ManageEngine
OpManager

11 ネットワーク障害からビジネスを救う ベストプラクティス

ネットワーク管理のベストプラクティスガイド

-Vignesh Karthikeyan

アジェンダ

イントロダクション 1

1. 既存のコンフィグを削除し、すべての機器を再設定 2

2. 監視する適切なパラメーターを選択 3

3. ネットワーク内のインターフェースを監視 4

4. 障害ではなく、症状を監視 5

5. 機器のグループ化とタスクの自動化 6

6. SyslogとTrapを使用する利点 7

7. 監視していない機器は重要 9

8. 計画変更の実装 10

9. 細かいアップデートを無視しないこと 11

10. ネットワークが小規模なうちにタスクを自動化 12

11. 適切なネットワーク管理ツールを選択 13

イントロダクション

- 2017年2月18日、 Slack、Buffer、Business Insider、その他多くのウェブサイトやサービスが応答しなくなりました。これらのサイトは人気の高いクラウドベースのサービスであるAmazon S3を使用しています。Amazon S3が突然5時間にわたり停止したため、その上で稼働するサービスも停止せざるを得ない状況となりました。Amazonが自身のAWSステータスダッシュボードを更新できなくなったほど、非常に深刻な障害でした。

- 2017年5月には、世界的な航空会社システムに障害が発生し、75,000人の乗客に影響を及ぼしました。この障害は、数時間では復旧せず3日間にわたり、726ものフライトがキャンセルされたと伝えられています。航空会社は評判の悪化とともに8000万ポンドの財務上の損失を被ったことになります。

- 2011年4月には、アフリカのジョージア国の女性がスクラップ金属を探している間に偶然ケーブルを傷つけてしまいました。このケーブルは重要なネットワークケーブルであり、アルメニア共和国全土で5時間もの間インターネットが使えない状態になりました。

上記の例の共通点は何でしょうか。それらはすべてネットワークのダウンタイムにより発生した問題です。ネットワークがダウンしたことにより、何百万ドルもの損失が発生しました。

不適切な戦略計画や無計画な採用プロセスなど、重要な決定が誤っていた場合、成功したビジネスを停止させる可能性さえあります。しかし、これらよりもさらに大きな懸念を引き起こす一つの問題があります。それは、不十分なネットワーク管理です。採用やビジネス戦略の成功可否は数カ月、さらには数年判断しますが、ネットワーク管理の質が悪いと、ビジネスは数秒で完璧に破壊できます。

このホワイトペーパーでは、ネットワークのダウンタイムや、不十分なネットワーク管理から生じる潜在的な損失を防ぐのに役立つ、ネットワーク管理のための11のベストプラクティスを紹介します。

ベストプラクティス＃1

既存のコンフィグを削除し、すべての機器で再設定

すべてのネットワーク機器には、デフォルトのコンフィグ一覧が付属しています。ネットワーク管理者の多くはデフォルトのコンフィグを削除し、環境に合わせた設定に書き換えますが、ネットワークシステムには必要ないパラメーターについては特に設定せずにスキップする傾向があります。管理者に重要ではないと見なされるこれらのパラメーターには、デフォルトの認証情報とコンフィグが使用されています。見落としてデフォルトのまま放置された設定は、大きなセキュリティ脆弱性となります。

“

嬉しくない事実

組織内のデータ漏洩/侵害の80%は、不適切またはデフォルトのクレデンシャル情報が原因で発生しています。

組織内で使用しないため、変更されなかった重要なコンフィグ考えてみましょう。これは組織のネットワーク全体を露出させ、ネットワークへの外部からの侵入を容易にします。使用していない設定であっても、デフォルトの機器設定（「admin」、「password」、許可されている認証情報の組み合わせなど）を必ずすべて削除する必要があります。

ネットワーク管理で機器のセキュリティを確保するための重要な手順

1. 新しい機器をネットワークに追加するときは、その機器に付属しているすべてのデフォルトコンフィグ（使用しないものも含む）が再設定されていることを確認します。
2. 未使用のコンフィグであっても、辞書的な認証情報を使用しないでください。
3. ネットワークで使用されているコンフィグだけでなく、使用されていないものに対しても、認証情報を定期的に変更します。
4. ポイント2と3を実装するための強力なパスワードポリシーを適用します。

ベストプラクティス＃2

機器の種類と重要度に基づき監視する適切なパラメーターを選択

ネットワーク内のすべての重要な機器とインターフェースを監視することは、ネットワークの落とし穴からビジネスを保護するための重要な鍵です。ただし、ただ監視するだけではなく、各機器とインターフェースで監視すべきパラメーターを検討する必要があります。

すべての機器ですべてのパラメーターを監視する必要はありません。また、機器に対して監視するすべてのパラメーターが重要というわけでもありません。ネットワーク内の各機器を監視するためのパラメーターの正しい組み合わせを決める必要があります。

監視間隔はどれくらいが適切か？

効果的なネットワーク監視に寄与するもう1つの重要な要素は監視間隔です。重要な機器やパラメーターに対しては監視間隔を短くし、重要度が下がるにつれて長く設定します。

機器で監視するパラメーターを決定するときには、2つの要素を考慮する必要があります：

- **機器の重要度**：プライマリサーバーと他の重要な機器は、それらすべてのパラメーターを監視する必要があります。プリンターテスト機器など、機器の重要性がそれほど高くない場合は、その機器またはインターフェースが機能しているか確認できる基本的なパラメーターのみを監視します。これにより、管理ツールに不要な負荷が掛からなくなり、ネットワーク内のトラフィックが減少します。

- **機器タイプ**：機器タイプが異なれば、監視する必要がある基本パラメーターも異なります。たとえば、温度の急激な上昇はCPUが過度に使用されていることを示しているため、温度はCPUにとって不可欠なパラメーターです。

以下の手順で、どのパラメーターを監視する必要があるか判断します：

- 重要度の高い順にネットワーク内のすべての機器を分類して優先順位リストを作成します。重要度に応じて高、中、低と分類します。
- 重要度高の場合は、すべてのパラメーターを監視します。
- 重要度中の場合は、機器のタイプとベンダーに応じて、必須パラメーターといくつかの追加パラメーターを監視します。
- 重要度低（テストまたはダミー機器など）の場合は、機器のステータスに関する情報を提供する基本的なパラメーターのみを監視します。

ベストプラクティス＃3

機器としての重要度を重視しながらネットワーク内のインターフェースを監視

ネットワーク監視の一般的な定義は、ダウンタイムと潜在的なビジネス損失を防ぐために、ネットワーク内の機器を監視することです。多くのネットワーク管理者はこの定義を実直に守り、ネットワーク内の機器を監視するだけに留まりがちです。

“

嬉しくない事実

機器インターフェースの障害が、主要なダウンタイム全体の25%を占有しています。

しかし、機器障害またはネットワーク障害は、必ずしも機器内の障害だけによって発生するものではありません。機器を相互に接続するインターフェースで障害が発生することがあるので、ネットワーク内の機器と同じくらいインターフェースを監視することが重要です。

現在、ほとんどの監視ツールには、ベンダー固有のインターフェース用のテンプレートが付属しています。それらを活用して、ネットワーク内のインターフェースのパフォーマンスを詳細に分析します。

インターフェースが稼働しているかの確認は、定期的なポーリングだけで完了させるべきではありません。インターフェースのパラメーターがしきい値を超えたときにアラートを受け取るように、ネットワーク監視ツールでインターフェースのしきい値を設定します。

Linux機器のethXのようなネットワーク内のすべてのインターフェースに注意してください。ルーター・スイッチにはループバック、イーサネット、アップリンク、そしてストレージにはファイバチャネルとループバックなど、数多くのインターフェースがあります。手間を考え、監視ツールによって監視されているインターフェースのみで潜在的な障害と警告の予兆を監視したいと思うかもしれません。重要ではない機器のインターフェースの監視パラメーターを制限したい場合もあるでしょう。しかし、監視ツールは、ネットワーク内のすべての重要なインターフェースを確実にカバーするようにすることが重要です。

監視ツールでインターフェースを監視する場合、インターフェースに対して行われたアップグレードや変更が、監視ツールで更新されていることを確認してください。これは、インターフェースの誤動作によるネットワークのトラブル防止に大いに役立ちます。

ベストプラクティス＃4

障害ではなく、症状を監視

ネットワーク監視の目的は、ネットワークが障害や想定外のダウンタイムに陥って業務が停止するのを防ぐことです。ほとんどのネットワーク管理者は、サーバーの停止やネットワークの停止など、ネットワーク内の障害を監視するためにネットワーク監視ツールを設定します。

ネットワーク内の障害を監視する際の難しい課題は、「障害自体は影響であり原因ではない」ことです。

より正確に言うと、ネットワークで障害（ネットワークのダウンタイムや特定の機器へのアクセス性の欠如など）が発生するたびに、大抵の場合は、その障害の原因は突然発生したも

のでないということです。障害の前に起こった一連の事象が、最終的な障害を引き起こした可能性があります。原因となったの事象（トリガー）が早期に特定され発見された場合は、適切な解決策を講じることができ、ほとんどの場合、これらの症状が最終的な障害にならないようにできます。症状を監視するという方法は、ネットワーク管理に対するはるかに積極的なアプローチです。

どのようにして症状を監視しますか？

- **複数のしきい値を設定**：ほとんどの監視ツールでは、事前に警告するために複数のしきい値を設定できます。この機能を使用して、重要な機器とパラメーターに複数のしきい値を設定します。
- **分析に始まり分析に終わる**：アラートの履歴を管理して分析します。特に繰り返し発生するアラートでパターンを検索します。見逃されているパターンが、障害の共通の根本原因である可能性があります。

ベストプラクティス＃5

監視ツールに機器を追加する際に、機器をグループ化して、関連する特定の監視タスクを自動化

ネットワーク監視の目的は、ネットワークが障害や想定外のダウンタイムに陥って業務が停止するのを防ぐことです。ほとんどのネットワーク管理者は、サーバーの停止やネットワークの停止など、ネットワーク内の障害を監視するためのネットワーク監視ツールを設定します。

効率的な機器グループ化のメリットは次の3点です：

- 機器の監視とメンテナンスを容易にします。
- 一括設定変更および機器更新を容易にします。

- 特定のパラメーターに基づいて機器をグループ化すると、ネットワークパフォーマンスの分析を詳しく調べるのに役立ちます。

機器タイプ、ベンダー、高帯域消費など、さまざまなパラメーターに基づいて複数のグループを作成する必要があります。機器のパフォーマンスをよりよく理解するために、各機器を複数のグループに分類します。

たとえば、Ciscoサーバーは、サーバー（機器タイプ）、Cisco（ベンダー）、および高帯域消費（ネットワークをより適切に管理できるようにするカスタムカテゴリ）のカテゴリに分類できます。この種の分類は、更新のインストールや、コンフィグ変更をより簡単にします。

監視ツールに追加されるすべての機器には、それぞれ監視すべき監視項目があります。これらの監視項目は機器のステータスとパフォーマンスに関する重要な情報を提供します。

監視ツールに機器を追加しながら、機器に対してこれらの重要な監視項目を有効にするプロセスを自動化すると、多くの手作業と時間を節約できます。

特定の種類の機器が検出されたときに選択した監視項目を自動的に有効にするために、監視ツールで事前にルールを作成します（ネットワーク監視に使用するツールによって異なります。ほとんどのツールは自動化をサポートしていますが、いくつかの無料のツールや基本的なバージョンではこれらの自動化をサポートしていません）。

ベストプラクティス＃6

SyslogとTrapを使用する利点

SyslogとTrapは、機器から監視ツールに送信される情報です。他のデータは、監視ツールは定期的に機器をポーリングして取得しますが、SyslogとTrapは 機器から監視ツールに自動的に送信されます。

ネットワーク監視の効率を向上させるために、SyslogとTrapをどう活用すべきでしょうか。

ネットワーク内のほとんどのパラメーターと機器は、定期的なポーリングを通じて監視されます。監視ツールが特定の間隔で機器をポーリングしてそのステータスを確認します。この手法の問題点は、

- 定期的なポーリング間隔で発生した機器障害がすべて表示されるわけではありません。
- 障害に対するアラート通知は、発生時に即座に起動する必要があります。これは定期的なポーリングでは実行できません。

たとえば、監視ツールが2分ごとにその可用性について機器をポーリングする状況を考えてみましょう。

機器の可用性に関するデータが監視ツールに表示されるのは、2分後、4分後になります。機器が3分後に停止し、30秒後に元に戻ったとします。その30秒の間、ネットワークでの処理は起こらなかったでしょう。しかし、監視ツールのグラフはその間に起こったその休止時間痕跡を捕らえることはできません。

このような状況ではSyslogとTrapを活用すべきです。3分間のダウンタイムが発生した場合、機器は監視ツールにTrapを送信し、Syslog情報はシステムが機能を停止したことを記録できます。

TrapとSyslogメッセージを有効活用するには、重大なエラーを示すTrapが受信されたとき、または受信されたSyslogにエラーメッセージが含まれているときにアラートを発行するように、ネットワーク監視ツールを設定します。

SyslogやTrapによって提供されたデータを利用するようにネットワーク監視ツールを設定することで、他の方法では見逃していたかもしれないエラーを見つけることができます。

ベストプラクティス#7

監視していない機器は、監視しているものと同じくらい重要

ほとんどのネットワーク管理者は、すべての機器を監視するわけではありません。重要な機器だけを監視するか、監視ツールの範囲外の重要でない機器を除外します。その理由は、ほとんどの監視ツールのライセンスは監視されている機器の数に基づいているため、重要でない機器を追加するとライセンスコストが増加してしまうからです。

この主張は合理的ですが、それには大きな落とし穴があります。経験豊富なネットワーク管理者なら誰でもこれを教えてくれるでしょう：

いつ機器が重要になるか誰も予測することはできません。

> **嬉しくない事実**
>
> 中小企業のネットワークのダウンタイムの1時間あたりの平均コストは約470万円です。
> そして、ネットワークのダウンタイムの最大の原因は、ハードウェア障害です。

テストマシンや重要ではない機器など、監視ツールに追加されていない機器を追跡することが重要です。
そのような機器に追加の機能を追加するとき、または機能の追加が重要になると感じる場合は、すぐにその機器を監視ツールに追加してください。

以前は重要でなかった機器を監視ツールに追加する場合、管理の手間から、監視するパラメーターの数を制限したいと感じるかもしれません。この場合でも、必要なパラメーターは監視してください。これらの機器が非常に重要になります。監視コストは、予防できる損失により採算を合わせることができます。

ベストプラクティス＃8

有用性と重要度に基づく計画変更の実装

いかなる変更も最小限のダウンタイムで実行されなければならず、重要な業務に影響を与えてはなりません。ネットワークへの変更を計画することは、ネットワークを効率的に管理する上で重要な役割を果たします。通常、最善の方法は、実稼働時間外にネットワークに変更を加えることです。これにより、ビジネスレベルへの悪影響がないことが確実になります。また、障害が発生した場合に備えて、変更をロールバックする時間の余裕も生まれます。

変更実装の最良なタイミングを知るためには、4つの点を加味する必要があります。

- **変更の重要性**：変更が重大なセキュリティバグの修正である場合は、できるだけ早く実施する必要があります。
- **変更期間**：実装に数分しかかからず既存のシステムに損傷を与えない重大なバグ修正は、稼働時間内に実装することができます。数時間を要する重大なバグ修正は、稼働時間外に実装する必要があります。
- **ネットワーク規模**：ネットワークが小規模で、バックアップサーバーがない場合は、最も重要な変更でさえ、稼働時間外まで待機する必要があります。
- **回復時間**：変更の実装中に障害が発生した場合、システムが回復するまでにどれくらい時間がかかるでしょうか。変更がいくら小さくても、変更に要するシステムの停止時間に回復のための時間も含まれていることを認識する必要があります。

承認の階層がある場合：変更承認の階層は、変更を実装ための承認を受ける必要のある一連の方々です。階層は、最も低いレベルで変更を実装する人から始まり、それからずっと上層部の管理者に達する必要があります。重要性や影響にかかわらず、すべての変更は、必ず変更承認階層を通過した後に実施する必要があります。

ベストプラクティス＃9

細かいアップデートを無視しないこと

ネットワークの変更実装プロセスとそれに伴うリスクの管理が複雑であるという理由で、重要なバグ修正、不可欠なコンフィグ変更ではない限り、ネットワークへの変更を行わない管理者が多くいます。この考え方により、ネットワーク管理者は機器ベンダーから提供された小さなアップデートを無視する傾向があります。

“

嬉しくない事実

重要でないアップデートをインストールしないと、機器の脆弱性が増します。このため、ほとんどのベンダーは、過去のアップデートがすべてインストールされるまで最新のアップデートインストールを許可しません。

重要でないアップデートを無視することで、一見すると不要なダウンタイムと変更プロセスを節約できるかもしれません。ベンダーが発行するすべてのアップデートが重要というわけではありません。しかし、ベンダーは通常、重要なアップデートの前に複数の小さなアップデートプログラムを発行します。重要なアップデートプログラムを実行するには、これらの小さなプログラムの一部が必要になります。

そのため、小さいアップデートを無視して重要なアップデートのみを行うことは、結果的に重要なアップデートプログラムのインストールが不適切に行われることになります。時々これらの小さなアップデートをスキップすることによって、実際に重要なアップデートを大きなセキュリティ脆弱性に変えるかもしれません。

毎日のスケジュールダウンタイムを避けて、最小のアップデートで対応できるようにするためのヒントをいくつかご紹介します：

- 機器製造元が発行するすべてのアップデート（機器固有およびベンダー固有）の仕様を確認します。これは、アップデートの目的を理解するのに役立ちます。
- 重要なアップデートのインストールを一旦待ちます（ただし、アップデートを無視することは絶対やめましょうしないようにします）。
- 複数の小さなアップデートをまとめて一度にインストールします。製造元によって発行されたすべての小さなアップデートをインストールする毎週の停止時間を設けます。

ベストプラクティス＃10

ネットワークが小規模のうちにタスクを自動化

“

嬉しくない事実

ネットワーク管理者の5人に1人が、組織のネットワークが現在のサイズの5分の1であった時に、基本的なタスクを自動化しておけば良かったと考えていることを明らかにしました。

ネットワーク規模が小さい場合は、管理を内製化することは簡単です。ネットワークが構築された初期段階では、ほとんどのネットワーク管理タスク（ダウンタイムのスケジュールや機器アップデートのインストールなど）はネットワーク管理者によって手動で行われます。
ネットワークの拡大に伴い、自動化の利用を検討する組織が多くあります。

ネットワーク管理の経験が豊富な方なら誰でも、上記のネットワーク管理アプローチは非常に問題があると言います。なぜでしょうか。手動によるアプローチは非常にミスが発生しやすく、次にネットワークが大規模化し、より複雑でマルチベンダー環境になるにつれて、何らかの種類の自動化を実装することがますます困難になります。したがって、必要性を感じていなくても、可能な限り自動化の力を活用しましょう。たとえそれが単純作業でも、後にメリットを享受できるでしょう。

ネットワークの初期段階で自動化できるもので、長期的に役立つもの
のリストです：

- ネットワーク監視ツールに新しい機器を追加するプロセス
- ネットワーク機器のダウンタイムの計画とスケジューリング
- メンテナンス作業とリモート操作の実行
- 任意の機器が特定のパラメーターの特定のしきい値制限を超えたときのアクションの実行
- データベースのバックアップ、および機器レベルとネットワークレベルの設定

ベストプラクティス＃11

適切なネットワーク管理ツールを選択

このホワイトペーパーに記載されているすべてのベストプラクティスのうち、これが最も重要です。要件、ネットワークの規模、ネットワーク管理の戦略にかかわらず、ネットワーク管理を成功させるのは、最終的には正しいネットワーク管理ツールを選択することです。

市場にはさまざまなネットワーク管理ツールがあります。それぞれが独自の機能を備えていますが、長所も短所もあります。組織に適したネットワーク管理ツールを選択することは、監視要件を慎重に判断し、市場にあるツールを分析することによって可能です。

適切なネットワーク管理ツールを選択しないことは、その仕事に適さない増員を行うことに似ています。それはネットワーク管理者としての仕事を複雑にするだけでなく、ネットワークの落とし穴に落にはまることになるでしょう。

自社に合わないツールの選定を防ぐ方法は次のとおりです：

- まず初めに、ネットワーク管理で達成すべき目標と要件を明確にし
- ます。
- ほとんどのツールには無料の試用期間があります。試してみましょう。
- 製品ベンダーにデモを依頼します。製品利用者が書いたレビューを読みます。
- 機能のセットアップおよび使用の容易さを分析します。
  正しいツールを決定するために、さまざまなツールの試用版を並行して使います。

正しいツールの選定についてご質問がある場合は、以下の「オンライン相談窓口」よりご相談ください。

■オンライン相談窓口■

https://www.manageengine.jp/online_meeting/

正しいネットワーク管理ツールを選定するのに役立つクリティカルメトリクス

- ネットワーク管理の要件はツールの機能と一致していますか？
- ネットワーク管理の要件はツール内で簡単に確認できますか？
- ツールがサポートする機器の数は、ネットワークの規模と一致していますか？
- ツールは、ネットワーク内にあるあらゆる種類の機器をサポートしていますか？
- 技術サポートはどうですか？
- ツールの拡張性はどうですか？
- 価格設定は会社の予算に受け入れられますか？

ZJMR2019416342