# Splunk IT Essentials Work

すべてのITデータを1つの画面にまとめてトラブルシューティングを迅速化

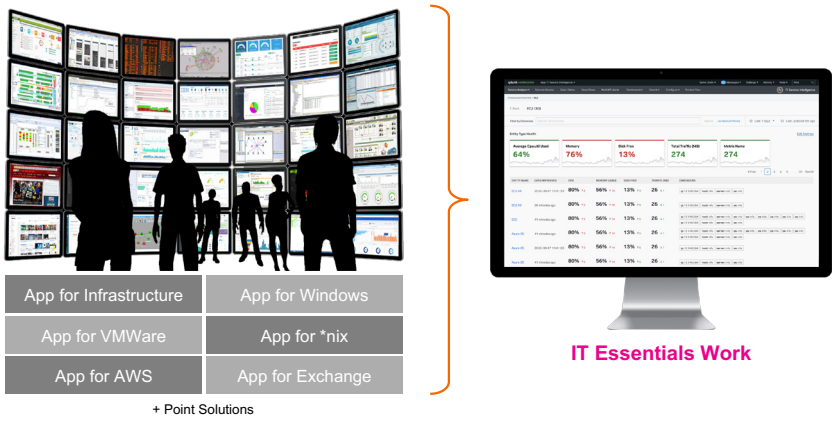
- すぐに使えるダッシュボードと受信データの自動入力(既存のSplunkアドオンを使用)によって**短期間で価値を実現**
- **ログとメトリクスの相関付け**によって、エンティティのコンテキストを迅速に取得
- **アラートイベントの詳細を正確に調査**することで、平均解決時間(MTTR)を短縮
- **すべてのインフラデータを一元的に可視化**することで調査を迅速化

**サポートされる監視対象のエンティティ**

- *nix
- Kubernetesノード
- Kubernetes Pod
- Unix/Linuxホスト
- VMwareクラスター
- VMwareデータストア
- VMware ESXiホスト
- VMWare vCenter
- VMware VM
- Windowsホスト
- その他

今日のITチームは、多種多様なツールやアプリケーションのデータスタックへの対応に追われています。IT環境内のすべてのコンポーネントを包括的に可視化できないために中途半端なインサイトしか取得できず、調査に時間がかかり、根本原因を特定できずにいます。また、本番環境の個々のエンティティにログインすることは、安全でないうえに非効率的です。必要な資格情報をすべて共有してから、「部屋ごと」に調査を行うのでは、貴重な時間と労力を無駄に消費してしまいます。また、タイミングよく調査を行わなければ、ポイント監視ソリューションからログが「削除」されてしまい、データが不完全なために分析はますます困難になります。ITチームは、本来は不要かもしれない再起動を行うように要求されることもあり、そのためにMTTRがさらに長くなり、ユーザー、従業員、顧客の不満が高まります。

**IT Essentials Workでは、Splunk Appsやサードパーティのポイントソリューションが1つのビューに集約されるため、コンテキストを切り替える手間を減らすことができます**




Splunk IT Essentials Work (ITE Work)を使用すれば、アラート対応の効率化、調査ワークフローの合理化、トラブルシューティングの迅速化を実現できるため、ITチームは高度なIT管理を簡単に始めることができます。Splunkによってツールを統合し、コストと複雑さを軽減し、すべてのITデータを相関付けて一元的に可視化することで、環境全体のパフォーマンスと健全性をより効果的に把握できます。

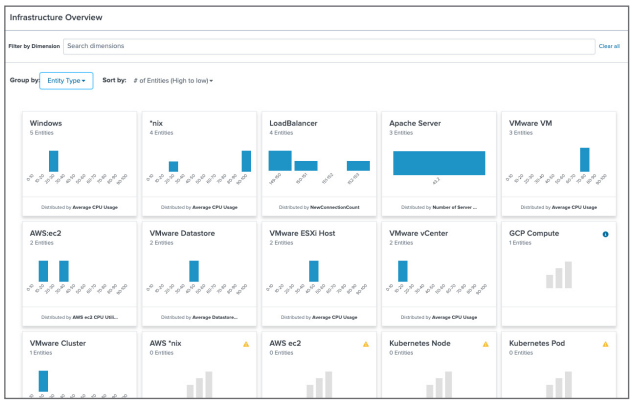
ユーザーは、規範的で厳選された習得しやすいコンテンツと、段階的なガイダンスを使用して、ITの一般的なタスクやユースケースにSplunkの導入を拡張および促進できます。また、ITE Workを使用すれば、メトリクスを使用してアラート対応を効率化し、合理的な調査ワークフローやログを使用したトラブルシューティングへと迅速に移行できるだけでなく、これらをすべて1つのワークスペースで実現できます。**これは、あらゆるITチームにとってモダナイゼーションを進める際の基盤となります。**

## 主要な機能

エンティティとは、サービス提供のために管理が必要なITコンポーネントを表します。一般的にエンティティはホストを表しますが、クラウドや仮想リソース、ネットワークデバイスやアプリケーションである場合もあります。IT Essentials Workは、各エンティティのログとメトリクスを相関付け、ログベースの分析を使用して、すべてのエンティティのパフォーマンスを監視および把握します。これによってサイロ化を防止し、データの取り込みとカスタムダッシュボードの構築に要する時間を短縮します。

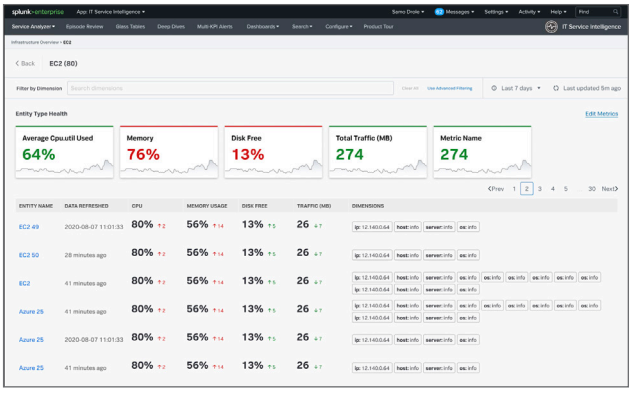
### インフラストラクチャオーバービューを表示しエンティティの健全性を監視

すぐに使えるダッシュボードには、さまざまなエンティティの主要なKPIの状態が表示されます。インフラストラクチャオーバービューのダッシュボードでは、エンティティレベルだけでなくインフラ全体の状態も把握できます。表示された内容から、CPU使用率が高いエンティティを特定し、そのエンティティをドリルダウンして原因を特定することができます。エンティティタイプ別にグループ化したり、フィルタを適用したり、特定のメトリクスデータに関連するログを確認する機能を使用してログベースの分析を実行できるため、トラブルシューティングを迅速かつシームレスに実行できます。



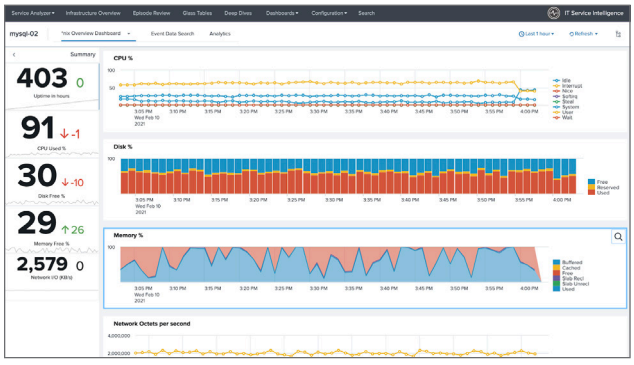

### アクティブなエンティティを包括的なビューにまとめてコンテキストの切り替えを削減

すべてのデータ(メトリクスやログイベントデータなど)を1つのビューで確認し、コンテキストやパフォーマンスに関する主要な要素を相関付けることができます。また、グループを定義することで、インフラのメトリクス、ステータス、アラート、調査結果を簡単にグループ化してフィルタリングすることができます。この包括的なビューでは、インフラの健全性を詳細に確認できるため、エンティティのパフォーマンスを監視して把握できます。1つのワークスペースで環境全体を可視化できるため、コンテキストの切り替えを減らしながら、トレンドを容易に見極め、調査を直ちに実行できます。



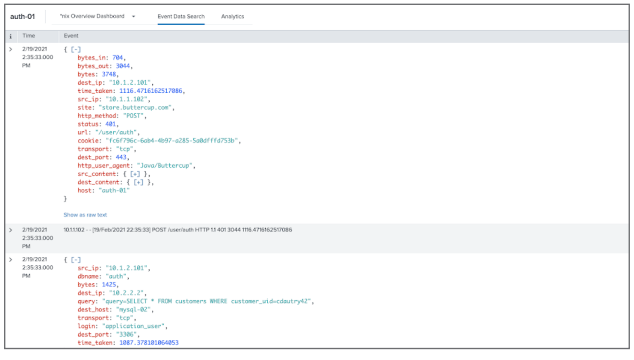

### データをドリルダウンして調査ワークフローを合理化

IT Essentials Workにはすぐに使えるダッシュボードが備わっているため、すぐに使い始めて、主要なKPIステータスの経時的な変化を確認できます。また、トレンドを簡単に見極め、KPIステータスが変化した時点を特定できるほか、エンティティの健全性のページからドリルダウンし、すべてのホストの平均CPU使用率、平均メモリー使用率、平均データストア遅延、平均ネットワークトラフィックなどのメトリクスも監視できます。さらに、IT Essentials Workを使用すると、状況の把握、障害のトラブルシューティング、特定の問題のエンティティレベルでの把握が可能になります。クエリやコードを書いたり、カスタムダッシュボードを作成する必要はありません。



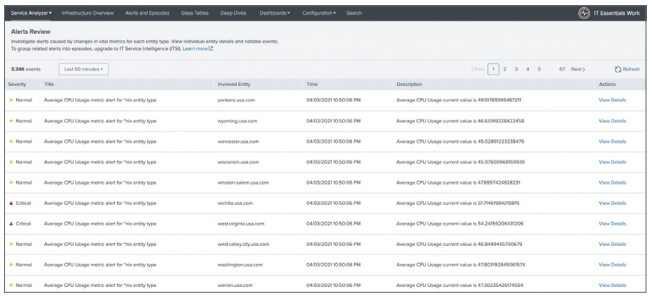

### イベントデータサーチで過去60分間の関連ログを表示

IT Essentials Workにはイベントデータサーチと呼ばれる機能があり、これを使用してインフラの健全性を素早く分析できます。イベントデータサーチ機能では、さまざまな種類のインフラに存在するエンティティのステータスを監視し、本番環境で問題を引き起こす可能性のある非アクティブなエンティティを特定します。また、この機能を使用して、データの取り込み率のばらつきに基づくエンティティのステータスを追跡し、個々のエンティティをドリルダウンしてログデータを分析して、エンティティのパフォーマンスを追跡できます。さらに、アプリケーションログにあるインフラデータを使用してトラブルシューティングを迅速化することもできます。



### アラートでトリアージを迅速化

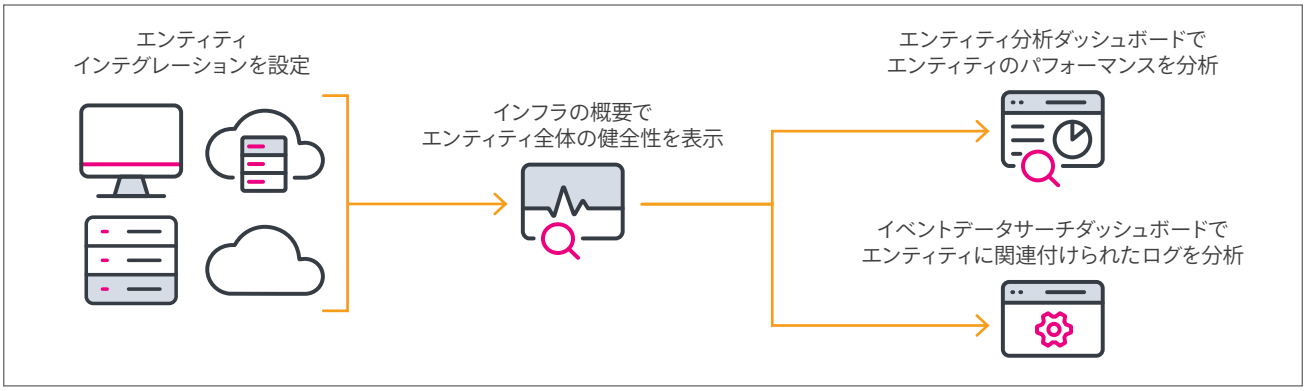
グループまたはエンティティレベルでアラートのトリガーをカスタマイズすることで、根本原因分析を迅速に行えます。また、アラートをトリガーした条件を把握し、アラートの重大度を評価し、トリガーされたすべてのアラートを表示してどのような行動を取るべきかを判断することで、アラートをより効果的にトリアージすることもできます。しきい値の設定、特定のインフラレベルでのアラート生成、さまざまな種類のインフラでのアラート分析を行うことで、最も重要なメトリクスのアラートを取得できます。




## 仕組み

IT Essentials Workでは、*nix、Windows、VMwareなどのデフォルトのすべてのエンティティインテグレーションにアクセスできます。エンティティのインポートが完了したら、インフラの概要画面でさまざまなエンティティタイプを表示して監視できます。また、個々のエンティティをドリルダウンして関連するログデータを分析したり、パフォーマンスメトリクスを追跡したりすることができます。

以下の図に、基本的なエンティティインテグレーションのワークフローを示します。ここではホスト、コンテナ、および仮想インフラをエンティティとして監視するように設定されています。




## メリット

業界のベストプラクティスに基づいた事前構築済みのコンテンツを、シンプルかつ容易な方法で活用できます。ITチームは、確実に連携しながら安全かつ迅速に調査を実施して、根本原因を特定できます。本番環境にログインしたり、アプリケーションやポイントソリューションを切り替える必要ありません。

- **使いやすい** – SPL (Search Processing Language)を使用する必要はありません。
- **短期間で価値を実現** – データ収集の処理方法が事前定義されているため、付属のダッシュボードにデータがすぐに収集されます。
- **わかりやすいインターフェイス** – 直感的なユーザーエクスペリエンスで、オンプレミス/ハイブリッド/クラウド環境のインサイトを取得できます。
- **複数のアクティビティに対応する単一のエクスペリエンス** – 1つのUIですべての状況を監視し、アラートの生成、トラブルシューティング、調査を実施できます。
- **迅速な根本原因分析** – 重要な問題に関するアラートを受信し、短時間で根本原因を特定できます。

ITE Workを使用すれば、ITモダナイゼーションに向けた第一歩を簡単に踏み出すことができます。準備が整ったら、ITE WorkとSplunk Infrastructure Monitoringを統合したり、サービスインサイトやイベント分析など、Splunk IT Service Intelligence (ITSI)の高度なユースケースをシームレスに導入したりすることができます。

### すぐに起動して実行可能

Splunk IT Essentials Workは、Splunkbaseから入手できる無料のAppです。ダウンロードして、ログベースの分析と迅速なトラブルシューティングを簡単に開始できます。ITE Workは、IT Essentials Learnと併せて使用することができます。どちらの製品もIT Cloud Foundationsの一部としてSplunk Cloudに含まれています。Splunk Cloudの無料トライアル版はこちらからお申し込みいただけます。

営業へのお問い合わせはこちら：https://www.splunk.com/ja_jp/talk-to-sales.html
〒100-0004 千代田区大手町1-1-1 大手町パークビルディング 8階
www.splunk.com/ja_jp
splunkjp@splunk.com



21-18794-Splunk-IT Essentials Work-PB-A4-JA-202111