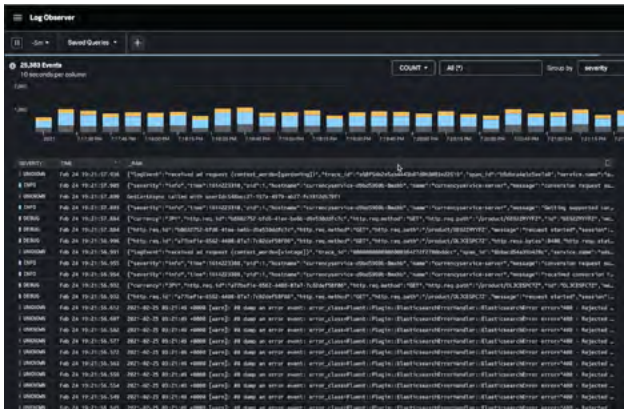
Splunk Log Observer

DevOpsチームのための迅速かつ直感的なログ調査

主要なメリット

- **カスタマーエクスペリエンスの向上：**統合オブザーバビリティソリューションでミッションクリティカルなアプリケーションを監視することで、カスタマーエクスペリエンスの状態を迅速に把握し、最適化できます。
- **開発者の生産性の向上：**ログ調査にはコーディングが不要で、価値実現までの時間が短縮し、問題特定のためのインサイトを問題の発生と同時にリアルタイムに獲得できます。
- **ダウンタイムの短縮：**コンテキストを維持したログでアプリケーションパフォーマンスとインフラストラクチャの監視が結び付けられ、発生している問題とその理由がワンクリックで表示できます。
- **ログ管理の強化：**ログ収集には制限がなく、DevOpsチームはログを簡単に管理できます。それにより、ログ管理にかかるコスト全体が低減し、組織全体のログの使用が最適化されます。
- **チーム間の連携の改善：**Splunk上のすべてのメトリクス、トレース、イベント、ログデータが一元化され、運用のセンターオブエクセレンスが構築されることで、あらゆるユースケースへの対応が可能になります。

DevOps向けの先進的なロギングソリューションであるSplunk Log Observerは、チームが既に使用しているSplunkソリューションの価値をさらに広げます。DevOpsチーム、SREチーム、プラットフォームチームは、Splunk Log Observerを使用することで、アプリケーションやクラウドインフラの動作の背後にある要因を理解することができます。操作はコーディング不要で直感的に行え、リアルタイムのログデータ、メトリクス、トレースをすばやく相関付けて、インサイトをただちに獲得できます。



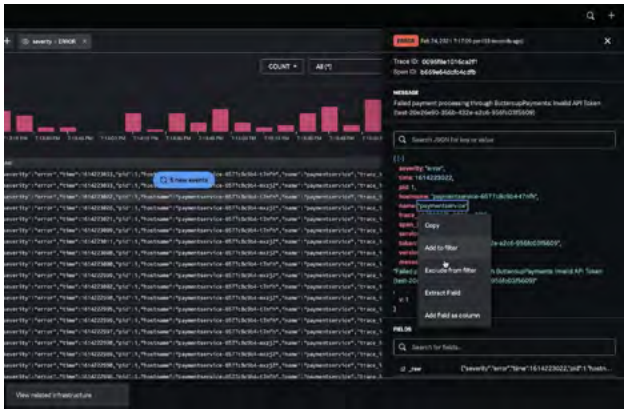
アーキテクチャ

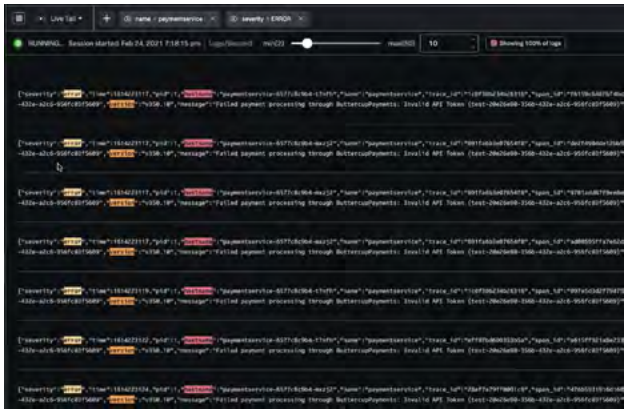
オブザーバビリティデータとエクスペリエンスを統合：

Splunk Log Observerは、Splunk Observability Cloudの一部であり、すべてのメトリクス、トレース、ログデータについて一貫したユーザーエクスペリエンスを提供します。これにより、問題の監視からトラブルシューティング、調査、解決までのライフサイクル全体にわたり、シームレスで効率的な単一のワークフローが実現します。エンドユーザーのエクスペリエンスに関する情報を必要とするフロントエンド開発者、最もパフォーマンスの高いAPIやサービスを構築するバックエンド開発者、日々オンコール対応を行うSREなど、あらゆるユーザーに対して、コンテキストに富んだ必要なインサイトが提供され、コラボレーションが円滑化され、障害を速やかに解決することができます。また、表面的でない深いインサイトを活用することで、問題にプロアクティブに対処し、発生を未然に防ぐこともできます。

Log Observer Connect：ツールを統合し、Splunk Observability CloudでのSplunk Enterpriseのデータの活用を可能にします。オブザーバビリティユーザーはLog Observer Connectを使用することで、Splunk Log Observerのコーディング不要の直感的なインターフェイスを介してSplunkインスタンスに送信されたデータを調査できるようになります。これにより、トラブルシューティングや根本原因分析が迅速化し、チーム間の連携も改善されます。

主要な機能





ノーコードの直感的なログ調査：ポイント&クリックでログを調査できます。コンテキストに沿ってログデータを簡単に検索、フィルタリング、視覚化し、関連するメトリクスやトレースにワンクリックでアクセスできます。

Live Tail：リアルタイムのログを、定義した属性に基づいて簡単に並べ替えて表示できます。ログはリアルタイムでサンプリングすることもでき、状況の読み取りがさらに容易です。

クエリーの保存と共有：他のユーザーが再利用してログ調査を迅速化できるように、有用なクエリーを保存できます。

DevOps視点のログソース統合：ウィザードを使って、AWS Cloudwatch、OpenTelemetry、GCP Stackdriver、Kubernetesを数分で関連付けることができます。さらに、Splunk Log Observerでこれらの形式のデータを整形して、Splunk Observability Cloud内で関連するメトリクスやトレースを検索、調査、コンテキスト化できます。

関連コンテンツ：Splunk Observability Cloudに含まれる製品間では、ログ、メトリクス、トレースが互いに連携します。ログの調査中に関連コンテンツのポインターが表示されるため、途中で行き詰ることなく直感的に調査を進めることができます。Splunk Infrastructure MonitoringやSplunk APMなどの他のSplunk Observability Cloud製品で、Splunk Enterpriseからの関連コンテンツを調査することもできます。

制限のないログ収集：Splunk Log Observerではすべてのログを保存できます。価値の高いログはインデックスされ、データに関するコンテキストが付加されて、リアルタイムで分析できるようになります。一方、価値の低いログは、指定した独自のストレージに保存されます。

パイプライン管理：ログ調査をより容易にするために、ログにコンテキストを追加し、フィールドを抽出し、アクションを適用するなど、ログが適切に処理されます。

Log Observerを介してオブザーバビリティワークフローに接続することで、既存のSplunkデータを最大限に活用できます。無料トライアル版のSplunk Observability Cloudをぜひご利用ください。

詳細については、ドキュメントのサイトをご覧ください。

無料トライアル版のSplunk Observability Cloudをぜひご利用ください。

© 2021 Splunk Inc. 無断複写・転載を禁じます。Splunk, Splunk>, Data-to-Everything, D2EおよびTurn Data Into Doingは、米国およびその他の国におけるSplunk Inc.の商標または登録商標です。他のすべてのブランド名、製品名、もしくは商標は、それぞれの所有者に帰属します。

21-21987-Splunk-Log Observer-A4-PB-JA-202512