です。たとえば、接続性、アドレッシング、メディア タイプ、デバイス、ラックのレイアウト、カードの割り当て、ケーブルの配線経路、ケーブルの識別、終端ポイント、電源情報、回線識別情報などを記述します。

トポロジ 文書の保守は構成管理を成功させるための鍵です。 トポロジ 文書が適切に保守される環境を構築するには、文書の重要性を強調し、いつでも更新できるように情報を使用可能にしておく必要があります。 ネットワークの変更が起こるたびに必ずトポロジ 文書を更新することを推奨します。

ネットワークトポロジドキュメンテーションは Microsoft Visio のようなグラフィック アプリケーションを使用して一般的に維持されます 。 Visionael のような他の製品は トポロジー情報を管理するために優秀な機能を提供します。

検証と監査の基準

構成管理パフォーマンス インジケータには、ネットワーク コンフィギュレーション標準規定と重要な成功要因を検証し、監査するメカニズムがあります。 構成管理のプロセス改善プログラムを実行することにより、パフォーマンス インジケータを使用して、一貫性に関する問題の特定と全体的な構成管理の改善を実現できます。

構成管理の成果を測定して構成管理プロセスを改善するために、職能上の枠を超えたチームを結成することを推奨します。 このチームの最初の目標は、構成管理パフォーマンス インジケータを実行して構成管理に関する問題を明らかにすることです。 次の構成管理パフォーマンス インジケータについて詳しく説明します。

- 設定の整合性チェック
- デバイス、プロトコル、およびメディアの監査
- 標準規定と文書のレビュー

これらの監査から得られた結果を評価した後、不整合を修正するプロジェクトを開始し、問題の初期原因を判断します。 考えられる原因には、標準規定文書の不備や一貫したプロセスの欠如などがあります。 設定のさらなる不整合を防止するために、標準規定文書の改善、トレーニングの実施、またはプロセスの改善を行うことができます。

監査は 1 か月に 1 回、または検証のみが必要な場合は 4 半期に 1 回実施することを推奨します。 過去の監査をレビューし、これまでに発生した問題が解決していることを確認します。 進捗と価値を実証するために、全体的な改善点と目標を定めます。 ネットワーク コンフィギュレーションにおける高リスク、中リスク、および低リスクの不整合の量を示すメトリックを作成します。

設定の整合性チェック

設定の整合性チェックでは、ネットワークの全体的な設定、その複雑さと一貫性、および起こりうる問題を評価します。 シスコ ネットワークの場合は、Netsys 設定検証ツールの使用を推奨します。 このツールはすべてのデバイスの設定を入力とし、現在存在している IP アドレスの重複、プロトコルのミスマッチ、不整合などの問題を明らかにするコンフィギュレーション レポートを作成します。 Netsys は接続性やプロトコルの問題を報告しますが、標準規定コンフィギュレーションを入力として各デバイスを評価することはありません。 コンフィギュレーション標準規定については手動でレビューするか、または標準規定コンフィギュレーションの相違点を報告するスクリプトを作成できます。

デバイス、プロトコル、およびメディアの監査

デバイス、プロトコル、およびメディアの監査は、ソフトウェア バージョン、ハードウェア デバイスとモジュール、プロトコルとメディア、および命名規則の一貫性に関するパフォーマンス インジケータです。 監査では最初に非標準規定問題を特定します。非標準規定問題がある場合は、問題の解決または改善を図るために設定を更新する必要があります。 プロセス全体を評価し、最適ではない設定または非標準規定の設定の導入がどのようにして回避されているかを判断します。

Cisco RME は、ハードウェア バージョン、モジュール、およびソフトウェア バージョンに関する監査とレポート作成が可能な構成管理ツールです。 シスコでは現在、IP、DLSW、フレームリレー、および ATM での不整合を報告する包括的なメディアおよびプロトコル監査を開発しています。 プロトコルまたはメディアの監査が開発されていない場合は、手動の監査を実施できます。手動による監査方法には、ネットワーク内のすべての同類デバイスに関するデバイス、バージョン、および設定のレビューや、デバイス、バージョン、および設定の抜き取り検査などがあります。

標準規定と文書のレビュー

このパフォーマンス インジケータでは、ネットワークおよび標準規定文書をレビューして、情報が正確かつ最新のものであることを確認します。 この監査には、最新文書のレビュー、変更または追加箇所の指摘、新しい標準規定の承認などが含まれます。

4 半期に 1 回、次の文書をレビューします。 標準規定コンフィギュレーション定義、推奨されるハードウェア コンフィギュレーションを含むソリューション テンプレート、現在の標準規定ソフトウェアのバージョン、すべてのデバイスおよびソフトウェア バージョンのアップグレード手順、トポロジ 文書、現在のテンプレート、IP アドレス管理。

関連情報

- テクニカルサポート - Cisco Systems