HrsTの
NW管理に役立つメモ

HrsT

14all.cgiの日本語対応

14all.cgiってMRTGとRRDTOOLの組み合わせで使うことがありますが、ここは日本。
やっぱり日本語を使いたいなぁ～と思うのは自然の流れです。

でも、14all.cgiは多言語対応していないので、どうやっても使えないんですよねぇ～
だから改造してみました。

対象は1.1p25ですが、同じような場所を改造すれば1.0p26でもいけるんじゃない？

改造内容はキャラクタセットを日本語にしてしまうだけ。今回はSift_JISです。

2か所632行と692行の変更でOKです。
 原文 print $q->header(@httphead), $q->start_html(@htmlhead);
 変更 print $q->header(@httphead,-charset=>'Sift_JIS'), $q->start_html(@htmlhead,-lang=>'ja-JP');

これで、configファイルに日本語を使っても文字化けしません。
そんだけです・・・

故障切り分けの**Ping**

どこかでトラブルが発生したとき、その原因となる機器を見つけたり、回復（疎通）確認に便利なのが、Pingコマンド。
Pingがなぜ便利なのか？　多くのOSに標準で実装されているので他人のパソコンでも利用できる点だと思ってます。
Pingの使い方

１．目的の機器の疎通確認

これはよく使うのですが、「○○サーバにつながらない」なんて連絡があったらとりあえず、そのサーバに対してPingを打つことで、サーバの死活確認を行う。応答があればアプリ側の問題。そうでなければNW側と思って良い。

２．応答時間によるNW状況の把握

Pingの応答時間は応答する機器のCPUの状況によって大きく変化するので、参考程度にしかならないが、遅延が大きい時や輻輳が発生しているときは、その機器はほかに比べて時間がかかることが多い。

３．故障機器を探す

NW構成図を参考に、手前または遠くからPing応答可能な機器に疎通確認を行い、どの機器と機器の間に問題があるかを探すことができる。手前から調べれば、応答がなくなった機器とその前の機器が怪しいことになる。

４．DNSの確認（nslookupコマンドの代わり）

nslookupやdigコマンドを使うのが本当だけど、名前解決がちゃんとできているかを確認したり、このサーバのIPアドレスなんだっけ？と思った時に使える。 Ping \\Server　や　Ping server.local など打てば、IPアドレスを教えてくれる。

ネットワークは**MRTG**で見よう

ネットワークって正直通信ができれば問題ない。そう思ってます。
でも、ネットワーク管理者としてはそれだけじゃ勤まらないと思います。
医者がカルテを作成するように、ネットワークも経過観察が重要です。

ネットワークの状況を見るというのは瞬間のパケットを見るではなく、トラフィックの推移や各機器のCPU利用率などを長期的に観察し、「いつもと違う」を発見することです。
そこでおすすめなのが「MRTG」Perl上で動作するので、Windowsでも利用可能です。私はWindows2008R2上で要所ルータ、サーバを監視しています。（会社方針でPC UnixがNGなんです）
さらにメールサーバや各機器からのLogをSyslogで集め、あるlogをカウントすることで、メールの流量やエラーの数なども監視し、トラブルが発生したときの状況把握に役立てています。
メールのエラー量を監視していると、ユーザアカウントが乗っ取られて迷惑メールを送信しだしても、あれ？いつもと比べて送信数が多いし、User Unknownが多ければ無差別に送信していることが目に見えてわかるのです。
これを数値ではなくグラフという形で表現してくれるのが、MRTGなのです。
ただ、MRTGは1つのグラフに2種類の整数しか表示できない点が、グラフ化において問題になることがあります。
そんな時はRRDTOOLを利用すると複数の値を表示できるのでお勧めです。

最後に、いくつかの専門書などではMRTGで設備増強のタイミングを予測するなんてありますが、一般企業で問題なく使えているネットワークではこの目的で役立った経験はまだありません。（サーバのメモリやCPU、ハードディスク監視では大活躍ですけどね）

トラブル時のジレンマ

ネットワークトラブルが発生したときどうするか？

1. 復旧を優先し、原因究明手段を捨てる
2. 原因究明を優先し、復旧を遅らす

大きく分けると、この2つになると思います。
ユーザーからすればさっさと復旧してほしいという思いが一番だと思うのですが、ネットワーク管理者としては、再発防止、適切な対応をする必要があり、復旧作業と合わせて状況把握、原因調査を行いたいと思ってしまいます。
おそらく機器の再起動、交換で治ってしまうことがほとんどだと思いますが、再起動するとログが消えてしまったり、カウンタがリセットされるなど、原因調査や報告書作成が困難になることがあります。
そのため、原因究明を行うと必然的に復旧が遅れてしまうのです。

そんな時に役立つコマンドは機器によって違いますが「Show Tech」です。
このコマンドはいくつかのステータス表示コマンドを一つで実行可能な便利なコマンド。
再起動や交換をする前に、このコマンド実行する時間くらいなら用意できると思います。

あとは、Telnetなら操作ログを残しておく。
あとから見直すのは醜いですが、あとからあのタイミングではどうだっただろう？なんて時系列を追いたくなった時は意外と役立ちます。Web設定だと難しいですけどね。

私がおすすめするトラブル時にやることは、操作ログを記録する。Show Techコマンドをとる。
そして再起動で治りそうならさっさと再起動してしまう。

ユーザは一秒でも早い復旧を望んでいるのですから・・・
　それに応えるのが、ネットワーク管理者だと思います。

Syslogを活用しよう

ネットワーク機器はログという機能が備わっているけど、意外と再起動すると消えてしまう物が多い。
RAM上に記録するので当然なんだけど、結構これが困った仕様なんだよね。

たとえば再起動を繰り返す不具合が発生したとき、Telnetやコンソールを使ってログにアクセスが難しいくらい短時間で再起動しているとみることはできない。
だけど、もしかしたらログに再起動の原因となっているエラーが記録されているかもしれないよね。

だから、こういう時に備えて、Syslogサーバにログを転送するようにしておくことが重要。
これなら、たとえ短時間で再起動を繰り返していても、Syslogサーバにエラーログが記録されている可能性がある。
再起動を繰り返すNW機器とにらめっこせずに、ゆっくりSyslogサーバのログを読めばいいのだから、とっても楽だよ。

でも、一つ問題があって、Windowsの場合、無償でサービスで動作するSyslogサーバの選択肢がないってこと。

NMSを活用しよう

NMS(Network Management System)って何？
　ネットワーク上の機器に対してPingやサービス死活、状態を監視、記録してくれるとっても便利なシステムです。
しらない・・・って人はとりあえずTWSNMPをググれ！！
ExPingとかで死活監視をしている人もいるかもしれないけど、それだったらTWSNMPを導入したほうが良い。
何がいいって、NW図で監視できるって便利じゃない？NW図上のノードに問題が発生したら、そのノードが点滅して教えてくれるから、NWに素人な上司に「ここが問題なんですよ」ほら光ってるでしょっていうとなるほど～って納得してくれるので、説明に時間がかからない。
あと、Pingだけでなく、サービスレベルの監視ができるので、DNSやDHCP、HTTP、FTP、SMTPなど細かく見ることができるので、ExPingでは見逃していた問題も発見できる。

ただ、NMSってピンきりで無償のTWSNMPからHPのOpenViewなど高価なものまで色々。
私のお勧めは、見た目が良くて比較的安価なNetCrunch。
知らない人にとっては見た目がとっても重要みたいで、TWSNMPで十分だったのに、こんなしょぼい画面だと使い物にならないって決めつけられてしまいました。OpenViewだってこんな画面ですよ。見た目じゃないし～って紹介したらOpenViewもだめ！！だって・・・

TWSNMPの気に入っている機能。それはインタフェースの状態によってノード間を接続している線が点滅してくれるので、SNMP対応機器に接続しているSNMP未対応機器まで監視できること。監視対象がちょっと広くなります。

Pingの応答速度は参考だ

Pingを打つと応答時間がわかる。
これは素人でもしっている人が多く、ホームページの表示が遅かったりしたときに、Pingで応答時間が数百ミリ秒かかっていて、ネットワークが遅いんだ！！って文句を言ってくる人がごく稀にいる。

まぁ、間違っているとは言わないけど、Pingの応答時間で判断するのって安易すぎます。
PingってLAN無いだと<1msなんて結果が返ってくるので、時間がかかる＝ネットワークが遅い。って思いがちですが、Pingの応答時間はその機器の処理能力によって変化することを知るべきです。

CPU使用率が100％な機器にPingを打つと応答がないとか、非常に時間がかかることがある。

だから、
応答時間が長い＝　ネットワークが遅い または Ping先に問題がある
と思った方が正しいと思う。

NW導入工事の完了試験項目で　Ping応答数ミリ秒以下なんて基準を決めたら、これで不合格になって困ってしまうこともあります。　あくまでPingは応答があること。にしておいた方が安全です。あくまで疎通確認のコマンドだということです。

うまく説明できた経験は・・・ゼロに等しい。

日頃、上司や一般の方にネットワークの話をするとき気を付けている「できるだけ専門用語を使わない」は無駄な努力では？と思うことがあります。

慣れない言葉で説明するほうが相手を混乱させてしまうことがありました。

こちらがわかりやすいようにと専門用語を避けると、余計にわからなくしてしまうのです。専門用語を使うとその単語が意味わからず名詞として聞き流せるけど、理解できる言葉で説明されると、NWに関する基礎知識がないと言葉は理解できるけど内容はさっぱりという状態になってしまいます。
また、説明する側も慣れていない言葉を使うので、うまく説明できずに墓穴を掘ってしまうのです。
だから、話をするときに気を付けるのは、専門用語をうまく使う。
悪い言い方だと、適度に専門用語を使って煙に巻く。ごまかす。

専門家が素人に専門分野を短時間で理解させるなんて無理なんです。
もし、理解できればその部分において専門家はすでに不要。

相手に理解させる部分は専門分野ではなく、目的と費用と稼働です。
詳細説明は添付資料にするくらいが丁度よい。
もし、相手が添付資料の説明を求めてきたら、「うまく説明できないかもしれない」といってから、相手が納得するまでとことん付き合いましょう。墓穴を掘る可能性も高いですが・・・熱意は伝わると思います。

ARPテーブルほど厄介なものはない

ネットワーク間の接続を行う際に設定するのはルーティングテーブル。これを固定にするかダイナミックにするかは、規模や機能や管理者のポリシーなどです。
この設定を間違えると「繋がらない」や「ループ」といったトラブルにつながります。
でも、ルーティングテーブルはトラブルが起きても修正すればOKだし、設定が間違っていなければ恒久的に安定運用ができるはずなんですよね。（たまに問題が発生するけど・・・）

で、タイトルのARPテーブルってやつなんですが、基本的に自動学習です。
一応固定で書けるけど、書くシチュエーションが思いつきません。見ることはよくあるのですが・・・
でね、この自動学習ARPテーブルが曲者なんですよ。
とくに、トラブル時にIPアドレスを持った機器を交換した時に繋がらないってなります。なんでか？それはARPテーブルに新しい機器が登録されないから。で、なんで〜〜って騒いでいたら自然回復（ARPテーブルが更新された）。

一番困ったのはNW機器の管理範囲外のARPテーブルを更新してほしい時。こっちは原因がわかっているのでARPテーブルの更新を依頼しても答えは「NO」。絶対にダメなんだって〜。まぁ、普通だったら数分待てば更新されるはずなので待っててもー向に学習されない。結局IPアドレスを別のに変更した経験があります。