ソリューション概要

エンタープライズ規模の Splunk を次のステージへ

ピュア・ストレージの FlashBlade と Splunk SmartStore でサイバーセキュリティの脅威の分析をよりシンプルに迅速に

マシンデータは近年急激な増加を見せており、これを利用することによって、ビジネス上のさまざまな問題が解決できるようになりました。膨大なデータの分析により、サイバーセキュリティの脅威の特定や、アプリケーションの性能問題の判別、さらには新製品開発のための知見を得ることができます。分散型スケールアウト・アーキテクチャのもとで、ホット、ウォーム、コールド（低速）データ層を全て分析する従来の方法は、IT インフラの複雑さや付随するコストといった問題もあり、ログ分析のニーズを満たすことはできません。このようなニーズに対応するには、クラウドライクな俊敏性とオールフラッシュの性能という条件を同時に満たす柔軟なアーキテクチャが必要です。ピュア・ストレージは、Splunk SmartStore と Pure Storage FlashBlade を組み合わせたソリューションを提供し、このニーズに応えます。

分散型 Splunk スケールアウト・アーキテクチャの課題

Splunk は、データ管理やネットワーク・セキュリティの課題解決に有効です。Splunk で IT インフラやビジネス・アプリケーションが生成するマシンデータを検索、分析、可視化することにより、ビジネスに価値をもたらす知見を提供できるようになっています。しかし Splunk に使用されている分散型スケールアウト・アーキテクチャは、10 年以上前に考案された、ストレージとコンピュートのコロケーションをベースとしたものであるため、データ量の飛躍的な増大がさまざまな課題を生じさせる結果となりました。

インフラ・コストの増大：分散型スケールアウト・アーキテクチャでは、データを複製することで高可用性を実現しているため、データの圧縮によってストレージ容量を増やすという Splunk のメリットは失われます。ストレージとコンピュートのコロケーションは、ストレージ容量を増やすにはコンピュートとストレージの両方を追加しなければならないという問題も生じさせます。また、分散型スケールアウト・アーキテクチャのもとで Splunk インデクサを使用する際には、各サーバーにつなぐストレージ容量を小さく抑えて、代わりにサーバーの数を増やすという手法がよく用いられます。サーバーの保守や障害対応時に扱うデータ量と必要な時間を最小限にするためですが、総所有コスト（TCO）増大の要因となります。

検索の高速化

- オールフラッシュの性能により、オブジェクトでのデータ操作や検索を高速化
- インデクサのバーストを最適化

TCO の削減

- ウォーム・データの単一のコピーを使用
- データ圧縮により、必要なストレージ容量を 30%～40% 削減

可用性の向上

- N+2 のイレイジャー・コーディングでデータを保護
- 障害発生時のノードのオフライン時間を 94% 短縮

大規模運用でもシンプルさを維持

- インデックス・ノードを追加し、データ・リバランスを 99.7% 高速化
- インデクサ・クラスタと FlashBlade オブジェクト・ストアの容量を拡張

検索性能の低下：分散型スケールアウト・アーキテクチャでの Splunk 検索は、データが古くなるにつれて検索性能が著しく低下します。古くなったデータは、ウォーム・バケットとコールド・バケット内のより安価で低性能なストレージ層に順次移されます。コールド・バケットでは、Splunk の TSIDX 削減機能によってストレージ容量が削減されますが、検索性能には大きな影響が生じます。各種法規制への対応を含むコンプライアンス、サイバーセキュリティ、証拠開示命令など、過去のデータが必要となる検索においては実用的な方式とはいえません。

インフラの複雑さと運用管理の負荷：分散型スケールアウト・アーキテクチャでレプリケーションによる高可用性を実現するには、全てのレプリカが常にオンラインであることが必要です。したがって、インデックス・クラスタ・サーバーの保守とソフトウェア・アップデートはシリアルに行う必要があり、これにはデータの退避、アップデート、リハイドレーションという一連の作業が伴います。さらに、インデクサ・クラスタの拡張とハードウェアの更新には、データのリバランスが必要で、これは複数回に及ぶこともあります。また、インデクサ・ノードに障害が発生した場合は、インデクサ・ノード内のデータを再構築する必要があります。このようなアーキテクチャの制限により、複雑さや時間、コストが大幅に増大し、コンピューティング・リソースの損失、データ移行、再構築プロセスにより、検索やインジェストの性能が低下します。

FlashBlade が Splunk SmartStore の可能性を最大化

Splunk SmartStore と FlashBlade の組み合わせは、従来の分散型スケールアウト・アーキテクチャの制約に対処すると同時に Splunk の機能を最大限に引き出すソリューションです。Splunk SmartStore は、コンピュートがストレージから分離され、ステートレス・インデクサ・サーバー、S3 オブジェクト・ストア、インデックス対応キャッシュで構成されています。

splunk> SmartStore	+	
Splunk SmartStore オンプレミスの Splunk 環境に クラウドの俊敏性とシンプルさを提供		**Pure Storage FlashBlade** オンプレミス環境向けの S3 互換超高速ストレージ オールフラッシュの性能によるスケールアウト機能を提供

FlashBlade を高性能な S3 オブジェクト・ストアとして活用する SmartStore ソリューションには多くのメリットがあります。

データが古くても迅速な検索と知見の抽出が可能：SmartStore のアーキテクチャは、コールド・バケットを排除し、ローカル・キャッシュを新たに採用しているため、最近のデータや最近検索したデータを検索するのに最適です。ただし、低性能で安価な一般的なオブジェクト・ストレージで SmartStore を使用した場合は、検索性能が制限されます。FlashBlade を使用する SmartStore ソリューションは、SmartStore キャッシュ外でのデータ操作や検索において優れた帯域幅と並列性を備えたオールフラッシュの性能を発揮します。また、各種法規制への対応を含むコンプライアンス、サイバーセキュリティ、証拠開示命令などに関する重要な非定型タスクを効率的に処理できるようになります。さらに、FlashBlade は帯域幅が大きく、SmartStore のインデクサのバースト対応に理想的です。

Splunk 環境全体の TCO を低減： SmartStore と FlashBlade の組み合わせはインフラの利用率を最適化し、ストレージを直接接続する Splunk の従来のアーキテクチャに比べてストレージとコンピュートの要件を緩和します。これにより、インデクサのサイズの設定にあたっては、ストレージを気にせず、インジェスト・レートと同時検索ボリュームに応じて決定できます。また、オブジェクト・ストレージ・ソリューションのデータ耐障害性機能を利用できるため、 SmartStore に保存するのはウォーム・データの単一のコピーのみとなります。さらに、FlashBlade は、優れたデータ圧縮技術により、オブジェクト層のストレージ占有量を 30%～40% 低減します。

可用性の向上：FlashBlade は、効率性に優れた N+2 のイレイジャー・コーディングを実装しています。SmartStore は、保存データ（Data at Rest）暗号化を採用した可用性の高いセキュアなソリューションです。Splunk SmartStore は、インデクサがダウンした場合でも、ウォーム・データを再構築する必要はありません。クラスタ内のノード間でメタデータのレプリケーションを行うだけで、Splunk のレプリケーション・ファクタと検索ファクタのパラメータを満たすことができます。ピュア・ストレージ社内の検証では、SmartStore と FlashBlade を組み合わせたソリューションでノード障害が発生した場合に、同様のデータセットを使用する従来の Splunk アーキテクチャと比較して、ノードのオフライン時間が 94% 短縮できることが実証されています。

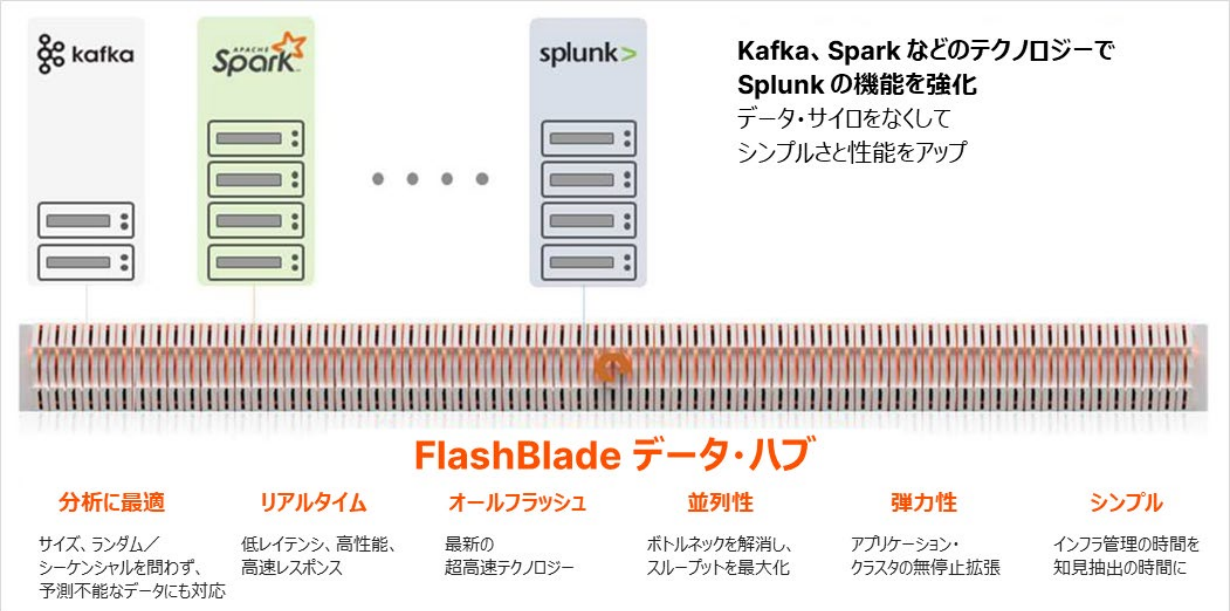
あらゆる規模の Splunk クラスタの管理を簡素化：SmartStore は、インデクサ・ノードの追加、データのリバランス、インデクサの削除を可能にすることで増大するニーズに対応し、Splunk インフラのデータ管理の簡素化を実現しています。クラスタ内のノード間でメタデータのレプリケーションを行うだけでよく、データの移行は不要です。ピュア・ストレージ社内の検証では、SmartStore と FlashBlade の組み合わせは、従来の Splunk と比較して、ノードの追加とデータのリバランスを約 99.7% 高速化できることが実証されています。インデクサのアップグレードは並行して行われます。SmartStore ソリューションと FlashBlade を組み合わせることで、インデクサ・クラスタのコンピューティングだけでなく、FlashBlade オブジェクト・ストアの容量と性能をシームレスに拡張できます。運用が簡素化されることにより、Splunk の管理者は、インフラ管理ではなく、インジェストやインデクシングに集中できるようになります。

SmartStore と FlashBlade がもたらすさらなるメリット

SmartStore と FlashBlade の組み合わせは、前述の他にもさまざまなメリットを提供します。お客様の成功をミッションとするピュア・ストレージだからこそ実現できるものです。

シンプルさと使いやすさ：ピュア・ストレージのソリューションの最大の特長は、シンプルさと使いやすさにあります。 SmartStore と FlashBlade のソリューションもその例に漏れません。Pure1 の AI 駆動型管理機能、フルスタック分析、予測型サポートにより、FlashBlade 環境の管理やプランニングをシンプルかつ効率的に行うことができます。

分析データの共有を可能にするデータ・ハブ：データ・ハブは、ストレージのためのモダンなデータ・セントリック・アーキテクチャです。エンタープライズでは、データ・ハブを導入することで、データ・サイロを集約してデータの共有を容易にし、Splunk をはじめとするモダン・アナリティクスやデータ集約型のワークロードを幅広く扱えるようになります。データ・ハブを介してアプリケーション間やチーム間でログ・データを共有することで知見の抽出が加速し、イノベーションの推進が実現します。



将来を見据えたアーキテクチャが IT 投資を保護： FlashBlade は将来への互換性を備えており、従来の Splunk アーキテクチャを使用中で、いずれは SmartStore を導入したいと考える組織にとって理想的なインフラ投資となります。 従来の Splunk 環境では、FlashBlade をコールド層に使用するソリューションが最適です。将来 SmartStore を導入する際には、その FlashBlade を高性能なオールフラッシュ・オブジェクト・ストレージ層として利用できます。ピュア・ストレージが提供する所有モデル Evergreen により、ストレージ再購入の必要はなくなり、ストレージが陳腐化する心配もありません。

SmartStore と FlashBlade でマシンデータ分析を高速化

Splunk SmartStore と FlashBlade の組み合わせは、オールフラッシュのクラウドネイティブ・アーキテクチャによる検索の高速化、管理コストの削減、可用性と運用効率の向上を実現し、Splunk 環境をモダナイズして次世代の検索・分析のための基盤の構築を可能にするソリューションです。旧来のログ分析アーキテクチャがビジネスの足枷とならないよう、次のステップを踏み出す時が来ています。

ピュア・ストレージ・ジャパン株式会社
お問い合わせ：03-4563-7443（代表）
https://www.purestorage.com/jp/contact.html