

グローバルなネットワークの監査と
コントロールのニーズに応えるために：
拡張性と可視性を実現するHP Network Automation software
ホワイトペーパー



PARTIDAS / DEPARTURAS					
vôo n. flight n.	destino destination	escalas via	horário/time previsto schedule	co	co
0030	NEWARK		21.20	2	
0094	HOUSTON		21.35	2	
0860	WASHINGTON		22.10	2	
016	WASHINGTON		22.10	2	
998	MIAMI		22.20		
90	MIAMI		22.25		
96	PARIS		22.25		
7	BUENOS AIRES		22.30		
7	BUENOS AIRES		22.30		
0	AMSTERDAM		22.30		
	LONDON		22.40		
	MADRID		23.00		
	MILAN		23.45		
TOKYO	LOS ANGELES		23.50		

目次

全社規模でのネットワーク変更管理	3
HP Network Automation software	3
Network Automation Multimasterによる拡張性、信頼性、可用性の向上	4
単一の管理コンソールから、一元化されたビューで分散型インフラストラクチャを確認	5
ベストプラクティス・ポリシーおよびコンプライアンス基準の一元的な適用	5
分散型インフラストラクチャ全体にわたるデータ冗長性により、災害復旧を促進	5
シームレスアクティブ/アクティブ高可用性によるフェイルセーフ・ネットワーク可用性	5
安定性と拡張性	6
効率的なタスク管理により、ワイド・エリア・ネットワーク(WAN)のトラフィックを減らし、 ローカル・エリア・ネットワーク(LAN)の使用を増加させます	6
分散型のタスク実行により、システムリソースの可用性が向上します	6
柔軟なNetwork Automation Multimasterアーキテクチャがシステムリソースのバランスを整えます	6
Network Automation Satelliteによるリモートオフィス管理の改善	6
重複するIPアドレスセグメントによって、リモートネットワーク統合が簡単になります	7
インテリジェント・リンクの冗長性がリモートネットワークの可用性を高めます	7
帯域幅の効率的な使用	7
信頼できる安全なプロトコルによるリモートオフィス・ネットワークへのアクセス	7
結論	8

ネットワーク自動化ソリューションの評価では、次の点を考慮する必要があります。

- 高い可用性が実現するか。また、その高可用性はサードパーティ・ベンダーによるものか。
- アーキテクチャは単一障害点を指し示すか。
- ネットワークが拡張した場合、そのソリューションはどのように対応するか。アーキテクチャに柔軟性が備わっているか。または「ワンサイズですべてに対応」型か。
- そのソリューションは分散型アーキテクチャを採用しているか。それとも単にフェイルオーバー・サポートだけを提供するものか。
- そのソリューションは、アクティブ/アクティブ高可用性を提供するものか。

全社規模でのネットワーク変更管理

古い諺に「見えないものを直すことはできない ("You can't fix what you can't see.)」、というものがあります。しかし今日の大規模で高度に分散したネットワークでは、ネットワーク全体の状態を確認したくてもネットワーク管理ツールによって制限を受けることになります。では、ネットワークのほんの一部しか確認することができなかったとしたら、どのように問題に対応したらよいのでしょうか。ネットワークのダウンタイムは相変わらず深刻な問題です。業界調査によると、ネットワーク・ダウンタイムは平均すると、企業にとって1分間で1万4,000ドルのコストに相当するとのこと。99.9%というきわめて高い可用性を実現するネットワークであっても、その金額は年70万ドル以上になります。また別の調査では、ネットワーク故障の48%が人による設定ミスであることが明らかになっています。ネットワーク全体に関係するエラーを引き起こす原因となる手作業での構成変更を追跡し、問題を解決したり、防止することができないと、ネットワークの可用性に深刻な影響が及び、セキュリティ違反が起こるおそれがあります。ネットワーク・インフラストラクチャのあらゆる要素に確実にアクセスできなければ、問題はさらに悪化します。

地理的または論理的境界の内側だけでネットワークを管理してもあまり意味はありません。多くの組織では、ローカルな変更情報を確認するため拠点ごとに管理ツールを備えています。その結果、同じ管理ツールのインスタンスが何十回も、孤立した環境内で実行されるだけで、ネットワーク全体に関するグローバルな可視性は得られません。問題を検出し、解決するために必要なのは、単一のビューでネットワーク全体を見通す可視性です。また構成のミスを防止するには、1カ所からネットワーク全体に対してベストプラクティス・ポリシーをプロアクティブに適用する必要があります。

まるで、地理的に分散した大規模なネットワークを管理しなければならない、という程度のことは課題としてたいしたことはないと言わんばかりに、多数の法律や規制により、災害復旧の機能を備えることが求められています。医療保険の相互運用性と説明責任に関する法律(HIPAA)やサーベンス・オクスリー法(SOX法)などの法律では、災害復旧ソリューションなどを利用してネットワーク運用の保護対策をとることが規定されています。

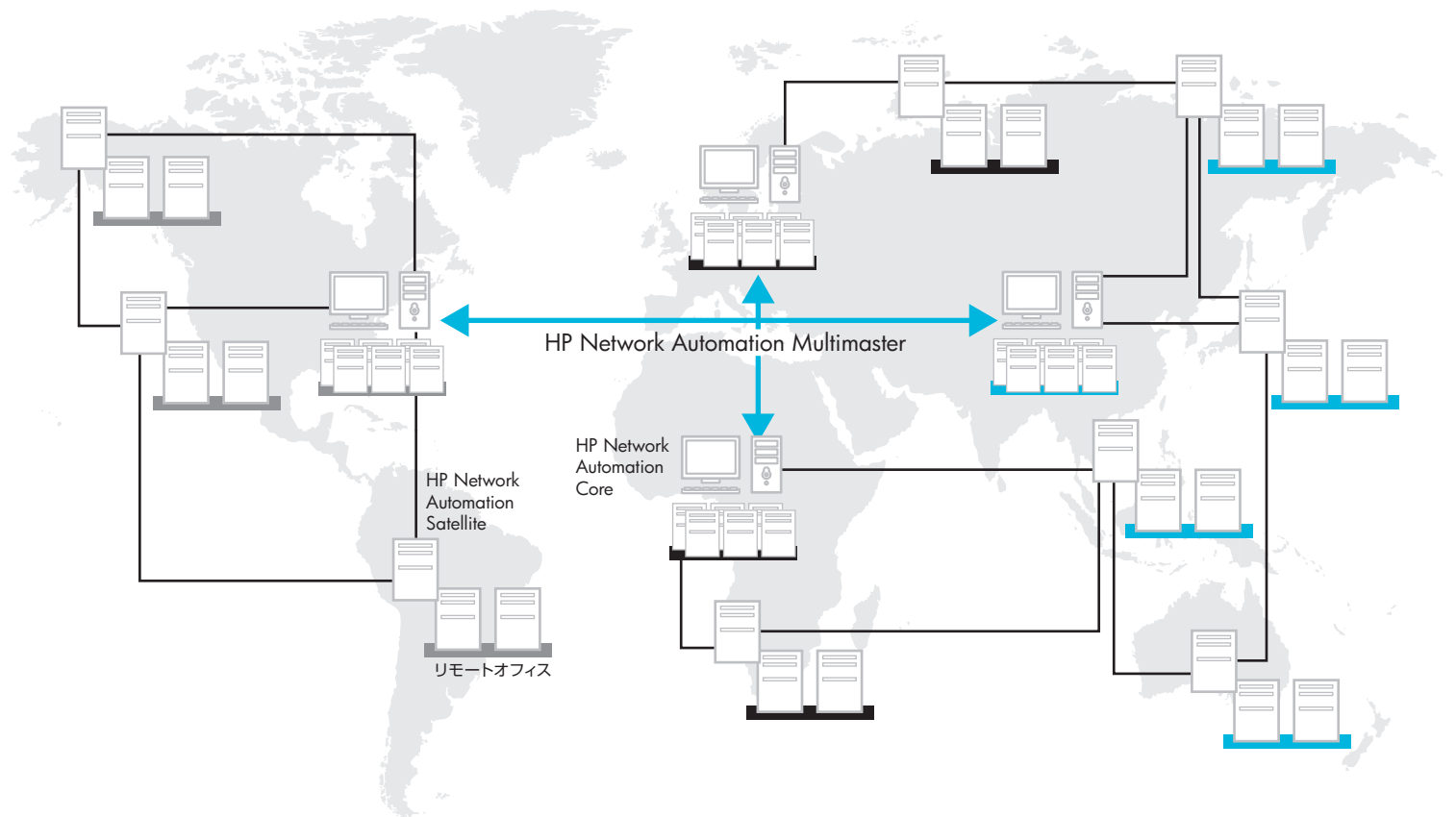
多くのソリューションで、構成変更の確認や、ネットワークポリシーの適用、災害復旧構成のバックアップが可能になってきましたが、こうした機能すべてを単一の仮想化管理ソリューションに統合して、地理的に分散したネットワーク全体にわたるグローバルな可視性とコントロールが必要です。

HP Network Automation software

HP Network Automation software(以下Network Automation)は、地理的に分散したネットワーク全体にわたって必要なグローバルな可視性とコントロールを提供します。Network Automationは、ペアメタル・プロビジョニングから、ポリシーベースの変更管理、コンプライアンス、セキュリティ管理まで、ネットワークデバイスの運用ライフサイクル全体を自動化します。

Network Automationは、さまざまな構成で使用することが可能なので、それぞれのエンタープライズ・ニーズに合わせるすることができます。HP Network Automation Multimaster softwareを利用してNetwork Automation Coreサーバの構成を実行し、たとえば世界中に分散するリモートロケーションのサポートなど、企業ネットワークをリアルタイムで可視化しコントロールすることができます。Network Automation Multimasterは自動的に情報を複製して複数の場所に配布できるので、新しい拠点でも

図1. Network Automationは、仮想化された単一のシステムを提供して分散型コンテンツを管理します。複数のNetwork Automation Coreサーバに対してNetwork Automation Multimasterを使用することで、ネットワーク環境から単一障害点がなくなり、迅速な災害復旧オプションやグローバルなポリシー適用が可能になります。



Network Automation Coreサーバを通じてすぐに情報を利用することができます。また、複数の拠点をまたがってネットワーク担当チームがベストプラクティスを活用し、ナレッジを共有できるようにし、企業全体にわたる運用が一貫性のあるものになります。

HP Network Automation Satellite softwareは、フル・プロトコル・アクセスが利用できない場合や、重複IPアドレスを使用する場合の、リモート・ネットワーク・デバイスへのアクセスで安全の強化を実現します。また、ネットワークに対してフェイルオーバー・サポートを提供することができます。

Network Automation MultimasterとNetwork Automation Coreを組み合わせると、以下を実行することができます。

- 単一の管理コンソールから、一元化されたビューで分散型インフラストラクチャを確認できる
- ベストプラクティス・ポリシーおよびコンプライアンス基準の一元的な適用
- 分散型インフラストラクチャ全体にわたるデータ冗長性により、災害復旧を促進
- Network Automation Coreサーバでのシームレスアクティブ/アクティブ高可用性を備えたフェイルセーフ・ネットワーク可用性

Network Automation Multimaster による拡張性、信頼性、可用性の向上

Network Automation Multimasterは完全分散型アーキテクチャを備えており、ネットワーク・インフラストラクチャ全体にわたる高可用性災害復旧を可能にします。Network Automation Multimasterは、拡張性と可用性に対する企業のニーズを満たす一方で、壊滅的なネットワークイベントが発生した場合に、社内および法規制関連のベストプラクティスへの取り組みを実現し、平均復旧時間(MTTR)を短縮できるアクティブ/アクティブな高可用性がもたらされます。

複数のNetwork Automation Coreサーバに対してNetwork Automation Multimasterを配備することで、ここで説明しているような数々の利点を得ることができます。

単一の管理コンソールから、一元化されたビューで分散型インフラストラクチャを確認

Network Automation Multimaster構成において他のNetwork Automation Coreサーバが代行するデバイスを含め、ネットワーク・インフラストラクチャ全体を単一のWebベース(HTTP)管理コンソールからローカル管理またはリモート管理することができます。一元化されたビューでネットワークを確認することが可能で、ネットワーク境界を横断する相互依存関係を容易に理解できるようになるので、情報に基づいて意思決定を下し、ネットワーク・インフラストラクチャを、より安全で、一貫性のある、予測可能な方法で管理できます。

ベストプラクティス・ポリシーおよびコンプライアンス基準の一元的な適用

ベストプラクティス・ポリシーを一元的に適用することが可能なので、管理者は、他の拠点で定義されたものを任意の拠点で使用することができます。また、ネットワーク・インフラストラクチャ向けのデータ・レプリケーションに加え、Multimeterアーキテクチャは、コマンドスクリプト、イベント通知規則、Network Automationポリシーなど、Network Automation Multimasterが実行されるNetwork Automation Coreサーバに追加されたデータをすべて伝達することにより、ネットワーク管理における一貫性を向上させます。

分散型インフラストラクチャ全体にわたるデータ冗長性により、災害復旧を促進

Network Automation Multimasterは、全体的なビジネスの継続性や、運用の継続性(COOP)、または災害復旧プランにおいて重要な役割を果たします。Network Automation Multimasterを実行することで、Network Automation Coreサーバは、レプリケーションによって最新の状態に保たれているNetwork Automationデータリポジトリ全体のコピーを保存することができます。Network Automation Coreサーバが停止したり、オフラインになった場合、データ完全性は別のNetwork Automation Coreサーバによって維持されるため、アクティブ/アクティブ高可用性が可能になります。オフラインサーバを復帰させる場合、そのデータは自動的に同期されます。さらに、Network Automation Coreサーバは、ネットワーク・デバイス・イメージ・ソフトウェアやNetwork Automationデバイスドライバを保守し、Network Automation Multimasterネットワーク全体にわたって同期をとることができ、データセンターが災害に見舞われた場合に再配備を迅速に実施し、MTTRの短縮を実現します。

シームレスアクティブ/アクティブ高可用性によるフェイルセーフ・ネットワーク可用性

Network Automation MultimasterとともにNetwork Automation Coreサーバを配備する場合、そのシステムから管理するデバイスを定義します。サーバが故障した場合も、そのデバイスを別のNetwork Automation Coreサーバから管理することができます。故障したサーバがオンラインに復帰した場合は、デバイスの管理を元のサーバに戻すことができます。

複雑なネットワーク管理では、構成とコンプライアンス管理が非常に重要です。Network Automationを利用すれば、成長するネットワーク環境を管理するために必要な可用性、可視性、拡張性を確保することができます。

安定性と拡張性

耐障害性と信頼性に加えて、Network Automation Multimasterには、変化し続けるネットワークのニーズに対応する拡張性が備わっています。使用可能な帯域幅を効率的に使用し、Network Automation Multimaster サーバにタスクをインテリジェントに配分し、複数のNetwork Automation Coreサーバの管理対象リソースのバランスを取ります。

効率的なタスク管理により、ワイド・エリア・ネットワーク(WAN)のトラフィックを減らし、ローカル・エリア・ネットワーク(LAN)の使用を増加させます

地理的に分散された設備の場合、Network Automation Multimasterを備えた複数のNetwork Automation Coreサーバを使用することで、ネットワークの利用率を向上させることができます。たとえば、デバイスがワシントン州シアトルに500台あり、フランスのパリに1,000台あるとします。これらのデバイスを管理するには、各拠点にNetwork Automation Coreサーバを配置する必要があります。結果的に、タスクはWANを利用することなく、ローカルに処理されることとなります。ローカルのNetwork Automation Coreサーバは、デバイス構成や画像アップロードといったタスクを実行することで、デバイスへのアクセス効率と信頼性が向上します。

分散型のタスク実行により、システムリソースの可用性が向上します

Network Automationはマルチスレッド型のタスクベース・ソフトウェアです。すべての管理タスクがキューに送られ、スケジュールに従って実行されます。Network Automation Multimasterを実行する複数のNetwork Automation Coreサーバにより、タスクを単一の中央サーバで実行するのではなく、負荷を分散させて複数のサーバで実行することができるため、システムリソースをより効率的に活用することが可能になります。

柔軟なNetwork Automation Multimasterアーキテクチャがシステムリソースのバランスを整えます

Network Automation Multimasterでは、複数のサーバでNetwork Automationの機能を利用することができます。たとえば、大規模なNetwork Automation環境で、複数の管理タスクを同時に実行しようとするサーバに大きな負荷がかかりネットワーク速度が低下してしまいます。これは、あまり好ましい状況ではありません。Network Automation Multimasterを使うことで、デバイスを割り当てずに任意の数のNetwork Automation Coreサーバに構成することができ、それをタスク生成やリモートプロキシ、その他類似のタスクに使用することができます。さらに、タスク実行を専用サーバにオフロードし、管理サーバのリソースを解放することが可能です。

Network Automation Satelliteによるリモートオフィス管理の改善

Network Automation Satelliteは、エンタープライズ・ネットワークにおけるNetwork Automationの利用範囲をさらに広げます。リモートオフィスのネットワークは従来、IPアドレス構成の競合やネットワークリンクの信頼性の低さから、管理が難しいとされてきました。しかしNetwork Automation Satelliteを利用することで、リモートオフィスをエンタープライズ管理に簡単に統合することができるようになりました。一元管理されるコンソールから、安全なコミュニケーション・リンクを通じてリモートオフィス・ネットワークを確実に管理できるので、各リモートネットワークを個別の領域として取り扱うことができます。

Network Automation Satelliteはまた、完全メッシュ型配備でのインストールが可能なため、リモートオフィス・ネットワーク管理で高い可用性やデータ冗長性を確保することができます。

Network Automation Satelliteをメッシュ方式で配備することにより、ここで説明しているような数々の利点を得ることができます。

重複するIPアドレスセグメントによって、 リモートネットワーク統合が簡単になります

Network Automation Satelliteは、ネットワークアドレスが、Network Automation Core サーバやNetwork Automation Multimaster サーバによって管理されているローカル・ネットワークと重複したり、競合しているリモートオフィス・ネットワークの管理を行うことができます。Network Automation Satelliteサーバは、Network Automation Coreサーバのスケールダウン・バージョンです。レルムIDによってリモートオフィス・ネットワークを識別し、そのIDをNetwork Automation Coreサーバに通知します。

インテリジェント・リンクの冗長性が リモートネットワークの可用性を高めます

Network Automationと同様に、Network Automation Satelliteサーバも、故障が発生したとき、他のNetwork Automation Satelliteサーバでフェイルオーバー・サポートを実行します。OSPF (Open Shortest Path First) ルーティングプロトコルは、リモートオフィスまたはサテライト配備によって確立され、Network Automation Coreサーバによる、リモートオフィス・デバイスへの最短で、もっとも信頼性の高いパスの検出を可能にします。

帯域幅の効率的な使用

Network Automation CoreサーバとリモートのNetwork Automation Satelliteサーバの間のトラフィックフローを管理するために帯域幅スロットルを利用することができますが、これは、帯域幅の影響を受けやすいリンクによるデバイス管理で特に重要になります。たとえば、Network Automation CoreサーバとNetwork Automation Satelliteサーバの間に256 KBリンクがある場合、サテライト・トンネルを設定して128 KBを使用し、トンネルの残り部分は他のトラフィックに割り当てることが可能になります。

信頼できる安全なプロトコルによる リモートオフィス・ネットワークへのアクセス

Network Automationは、リモートネットワーク上のNetwork Automation CoreサーバとNetwork Automation Satelliteサーバの間に、SSL(Secure Sockets Layer)を使って安全性の高い通信プロトコルを設定することができます。これはSSH(Secure Shell)をサポートしていないレガシーデバイスの管理や、Telnetやrloginなど保護されていないコマンド・ライン・インタフェースを使用するとき、重要になります。Network Automationは、プロトコルにかかわらず、データセンターとリモートオフィス間のデータストリームを保護し、安全性を確保します。さらに、Network Automation SatelliteサーバはTCP 443ファイアウォール・ポートをトラバースし、リモートオフィス・ネットワークとのシームレスな統合を可能にし、ファイアウォールの完全性を維持します。Network Automation Coreサーバによって開始されたTelnetおよびSSHセッションは、Network Automation Satelliteサーバが設定したSSLトンネルをトラバースし、要塞ホストやサードパーティ・ソリューションの必要性を減じます。

結論

複雑なネットワーク管理では、構成とコンプライアンス管理が非常に重要です。Network Automationを利用すれば、成長するネットワーク環境を管理するために必要な可用性、可視性、拡張性を確保することができます。Network Automationアーキテクチャでは、ネットワーク帯域幅をインテリジェントに利用することができ、またセキュリティ違反を犯したり、本稼働環境に影響を与えたりすることなく、企業のセキュリティポリシーやベストプラクティスを遵守することができます。ネットワーク構成やコンプライアンス・データの一元管理リポジトリでは、ネットワーク変更の標準化や監査における一貫性が保たれます。Network Automationは、こうしたメリットを現実のものとし、またネットワーク管理ツールの隠れたリスクの排除を支援します。

本ホワイトペーパーは、米ヒューレット・パッカートの

「The need for global network audit and control : employing HP Network Automation software for scale and visibility」を翻訳したものです。

お問い合わせはカスタマー・インフォメーションセンターへ

03-6416-6660 月～金 9:00～19:00 土 10:00～17:00 (日、祝祭日、年末年始および5/1を除く)

HP Software製品に関する情報は <http://www.hp.com/jp/hpssoftware>

記載されている会社名および商品名は、各社の商標または登録商標です。

記載事項は2008年5月現在のものです。

本カタログに記載された内容は、予告なく変更されることがあります。

© Copyright 2008 Hewlett-Packard Development Company, L.P.

本カタログは、環境に配慮した用紙と植物性大豆油インキを使用しています。



日本ヒューレット・パッカート株式会社
〒102-0076 東京都千代田区五番町7番地