N-Partner

N-Cloud 7

DATASHEET

Next Generation IT Operation Platform

Integrate Network Management, Flow Analysis and Log Reporting

N-Cloud は最新のログ分析管理プラットフォームです。政府機関、大企業、多国籍企業、教育機関やクラウドサービスなどの企業において効果を発揮します。ログ管理業務のニーズに対し N-Cloud は統合的プラットフォームとして使用できます。N-Cloud では企業や機関内部のすべてのログに対し効果的な保存と分析を手軽に行うことができ、ログデータの管理と素早い統合や判断を通して、ネットワークセキュリティの強化をサポートいたします。また、個人情報保護の法規や関連産業のニーズも満たすことができます。

N-Cloud ではアクセス権限の分割管理というコンセプトを採用しています。そのため、企業内の支社や部門ごとにグループを作成することが可能となり、グループ内のメンバーはその管理下にあるデータのみを閲覧できます。これは各グループごとに独立したログ管理プラットフォームを持っているのと同じです。また、本社の管理スタッフは国内外の支社を含む全体のログを管理することができるため、ネットワーク全体のセキュリティ状況を常に把握することができます。

アプリケーション（ソフトウェア）の機能

- ベンダーやノードに関係なく、各種 Syslog データの収集をサポート。
- システム状態のクエリが使用可能、ユーザーはソフトウェアのバージョン、CPU 使用率、メモリ使用率、Syslog とフローデータの通信量を調べることができます。
- Netflow v5/v9/v10、sFlow、Jflow、IPFIX などのフロー収集能力あり。
- 中国語、英語、日本語のウェブ（HTTP/HTTPS）操作インターフェースをサポート、ユーザー権限は使用ニーズに応じて調整できます。
- CLI（コマンドラインインターフェース）を採用、コンソールまたは SSH 接続を通してシステム操作が可能です。使用可能な基本的ネットワーク設定として、IP アドレス・ゲートウェイ・DNS・スタティックルートがあり、リブートとシャットダウンが可能です。また、セットアップページをサポートしていますので、リセットパスワードとリセットシステムにより出荷設定に回復できます。
- IPv6 環境をサポートすると同時に、IPv4 と IPv6 両方で運営できる環境です。
- ネットワーク設備を監視する SNMP コミュニティ v1/v2c/v3 をサポート、システムが特定のイントラネット IP が属するスイッチの位置を表示します。
- デバイスツリー図の作成をサポートしていますので、デバイスの関係を主従を基にルートディレクトリとサブディレクトリの関連順に並べて折り畳みと展開することができます。デバイスに異常が発生した際には、上層ディレクトリも同時に異常インジケータを表示すると共にアラームを送信します。
- SNMP を採用して CPU・メモリ使用率、インターフェーストラフィック情報、ブロードキャスト・エラー情報、ICMP など設備状態の監視をサポートすると共に警告値およびアラーム送付を設定できます。
- 設備の CPU・メモリ使用量をグラフ化するドリルダウンクリック機能をサポート、ドリルダウン後に TopN レポートと Syslog・フローの関連性にジャンプし、自動的にトラフィックランキングを作成します。また、監視機能では OID・MIB の自動設定をサポート、必要な項目の状態を監視します。
- ネットワークトポロジー作製をサポートしており、自動的にグラフを作成してインターフェースの負荷を色により表示します。
- 多くの条件を入力して論理演算 (or/not) を行うことが可能です。条件にはイベントキーワード 、IP、重大度 など各種引数が含まれており、入力条件に制限はありません。
- IP ネットワークセグメントの名称解析に対応する機能により、イベントおよびレポートにおいて IP とネットワークセグメント名称を表示します。
- ポート名称解析機能により、管理者はポートに対応する名称を定義できます（ 例：Port 80 を Http など）。
- サービス・部門・支店等を単位とするパケットサイズ（64・128・256・512 バイト）のチャートを表示。
- IP の位置情報（国別）、メジャーなサービス（Google・Facebook・Line など）、不正なドメインと IP のデータベースをサポートしています。また、ログおよびトラフィックを対照できる機能があり、部門または組織の IP トラフィック関連グラフを表示すると共に、データベースを自動更新するシステムを内蔵しています。
- Syslog プロトコルを通してログを受信することができ、またノーマライゼーション機能を内蔵していますので、ログ内の日付、イベント名称、重大度 、IP アドレス、ユーザーネーム、パケット・バイト通信量などのデータが同じグラフ内の異なるフィールドにそれぞれ表示されます。
- リアルタイムフロー分析と統計機能を内蔵、トラフィックの送信元と宛先 IP アドレスの範囲、ホスト、ユーザーネーム、アプリケーションポート、プロトコル、ネットワークインターフェース、トラフィック送信ノード、MAC アドレス、国、パケットサイズ分布などを監視し TOP N レポートやリアルタイムトラフィック（パケット・バイト）の折れ線グラフを作成することができます。また、しきい値を手動で設定し、しきい値を超えた場合には自動的に警告を出すことができます。
- フローの異常なトラフィック分析機能を内蔵、異常なトラフィック（DDoS、Host Scan、Port Scan、Flooding、Burst Session など）をリアル タイムで分析します。
- システム上で特定の IP と MAC コマンドをネットワークとファイアウォールやスイッチングハブ のようなセキュリティノードからブロックすることができ、複合的な防御を行います（注：一部のノードはこの機能をサポートしていません）。
- 自動ブロックシステムにより、自動的に複合的防御を行う条件を設定できます。
- ドリルダウンにより詳細を閲覧可能。

アプリケーション（ソフトウェア）の機能

- 円・棒・曲線グラフなど多くのグラフフォームを内蔵、必要に応じてレポートをカスタマイズできます。
- トラフィックグラフにより Max/Avg/PCT 95 の数値を表示します。
- イベント表示するフィールドとイベント の PDF ファイルをエクスポートするフィールドを設定できます。
- 中国語のレポート作成と PDF のエクスポートをサポート。
- PDF としてエクスポートする際のロゴとレイアウトを設定できます。
- Windows AD 機能を内蔵、イベント の IP よりユーザーネームを解析します。
- 各種ホストのユーザーがログイン・ログアウトした監査ログ レポートをサポート（Linux、Windows server 2003 / 2008 / 2012 / 2016 等）。
- 異常なログイン行為を検知して警告。
- 各種データベースのユーザーがログイン・ログアウトした監査ログ レポートをサポート（Oracle、MSSQL、MySQL 等）
- Windows ファイルで共有される監査ログ レポートをサポート。
- 内蔵ダッシュボードでイベント の内容、警告の現状とイベント 統計などの情報をリアルタイムで表示します。また、ニーズに応じてダッシュボードの内容やフレームサイズ、画面配列などを定義、調整できます。各時間区分（1 時間・1 日・1 週間など）におけるイベント 統計レポート、トラフィックグラフとシステム状態を把握することができます。
- アクセスコントロールリストをサポート、管理を実施できる IP ホワイトリストを制限します。
- Syslog のローデータバックアップをサポート。
- ユーザーの操作履歴を完全に記録し、PDF によりエクスポートできます。
- オープンインターフェースを採用していますので、ユーザーはオープンインターフェースでイベント 情報を取得できます。
- フレキシブルなアラーム設定、異なるレポートまたはアラームタイプにより、異なるメールグループを指定できます。
- CPU、ファン、ハードディスクの状態を監視でき、異常がある場合管理者に対し自動的に警告します。
- SNMP トラップをサポート、ハードウェアに異常がある場合、直ちに警告します。
- SNMP エージェントをサポート、システムの稼働状況を把握できます。
- 独自開発の最新圧縮ストレージ技術、国際的に使用される暗号化ハードウェアの有効性を検証するためのベンチマーク FIPS140-2 とハッシュ化規格 SHA-256・SHA2-512、そして AES を採用することで、データの完全性と否認防止を確保しています。その圧縮比は 10 倍に達し、ストレージ空間の利用率を大幅に高めました。
- 本システムは N-Partner に接続しており、最新バージョンのソフトウェアが自動的にダウンロードされます。
- WMI による Windows Server ログの取得をサポート。
- 2D・3D により世界中の攻撃状況をリアルタイムで表示。
- わずか 48 秒で 1000 万の Syslog データのトップ 1000 を集計します。わずか 250 秒で 1 億フローのデータ内から IP を特定します。
- Syslog 収集能力は 10,000 EPS 以上、最高レベルのフローモジュールの収集能力は最高で毎秒 20,000 フローになります。
- ICMP を使用して、監視ノードに対し常にノード可用性とラウンドトリップタイムの監視を行います。
- 管理下にあるネットワーク設備とサーバーの CUP・メモリ・ディスク使用率、帯域幅と品質測定値に対し、傾向予測機能によって短期と将来の傾向を予測した線グラフを表示します。
- IP アドレスを対応するスイッチやインターフェースの情報と自動的に関連付け、ユーザーが過去のマッピング記録を追跡および照会できるようにします。
- アプリをダウンロードすることで、モバイルデバイスによるリアルタイムでの監視と障害通知の送信ができます。
- 2 層式の TOP N レポート機能を持ち、1 層目の TOP N ランキングのすべての結果に対し、新たな統計条件を設定後に 2 層目を作成できます。1 層目の IP トラフィックランキングが 2 層目ではイベントランキングであるなど、2 つの TOP N レポートで設定される統計条件は異なっていても構いません。

アプリケーション（ソフトウェア）の機能

- 内蔵 Top N モジュールでは、ユーザーは Top N 統計レポートをいつでも作成、クエリすることができます。また時間的統計範囲、イベントキーワード、送信元と送信先 IP、送信元と送信先ポート、ノード、チャートタイプなどのパラメータを選択して毎時、毎日、毎週、毎月、四半期、半年、年次など、さまざまな種類のレポートを作成できます。
- イベント モジュールを内蔵、ユーザーは Syslog とフローのイベント 詳細をいつでもクエリできます。
- データベース容量の日数予測機能。
- データベースのバックアップとリカバリ機能をサポートしています。
- Syslog・フローの使用量履歴（過去 1 時間、過去数日等）に基づき、演算方式の自動学習機能によりベースラインを自動で設定、イベントあるいは IP の異常なスパイクをただちに分析します。そしてランチャート形式でスパイクが発生した時間を正確に表示してユーザーに警告を送信します。また、本システムは合理的な動態しきい値を自動的に設定ますので、手動でしきい値を設定する必要はありません。
- 監視レポートを内蔵していますので、ユーザーは異なる条件に応じて監視条件を設定でき、異常発生時にはただちに管理者に通知できます。
- オフラインレポートはグループ化機能をサポート。
- PDF・XML・CSV など、多様なエクスポートフォーマットサポート。
- アクセス権限分有方式により各ドメインは個別に実行され、独立したレポート分析が行われます。
- 高可用性フレームワークをサポート、システム運営が中断することはありません。

アクセス権限分有方式による管理

管理グループを本社、支社、支社の一部門等で分有することができる N-Cloud のアクセス権限分有方式による管理で、企業における分有管理のニーズに対応できます（図 1）。例えば、台中支社が管理する設備について、他の支社の管理者は監視権限を持ちません。しかし本社の管理者は支社の設備情報を監視する権限を持ちます。

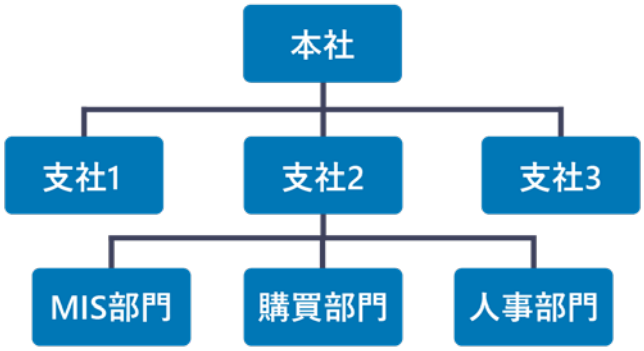


図 1

N-Cloud のアクセス権限分有方式の管理では、フレキシブルな分割管理のフレームワークを提供し、大型企業の管理ニーズに対応することが可能です。

各種データの集中管理センター

N-Cloud ではネットワーク（ルーター・スイッチ、情報キュリティ（ファイアウォール・IDP/IPS・Web キャッシュ・アプライアンス・WAF・UTM）、サーバー、データベース、大型ホスト等の設備の Syslog データの収集をサポートしています。N-Cloud では Netflow、jFlow、sFlow などの異なるベンダーやデバイス Syslog と異なるフォームのトラフィックデータを収集できます。システム上ではネットワーク全体のデータセキュリティ上の危険度分析、Top N ランキング、監査ログ 、トラフィック管理、これまでの傾向の分析、リアルタイムでブロックした異常攻撃などの情報を素早く監視することができます。そしてこれらのデータについて関連性分析を行い、管理者に比較のためのデータを提供します。

高可用性フレームワークをサポート

N-Cloud 専用の N-LB（ロードバランサー）を組み合わせることで、多数の N-Center・N-Receiver を相互にバックアップできます（図 2）。これによりデータを 24 時

間途切れることなく収集することができます。N-Cloud では Syslog とフローの送信設備数に制限がありません。また受信するログとトラフィック数にも制限はありません。受信できるログ EPS は少なくとも 10,000EPS(Event per Second) であり、企業において個人情報を保護するための最高のツールです。

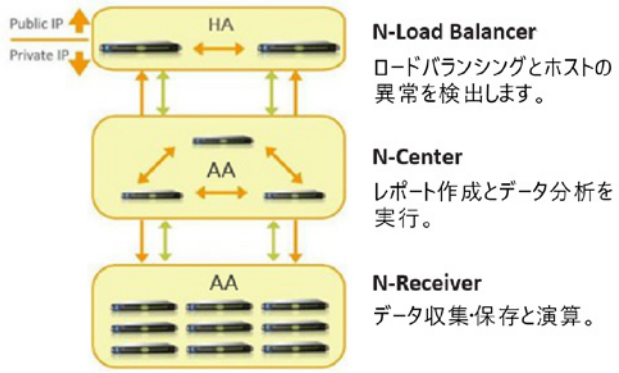


図 2

フレキシブルな N-Cloud のフレームワーク

N-Cloud は 3 つの部分から構成されています
(一) N-Load Balancer：
ロードバランシングとホストの状態の検出。
(二) N-Center：
ユーザーのクエリ業務とデータ交差分析を処理。
(三) N-Receiver：
ログデータの保存と分析・演算。

このフレームワークには高い拡張性があり、ユーザーのニーズと将来のデータ量、ユーザー数の成長予測に応じて適宜調整を行います。ですから保存したデータが大幅に増加した際も拡張できないという問題は起こりません。

N-Cloud の大型プラットフォームを設置する場合、設置中でも数百のユーザーが接続してクエリが可能であり、千以上のドメインを取得できます。教育関係のネットワークセンターの例では、ネットワークセンターに N-Cloud を一つ設置することで、数百校の中学校が使用する N-Cloud をすぐに提供できます。しかも、各学校におけるログの設置も不要です。すべての中学校で同じサービスを使用するため、問題が発生しても容易に解決できます。

ユーザーのニーズに応じて以下のようにカスタマイズ可能

- 100 人以上がオンラインで使用可能
- ログを使用するグループは 1000 以上まで設定可能
- Syslog 受信能力は 100,000EPS 以上
- フロー受信能力は 100,000EPS 以上
- Syslog・フローの送信元ノードの制限なし
- ニーズに応じてデータ保存数とデータ保存期間をカスタマイズ可能
- N-Reporter7 を N-Cloud にアップグレード可能

多数のクエリ条件を入力して論理演算とレポートを作成

データをクエリする作業はネットワークセキュリティシステム導入後の作業時間として最も多くなるものです。受信した Syslog とフローデータが増加した後、クエリ条件を弾力的に入力できること、そして素早いクエリ結果の表示はネットワークセキュリティシステムにおいて必要となる基本的能力です。
N-Cloud ではスマートクエリ機能を備え、そこに理論演算を組み合わせることにより、ユーザーの様々なクエリ作業に対応します。

イベントの表示と入力可能なパラメーター項目

- Syslog に基づくクエリ、またはフローに基づくクエリ
- 設備
- 設備のインターフェース
- 発生時間
- イベント のキーワード
- ユーザー名称
- 送信元・宛先 IP（CIDR と不連続セグメントをサポート）
- 送信元・宛先ポート
- 送信元・宛先国

- パケット・バイトサイズ
- イベント重大度 レベル
- イベント に対する処理（ブロック・Permit など）
- パケット・バイト使用量サイズ
- ポリシー ID
- AS 番号

論理演算とは、「Or」と「Not」を使用して、複数のクエリ条件間で示された関連性の結果のことです。複数のイベントキーワードをクエリする場合、入力キーワード間に「Or」を入力できます。特定のキーワードがレポートに表示されないようにしたい場合、「Not」コマンドを使用します。
N-Cloud では、「イベントキーワード」の論理演算をサポートしているだけでなく、ユーザーは「IP」に対する論理演算、また異なるオプション間で同時に論理演算を実行することもできます。以下にいくつかの操作例を説明します。

イベントキーワード

P2P+Streaming:
P2P または Streaming を含むすべてのイベント を同時にクエリしたい場合。
P2P+Streaming!BT:
P2P または Streaming を含むすべてのイベント をクエリしたいが、BT を否定したい場合。
[IP]
192.168.1.0/24+192.168.2.0/24
上記 2 つのセグメントのすべてのイベント をクエリしたい場合。
192.168.1.0/24+
192.168.2.0/24! 192.168.1.100-200
上記 2 つのセグメントのすべてのイベント をクエリするが、192.168.1.100-200 のセグメントのイベント を否定したい場合。

イベント のクエリ条件は実際のニーズに応じて多くの条件を入力できます。N-Partner の『Smart DB』では N-Cloud にイベント を迅速にクエリする能力を与えています。そのため、理論演算の際に多数の条件でクエリを行っても結果表示が遅延することはありません。

フローモジュールによるトラフィック分析

フロー（Netflow/sFlow など）データはネットワーク管理業務においてトラフィック分析などの重要な役割を果たしています。管理者はフローデータから、どの IP、あるいはどの部門の使用量が多いか、またはどのプロトコル（Port 80、Port 21 など）が帯域幅を占めているかなどの情報を知ることができます。
フローモジュールを使用することで、トラフィック Top N 分析やドリルダウンによるクエリ、特定の対象に対する長期トラフィックグラフの作成、特定の IP または部門単位でのトラフィック使用記録の作成など、管理者のフロー分析のニーズに対応することができます。
フローモジュールは Netflow v5/v9、sFlow v4/v5；J-Flow などのフォームをサポートしています。また、フローデバイスはないがファイアウォールが内蔵されている環境でも運用可能です。ほとんどのファイアウォールは Syslog をサポートしているため、通過する Syslog データにネットワーク接続情報をパッケージ化して出力することができます。ですから企業内においてファイアウォールを利用して Syslog データのトラフィック分析を行うこともできます。

多様で豊富なリアルタイムオンラインレポート

N-Cloud のリアルタイムオンラインレポートシステムでは、レポート内容と統計グラフ（円グラフ・棒グラフ・曲線グラフなど）の動態表示をサポートしています。ですので、ユーザーはグラフのフォームを好みに合わせて選択できます。レポート機能では演算理論（Or・Not）をサポートしていますので、ユーザーは実際の状況に応じて多くのパラメーターを組み合わせ、レポートの結果をよりユーザーの実際のニーズに応じたものにできます。例として、サーバーが深刻な攻撃を受けたイベントの日報、スタッフが SNS やストリーミングサービスなどを使用したトラフィックの週次レポート、データベースアクセス記録月次統計などがあります。

カスタマイズ可能なフィルターレポートにより異常を監視

管理者は様々な設定条件によりカスタマイズされたチャートレポートを作ることが可能です。これによりイベントやトラフィックの長期的変化が監視しやすくなります。例として、Telnet・SSH Login Fail の数量からパスワードの推測が行われていないか、深夜における特定の

ホストへの接続回数やトラフィックから異常がないかを監視する、Port445 接続とトラフィックによりワームに感染していないかなどがあります。カスタマイズされたレポートではしきい値の設定も可能です。イベント の回数が激増した場合、または異常なトラフィックが発生した場合などにシステムは警告を管理者に通知します。
フローモジュールを追加したカスタマイズレポートでは、同一のレポート画面内にイベント 、bps、pps とセッションの曲線グラフを同時に作成することで、ユーザーは一歩進んだ対照分析を行うことができます。

定期的なオフラインレポート配信

スケジュールに基づいてレポートが定期的に自動作成されますので、ユーザーはレポート作成業務を行う必要がありません。N-Cloud はレポート保存機能においてユーザーが設定したレポート作成パラメーターに基づき、指定された電子メールに自動的にレポートを送信します。

レポート作成パラメーターは以下の通りです

- イベント レベル
- 勤務時間（毎日の時間帯）
- 勤務日（ユーザーは日曜日から土曜日まで選択できます）
- レポート種類（毎時、毎日、毎週、半月、毎月、四半期、半年、年次）
- レポート送付時間
- 指定されたレポート受信者
- レポートフォーマット (HTML、PDF、 XML、CSV)

SNMP によるデバイスモニタリング

SNMP による監視でノードの CPU・メモリとインターフェースでのトラフィックデータを定期的に取得できます。これらの情報はクリアなグラフによって表示されます。この他、管理者は監視対象となるしきい値を設定できます。例として、CPU・メモリが 80%またはインターフェースでのトラフィックが大量になった際には警告とメールによる通知を行います。
SNMP 設備管理の状態をツリー図を使用した階層式の表示により表示します。また、グラフにより管理者は現状を明確に把握できます。例として、デバイス異常の場合には炎が表示され、上層でも同時に「！」が表示され、管理下のデバイスに異常があることをアラーム音により管理者に通知します。

内蔵 AI により、過去データに基づく傾向分析レポートを自動作成

N-Cloud に内蔵されている AI テクノロジーは収集された Syslog・フローの過去データに基づいて発生回数、パケット数またはバイトがスパイクするイベントや IP があるかを自動的に検出します。その上でネットワーク上の異常に IT 管理者が即座に対応できるよう、スパイクが発生した内容をメールします。行動ベースの検出と分析機能により、ユーザーは推測と合理的なしきい値設定の必要がなくなり、ネットワーク環境中の注意すべき変化を確実に把握できるようになります。これにより、ネットワーク運営業務がより気軽になります。N-Cloud は強力なイベント クエリとレポート作成システムであるだけでなく、傾向分析も実行できるアナライザーです。

アクションモジュールによる統合的防御

ユーザーは効果的な分析結果を運用してより高度な処理を行うことが可能です。アクションモジュールを使用することにより、IT 管理者はセキュリティ イベントの深刻度に基づく防御操作 (通常は異常な IP のブロック) を的

確に実行し、ネットワークを正常な状態に戻すことができます。
N-Cloud のアクションモジュールでは、ユーザーはウェブインターフェイスで IP ブロックのコマンドを直接出すことが可能です。また、インターネットの入り口にあるネットワークまたはセキュリティノードに対し IP ブロックコマンドを出すことで、ただちに防御を開始できます。
(注 : 一部サポート対象外のベンダーあり。)

国際的規格を採用

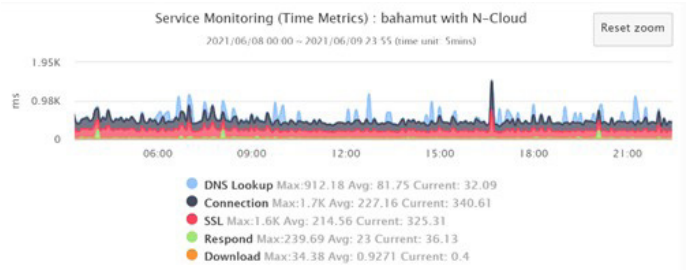
国際的に使用される暗号化ハードウェアの有効性を検証するためのベンチマーク FIPS 140-2、ハッシュ化規格 SHA2-256、SHA2-512 暗号化規格である AES を採用、データの完全性と否認防止を確保します。
https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=3002

N-Probe・エクスターナルレシーバー追加モジュール

ネットフローデータによる DNS 内容分析機能の他、N-Partner の関連商品 N-Probe では以下の追加機能を使用できますので、ユーザーの実際のニーズに応じてご購入いただけます。ユーザーのネットワークフレームワークが異なる地域のサーバールームまたは支社等に分散しており、それらがインターネット・VPN で接続されている場合、N-Probe を各地に設置し、エクスターナルレシーバーモジュール機能を起動させます。その上でローカルノードにおいて SNMP・フロー・Syslog(TCP と UDP プロトコル Syslog を含む) を収集後、暗号化と圧縮を行い N-Reporter・N-Cloud に転送します。同時に送信元 IP を保存してその圧縮率を 5 倍にすることで、インターネット・VPN の帯域幅の負荷が大幅に低下すると共に、送信中のデータの完全性と安全性が強化されます。エクスターナルレシーバーはストアアンドフォワード機能をサポートしていますので、接続中のインターネット・VPN が切断した場合でも、エクスターナルレシーバーが SNMP・フロー・Syslog データを一時的に保存するため、接続の回復後に再度 N-Reporter・N-Cloud に転送します。

エクスターナルレシーバーは HA（高可用性）フレームワークを設置できるため、可用性を向上させることができます。また、エクスターナルレシーバー
モジュールには SNMP 監視機能が含まれていますので、ローカルノードに対し SNMP ポーリングを実施し、IP・MAC と MAC・ポート対応テーブルを取得して、ネットワーク管理をサポートします。

N-Probe ではパフォーマンスモニターモジュールを持ち、ICMP Ping パケットにより各計測ポイントでのラウンドトリップタイムを監視する機能があります。もう一つの機能として、人がウェブサービスを閲覧するプロセスをシミュレーションした上で、N-Probe がプロセス中のいくつかの段階のレスポンスタイムを個別に記録します。記録されるレスポンスタイムとして、DNS クエリと応答、ウェブサーバーとの接続完了、SSL 送信、ウェブページの応答と内容のダウンロードなどがあり、これらのデータによりタイムチャートを作成します。ユーザーエクスペリエンス（UX）を向上させるため、管理スタッフはパフォーマンスモニターモジュールを含む N-Probe をネットワーク上のあらゆる位置（オフィス、支社内、通信事業者がリースする IDC など）に設置することが可能です。N-Probe は異なる場所からこれらのデータを計測し、収集された遅延データを N-Reporter・N-Cloud に送信してグラフを作成することで、ユーザーによる各監視ポイントでのネットワーククオリティの監視に用いることができます。これにより、多くのポイントにおける多角的で継続的な監視と分析が可能になります。この他、N-Reporter・N-Cloud の傾向予測機能を組み合わせることにより、数時間後から数か月後までの状況予測が可能となり、遅延が激しくなる前に警告を行うことで早めに対応することができます。



1. DNS クエリと応答
2. TCP コネクション
3. SSL
4. レスポンド
5. ファーストページダウンロード

Syslog とフローの転送機能

ユーザーは、Syslog およびフローデータの転送機能を定義できます。この機能により、受信したデータの送信元 IP が維持され、他の受信デバイスに転送されます。

仕様

	NP-CLD-BALANCER-JP	NP-CLD-RECEIVER-JP	NP-CLD-RECEIVER-H-JP	NP-CLD-CENTER-JP
CPU	Intel Xeon Processor E3-1240 V6 (8M Cache, 3.70GHz)	Intel Xeon Processor E3-1240 V6 (8M Cache, 3.70GHz)	Intel Xeon Processor E3-1240 V6 (8M Cache, 3.70GHz)	Intel Xeon Processor E3-1240 V6 (8M Cache, 3.70GHz)
Memory	16G DDR4 x 1	16G DDR4 x2	16G DDR4 x4	16G DDR4 x2
Ethernet Controller	Dual Port GbE LAN	Dual Port GbE LAN	Dual Port GbE LAN	Dual Port GbE LAN
IPMI	Integrated IPMI 2.0 and KVM with Dedicated LAN	Integrated IPMI 2.0 and KVM with Dedicated LAN	Integrated IPMI 2.0 and KVM with Dedicated LAN	Integrated IPMI 2.0 and KVM with Dedicated LAN
I/O Port	1 VGA, 1 COM	1 VGA, 1 COM	1 VGA, 1 COM	1 VGA, 1 COM
Power Supply	350W Platinum Level	350W Platinum Level	600W Platinum Level	350W Platinum Level
SATA DOM	8GB	8GB	8GB	8GB
HDD	N/A	12TB (4x4T with RAID 5)	4x14T with RAID 5, up to 8x14T with RAID 6	8TB (3x4T with RAID 5)
RAID Card	N/A	Supports RAID 0, 1, 5, 6, 10, 50, and 60	Supports RAID 0, 1, 5, 6, 10, 50, and 60	Supports RAID 0, 1, 5, 6, 10, 50, and 60
AC Power	100v-240v, 4.2-1.8A, 50-60Hz	100v-240v, 4.2-1.8A, 50-60Hz	100v-240v, 7.5A, 50-60Hz	100v-240v, 4.2-1.8A, 50-60Hz
Operating Temperature	0°C-50°C (32°F-122°F)	0°C-50°C (32°F-122°F)	0°C-50°C (32°F-122°F)	0°C-50°C (32°F-122°F)
Operating Relative Humidity	8% to 90% (Non-condensing)	8% to 90% (Non-condensing)	10% to 85% (Non-condensing)	8% to 90% (Non-condensing)
サイズ	1U Rackmount, 19 Inch Standard Wide Rack-Mount Industry Server	1U Rackmount, 19 Inch Standard Wide Rack-Mount Industry Server	2U Rackmount, 19 Inch Standard Wide Rack-Mount Industry Server	1U Rackmount, 19 Inch Standard Wide Rack-Mount Industry Server
機能	専用OSとプログラムを内蔵し、接続とデータ受信の負荷分散と高可用性（HA）を実現。	専用OSとプログラムを内蔵し、データの保存、クエリ、演算が可能。	専用OSとプログラムを内蔵し、データの保存、クエリ、演算が可能。	専用OS、データベース、プログラムを内蔵。N-Cloudの監視とユーザーインターフェースの提供、データ分析、アラート送信を実行。

VM 最小システム要件

	NP-CLD-BALANCER-VM-JP	NP-CLD-RECEIVER-VM-JP	NP-CLD-CENTER-VM-JP	NP-CLD-E-REC-VM-JP
CPU	E-2334(8Mキャッシュ, 3.40 GHz, 8 core)	E-2334(8Mキャッシュ, 3.40 GHz, 8 core)	E3-1231 v3 (8M cache, 3.40 GHz)	E3-1231 v3 (8M cache, 3.40 GHz)
Memory	32GB	64GB	32GB	32GB
HDD	128GB(System)		2TB	500GB

VM 注意事項

1. VM のシステム要件は最小システム要件です。実際の必要に応じてハードウェアの規格をお選びください。
2. サーバーを 1 台設置し、VMware Esxi 6.0、またはそれ以上のバージョンをインストールしてください。
3. N-Cloud を使用する際、最高のパフォーマンスを発揮するためには 8 コア以上の CPU が必要です。N-Center と N-Receiver の仮想マシンは少なくとも 64G かそれ以上のメモリが必要です。N-LB 仮想マシンでは 32G かそれ以上のメモリが必要です。
4. エクスターナルレシーバー使用時に最高のパフォーマンスを発揮するためには 32G のメモリが必要です。
5. VMware サーバーの管理に使用するため、VMware vSphere クライアントまたは VMware Web クライアントをインストールする Windows コンピューターをご用意ください。
6. 環境内に N-Probe・エクスターナルレシーバーがある場合、フローと Syslog トラフィックを受信するための N-Reporter・N-Cloud システムをご用意ください。
7. N-Center VM と N-Receiver VM は 500G、1T、2T の 3 バージョンをお選びいただけます。エクスターナルレシーバー VM は 500G のみとなります。

部品番号

部品番号	表示内容の説明
NP-CLD-BALANCER-VM-JP	N-Balancer VM version. Do load balancing for N-Receiver and N-Center. Include 1 year MA
NP-CLD-RECEIVER-VM-JP	N-Receiver VM version. Data receiver. Include 1 year MA
NP-CLD-CENTER-VM-JP	N-Center VM version. Provide portal, reporting and analysis result. Include 20 domains license (max up to 120 domains). Include 100 SNMP devices (max up to 1000) and 1 year MA
NP-CLD-BALANCER-JP	N-Balancer platform. Support up to 150,000 EPS. Do load balancing for N-Receiver and N-Center. Include 1 year MA
NP-CLD-RECEIVER-JP	N-Receiver platform. Data receiver. Support up to 10,000 EPS. 4T HDD*4. Include 1 year MA
NP-CLD-RECEIVER-H-JP	2U N-Receiver platform. Data receiver. Support up to 20,000 EPS. 14T HDD*4. Include 1 year MA
NP-CLD-CENTER-JP	N-Center platform. Provide portal, reporting and analysis result. Include 20 domains license (max up to 120 domains). Include 100 SNMP devices (max up to 1000) and 1 year MA
NP-CLD-E-REC-JP	External-Receiver platform. Collect and forward data. Include 1 year MA
NP-CLD-E-REC-VM-JP	External-Receiver VM version. Collect and forward data. Include 1 year MA
NP-CLD-JP-10Domains	Add 10 domains license for N-Center platform
NP-CLD-JP-100Domains	Add 100 domains license for N-Center platform
NP-JP-20SNMP	Add 20 managed SNMP devices
NP-JP-50SNMP	Add 50 managed SNMP devices
NP-JP-200SNMP	Add 200 managed SNMP devices
NP-JP-500SNMP	Add 500 managed SNMP devices
NP-JP-Ticket-G	Ticket System Module. Gold Version with 1 Year MA
NP-JP-Ticket-P	Ticket System Module. Premium Version with 1 Year MA
NP-JP-PS-T	4 Hours Training coupon
NP-JP-PS-I	One-Day Professional Service
NP-JP-PS-U	N-Reporter/N-Cloud Hardware Upgrade

ネットワーク管理＋情報セキュリティがオールインワン

ネットワーク管理者のために一つ上のソリューションを

全体
把握

異常
対処

防御
強化

YouTube

N-Partner

Tel : +886-4-23752865　Fax : +886-4-23757458
業務についてのお問い合わせ：sales@npartner.com
技術サポート：support@npartner.com