Colasoft

Colasoft nChronos

技術白書

ウェブサイト: https://www.colasoft-japan.com
メールアドレス: support@colasoft-japan.com

目次

1 前書き

概述

本書では、Colasoft のネットワーク遡及分析システムの構成、アーキテクチャ、技術特性、応用価値について説明します。

対象読者

この文書は主に以下のエンジニアに適用されます:

- システムエンジニア
- テクニカルサポートエンジニア

専門用語

本書での専門用語は図 1.1 に示すように記載されています:

図 1.1　専門用語

専門用語	定義
分析対象	分析対象とはネットワーク内の各ノード要素, たとえば、ネットワークプロトコル,物理アドレス,IP アドレスなどを指ます。
分析サーバー	分析サーバーはネットワークリンクに対してトラフィック収集、統計分析、データのリアルタイムストレージを行います。同時に、通信口を提供して、それぞれ分析コンソールと分析センターとデータのインタラクティブを行って、全体の遡及分析システムの核心です。
分析コンソール	分析コンソールは、ヒューマンマシンインタフェースを提供してから、分析サーバに接続し、各種の通信データをリアルタイムで出力します。ユーザーは、分析コンソールを通じて、異なる幹線ネットワークの分析サーバに接続して、幹線ネットワークのネットワーク通信状況を見るおよび分析することができます。
分析センター	分析センターは統一的で集中的な監視分析プラットフォームを提供して、各ネットワークリンクに配置された分析サーバー内のデータを定期的に収集と統計することによって、集中的なデータ展示を提供します。同時に、分析サーバについての集中管

専門用語	定義
	理、監視、分析レポートと警報などの機能があります。

専門用語	定義
フィルター	カスタムのフィルター条件或いはルールを設定して、指定されるデータを見つけ出します。
ＩＰペア	IP アドレスをペアで表示しますが、送信元アドレスと宛先アドレスを区別しません。
詳細な分析	特定のネットワークオブジェクトに対して詳細な分析を実行します。現在、詳細な分析でサポートされているネットワークオブジェクトには、ネットワークアプリケーション、IP アドレス、物理アドレス、ネットワークセグメント統計、およびアラームログが含まれます。
タイムウィンドウ	タイムウィンドウでは、4 分、40 分、4 時間、16 時間、240 時間、240 日および他の時間スパンを選択することができます。時間スパンが短い場合、少ないデータ量と細かいデータが提供されています。タイムウィンドウを使用することによって、ネットワークの履歴データを簡単に特定することができます。
タイムピッカー	分析サーバーは数時間、数日、数週間、さらには数か月のデータを保存するため、特定の時間範囲のデータを表示する場合は、時間セレクターで時間範囲を選択して、その時間範囲のデータを表示できます。
データストレージ	分析サーバーは RAID アレイを採用しており、統計データやデータパケットストレージなどの大容量データストレージ機能を備えています。 データストレージを介して、分析コンソールのデータクエリと取得にリアルタイムで応答し、履歴データの遡及的分析を実行できます。
データマイニング	ユーザーのニーズに応じて、期間やネットワークオブジェクトごとにデータを取得することで、ユーザーが必要とするデータをすばやく取得できます。
特徴アプリケーション	データストリームの固有値シグネチャに基づいてカスタマイズされたアプリケーション。
統計データ	統計は、分析サーバーによってキャプチャおよび分析されたネットワーク操作情報です。 統計データは、分析コンソールによるデータクエリと分析のために分析サーバーに保存されます。分析サーバーのストレージスペースがいっぱいになると、統計データは循環的に保存されます。つまり、最も古いデータが削除され、最新の統計データが保持されます。

専門用語	定義
Web アプリケーション	URL 分析アプリケーションの場合、現在のバージョンは HTTP ベースのアプリケーションの分析のみをサポートしており、Web アプリケーションには複数のトランザクションを含めることができます。

2 nChronos について

Colasoft nChronos は、Colasoft が立ち上げたまったく新しいネットワーク遡及分析製品であり、エンタープライズネットワーク管理の新しいソリューションを提供します。 このシステムは、大容量ストレージと統合された高性能データパケット取得およびインテリジェント分析ハードウェアプラットフォームであり、ネットワークの主要ノードに分散および展開できるため、ネットワーク通信データパケットの高性能リアルタイムインテリジェント分析を実現します。 このシステムは、さまざまなネットワークパフォーマンスとアプリケーションパフォーマンスの主要なパラメータのリアルタイム分析を提供し、ネットワーク通信トラフィックをキャプチャして保存することもできます。ネットワーク異常、アプリケーションパフォーマンス異常、ネットワーク動作異常のリアルタイム検出、およびインテリジェントなレトロスペクティブ異常の原因を分析し、主要なビジネスシステムの運用保証機能と問題処理効率を向上させます。

2.1 Colasoft nChronos の概要

ネットワーク情報の包括的な構築と急速な発展に伴い、ますます多くの主要なサービスとアプリケーションがネットワーク上で実行され、企業は常にビジネスの中断やネットワーク障害による経済的損失などのさまざまな運用上の脅威に直面しています。

従来のポータブルネットワーク分析製品は、ますます複雑なネットワークの問題に直面しており、多くの欠陥があります。 新しいネットワーク管理の課題に対して、Colasoft は高性能 nChronos を提供します。

Colasoft nChronos の主な機能は次のとおりです:

- 時間による履歴ネットワークトラフィックを遡及的に解析する
- ネットワークデータをレベルごとにドリルダウンと検索
- リモートリアルタイム分析、監視、管理
- ネットワークの生の通信データのリアルタイム収集と分析
- 大容量のデータストレージと長期的なネットワークトラフィックの監視

2.2 システム構成

Colasoft nChronos は nChronos サーバー(以下「サーバー」という) 、nChronos コンソール（以下「コンソール」という）および分散ネットワーク分析センター（以下「分析センター」という）から構成されています。

サーバー

サーバーは、ターゲットネットワークのトラフィックの収集、分析、および保存を担当します。 同時に、サーバーは、コンソールおよびシステム全体のコアである分析センターとのデータ対話のための通信ポートを提供します。

コンソール

コンソールは、サーバーに接続し、さまざまな通信データをリアルタイムで出力するためのヒューマンコンピューターインタラクションインターフェイスを提供します。 ユーザーは、コンソールを介してさまざまなブランチネットワーク内のサーバーに接続し、ブランチネットワークのネットワーク通信ステータスを表示および分析できます。

分析センター

分析センターは、統合された集中型の監視および分析プラットフォームを提供し、各ネットワークリンクに配置されたサーバーによって報告された統計データを定期的に収集して統計データを収集することにより、集中型のデータ表示を提供します。 同時に、サーバーの集中管理、監視、分析レポート、およびアラームの機能を実現します。

2.3 システムアーキテクチャ

nChronos は、ソフトウェアとハードウェアの統合設計を採用しており、使いやすく、展開も簡単です。 システムはサーバーをコアとし、ネットワークデータをリアルタイムで収集、分析、カウント、保存します。

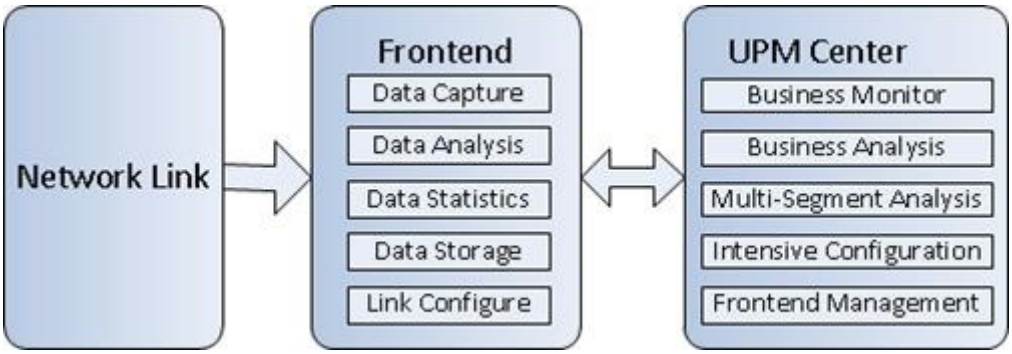
コンソールとサーバーは B/S（ブラウザ/サーバー）テクノロジーアーキテクチャを採用しており、サーバーはコンソールコマンドにリアルタイムで応答し、対応するデータを時間内に返します。 ユーザーが指定されたターゲットネットワークを監視および分析する必要がある場合、ユーザーはコンソールを介してサーバーに接続し、リモートリアルタイム分析および遡及的分析を行うことができます。

コンソールはサーバとの 1 対の同時接続をサポートします。つまり、1 つのコンソールが複数のサーバのデータを同時に管理および分析できる

分析センターとサーバーは B/S（ブラウザ/サーバー）アーキテクチャを採用し、定期的なハートビートを介してデータを交換することで、グローバルネットワークの集中監視と管理を完了します。

分析センターとサーバーの機能アーキテクチャを図 2.2 に示します。

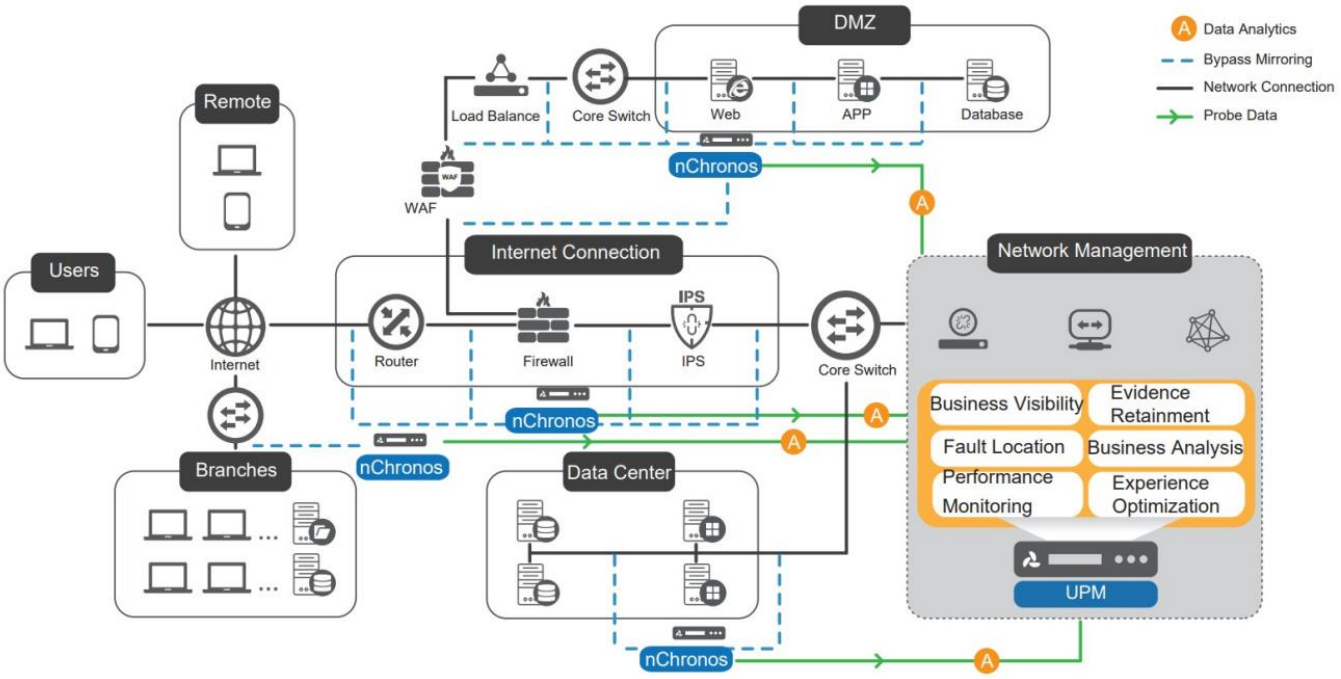
図 2.2 分析センターとサーバーの機能アーキテクチャ



2.4 nChronos の展開

nChronos は「分散展開と集中管理」の設計コンセプトに基づいており、インストールと展開は簡単です。 サーバーはネットワークリンクに配置され、ネットワークトラフィックの収集と分析を監視します。コンソールは、ネットワーク内の任意のサーバーに接続して、リアルタイムの監視と遡及的分析を行うことができます。 分析センターは、各ネットワークリンクに配置されたサーバーを管理し、サーバーから報告されたさまざまな統計データを表示します。ユーザーは、分析センターを通じてネットワークの分散および集中管理を実現できます。 典型的なシステム展開を図 2.3 に示します。

図 2.3 システム展開



3 技術の特徴

nChronos は、単一のネットワークカードの 10 ギガビット処理パフォーマンスをサポートし、バックボーンリンク上の大規模トラフィックの回線速度分析機能を実現します。 同時に、システムはマルチチャネルネットワークトラフィックのマルチ NIC キャプチャ、集約、および分析をサポートします。

3.1 遡及的な解析

データを長期保存

長期間にわたる大容量データの保存をサポートします。生パケット、データフロー、ネットワークセッション、アプリケーションログなど様々な統計データを長期的に保存し、ユーザーの重要なネットワークトラフィックに対して、ワイヤスピード解析を行うことができます。

遡及的なフォレンジック機能

nChronos を利用して、保存された大量データに対する迅速な遡及的解析を行うことができます。ストレージ容量が十分である場合、過去 240 日以内で発生したネットワークアクティビティ、アプリケーションデータ、及びホスト通信データを遡及的に解析することで、ネットワーク問題を追跡し、フォレンジック調査を行います。さらに関連する生データのダウンロードをもサポートします。

大量データをドリルダウン

nChronos は任意時間帯の大量データに対する迅速な検索とドリルダウンをサポートします。ユーザーは大量且つ複雑なデータを関連させ、フィルタリング、ドリルダウンすることで、迅速に解析することができます。nChronos は強力なフィルターを提供しているので、ユーザーはフィルタリングし、ドリルダウンすることで、迅速にトラブルを検出し、トラブルの関連データを抽出し、トラブルシューティングのために包括的な解析方法を提供します。

七層のプロトコルデコーディング

インターネットにおける各ネットワーク通信プロトコルのデコード解析能力を持っていて、ネットワーク各層の通信状況の把握に役立ちます。

インテリジェント解析

強力なインテリジェント解析モジュールを提供し、ネットワーク各層のトラブルに対し、インテリジェント解析を行うことができます。アプリケーションデータフローを再構築し、データフロー交互のグラフィカルなビューを提供して、ネットワークとアプリケーション問題のトラブルシューティングに役立ちます。

セキュリティ解析

ワーム、DoS 攻撃、ARP 攻撃、TCP ポートスキャン、不審セッションなどセキュリティイベントのインテリジェント診断を提供することで、問題ホストを迅速に特定することができます。

アプリケーションアクセス記録

一般的なインターネットアプリケーション（例えば DNS、Email、FTP、HTTP など）のユーザーアクセスアクティビティの詳細なログ記録を提供することで、ユーザーのインターネットアクセスアクティブティをより正確に解析することができます。

3.2 アプリケーション監視

アプリケーションをカスタマイズ

ユーザーは、IP アドレス、通信ポート、IP セッション、通信特徴、URL などの条件に基づき、アプリケーションをカスタマイズすることで、アプリケーション通信を正確に識別と統計することができます。アプリケーションのトラフィックを整理し、各アプリケーションシステムのトラフィック変化傾向を詳しく分析することで、各アプリケーションのトラフィック分布を把握することができます。

強力なアプリケーション監視機能

重要なアプリケーション通信に対し、アプリケーションアクセスのネットワーク転送パフォーマンスパラメータとアプリケーションシステムのレスポンス時間指

標を含め、リアルタイムにアクセスパフォーマンス解析を行うことができます。すると、ユーザーはいつでもアプリケーションのアクセスパフォーマンスの重要指標を把握し、アプリケーションパフォーマンスに影響を与える原因を特定することができます。

アプリケーショントランザクション処理解析

重要アプリケーションのトランザクション処理時間、処理状態、処理数量などを監視、解析することで、アプリケーションパフォーマンスのリアルタイムな解析を実現し、アプリケーション処理上の異常をタイムリーに発見し、アプリケーションシステムの最適化に科学的な根拠を提供することができます。

3.3 トラフィック統計

総合的なトラフィック統計

ネットワークリンク、ホスト、アプリケーション、ネットワークセグメント、セッションなどの通信トラフィックを統計、解析し、監視されたリンクの任意時間帯の各重要トラフィックパラメータの変化状況をグラフィカルに表示することができます。ユーザーは、ネットワークのトラフィック状況と変化傾向をリアルタイムに把握することができます。

豊富なトラフィック統計パラメータ

異なるオブジェクトに対して、送受信バイト数、パケット数、レスポンス時間、平均パケット長さ、TCP 状態など 140 種類のトラフィック統計パラメータを提供し、様々なトラフィック解析需要を満たすことができます。

データのサードパーティの解析をサポート

すべてのトラフィック統計データは時間帯により便利にエクスポートすることができます。エクスポートされた統計データの二次処理に役立ちます。

3.4 包括的な再生分析

システムはローカルデータパケットの再生をサポートし、ユーザーがシーンをすばやく復元できるようにします。 データの再生とリアルタイムの取得では、異な

るリンクを使用して、リアルタイムの取得のパフォーマンスに影響を与えることなく同時に実行します。

再生する必要のあるデータパケットは、サーバーをバックトラックしてローカルにアップロードすることで追加できます。

データパケットの再生は、インテリジェントなアラーム分析、迅速なレポート生成、詳細なデータパケットマイニング、マルチセグメント分析など、リアルタイム収集のすべての機能もサポートします。 また、設計方法はリアルタイム取得と完全に一致しているため、ユーザーはデータパケット再生機能をすばやく使用できます。

スマートアラーム

トラフィック、アプリケーションパフォーマンス指標、データフロー特徴、Ｅメール内容、ドメインなどにより、アラームを設定し、ネットワークアクティビティ異常にアラームを出します。

アラームのカスタマイズをサポート

複数のトラフィックパラメータを組み合わせてアラームを設定することができます。ユーザーは実際のネットワーク状況により、弾力的にアラームパラメータを調整し、より正確にネットワーク異常アクティビティをします。

アラート追跡機能

アラームをトリガーした通信データにたいする詳細なインテリジェント解析を行い、対応するデータ根拠を提供することができます。アラームをトリガーするオブジェクトを追跡し、異常ホストの通信アクティビティをより正確に把握することができます。

4 運用利点

Colasoft nChronos はネットワーク 7 層プロトコル解析技術、ハイパフォーマンスデータ保存とインテリジェントデータドリルダウン技術、分散的なデータ処理技術を統合させたハイパフォーマンスプラットフォームです。ユーザーのために、他のネットワークとセキュリティ製品と比較して、かけがえのない価値を提供します。

4.1 セキュリティ解析

パケットレベルのネットワークアクティビティ解析を通じて、ネットワーク通信を詳細的に調査することで、ネットワーク攻撃、ワーム、トロイなどネットワークセキュリティを危険にさらす異常アクティビティを迅速に発見することができます。

4.2 トラブルシューティング

トラブルが発生したときの通信データを迅速に検索、インテリジェント解析することで、問題点を正確に特定し、トラブルの原因を詳細的に分析することができます。

4.3 ネットワークアラーム

リアルタイムなネットワーク通信解析を通じて、ネットワークにおける各異常を発見し、アラームを出します。潜在的なネットワーク問題が緊急事態に発展し、不必要な損失を引き起こすのを避けることができます。

4.4 方策の根拠

ネットワークアクティビティと運行傾向のトレンドデータを提供し、パフォーマンスの最適化、新しいアプリケーションの配備、帯域幅の計画、セキュリティポリシーなどの方策のために、科学的な根拠を提供します。

4.5 誰が責任を取るべきかを決める

アプリケーション異常の根本的な原因を正確に解析することで、誰が責任を取るべき根拠を提供し、各運用・保守部門の協力効率を上げます。

4.6 アプリケーションを整理

アプリケーションタイプに基づき、ネットワーク通信を分類し、解析することにより、アプリケーション通信状態を把握することができ、方策の根拠を提供することもできます。

4.7 アプリケーション監視

アプリケーショントラフィック、ネットワーク転送品質、アプリケーションパフォーマンスをリアルタイムに監視、解析することで、運行上の異常をタイムリー発見し、重要アプリケーションのためにより良いネットワークサービスを提供します。

4.8 デジタルフォレンジック

迅速且つ正確にトラブルが発生したところを追跡、特定し、サイバー犯罪の証拠を見つけ、セキュリティイベントの鑑定とフォレンジックを完成し、より良いセキュリティポリシーを作ることができます。