



システムの運用／監視に 関する考察

第1回Admintech.jp & ぱりかた合同勉強会

Masa@Admintech.jp

本日のAgenda

- ・システム....って？
- ・システム運用／監視の背景にせまる
- ・システム監視の実装について



本日のAgenda

- ・ システム....って？
- ・ システム運用／監視の背景にせまる
- ・ システム監視の実装について



どんなシステムがあります？

- ・会社の業務を行うための「システム」
- ・お客様との商取引を行う「システム」
- ・お客様にサービスを提供する「システム」
- ・システムをバックアップするための「システム」
....などなど。

システムをめぐる昨今の「流れ」

- Internet回線の高速化
- 迅速な意思決定が求められる
- グローバリゼーションへの対応
- 各種法令による要請
- 企業業務の継続性／可用性の向上

....「システム」への依存は、年々大きくなっている
さらに、ITへの投資も。

本日のAgenda

- ・ システム....って？
- ・ システム運用／監視の背景にせまる
- ・ システム監視の実装について



システム構築のありがちな風景

- ・ 良く分からぬからSIerにお任せ！
- ・ UNIX(と言うかLinux)を使うと安くて済むよねー
- ・ とにかく安く済ませたい
- ・ システムは作ったらおしまい！



考えていますか？

- ・ どういった設計にするか、理解していますか？
- ・ 本当にUNIX(というかLinux)は安いの？
- ・ どこまでお金をかけますか？
- ・ その「システム」はどの程度重要な「システム」ですか？

そして....

- ・ システムの「運用」は考えていますか？

システムの運用／監視とは？

- ・ 運用とは、簡単に言うと
「システムが常に正しく動くようにすること」
- ・ 監視とは、簡単に言うと
「システムが正しく動いているかどうかを
確認すること」
- ・ あまり表には出ないが、非常に重要な部分
- ・ 運用／監視を考えないままシステムを
構築すると、後で.....orz

本日のAgenda

- ・ システム....って？
- ・ システム監視の背景にせまる
- ・ システム監視の実装について



何を監視するの？

- ネットワーク
- サーバのリソース
- 各種プロセスの稼働状況
 - 及び、各種ジョブの実行状況
- ログ

どうやって監視するの？

- ICMPによる死活監視
- SNMPを用いた各種情報の収集／アラート検知
- 各種プロトコルに基づいたポートの稼働状況確認
- 監視Agentを用いた情報収集

そもそも...どこまで監視できるの？

- 監視できるもの；
 - リモートで情報が取得できるもの
 - 複数のユーザが共通で使用しているもの
 - 機器は、電源が落ちないことが前提

- 監視できないもの；
 - リモートで情報が取得できないもの
 - 個人が使用しているもの

ICMPによる死活監視

- 一般的に良く使われている。
- 監視の実装がしやすい。(監視対象の機器でICMPIに応答してくれればOK)
- 実際の障害以外でも、応答が無い場合がある。(ネットワークが混雑しているときなど)
- ICMPv6での監視は、現段階ではちょっと危険かも....

SNMPを用いた情報収集／アラート検知

- ・ 比較的簡単に機器の情報収集、及びアラート検知ができる
- ・ 一般的には、SNMP Trapを用いたアラート検知を用いることが多い
- ・ アラート発生時に_(比較的)リアルタイムに把握可
- ・ 途中のネットワークの状況次第では、届かないことも....
- ・ バージョンがちと複雑(1/2c/3)→RFC3410
- ・ MIBのコンパイルも場合によっては....面倒

各種プロトコルに基づいたポートの稼働状況確認

- 監視サーバから各プロトコルに応答を行うメッセージを送り、反応を見る。
(例; HTTPでのGETコマンド)
- 対象機器にてポートをListenしているかどうか確認できる。
- 中には、プロセスがHang-Upしていても大丈夫なものが....

監視Agentを用いた情報収集

- ・ 監視対象になる機器にAgentを導入し、Agentが適時Managerに情報を出力する
- ・ 設定次第で、様々なものが監視できる
- ・ なかには、監視システムが稼動システムに影響を与えることも....
- ・ ログ監視については注意してね

ではどうやって監視しよう？(Network機器の場合)

- ICMPによる死活監視
 - 必須。冗長化している場合にも、切り替わりを監視するのに必要
- SNMPによる情報収集／Trap検知
 - 必須。トポロジーの変化、及びサーバとの結線の状況変化を把握することができる
- Powershellを用いた情報収集／設定変更
 - F5社のBIG-IPが対応した(3/26)
- 可能であれば、サービス用のNetworkとは別に、監視用のNetworkを構築しておく。
 - ルータであればInterfaceの追加。スイッチ／FW／負荷分散装置etc.であれば別VLANを作成する。

ではどうやって監視しよう？(サーバの場合)

- ICMPによる死活監視
- SNMPによる情報収集／Trap検知
- 各種プロトコルに基づいたポートの稼働状況確認
- 監視Agentを用いた情報収集
- システムの重要度によって、監視の実装を考えてください
- 監視用のNetwork構築も、必要に応じて行う

ではどうやって監視しよう？(アプリケーションの場合)

- ・各種プロトコルに基づいたポートの稼働状況確認
- ・監視Agentを用いた情報収集

でもその前に....

- ・アプリを開発する場合には、できるだけログを出すようにしてください！

監視を行ったうえで....

- 本当に障害を事前に検知できる?
 - 正直、できないものはできない！
 - でも、やらないよりはねえ....
- 障害発生時の切り分けは?
- そのメッセージ、本当に障害？

さいごに

- ご静聴、ありがとうございました。
- 後日、質問があります場合には
<mailto:NetWork@ml.admintechn.jp>
にMailをください。

