Colasoft®
Maximize Network Value

nChronos

Network Forensic Analysis Application

技術白書

(nChronos 5.0)

お問い合わせ

電話番号

090-7197-9436

Sales

sales.jp@colasoft.com

技術サポート

support.jp@colasoft.com

ウェブサイト

http://www.colasoft.com/jp/

目次

はじめに

要約

本文書は、nChronos の構成要素、アーキテクチャー、特徴、および運用利点について説明します。

対象読者

本文書は、主に以下のエンジニアを対象として、作成されたものです。

システムエンジニア
技術サポートエンジニア

専門用語

本文書でよく使用される専門用語は、表 1 に記載されています。
専門用語リスト　表 1

専門用語	説明
nChronos サーバー	nChronos の中核として、目標ネットワーク（ネットワークリンクとも呼ばれる）のトラフィックデータのキャプチャー、解析、または保存に役立ちます。そして、通信ポートを介して nChronos コンソールと通信します。サーバーとも呼ばれます。
nChronos コンソール	データプレゼンテーションプラットフォームとして 、nChronos サーバーに接続し、ネットワークトラフィック状況を表示、および解析するためのさまざまな統計情報を提供します。また、遡及的解析、新たな解析とデータのドリルダウンをも提供します。コンソールとも呼ばれます。
解析オブジェクト	プロトコル、アドレス、ポート、セッション、アプリケーション、ホスト、ネットワークセグメント、目標ネットワーク、およびその他の要素を含むネットワーク要素です。
キャプチャーインターフェース	nChronos サーバー上のネットワークインターフェース/ポートで、一般にはミラーポートに接続されています。目標ネットワークトラフィックをキャプチャーします。
管理インターフェース	nChronos サーバー上のネットワークインターフェース/ポートで、一般的にはインターネット接続に使用されています。nChronos コンソールとサードパーテ

専門用語	説明
	ィーアプリは、nChronos サーバーに接続して、統計情報と解析データを取得することができます。
ネットワークリンク	nChronos がネットワークトラフィックをキャプチャーし、統計と解析を行うためのネットワークオブジェクトです。
バックインタイム解析	遡及的解析とも呼ばれます。詳細な解析プレゼンテーション、データのドリルダウン、新たな解析およびネットワーク履歴データなどさまざまな統計情報が提供されています。
タイムウィンドウ	タイムウィンドウでは、4 分、20 分、1 時間、4 時間、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。
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。
ドリルダウン	アプリケーション、ネットワークセグメント、アドレスおよびセッションを含むネットワークオブジェクトに対するレベルごとの革新的な解析です。
エキスパートアナライザ	パケットレベルの解析システム。さまざまな選択されたネットワークオブジェクトの統計情報およびパケットのオリジナルデコード情報を提供します。
Web アプリケーション	URL ベースのアプリケーションで、ホスト名、IP アドレス、ポート番号及ぶ URL パラメータによって定義されます。
特徴アプリケーション	データフローの特徴によって、ASCII、Hex、 UTF-8 または UTF-16 で定義されるアプリケーションです。
パフォーマンス解析	アプリケーションのサービスパフォーマンスに対する解析です。

概要

nChronos は Colasoft のネットワーク遡及的解析製品で、企業のネットワーク管理に革新的なソリューションを提供します。nChronos は大量データを保存できる、ハイパフォーマンスのパケットキャプチャーとインテリジェント解析プラットフォームです。ネットワークの重要なノードに配備することで、ネットワーク通信パケットのリアルタイムなハイパフォーマンス解析を実現することができます。ネットワーク通信トラフィックをリアルタイムにキャプチャーし、保存できます。長期にわたるネットワーク通信データに対する迅速なドリルダウンと遡及的な解析を行うことで、迅速にネットワーク異常とアプリケーションパフォーマンス異常を発見し、トラブル原因を特定して、アプリケーションシステムの運用維持能力とトラブルシューティング効率を向上させます。

nChronos について

Colasoft は、複雑なネットワーク管理の問題を解決し、ポータブルネットワーク解析製品の欠点を克服することを目的とした、ハイパフォーマンスの nChronos を提供します。nChronos は、中断することなく、ネットワークデータを長期的に保存し、数回のクリックで特定の時間範囲の履歴データを検索することができます。したがって、フォレンジックすることによって、ネットワークパフォーマンスをマークし、ネットワークユーザーの活動を監査します。

Colasoft nChronos の役割：

リアルタイムにネットワーク状態を監視する
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
LAN とインターネットを介し、ネットワーク統計をリモート確認する
E メールでネットワークの異常をタイムリーに警告する
予算を軽減し、ネットワーク管理の効率を向上させる

構成要素

nChronos は nChronos サーバーと nChronos コンソールからなっています。

nChronos サーバー

nChronos の中核として nChronos サーバーは、データーセンターみたいに、目標ネットワークのトラフィックデータをキャプチャー、解析、保存します。nChronos サーバーには、少なくとも 2 つのネットワークアダプタが含まれています。一つは、一つはキャプチャーインターフェース、もう一つは管理インターフェースと呼ばれます。キャプチャーインターフェースを利用して、nChronos サーバーはスイッチ、またはタプのミラーポートを介し、目標ネットワーク上の全てのパケットをキャプチャーします。そして、解析と保存のために、キャプチャーされたパケットを解析と統計モジュールに配信します。一方、管理インターフェースを利用して、nChronos サーバーは、nChronos コンソールおよびサードパーティーアプリケーションと通信できます。一つの nChronos サーバーは同時に複数の nChronos コンソールに接続されることができます。

nChronos コンソール

データプレゼンテーションプラットフォームとして nChronos コンソールは、nChronos サーバーに接続し、プレゼンテーションと二次解析のための統計データや他のネットワークトラフィックを取得します。nChronos コンソールは、ネットワークトラフィックの秒レベルのトレンドチャート、リアルタイム利用率、トップアプリケーション、トップホスト、トップネットワークセグメント、およびネットワークの異常を警告するさまざまなカスタムアラームを提供します。さらに nChronos コンソールは、履歴時間のネットワークデータを解析、レベルごとにネットワークオブジェクトをドリルダウン、サーバーからパケットをダウンロード、エキスパートアナライザでパケットをデコードすることができます。一つの nChronos コンソールは、複数の nChronos サーバーに接続することができます。

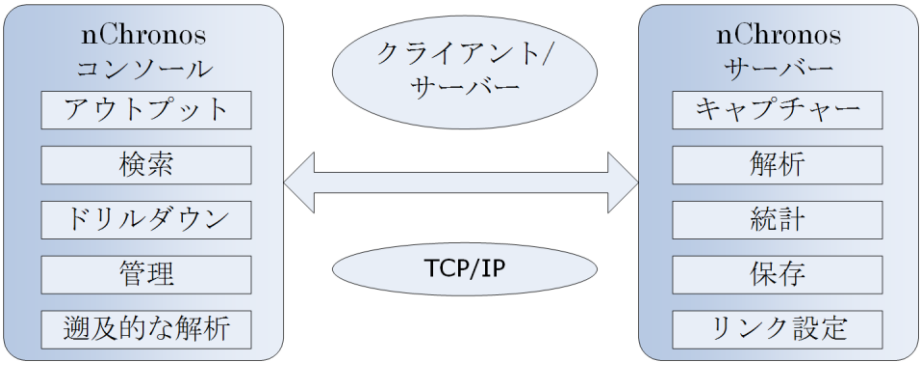
アーキテクチャー

nChronos コンソールは C/S（クライアント/サーバー）技術を利用して、nChronos サーバーと通信します。nChronos サーバーは、nChronos コンソールからのコマンドにレスポンスして、リアルタイムに対応のデータを返します。目標ネットワークのトラフィックを監視、または解析する必要がある場合、nChronos サーバーを nChronos コンソールに接続し、目標ネットワークに関する統計と解析データを取得することができます。

nChronosコンソールとnChronosサーバーは、TCP/IPプロトコルを使用してインターネットで通信を行います。nChronosコンソールは複数のnChronosサーバーに接続することができます。nChronosサーバーの設定は、専用のアクセスポートを介して、ウェブページブラウザで行われています。したがって、全てのnChronosサーバーは、世界中でリモート管理することができます。nChronosコンソールは、IPアドレス、アクセスポート番号、ユーザー名、およびパスワードを利用して、任意nChronosサーバーに接続することができます。

nChronos コンソールと nChronos サーバーの機能アーキテクチャーは図１のようです。

図１　nChronos の機能アーキテクチャー

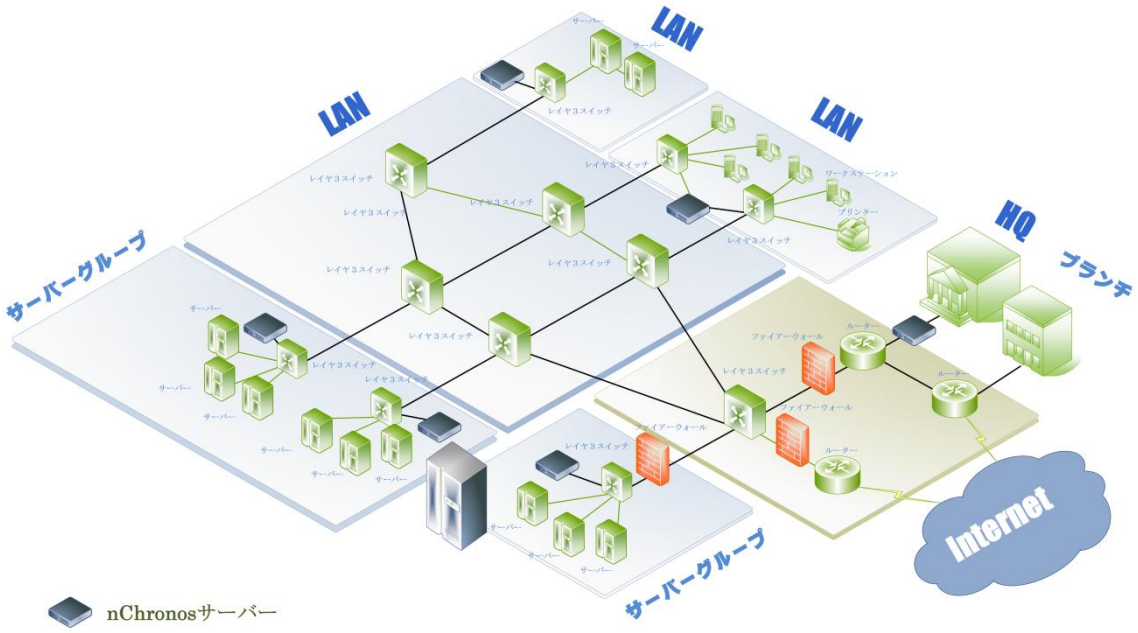


デプロイメント

異なるネットワークと複数ネットワークリンクを持つネットワークでは、nChronos はローカルネットワークのネットワークデータをキャプチャーまたは保存するほかに、分散的デプロイメントとリモート監視をもサポートしています。重要なネットワークリンクの場合、複

数の nChronos サーバーを配備することができ、ユーザーはデータ解析とネットワーク管理のため、いつでもどこでもリモート nChronos サーバーに接続することができます。さらに、nChronos コンソールを使用して、重要なネットワークリンクのトラフィックをリアルタイムに監視することができ、一旦異常が発生したら報告することもできます。nChronos のデプロイメントは、図 2 のようです。

図 2　nChronos のデプロイメント



技術ハイライト

nChronos は一つのネットワークアダプタのギガビット処理性能をサポートし、バックボーンリンクにおける大きなトラフィックのワイヤスピード解析を実現できます。そして、複数ネットワークアダプタのトラフィックを同時にキャプチャーしたり、複数ネットワークリンクのトラフィックを同時に解析したりすることができます。

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。

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。

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。

スマートアラーム

リアルタイムなスマートアラーム

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。

アラーム追跡

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。

インテリジェントレポート管理

レポートのカスタマイズをサポート

nChronos は、デフォルトでトラフィック、IP アドレスアプリケーション分布、アラーム統計及びアプリケーションパフォーマンス解析など 10 種類以上の解析レポートを提供し、異なる角度から履歴のネットワーク通信状況を前面的に把握することができます。そして nChronos はレポートのカスタマイズをサポートし、ユーザーはレポートオブジェクトを指定したり、各レポートモジュールで表示するフィールドを設定したりすることができます。

レポートの定期生成と自動送信

nChronos では、レポートをスケジュールし、定期的に生成することができます。毎時、毎日、毎週、毎月レポートを生成し、さらに指定の受信者アドレスにレポートを自動的に送信することができます。

レポートのデータ比較

レポートはデータの比較をサポートします。ある時間帯のデータは先月同期のデータ、または去年同期のデータと比較することで、データの変化状況を直接に示すことができます。

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。

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。

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。

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。

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。

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。

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。

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。

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。