ITVision – Estudo para o Desenvolvimento de um Sistema

Encomendado pela Verto Technologies

versão do documento: 1.1

INTRODUÇÃO

O objetivo deste estudo é servir de base para a tomada de decisão para o desenvolvimento de um sistema de gestão de TI voltado para empresas de médio e grande porte. Este sistema deverá ser capaz de oferecer informações de alto nível voltadas tanto para a direção das empresas quanto para o corpo gerencial e técnico . Para isso, ele deverá se utilizar de dados gerados por sistemas do tipo FOSS (Free and Open Source Software), integrando-os em um software que irá gerar, em última instância, um gráfico de medida de eficiência da gestão dos serviços de IT como apresentado na Figura 1. Nele, os vetores representam grandezas relacionadas à infra-estrutura computacional calculadas a partir de medições do funcionamento de cada sistemas individualmente. Para tal, toda a infra-estrutura computacional da empresa deverá ser mapeada e monitorada.

Figura 1 – Medidor de Eficiência de TI.

Um **SISTEMA PILOTO** deverá ser desenvolvido em paralelo ao desenvolvimento deste estudo para se atender às imediatas de um cliente da Verto. Este sistema será utilizado como teste de conceito para o desenvolvimento do **SISTEMA FINAL** acima descrito. Ele será ainda utilizado no auxílio do entendimento das funcionalidades do sistema, na verificação da viabilidade técnica do projeto e na avaliação do esforço a ser aplicado para a construção mesmo.

O resultado final deste estudo deverá ser um conjunto de definições de funcionamento do sistema, com avaliação de seu tamanho (número de telas, número de rotinas e seus graus de complexidade) e as estimativas de custo e prazo em função do que foi definido.

O presente documento será escrito em etapas e poderá ser modificado ao longo do projeto para contemplar todas as informações e definições que ainda serão discutidas. Ele deverá ser a referência de todos dos dados do projeto incluindo a documentação técnica conceitual, de desenvolvimento e de uso do sistema.

TAREFAS E CRONOGRAMA

A seguir estão listadas as tarefas a serem executadas para o desenvolvimento do **SISTEMA PILOTO** e do **SISTEMA FINAL**. O **SISTEMA PILOTO** já teve o seu desenvolvimento iniciado e encontra-se em operação no cliente. Sua evolução tem sido feita sob demanda e com baixo nível de controle e teste. Tendo servido como prova de conceito, ele agora deverá atingir os requisitos mínimos para atender plenamente ao cliente, sendo fundamental a inclusão dos medidores de eficiência. O **SISTEMA FINAL** deverá ser implementado desde seu início com base nos conceitos discutidos e/ou implementados no PILOTO. Grande parte do código deverá ser re-escrito. Todos o sistema de banco de dados deverá ser criado. Parte do código e da lógica utilizada no PILOTO deverá ser re-aproveitada e muitas novas funcionalidades deverão ser implementadas. A seguir estão as listas de tarefas com prazos para entrega de cada funcionalidade.

SISTEMA PILOTO:

Melhorias pontuais (**entregue**)

- Melhoria nos relatórios (discutida com o José Antonio)
- Backup do sistema
- Implementação de sessão para usuários administradores
- Re-inicialização e desligamento do servidor
- Criação de documentação para usuários
- Criação de documentação para administradores

Criação de máquinas virtuais com a última versão (**entrega prevista para 12/02/09**)

- automação da instalação (revisar e testar)

Criação de tela com medidor de eficiência (gráfico setas) (**entrega prevista para 20/02/09**)

- Inclusão de “Disponibilidade” no medidor
- Inclusão de “Tempo de resposta” no medidor
- Inclusão de “Integridade” no medidor (Inferir)
- Inclusão de “Gerenciabilidade” no medidor (Inferir)

Implementação de sub-sistema de Continuidade de Serviço (**previsto para 06/03/09**)

Auxilio ao diagnostico (detecção já implementada pela monitoração)

Apresentação de contingência e Recuperação

Configuração de diagnostico/contingência/recuperação por importação de arquivo

Cluster de ITVision (**previsto para 13/03/09**)

Integração de base de informações para mais de uma instância do ITVision

Sincronização automática (?) de configuração

Alteração das telas de apresentação para contemplar cluster

Conexão segura (VPN ou SSL)

Distribuição dos dados aferidos com sinalização após falha de comunicação

Distribuição de logs com sinalização após falha de comunicação

Alteração das telas de relatórios para contemplar cluster

Alteração dos algorítimos para cálculo de eficiência

Alteração das telas do medidor de eficiência

SISTEMA FINAL: (**ainda sem previsão de entrega**)

Base de Dados para o ITVIsion

Criação de base de dados para abrigar os dados do PROJETO 1

Implementação de métodos de acesso a diversas bases de dados simultaneamente

Implementação de telas (html) para LISTAGEM, INCLUSÃO, INCLUSÃO EM MASSA, ALTERACÃO, EXCLUSÃO de:

usuários

grupos de usuário

sistema de permissão tela X usuário ou grupo

preferências dos usuários

sítios (local de instalação de unidade de cluster do ITVision)

comandos de checagem

Itens de configuração (SW, HW, SERVICO) por sítio

contatos para alerta

aplicações

sub-aplicações

associação contatos x (sub-)aplicações

medidores de eficiência

referências de conformidade para medir eficiência (ver ex. abaixo)

CONF	CUST($)	DISP(%)	EFIC(s)	...
0	1000	96,0%	1,00	...
1	1000	97,5%	0,80	...
2	1000	98,5%	0,60	...
3	1000	99,2%	0,40	...
4	1000	99,9%	0,20	...
5	1000	100%	0,01	...

lista de falhas

procedimentos de contingência e recuperação X falhas

configurações diversas no sistema

configuração de sistema de log

Interface WEB

Implementar funcionalidades para sistema de permissões de acesso

Melhorar aparência e estilo para melhor navegabilidade e visualização

Automatizar geração de tabelas para criação listagens

Apresentação gráfica de aplicações deve individualizar os IC's

Criação de gráficos para relatórios (pizza, estado, entre outros – estudar)

Criação de mecanismo de dash-board (estudar)

Mecanismos AJAX para atualização automática de informações

Migração de todo o código existente para a nova versão(!)

Monitoração e Alerta

Formalização (documentação) dos conceitos discutidos

Implementar conceito de aplicações, sub-aplicações

Implementar o conceito de cluster de IC's, de aplicações e de sub-aplicações

Implementação de máquina de estados para cálculo de estado de uma aplicação

Implementar sistema de envio seletivo de emails para contatos

Criação de log circular

Sumarização de log

Depuração de problemas com gmail (procurar alternativa)

Migração de todo o código existente para a nova versão(!)

Medição de eficiência

- Criação de algorítimos para cálculo de:
  - disponibilidade
  - gerenciabilidade
  - tempo de resposta
  - continuidade de serviço
  - [Os cálculos de integridade, segurança, nível de serviço, capacidade, custo e escalabilidade só serão definidos no futuro.]

Relatórios

- Criar relatórios gráficos, textuais e impressos de:
  - resumo de alertas
  - ocorrência por tipo de alerta
  - problemas mais freqüentes
  - ocorrência por aplicação e por sub-aplicação
  - ocorrência por sítio
  - ocorrência por tipo de IC's

Administração do sistema

- Backup salvando o arquivo em máquina local de:
  - todas as bases de dados
  - logs alertas
  - configurações de email
  - configurações de sistema (rede, etc...)
- Restore a partir de backup executado
  - verificação de versão, data, status
  - restore seletivo de base de dados
  - restore seletivo de logs
  - restore seletivo de configuração de sistema
- Manutenção (Stop, Start, Restart) dos sub-sistemas (FOSS existentes) de:
  - servidor de banco de dados
  - servidor de http
  - monitoração
  - detecção de novos equipamentos de rede
  - detecção de computadores e software

Sub-sistema de monitoração

- Instalação de base de dados de configuração (sistema FOSS existente)
- Mecanismos de sincronização desta base de dados com a criada para o ITVIsion
- Tela para execução manual de comando de checagem

Sub-sistema de detecção de novos equipamentos de rede

- Instalação, estudo e testes
- Integração e sincronização dos dados recolhidos
- Integração das informações de monitoração dos equipamentos
- Inclusão das informações de monitoração nos cálculos de eficiência
- Ativação de sistema de gerenciamento de configuração quando na detecção ou desaparecimento de um IC.

Sub-sistema de detecção de computadores e software

- Instalação, estudo e testes
- Integração e sincronização dos dados recolhidos
- Ativação de sistema de gerenciamento de configuração quando na detecção ou desaparecimento de um IC (mesmo utilizado no sub-sistema anterior).

Sub-sistema de gerenciamento de Mudança/Incidente/Configuração

- Implementar base de dados para gerenciamento de diagnóstico/procedimento
- Implementar base de dados para gerenciamento de incidentes e tipos de incidentes
- Criar telas para o gerenciamento da base de diagnóstico/procedimento
- Criar associação IC, alerta (falha) e diagnóstico/procedimento
- Criar telar para listagem, inclusão, deleção e alteração de incidentes
- Criar tela para abertura de chamado
- Integrar abertura de chamado com autenticação padrão para que não usuários do ITVision possam abrir chamados
- Criar relatórios de ocorrências de mudança, incidente (chamados) e de configuração
    - listagem
    - gráfico pizza
    - resumo e sumarização
    - ordenação por tipo de ocorrência

DEFINIÇÕES

Visão Geral do Sistema: Para se medir a eficiência em TI deverão ser utilizadas informações provenientes de uma série de sistemas especialistas tipo FOSS. É através destas informações que deverá ser criado o algorítimo para se medir os vetores indicados na Figura 1. Este algorítimo deverá ter como referência o padrão CMMI para o cálculo do nível de maturidade conforme apresentado na Tabela 1.

As principais funcionalidades que o sistema deverá prover são:

- Service Desk / Helpdesk
- Gerenciamento de Falhas (Monitoração)
- Gerenciamento de Incidentes
- Gerenciamento da Configuração
- Gerenciamento de Mudanças
- Gerenciamento do Nível de Serviço
- Gerenciamento Financeiro para Serviços em TI (?)
- Gerenciamento da Disponibilidade
- Gerenciamento da Capacidade (?)
- Gerenciamento da Continuidade dos Serviços em TI
- Gerenciamento de Performance (Rede e Servidores)
- Gerenciamento de Usuário e Grupos

Nível de Conformidade	Compliance com o Padrão	Denominação	Definição
0	0%	INEXISTENTE	Ausência total de gerenciamento do processo.
1	20%	INFORMAL	A organiza,cão reconhece a necessidade de gerenciar o processo. Contudo não há procedimentos organizados nem documentados e nem comunicados.
2	40%	ORGANIZADO	Já há definição dos processos mas não há treinamento formal. A responsabilidade pelos processos é de seus executores.
			Os procedimentos são padronizados, documentados

3	60%	BEM ESTRUTURADO	comunicados e treinados. Já há algum grau de controle. Há início de uso de indicadores.
4	80%	GERENCIADO	Processos integrados e alinhado, monitorados por indicadores consistentes. Ferramentas automatizadas são usadas de forma limitada.
5	100%	OTIMIZADO	Os processos são automatizados e alinhados com as melhores práticas, baseados em resultados e na melhoria contínua.

Tabela 1 – Padrões de Referência: COBIT

Os sistemas tipo FOSS a serem utilizados serão:

- Helpdesk
- Gerenciamento de Projetos
- Gerenciamento de Performance (Rede e Servidores)
- Detecção de Intrusão (IPS)
- Gerenciamento de Falhas (Monitoração)
- [acrescentar quando necessário]

Para a integração desses sistemas deverá ser criada uma base de informações que será comum a todas as aplicações. Esta base deverá guardar informações a respeito dos ativos de TI existentes na empresa. Estas informações deverão ainda seguir as recomendações definidas do ITIL buscando a conformidade com este padrão compondo assim uma base de dados tipo CMDB (Configuration Management Database).

Deverá ser criado portanto, um sistema central (batizado de ITVision na execução do projeto piloto) que irá manipular e compartilhar as informações armazenadas no CMDB e deverá conter interfaces com todos os demais sistemas geradores de informação. As informações a respeito dos ativos de TI deverão ser trocadas em ambas as direções. Estas interfaces poderão ser feitas através de API's (Application Program Interfaces) criadas no sistema central, através das bases de dados de cada sistema ou através das API's disponibilizadas nos sistemas FOSS geradores de informações.

Além de gerar informações, os sistemas FOSS deverão ainda prover as funcionalidades por eles propostas, agregando assim uma série de capacidades ao sistema central. Assim, esses sistemas FOSS geradores de informação passarão a ser denominados de **sub-sistemas** e irão

compor a solução final. A Figura 2 apresenta o diagrama de blocos da composição e integração do sistema central com os sub-sistemas.

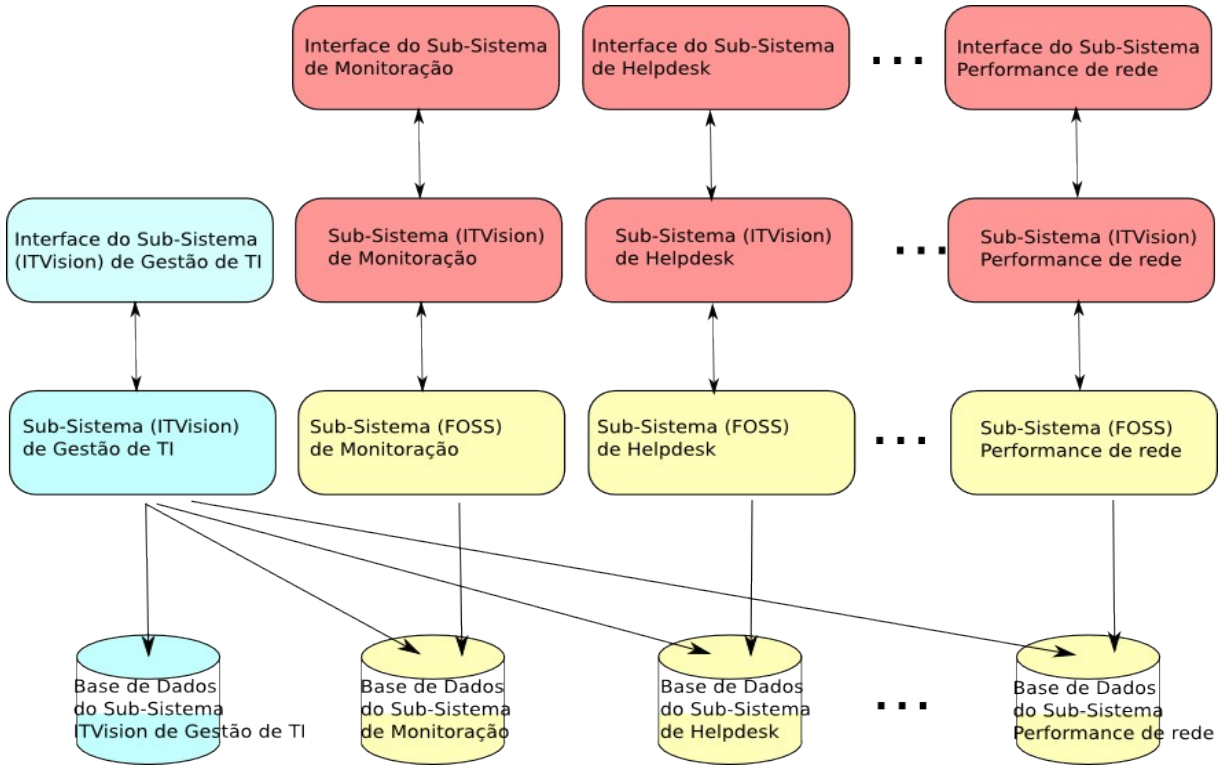

Figura 2 – Integração entre os sub-sistemas FOSS e o ITVision

Nesta figura os blocos azuis representam o sistema central ITVision. Os blocos vermelhos correspondem as funcionalidades que devem ser adicionadas aos sub-sistemas FOSS que são representados em amarelo e podem vir a ser alterados para inclusão de interfaces a serem utilizadas pelo ITVision central.

Definição do Sistema de CMDB: O ponto central para a criação de um CMDB é a definição dos Itens de Configuração - IC's. É em torno desta entidade que todo o sistema ITVision se desenvolverá. Ele deverá receber e fornecer informações para todos os demais sub-sistemas. Os sub-sistemas de auto-detecção de IC's para computadores e para equipamentos de rede são os que tipicamente deverão fornecer informações ao CMDB. Os sub-sistemas de gerenciamento de configuração e de mudança poderão alterar as informações do CMDB que irá fornecer as informações necessárias para os sub-sistemas de helpdesk, gerenciamento de incidentes, falhas, nível de serviço, financeiro, disponibilidade e capacidade, continuidade do serviço e de performance.

... AS DEFINIÇÕES A SEGUIR DEVEM SER COMPLETADAS...

Definição do Sub-Sistema de Service Desk / Helpdesk:

Definição do Sub-Sistema de Gerenciamento de Falhas (Monitoração):

Definição do Sub-Sistema de Gerenciamento de Incidentes:

Definição do Sub-Sistema de Gerenciamento da Configuração:

Definição do Sub-Sistema de Gerenciamento de Mudanças:

Definição do Sub-Sistema de Gerenciamento do Nível de Serviço:

Definição do Sub-Sistema de Gerenciamento Financeiro para Serviços em TI (?):

Definição do Sub-Sistema de Gerenciamento da Disponibilidade:

Definição do Sub-Sistema de Gerenciamento da Capacidade (?):

Definição do Sub-Sistema de Gerenciamento da Continuidade dos Serviços em TI:

Definição do Sub-Sistema de Gerenciamento de Performance (Rede e Servidores):

ALGUMAS INFORMAÇÕES SOBRE SISTEMAS FOSS PESQUISADOS

1 - Lista de sistemas similares existentes no mercado:

- HP openview
- Ciscoworks
- Cricket
- Nagios

2 - Pesquisa de ferramentas *open source*

Aproximadamente 40 ferramentas entre simples e sofisticadas
Critérios: finalidade , licença , atividade , maturidade , comunidade

Nagios:
Finalidade: Monitoração de servidores e serviços
Licença: GPL2
Atividade: 5
Maturidade: 4
Comunidade: 5
Complexidade: 3

Nmap:
Finalidade: Segurança - Scan de portas e serviços
Licença: GPL2 (http://nmap.org/data/COPYING)
Atividade: 4
Maturidade: 5
Comunidade: 3
Complexidade: 1

Snort:
Finalidade: Segurança - network intrusion prevention and detection system
Atividade: 5

Maturidade: 5
Comunidade: 5
Complexidade: 5

Estudo das licenças *open source* (GPL, GPL2, GPL3, BSD, BSDLike etc...)
    Critérios: uso , alteração , distribuição , subcontratação , encapsulamento

Estudo das ferramentas *open source* selecionadas (~10)
    Critérios: instalaçao , uso , adaptabilidade , facilidade de alteração

Estudo de Linux para Apliance (~3)
    Critérios: compatibilidade , capacidade de customização , licença

Definição de plataforma de desenvolvimento
    Critérios: adequação , segurança , mão-de-obra

Estudo para criação de sistema de integração (resultados e logs)
    Critérios: acesso , consolidação , uso/disponibilização

Estudo para criação consolidação de resultados
    Critérios: métricas , regras de negócios , generalização

Estudo para criação de sistema de visualização/sinalização
    Critérios: interface , generalização

Estudo de cronograma e custos
    Critérios: timeline/gant , equipe de desenvolvimento , custos

Visto
Snort (SnortSMS) : Open source IDS
Nmap: Port scanner

Segurança

Nessus : UNIX vulnerability assessment tool
NetFlow and
cflowd: A flow analysis tool currently used for analyzing Cisco's NetFlow enabled switching method.
Nikto: Open Source (GPL) web server scanner (or test your IDS system)
John the Ripper: A powerful, flexible, and fast multiplatform password hash cracker
Nbtscan : Gathers NetBIOS info from Windows networks
OSSEC HIDS : An Open Source Hostbased Intrusion Detection System
Yersinia : A multiprotocol lowlevel attack tool
Mantra: (Monitor and Analysis of Traffic in Multicast Routers) is a tool for monitoring various aspects of multicast at the router level.
RTG: is a flexible, scalable, highperformance SNMP statistics monitoring system.
Panoptis: A project to detect and block DoS/DDoS attacks (NO!)
Honeyd: is a small daemon that creates virtual hosts on a network
Prelude: is a Universal "Security Information Management" (SIM) system.

VER: http://www.freefire.org/tools/index.en.php

Yersinia is a lowlevel protocol attack tool useful for penetration testing. It is capable of many diverse attacks over multiple protocols, such as becoming the root role in the Spanning Tree (Spanning Tree Protocol), creating virtual CDP (Cisco Discovery Protocol) neighbors, becoming the active router in a HSRP (Hot Standby Router Protocol) scenario, faking DHCP replies, and other lowlevel attacks.

Monitoracao:
==========
www.nagios.org
www.groundworkopensource.com

www.zabbix.com
http://www.zenoss.com/

Inventario:
==========
http://www.ocsinventoryng.org/

Log
==========
http://www.intersectalliance.com/projects/index.html

Cisco:
==========
http://cosinms.sourceforge.net/

G. Projetos:
==========
http://www.softwareprojects.org/freeprojectmanagementsoftware.htm
google em "netoffice sourceforge"
http://www.projectopen.com
http://ganttproject.biz
http://www.gptools.com.br
http://www.jabber.org
http://www.openacs.org
http://www.taskjuggler.org/
http://projectory.sourceforge.net/
http://dotlrn.org
http://dotlrn.org/users/mitsloan/

OLAP http://www.pentaho.com/

Câmera web:

==========

zoneminder

Plataforma Ajax: (usada no groundwork)

==========

http://gauva.sourceforge.net