Splunk Enterprise を実装したビッグデータ向け Cisco UCS 統合インフラストラクチャが実現する運用の可視化とデジタル インテリジェンス

ソリューション概要
2014 年 11 月

概要

包括的統合インフラストラクチャ

- ビッグデータ向け Cisco UCS® 統合インフラストラクチャは、業界をリードするパフォーマンス、容量、拡張性を Splunk Enterprise 導入に提供します。

リアルタイムの運用インテリジェンス

- Cisco Unified Computing System™ (Cisco UCS) 上での実行用に最適化された Splunk Enterprise は、クリックストリーム、トランザクション、ネットワーク アクティビティ、通話記録など、あらゆるデータを監視および分析し、コンピュータで生成されたデータから知見を導き出します。

強力な検索、分析、視覚化機能

- Splunk Enterprise は、IT システムやセキュリティ デバイス、テクノロジー インフラストラクチャが生成した大量のデータ ストリームを、素早く簡単かつ安全に分析するための手段を提供します。

Cisco UCS 上に構築するメリット

- Cisco UCS のアーキテクチャは、ユニファイド ファブリック、統合管理、および高度な監視機能を提供します。
- また、Cisco UCS サービス プロファイルを利用した迅速で一貫性のある導入により、圧倒的なパフォーマンスを実現します。

アーキテクチャの拡張性

- Splunk を実装した Cisco UCS のアーキテクチャは、スイッチング インフラストラクチャ用の複雑なレイヤを追加することなく、アーキテクチャを最大限まで拡張できるように設計されています。

Splunk Enterprise を実装したビッグデータ向け Cisco UCS® 統合インフラストラクチャは、拡張可能な統合インフラストラクチャ プラットフォームにより、インテリジェントな運用を実現します。

今日のデータセンターでは、最新のアプリケーションをサポートするために階層化された複数のシステムが相互接続され、それによって境界があいまいになり、複雑化しています。問題が発生した場合は、根本原因を特定したり、インフラストラクチャ全体の可視化により障害をプロアクティブに検出し、回避することが必要となりますが、これは企業にとって大きな課題となっています。さらに 、仮想化やクラウド インフラストラクチャが新たな複雑さをもたらし、制御や管理がいっそう困難な環境を作り出しています。

IT およびセキュリティ インフラストラクチャ用の従来の管理/監視ツールでは、変化の激しい環境に対応できません。こうしたツールは、柔軟性に乏しく、コストがかかり、機能も不十分です。さらに通常は拡張性に乏しく、今日の環境やアプリケーションに必要な複雑さに対応できるようには設計されていません。また、特定の機能向けに設計されているために、データセンターの複数のテクノロジーにまたがる問題の解決には役立ちません。こうしたツールの監視アプローチは、フィルタリングや集約をベースとしています。問題が発生した場合に、IT やセキュリティ データを絞り込み、詳細分析を行うための機能は実装していません。また、リレーショナル データベースを基に構築された従来の監視ツールは、今日の膨大で複雑なマシン データには対応できません。

Splunk Enterprise のメリット

Splunk Enterprise は、業界をリードするマシン データ用プラットフォームです。マシン データは、ビッグデータの中でも最も増加スピードが速く、かつ最も複雑なデータの 1 つです。また、最も価値があるデータの 1 つでもあり、マシン データには、ユーザ トランザクション、顧客のアクティビティ、センサ計測値、マシンの動作、セキュリティ脅威、および

© 2014–2015 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

不正行為などに関する、信頼性の高い記録が含まれています。アプリケーションを支えるコンピューティング、ネットワーキング、ストレージ デバイスのみでなく、IT インフラストラクチャの運用を可能にするセキュリティ デバイスや技術インフラストラクチャ（電源リソースや冷房リソース）からのデータも組み込まれます。

Splunk Enterprise は、物理、仮想、またはクラウドを問わず、IT システムとインフラストラクチャが生成する大量のマシン データ ストリームを分析するための、速くて簡単、かつ安全な手段を提供します。パッケージ アプリケーション、カスタム アプリケーション、アプリケーション サーバ、Web サーバ、データベース、ネットワーク、仮想マシン、ハイパーバイザ、オペレーティング システムなど、あらゆるソース、形式、場所からライブ データを収集し、インデックスを作成し、活用します。カスタム パーサーやアダプタ、バックエンド データベースは不要です。

データのインデックスが作成されると、さまざまなデータ ソースの複雑なイベントを相互に関連付け、Splunk の強力な検索、分析、視覚化機能を利用できます。

また、サービス、システム、およびインフラストラクチャ内で問題が発生した場合は、その原因と現在の状況をリアルタイムで把握できます。リアルタイムでの可視化によりインテリジェントな運用を実現し、顧客のエクスペリエンスやトランザクション、その他のビジネス指標から、重要な知見を獲得してください。

Splunk Enterprise の導入で中核となるコンポーネントは、Splunk インデクサ、検索ヘッド、フォワーダです。

- **Splunk インデクサ**は、Cisco UCS C220 M4 および C240 M4 ラック サーバのコンピューティング能力とストレージ容量に合わせて最適化されています。ディスクへのデータの迅速な書き込みだけでなく、ディスク上のデータの読み取り、データの圧縮解除、ナレッジの抽出、結果報告など、検索に関する多くの作業を行います。したがって、データのボリュームを拡張する際は、インデクサも増やす必要があります。インデクサは、大量データの処理、検索時のリソース競合の緩和、検索のパフォーマンス向上に役立ちます。
- **検索ヘッド**は、複数のインデクサにまたがって情報を検索し、通常は CPU とメモリの両方を大量に使用します。Cisco UCS C220 および C240 M4 サーバに搭載された多数の Intel® Xeon® プロセッサ コアにより、Splunk Enterprise は優れた検索性能を実現します。
- **フォワーダ**は、データを収集してインデクサに転送します。通常、フォワーダはリソースをあまり多く使用しません。

検索およびインデックス作成に必要なシステム リソースは、インデックス対象のデータ量と検索負荷によって異なります。ユーザの要求を満たせるように、Splunk Enterprise は水平方向に拡張できるように設計されています。検索またはインデックス作成のパフォーマンスを強化したい場合、動作を中断せずに、検索ヘッドまたはインデクサ システムをアーキテクチャに簡単に追加できます（後の表 2 を参照）。この機能により、Splunk Enterprise は、数百ギガバイトからペタバイト データのインデックス作成に対応したソリューションへと簡単に拡張できます。

© 2014–2015 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Splunk 分析プラットフォーム向け Cisco UCS 統合インフラストラクチャ

データセンター全体の数テラバイトものデータを収集して、インデックスを作成し、レポートするように拡張できる Splunk Enterprise の機能を考えた場合、拡張性と信頼性が高く、管理の容易なインフラストラクチャが不可欠です。このニーズに対応するため、シスコは Splunk の認定アーキテクトと協力して、Splunk Enterprise の要件分析を行いました。この共同作業の成果が、高度に調整されたバージョンであるビッグデータ向け Cisco UCS 統合インフラストラクチャです。

ビッグデータ向け Cisco UCS 統合インフラストラクチャは、ビッグデータ向けシスコ共通プラットフォーム アーキテクチャ（CPA）の第 3 世代です。Cisco UCS 統合インフラストラクチャ ソリューションは、さまざまなアプリケーションのスケールアウト需要を満たすように設計された拡張可能なアーキテクチャであり、高パフォーマンス、大容量、高い拡張性、およびデータと管理のスムーズな統合機能を備えています。最新バージョンでは、Intel Xeon プロセッサ E5-2600 v3 製品ファミリを搭載したパフォーマンスと容量の向上により、この定評のあるシスコ ソリューションがさらに拡張されます。

ビッグデータ向け Cisco UCS 統合インフラストラクチャは、以下のコンポーネントで構築されています。

- **Cisco UCS 6200 シリーズ ファブリック インターコネクトは、**システム全体を対象に、接続と管理を一元化します。ファブリック インターコネクトは、Cisco UCS サーバに高帯域幅で低遅延の接続を提供し、Cisco UCS Manager によりすべての接続デバイスの管理を統合します。Cisco UCS ファブリック インターコネクトは冗長ペアで導入されるため、通常クラスタ化される多数のビッグデータ アプリケーション用サーバに必要な、完全なアクティブ-アクティブの冗長性、高パフォーマンス、拡張性を実現します。Cisco UCS Manager は、Cisco UCS サービス プロファイルを使用した迅速で一貫性のあるサーバ構成、高度な監視機能を提供し、クラスタ全体の継続的なシステム管理タスクを単一の操作として自動化します。
- **Cisco UCS C220 M4 および Cisco UCS C240 M4 サーバ**は、広範囲のコンピューティング、I/O、ストレージ容量の要求をコンパクトな設計でサポートするエンタープライズ クラスのシステムです。サーバには Intel Xeon プロセッサ E5-2600 v3 製品ファミリ、次世代の DDR4 メモリ、12 Gbps の SAS スループットが組み込まれており、旧世代のサーバよりはるかに優れたパフォーマンスと効率性を実現します。このサーバは、デュアル Intel Xeon プロセッサ E5-2600 v3 シリーズの CPU を使用しており、最大 768 GB のメイン メモリ（ビッグデータ アプリケーションの場合は、通常 128 または 256 GB）と、さまざまなディスク ドライブおよび SSD オプションをサポートしています。Cisco UCS 仮想インターフェイス カード（VIC）は、高帯域幅で低遅延のクラスタ接続用に最適化されており、Cisco UCS Manager によりオンデマンドで構成された最大 256 台の仮想デバイスをサポートします。

© 2014–2015 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Splunk Enterprise 用 Cisco UCS リファレンス アーキテクチャ

4 つの Splunk 用 Cisco UCS リファレンス アーキテクチャは、ビッグデータ向け Cisco UCS 統合インフラストラクチャと、Splunk Enterprise 固有のリソース要件に対応するように調整された CPU および I/O サブシステムに基づいています。各リファレンス アーキテクチャは、Cisco UCS C220 M4 または C240 M4 ラック サーバによる Cisco UCS インスタンスに基づいています。表 1 および 2 で示されているように、各アーキテクチャでは、ディスク容量とパフォーマンス、および Splunk Enterprise コンポーネントのサーバ分散が異なります。容量と保持には逆の相関関係があり、インデックス ボリュームを小さくすると保持容量を大きくできることに注意してください。

- **大容量（単一インスタンス）**では、単一サーバを必要とする Splunk Enterprise 導入において、高いデータ保持能力を実現します。
- **高パフォーマンス（単一インスタンス）**では、単一サーバを必要とする高パフォーマンスの Splunk Enterprise 導入において、高速な I/O パフォーマンスを実現します。
- **大容量の分散導入**では、高パフォーマンスで大容量の Cisco UCS C240 M4 サーバをインデクサ、高パフォーマンスの Cisco UCS C220 M4 サーバを検索ヘッダとして使用するように設計されています。
- **高パフォーマンスの分散導入**では、高パフォーマンスの Cisco UCS C220 M4 サーバを計算量の多いインデクサ、高パフォーマンスの Cisco UCS C220 M4 サーバを検索ヘッドとして使用するように設計されています。

表 1. Splunk Enterprise の単一インスタンス リファレンス アーキテクチャ

	大容量（単一インスタンス）	高パフォーマンス（単一インスタンス）
インデクサ	Cisco UCS C240 M4 ラック サーバ（以下を搭載）： ・Intel Xeon プロセッサ E5-2680 v3 CPU（24 コア）X 2 ・256 GB のメモリ ・Cisco 12 Gbps SAS モジュラ RAID コントローラ（2 GB フラッシュバック式書き込みキャッシュ搭載） ・Cisco UCS VIC 1227 ・1.2 TB 10K SAS ドライブ X 24、RAID 10 構成 ・120 GB SSD X 2、オペレーティング システム用	Cisco UCS C240 M4 ラック サーバ（以下を搭載）： ・Intel Xeon プロセッサ E5-2680 v3 CPU（24 コア）X 2 ・256 GB のメモリ ・Cisco 12 Gbps SAS モジュラ RAID コントローラ（2 GB フラッシュバック式書き込みキャッシュ搭載） ・Cisco UCS VIC 1227 ・800 GB SSD-EP X 6、RAID 5 構成 ・1.2 TB 10K SAS ドライブ X 2、オペレーティング システム用
推奨されるインデックス容量	最大 250 GB/日 （4 か月保持容量）	最大 250 GB/日 （1 か月保持容量）
サンプル保持容量	1 年 （80 GB/日インデックス容量）	3 ヵ月 （80 GB/日インデックス容量）
合計ストレージ容量	14.4 TB	3.9 TB
Splunk インデックス容量	2:1 圧縮時： 28.8 TB（推定）	2:1 圧縮時： 7.8 TB（推定）
使用例	・高性能と長時間のデータ保持が要求されるユーザ	・非常に高速な応答が要求されるセキュリティ、業務、ビジネス インテリジェンス ・非常に高速な複数同時検索

分散システムの拡張性

分散アーキテクチャでは、インデクサと検索ヘッドはクラスタ モードでも非クラスタ モードでも構成できます。検索ヘッドとインデクサを最大 80 台のサーバに追加することによって、アーキテクチャを拡大できます。ネットワーキング インフラストラクチャを追加する必要はありません。Splunk Enterprise は、以下のガイドラインに従って検索ヘッドとインデクサのクラスタ化をサポートします。

© 2014–2015 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

表 2. Splunk Enterprise の分散リファレンス アーキテクチャ

	大容量を実現するための分散導入	高パフォーマンスを実現するための分散導入
インデクサ	以下を搭載した Cisco UCS C240 M4 ラック サーバ X 16: ・ Intel Xeon プロセッサ E5-2680 v3 CPU(24 コア) X 2 ・ 256 GB のメモリ ・ Cisco 12 Gbps SAS モジュラ RAID コントローラ(2 GB フラッシュバック式書き込みキャッシュ搭載) ・ Cisco UCS VIC 1227 ・ 1.2 TB 10K SAS ドライブ X 24、RAID 10 構成 ・ 120 GB SSD X 2、オペレーティング システム用	以下を搭載した Cisco UCS C220 M4 ラック サーバ X 16: ・ Intel Xeon プロセッサ E5-2680 v3 CPU(24 コア) X 2 ・ 256 GB のメモリ ・ Cisco 12 Gbps SAS モジュラ RAID コントローラ(2 GB フラッシュバック式書き込みキャッシュ搭載) ・ Cisco UCS VIC 1227 ・ 800 GB SSD-EP X 6、RAID 5 構成 ・ 1.2 TB 10K SAS ドライブ X 2、オペレーティング システム用
検索ヘッド	以下を搭載した Cisco UCS C220 M4 ラック サーバ X 3: ・ 上記の CPU、メモリ、RAID コントローラ、Cisco UCS VIC 構成 ・ 600 GB 10K 小型フォーム ファクタ(SFF)SAS ドライブ X 2	
管理ノードおよびマスター ノード	以下を搭載した Cisco UCS C220 M4 ラック サーバ X 2: ・ Intel Xeon プロセッサ E5-2620 v3 CPU(12 コア) X 2 ・ 128 GB のメモリ ・ Cisco 12 Gbps SAS モジュラ RAID コントローラ(2 GB フラッシュバック式書き込みキャッシュ搭載) ・ Cisco UCS VIC 1227 ・ 600 GB 10K SFF SAS ドライブ X 2	
ネットワークの利用	シスコ UCS 6296UP 96 ポート ファブリック インターコネクト X 2	
推奨されるインデックス容量	最大 4 TB/日 (4 か月保持容量)	最大 4 TB/日 (1 か月保持容量)
複製を含む推奨されるインデックス容量	最大 2 TB/日	最大 2 TB/日
サンプル保持容量	1 年 (1.25 TB/日インデックス容量)	3 ヵ月 (1.25 TB/日インデックス容量)
合計ストレージ容量	230.4 TB	62.4 TB
Splunk インデックス容量	2:1 圧縮時: 460.8 TB(推定)	2:1 圧縮時: 124.8 TB(推定)
使用例	長期間のデータ保持を必要とする企業	多数のユーザの同時利用をサポートするために高速な応答が求められる企業
サーバ	21	21
ラック スペース	41 ラック ユニット(41RU:ファブリック インターコネクトを含む)	25 ラック ユニット(25RU:ファブリック インターコネクトを含む)

© 2014–2015 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

- **検索ヘッド クラスタ**は、交換可能で高可用な Splunk Enterprise 検索ヘッドのグループです。同時利用ユーザ数を増やし、シングル ポイント障害を排除することで、検索ヘッド クラスタは総所有コスト（TCO）を削減します。クラスタリングのフェールオーバーには、3 個の検索ヘッドが必要です。
- **インデクサ クラスタ**は、システムのインデックスを高可用にするために相互のデータを複製するように構成されている Splunk Enterprise インデクサのグループで構成されます。同一のインデックスのコピーを複数保持することにより、データ損失を防ぎ、検索データの可用性を向上させます。

Cisco UCS 統合インフラストラクチャによる Splunk Enterprise の大規模な拡張

Splunk Enterprise は、すべてのマシン生成データを監視し、組織全体でアクセス、活用できるようにすることで、クラス最高レベルの運用の可視化と、デジタル インテリジェンスを実現します。ビッグデータ向け Cisco UCS 統合インフラストラクチャは、コンピューティング、ストレージ、接続、および統合管理機能により、Splunk Enterprise プラットフォームをシンプルに導入できる、信頼性と拡張性の高い統合インフラストラクチャを提供します。これにより、TCO を削減しつつ、Splunk Enterprise のパフォーマンスと高可用性を保証することができます。

Splunk Enterprise 用の Cisco UCS リファレンス アーキテクチャは、Splunk の導入で必要となる大規模な拡張性をサポートします。このドキュメントで説明したリファレンス アーキテクチャでは、最大 80 台のサーバと 1 組の 96 ポート ファブリック インターコネクトをサポートしています。Cisco Nexus® 2232PP 10GE ファブリック エクステンダをネットワーク ファブリックに組み込むことにより、最大 160 台のサーバを単一の Cisco UCS ドメインでサポートできます。Cisco Nexus 9000 または 7000 シリーズ スイッチの使用により、複数の Cisco UCS ドメイン（最大数千台規模のサーバ）をサポートできます。

詳細情報

Cisco UCS の詳細については、http://www.cisco.com/web/jp/go/ucs [英語] を参照してください。

Splunk Enterprise の詳細については、http://www.splunk.com [英語] を参照してください。

Cisco UCS SmartPlay プログラムの詳細については、http://www.cisco.com/jp/go/smartplay [英語] を参照してください。

Cisco UCS ビッグデータ ソリューションの詳細については、http://www.cisco.com/go/bigdata [英語] を参照してください。

ビッグデータ向け Cisco UCS 統合インフラストラクチャの詳細については、http://blogs.cisco.com/datacenter/cpav3 [英語] を参照してください。

©2015 Cisco Systems, Inc. All rights reserved.
Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。
本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。
「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1502R)
この資料の記載内容は2015年2月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

お問い合せ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

LE-44701-02 15.04