2004/7/22 付

米紙 NetworkComputing 記事より

製品プレビュー

基本に戻ろう！遂に、簡単に導入・設定可能な監視アプリケーションが登場。

ネットワーク管理アプリケーションは、単純な監視からだれがコーヒーを入れたかを告げる（アメリカンジョーク）以外すべてを行う基本原因分析までの範囲となります。SNMPc は簡単な監視ではどのような恩恵をうけるかを判りやすく見せています。1987 年から Castle Rock 社はネットワーク監視と管理製品を開発してきました。SNMPc は Windows ベースの世界最初の製品でした。今回、バージョン 7.0 は 2 種類で出荷されます。つまり、ワークグループ版とエンタープライズ版です。

バージョン 7.0 において新たに追加された機能

- リダンダントバックアップサーバ（このような低価格製品では異例な最新鋭機能）上でのディザスター・リカバリー（災害復旧）機能。
- 勘定系と監査機能を含むユーザセキュリティ機能
- TCP サービスポーリングのカスタム化
- マップ編集トラッキング

バージョン 7.0 はまたイベントアクションフィルタやイベントビュー範囲の管理も改良しました。ところで、私はエンタープライズ版を Windows2000 サーバ、600-Mhz Dual Processors、512MB RAM 上にインストールしました。マネージメントコンソールにログインした後、200 デバイスがある 2 つのネットワークサブネットをディスカバリしてマップを埋めました。Cisco デバイス、HP、SMC や 3COM などの様々なデバイスをディスカバリするのに少し時間が掛かりましたが、これはネットワークのサイズを考えると理解できる範囲です。

バックアップ

リダンダントバックアップサーバをテストするために、私のプライマリーサーバに似たサーバに SNMPc をインストールしました。手順は簡単です。設定オプションとして両方のサーバの IP アドレスを入力して、バックアップサービスオプションをイネーブルにするとともに、バックアップサーバのアクティブポーリングをディセーブルにしました。それから、プライマリーサーバをオフラインにしました。デフォルトコンフィグレーション設定を使うと、バックアップサーバは、プライマリーサーバがダウンしたことを察知して 2 分以内にポーリングオペレーションを引き継ぎました。全てのセッティングはユーザ情報、デバイス設定、コンフィグレーションオプションを含めて保たれました！プライマリーサーバに接続したリモートポーリングエージェントは、バックアップサーバに自動的にバックアップされた。従って、どのポーリングデータも稼動データも失わなかったわけです。唯一マイナス点は、プライマリーサーバのデータベースファイルバックアップやエクスポートが、一日に一回しか自動的に行われないため、それ以上の頻度で設定することができません。従って、システム設定にメジャーな変更を加える度にマニュアルでサーババックアップを取らなければなりません。

SNMPc はエクスポーラライクなインタフェースを使用してオペレーション表示を行っています。デフォルトでは、コンソールウインドウが 3 のパネルに分割されていますので、その結果すべてのオペレーションは表示されます。左のパネルは、5 つのタブが用意されています。つまり、マップ、MIB,トレンド、イベント、メニューです。マップタブは、発見したデバイスをサブネット毎に分類して表示します。MIB タブにて、デバイスメーカの選択したデバイスとプライベート MIB を見ることができます。トレンドタブからは、デバイスから一定期間の情報を収集したトレンドレポートを作ることができます。ドロップダウンメニューから、共通変数を選択してインタフェース使用率（ビット・秒単位で）やインタフェース利用率（パー

センテージにて表記) のレポートを作ります。私は、数回マウスをクリックして、少しデータ収集時間を待って、いくつかのレポートを作成し、レポートをスクリーンで見ました。イベントタブはアラートを設定して、何人の管理者にアラートを上げるか設定します。私は、WEB サーバを標準のポートではなくポート 8080 上で稼動させ、SNMPc を使ってサーバポーリングする TCP ポートサービスのカスタム化を行いました。サーバの監視ポートがダウンした場合、イベント状態を設定してオンスクリーンアラームと WAV サウンドにて連絡させるようにしました。
それから、WEB サービスをマニュアルにてストップさせました。SNMPc は、カスタムポートを使って私にサービスがダウンしたと伝えてきました。
コンソールウインドウの下段には、イベントログアラームパネルがあります。そこから、8つまでのログビューを設定して特定のオブジェクトやステータスをフィルタかけることができます。

ログは全てのアラームと、カレント及びヒストリーイベント用のタブビューを含むアプリケーションによって生成された全てのアラームとポーリングログメッセージを表示します。私は、クリティカル―赤アラームをもつ全てのデバイスをフィルタして、そのステータスのデバイスをすべて見ました。
また、メールサーバにフィルタをしてサーバのヒストリデータ、つまりサーバステータスと監視されている SMTP サービスステータスの両方を見ました。コンソールウインドウ中央のメインパネルは、デバイスマップ、生成レポート、グラフ、チャートを表示します。サブネットアイコンをクリックすると、ディスカバリされたデバイスを表示した新たなウインドーが現れます、そこにはディスカバリ完了デバイスがカラーステータスによって表示され、小さなインジケータには、SNMP か ICMP によってディスカバリされたことが判るようになっています―
これは一般的なモニターシステムの機能ですが、、。

アクセスコントロール

SNMPc のユーザ追加や設定は、とても簡単です。3 つのセキュリティレベルがあります。スーパバイザー、オブザーバー、オペレータです。
スーパバイザーは、このソフトウェアの全ての機能を完全制御しますが、オペレータとオブザーバーはサブネットやレポートを閲覧する機能や編集する機能に制限が加えられています。いくつかのユーザをつくり、特定のサブネットにアクセル定義や、各ユーザ用のレポートグルーピング化を定義しました。残念ながら、ユーザをグループ化することはできませんでした。個々に対して、一つずつ許可をあたえるしかありません。

サブネットアイコンをクリックすると、ディスカバリされたデバイスを表示した新たなウィンドウが現れます。しかし、各ユーザ用の期限日をセットすることはできません。つまり、全てのユーザに対するグローバル設定しかないということです。SNMPc は、今年後半発売すると言っていますが、WEB フロントエンドは持っていません。私は、コンソールアプリケーションと JAVA コンソールを使いリモートから SNMPc にアクセスしました。両方共、インストールや設定が簡単ですが、デフォルトではリモートコンソールと1セッションしか許可されていません。多数のコンソールセッションの利用や JAVA コンソールをご所望の向きには、リモート・エクステンション・ライセンス (RAX) が必要です。ユーザ設定によってセキュリティ対策としてリモート管理ログインをディセーブルできます。これは、リモートコンソールを使っている時は、うまく動いたが JAVA コンソールからは許可されてしまいました。但し、これは、IP アドレスにて制限をかけられます。これは、大きな問題ではありません、理由はリモートコンソールしかローカルコンソールを完全制御できないからです。JAVA コンソールは単に Read Only アクセスであるからです。SNMPc の開発は正しい方向にて進展しています、その結果監視とトレンドネットワークに有効な機能を追加できています。価格については、IT 予算が少ない法人においても魅力的です。

Network Computing Sneak Preview より
記者：Mr. Ian Brown.
SyracuseUniversity のネットワークコンサルタント。