

OPMON TECHPAPER: RECURSOS E FUNCIONALIDADES

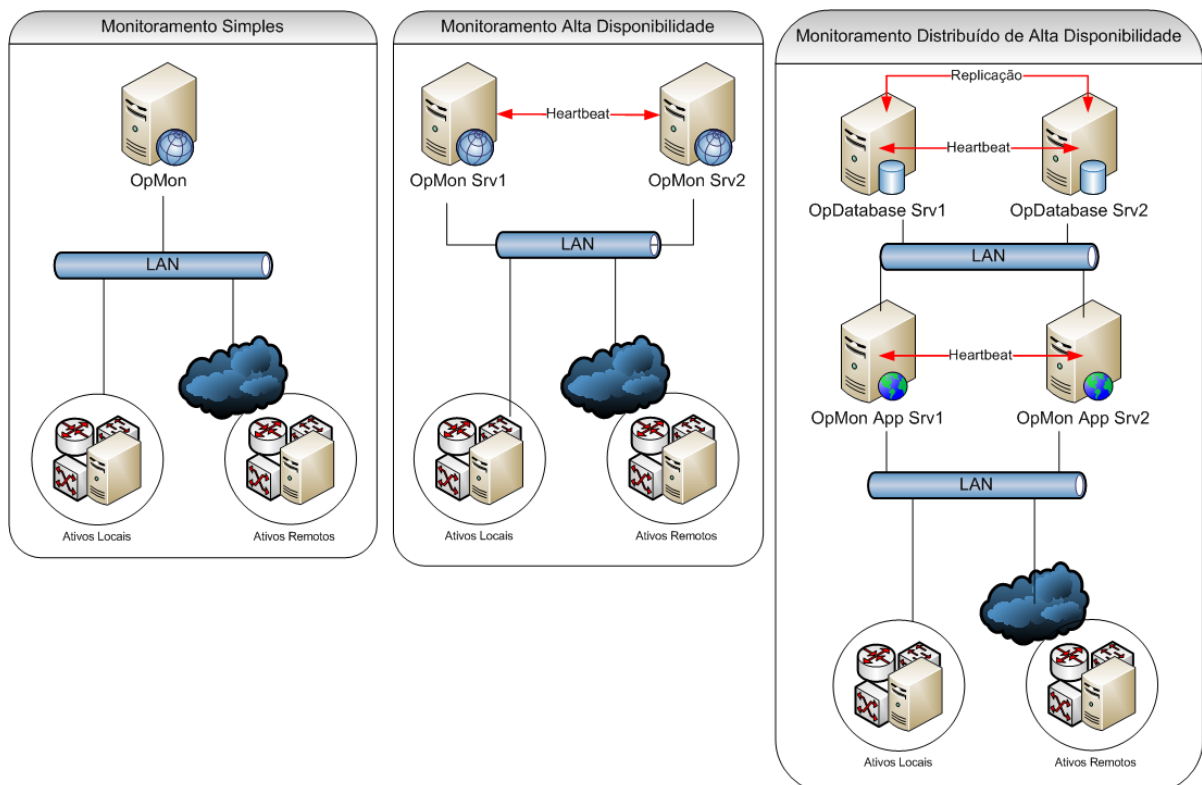
CARACTERÍSTICAS GERAIS

Plataforma de gerenciamento de infraestrutura de TI, Telecom e Processos de Negócios. Através de uma **console única de gerenciamento**, o OpMon envia alertas de e-mails e SMS para os administradores quando os recursos de aplicativos, sistemas operacionais, banco de dados e outros atingem os limiares definidos. Ao detectar eventos previamente configurados, que determinam as quebras dos SLAs estabelecidos, envia alertas, podendo executar scripts, enviar e-mails ou SMS, além de exibi-los na interface web.

Efetua checagens e verifica se os limites (thresholds) são excedidos. Sejam valores absolutos, travamentos ou atrasos, os alertas são gerados e cada um deles representa um tempo de indisponibilidade, registrado nos relatórios de SLA. Todas as checagens/coletas são armazenadas em BD relacional e, por meio dos relatórios, possibilitam planejar capacidade, fazer comparações e análises para tomadas de decisão. Permite, também, que os SLAs sejam especificados por aplicação, por servidor, ou pela combinação de ambos, com visualização por interface gráfica e relatórios em HTML. Com a solução é possível, ainda, fazer a filtragem de informações por horário, aplicação ou servidor, usando apenas interface gráfica.

ARQUITETURA

A solução OpMon é composta por um ou mais servidores de gerenciamento, com uma suíte de software, que monitora um número ilimitado de objetos ou serviços - elementos de infraestrutura, banco de dados, aplicações e processos de negócio. Desenvolvido para operar em ambientes de **alta disponibilidade**, possibilitando que os componentes de hardware e software da plataforma tecnológica sejam redundantes e escaláveis **através de suporte a instalação em cluster**.



O gerenciamento é feito por um equipamento central, com os respectivos agentes distribuídos, e um ou mais consoles instalados, com a utilização de menos de 5% de CPU e memória dos hosts-alvo. Acessada por meio de uma interface web, HTTPS com SSL de 128 bits, permite que as informações, coletadas em diversos pontos e armazenadas no BD, possam ser visualizadas em uma console única, acessada de qualquer local, com usuário e senha predefinidos. Cada usuário pode ter uma visão gráfica específica e diferenciada do sistema, de acordo com as suas atribuições.

RECURSOS DE INFRAESTRUTURA E TI QUE PODEM SER MONITORADOS

- Roteadores;
- Switches;
- E-mail;
- Access Points;
- Impressoras;
- No-breaks;
- Máquinas virtuais;
- Appliances;
- Notas Fiscais Eletrônicas (NFe)
- Nota Fiscal do Consumidor Eletrônica (NFCe);
- SiTEF;
- Câmeras de Segurança IP, Indoor e Outdoor;
- UTM de qualquer fabricante;
- Controle de Acesso (Catracas);
- Relógios Ponto;
- Sistemas operacionais, como Linux (Cent OS, Debian e RedHat) e Windows;
- Plataformas de virtualização baseadas em VMware, Hyper-V, XEN e RHEV;
- Bancos de dados como MS-SQL, MySQL, Oracle e Postgresql;
- Frameworks de aplicações como Websphere, Weblogic, J2EE e .NET;
- Informações de aplicações de gerenciamento de hardware de qualquer fabricante. Exemplo: Dell OpenManager;
- Equipamento medidor de umidade e de temperatura (HWg-STE);
- Storages HP, NETAPP, IBM, DELL e EMC;
- Centrais Telefônicas analógicas e IP de qualquer fabricante;
- **Qualquer equipamento, específico de TI ou não, com de capacidade de comunicação IP.**

SISTEMAS E APLICAÇÕES QUE PODEM SER MONITORADOS

- Gerenciamento de níveis de produtividade dos funcionários;
- Gerenciamento de níveis de produção fabril;
- Gerenciamento do nível de combustíveis de geradores;
- Gerenciamento de callcenters;
- Capacidade energética;
- ERP (Enterprise Resource Planning);
- SCM (Supply Chain Management);
- Gerenciamento de experiência do usuário (CEM – Customer Experience Management);
- Service Desk;
- Supply Chain Design;
- E-commerce e E-procurement;
- **Qualquer sistema, aplicação ou processo de negócio que permita a coleta de dados.**

INDICADORES

- Possibilita o agrupamento de dispositivos (IC - itens de Configuração) com Indicadores chave de desempenho (KPIs);
- Hierarquia de acessos: cada usuário pode visualizar somente os elementos (ICs e KPIs) para os quais possui autorização;
- Coleta de KPIs de forma ativa. É possível configurar intervalos customizados para cada indicador;
- Configurações de regras para suprimir alarmes falsos positivos.

POSSIBILIDADE DE INTEGRAÇÕES

Desenvolvimento de integrações não nativas:

A OpServices disponibiliza interfaces de comunicação para integração com outras soluções desenvolvidas. O OpMon suporta as seguintes interfaces:

- Web Services;
- Acesso direto à base de dados SQL.

Integração com Service Desk:

Integração webservices entre o OpMon (gerenciamento de TI) e soluções de Service Desk. As integrações desenvolvidas e documentadas são com OTRS e Qualitor. Entre os recursos disponíveis estão:

- Integração desenvolvida com tecnologia webservices;
- Abertura automática de incidentes no Service Desk a partir de eventos do OpMon;
- Associação do IC ao chamado de incidente no momento do seu registro;
- Flexibilidade de definições na abertura de chamados (Serviço, SLA, Prioridade, Responsáveis);
- Registro automático de comentário/ação no OpMon com número do chamado;
- Processo de atualização do CMDB a partir do inventario e monitoramento do OpMon;
- Gerenciamento da configuração dos ICs no CMDB com versionamento automático;
- Dashboards e relatórios customizáveis de KPIs do Service Desk no OpMon.

INTERFACE

O OpMon possui interface web para operação em todas as suas funcionalidades. Pode ser executado em navegadores Google Chrome, Microsoft Internet Explorer e Mozilla Firefox, em suas versões mais recentes.

- Suporte nativo a personalização de temas através dos seguintes recursos:
 - Temas de cores pré-configurados;
 - Suporte ao desenvolvimento de novos temas de cores;
 - Recurso de upload de logotipo do cliente;
 - Carregamento do logotipo cadastrado de forma automática em todos os relatórios a serem exportados em formato PDF e telas do sistema.
- Controle de acesso através de usuário e senha;
- Suporte a multi-idioma, com português e inglês nativo nos sistema;
- Possibilidade de configuração de thresholds e limites de tempo de checagem via interface gráfica. Não existe a necessidade de implantação de outros recursos ou codificações;
- Visões e recursos da console de operação;

- Visão de topologia de rede: representação gráfica automática de todos os relacionamentos de parentesco entre os dispositivos (ICs) monitorados e o estado atual do monitoramento atualizado conforme tempo de checagem configurado;
- Visão por localidade e por estrutura organizacional;
- Mapa de rede autogerado pela plataforma;
- Status de criticidade através de cores (verde, amarelo e vermelho) para identificar problemas de configuração ou alcançabilidade nos dispositivos gerenciados. Essa visão permite visualizar rapidamente os principais problemas encontrados na infraestrutura.
- Apresentação de todos os eventos e alarmes do ambiente em interface única com a possibilidade de que o usuário possa fazer drill downs através da expansão de indicadores para níveis detalhados de informação, de acordo com o evento ou alarme selecionado;
- Busca avançada via diversas combinações de filtros:
 - Busca textual através da descrição de um IC, grupo de ICs, atributo de IC e grupo de atributos de IC;
 - Busca via retorno de uma checagem ou monitoração (habilitada ou desabilitada);
 - Níveis do estado atual da monitoração (Alerta, Crítico, Ok, Inalcançável, Desconhecido, Instabilidade, UP, Fora);
 - Níveis do estado atual da monitoração (hard state e soft state);
 - Notificações (habilitada ou desabilitada);
 - Documentação (com ou sem);
 - Ação/parada agendada (sem, ações, paradas, ações e paradas, ações ou paradas).

SEGURANÇA

Credenciais, Dados e Perfis de Usuários:

- Criação e definição de perfis de usuários através de hierarquias e atribuição de diferentes níveis de autorização;
- Autenticação externa da solução via protocolo LDAP ou AD (Microsoft Active Directory).

Criptografia e autenticação das informações:

- Criptografia e autenticação de maneira segura de todas as transferências de dados entre os servidores de rede dos sistemas, seus agentes ou estações de trabalho. Também possibilita a existência de fluxos de dados de qualquer protocolo não criptografado em quaisquer partes da solução;
- Utilização de HTTPS (HTTP com criptografia e identificação segura), de acordo com parâmetros comuns de mercado;
- Suporte à instalação de certificados X.509 próprios para a URL em que o acesso for disponibilizado;
- Utilização de LDAP Seguro (LDAPS ou StartTLS), com o uso de criptografia e/ou autenticação segura e/ou certificados digitais.

Registros - Operações e Trilhas de Auditoria:

- Registro detalhado (log) de todas as mudanças no sistema de gerenciamento como: alarmes, incidentes, operações, autenticação de usuários entre outros;
- Envio para servidores de syslog de todos os registros gerados de forma imediata, após a ocorrência de cada evento;
- Geração de trilhas de auditoria com as informações sobre os eventos referentes à autenticação de usuários e todas as suas ações (identificação de usuário, data de alteração, local de alteração e ação realizada);
- Recurso para busca através de variáveis textuais e por períodos de tempo (meses, horas, etc.)
- Registros de logs, auditoria e syslog internos **vitalícios**. Não existe possibilidade de alteração ou exclusão de qualquer um destes itens;
- Período ilimitado para manutenção de registro de logs, auditoria e syslogs internos;

BACKUP

- Rotina automática pré-programada de backup (parcial ou total) das configurações e da base de dados;
- Recurso para backup manual (parcial ou total) da base de dados e configurações;
- Recurso de restauração de backup (parcial ou total) para recuperação das configurações e da base de dados;
- Disponibilização automática dos arquivos gerados pelo backup através de um compartilhamento de rede.

CATÁLOGO DE SERVIÇOS

Criação de estruturas de Catálogo de Serviços via interface do sistema **com possibilidade de mapear todas as dependências lógicas para a entrega de um serviço**. As dependências podem ser organizadas de forma hierárquica, serial, contingente/paralela e, inclusive, com interdependências entre serviços. **Permite a descoberta da causa-raiz dos problemas, do impacto do incidente e os usuários afetados:**

- Possibilidade de cadastro e manutenção da descrição de serviços e dos seus atributos;
- Suporte a definição dos atributos para cada serviço do catálogo:
 - Definição de tipos de serviço: TI, Negócio e Negócio Vital, por exemplo, ou através de customização criando novos ou alterando nomes;
 - Definição do responsável pelo serviço (negócio e técnico);
 - Definição de quem são os usuários, quem são os usuários chaves, a estrutura da unidade organizacional e as localidades afetadas;
 - Definição do **custo por hora** de cada serviço afetado dentro do catálogo;
 - Definição da data de revisão de cada serviço;
 - Recurso para a criação de descrição dos serviços, dos processos de negócio dependentes, dos entregáveis do serviço e das aplicações envolvidas;
 - Recurso para a criação de cortes de tempo para a definição dos períodos de disponibilidade (24x7, 8x5 ou customizado) de cada serviço, do tempo de resolução e do tempo médio para cada atendimento;
 - Definição de sazonalidade para um serviço através da escolha de dias aplicáveis dentro de um mês;
 - Definição de criticidade, prejuízo financeiro ou de imagem, complexidade, usuários VIP, percentual de usuários afetados e relação de dependências;
 - Definição de atributos personalizáveis;
 - Recurso para a criação de serviços de TI associados aos ICs que os suportam;
 - Recurso para a criação de serviços de infraestrutura de TI com a possibilidade de associação de itens de configuração (IC) a estes serviços;
 - Recurso para a criação de hierarquia de serviços do catálogo através de dependências com relacionamento do tipo pai e filho;
 - Visualização, através de dashboards gerados automaticamente, da disponibilidade dos serviços do catálogo, de todos os elementos que os compõem e de todas as suas correlações e interdependências. Todas as alterações na sua estrutura refletem automaticamente no dashboard padrão;
 - Navegação detalhada (drill-down) através do dashboard do catálogo de serviços;
 - Recurso para a monitoração automática dos serviços do catálogo;
 - Apresentação da visão de monitoramento dos catálogos de serviços de acordo com os tipos definidos na solução;
 - Suporte a gráficos de capacidade em tempo real para a visualização de percentual de disponibilidade e tempo de disponibilidade para cada serviço do catálogo;
 - Recurso para análise de impacto via interface central de monitoramento.

GERENCIAMENTO DE ITENS DE CONFIGURAÇÃO

- Recurso para registro, armazenamento, gerenciamento de ICs e seus respectivos atributos através de BDGC (Banco de dados de gerenciamento de configuração).
- Visualizações dos ICs e de seus atributos conforme o login de cada usuário: pessoa, unidade organizacional ou localidade;
- Recurso para o cadastro via interface da estrutura das organizações e pessoas para a comunicação sobre alarmes e escalonamento de ações:
 - Registro organizacional com adição e exclusão de pessoas para comitês, comissões, equipes, grupos e subgrupos de trabalho;
 - Registro de informações sobre os contatos: nome, telefone, e-mail, endereço, localização e outras informações;
 - Adição de atributos nos tipos de IC através de assistentes;
- Relacionamentos e dependências ente ICs e AICS;
- Recurso para definição de estruturas hierárquicas de categorias de IC;
- Parada agendada para planejamento de interrupções de monitoramento de ICs sem gerar alarmes. Programação de interrupções periódicas e interrupções ocasionais de forma automática;

DISCOVERY (DESCOBERTA AUTOMÁTICA DE ICs DA INFRAESTRUTURA)

- Descobrimto e registro automático dos IC presentes na infraestrutura através de recurso de “discovery”;
- Descobrimto de topologia de nível 2 e nível 3 da rede LAN e WAN;
- Métodos de pesquisa suportados pelo descobrimto de nível 2:
 - Consulta a tabelas ARP;
 - Consulta a tabelas de Endereçamento IP;
 - Consulta a tabelas de protocolos proprietários de descobrimto, como o Cisco CDP;
 - Consulta a tabelas de roteamento;
 - Consulta a informações de Spanning Tree;
- Inclusão manual de IC no CMDB (Configuration Management Database) através de:
 - Modelo (template) de IC com as informações que serão pré-incluídas nos campos dos IC gerados;
 - Definição de um padrão de rotulação para definição de nomes de identificação do IC, com definição de prefixos e sufixos com variação sequencial.

MONITORAMENTO DE BANCO DE DADOS

Gerenciamento de serviços de bancos MySQL, Oracle, Postgresql, MS SQL e Firebird.

Microsoft SQL Server (2005, 2008 e superior) e MySQL em todas as suas versões com a monitoração dos parâmetros:

- Banco de Dados SQL Server e MySQL Server;
- SQL-Agent;
- SQL-Buffer-Cache-Hit-Ratio;
- SQL-Full-Scans-Sec;
- SQL-Number-Deadlocks-Sec;
- SQL-Page-Splits-Sec;
- SQL-Server-Stats;
- SQL-Target-Total-Server-Memory;

- SQL-Replicação;
- SQL-Usuários Bloqueados, Conectados e Ativos;
- SQL-Transações;
- SQL-Batch Request;
- SQL-Databases / SysFiles;
- SQL-Crescimento de DataFiles;
- SQL-Free Pages;
- SQL-Latch Waits;
- SQL-Lock Blocks;
- SQL-Lock Waits;
- SQL-Crescimento de Log Files;
- SQL-Page Reads e SQL-Page Writes;
- SQL-Compilations;
- SQL-Target Server Memory;
- SQL-Total Server Memory;
- "Select" ou "stored procedure" (e seus tempos de resposta);
- Percentual de utilização dos processadores pelos processos do MS SQL Server (exibição das sessões que mais consomem este recurso com sua respectiva utilização e comando SQL sendo executado).

Base de dados Oracle:

- Monitoramento de diversos indicadores Oracle com possibilidade de, a qualquer momento, alternar instâncias gerenciadas;
- Monitoramento de schema e seus indicadores: user name, default tablespace, temp tablespace, profile, grants;
- Gerenciamento de sessões:
 - Lista de sessões ativas por instâncias;
 - Detalhamento do que está em execução em cada sessão;
 - Sessões em espera;
 - Top sessões em espera por eventos.
- Gerenciamento detalhado:
 - Tablespace;
 - Datafiles;
 - Redo e archives;
 - Rollback segments;
 - Performance com indicadores de: alocação de memória e recursos, shared SQL area, multi threaded server;
 - Lock contents;
 - Perfis e segurança;
 - Arquivos de controle;
 - Parâmetros de inicialização;
 - Especificações RAC;
 - Eventos recentes;
- Administração da base de dados como: usuários, sessões, rollback segments, objetos, parâmetros, job scheduler;
- Relatórios de base de dados:
 - Espaço por usuário;
 - Trablespace por usuários;
 - Datafile fragmentation;
 - Object extent;
 - Multi instance.

DB2:

- Connection Statistics;

- Agents Statistics;
- DB Information;
- Transaction Statistics;
- Cache Performance;
- Buffer Statistics.

Instances:

- Number of local connections;
- Number of remote connections;
- Number of gateway connections;
- Created agents ratio;
- Agents registered;
- Agents waiting.

Database:

- Locking information (locks held, lock waits, deadlocks, etc.);
- Sort information (number of sorts, sort time, sort overflow, etc.);
- Buffer pool and I/O information (number of reads, writes, times, etc.);
- Desenvolvimento de agents customizados;
- SQL statement counts (commits, rollback, selects, etc.);
- Row counts;
- Internal counts;
- Application connection counts;
- Login information.

MySQL:

- Aborted_clients , Aborted_connects;
- Binlog_cache_disk_use, Binlog_cache_use, Bytes_received;
- Bytes_sent;
- Com_admin_commands, Com_alter_db, Com_alter_table, Com_analyze, etc.;
- Connections;
- Created_tmp_disk_tables, Created_tmp_files, Created_tmp_tables;
- Delayed_errors, Delayed_insert_threads, Delayed_writes;
- Flush_commands;
- Handler_commit, Handler_delete, Handler_discover, Handler_read_first, etc.;
- Key_blocks_not_flushed, Key_blocks_unused, Key_blocks_used, etc.;
- Max_used_connections;
- Not_flushed_delayed_rows;
- Handler_commit, Handler_delete, Handler_discover, Handler_read_first, etc.;
- Key_blocks_not_flushed, Key_blocks_unused, Key_blocks_used, etc.;
- Max_used_connections;
- Not_flushed_delayed_rows;
- Open_files, Open_streams, Open_tables, Opened_tables;
- Qcache_free_blocks, Qcache_free_memory, Qcache_hits, etc.;
- Questions, Rpl_status;
- Select_full_join, Select_full_range_join, Select_range, Select_range_check, etc.;
- Slave_open_temp_tables, Slave_retried_transactions, Slave_running;
- Slow_launch_threads, Slow_queries;
- Sort_merge_passes, Sort_range, Sort_rows, Sort_scan;
- Table_locks_immediate, Table_locks_waited;
- Threads_cached, Threads_connected, Threads_created, Threads_running;
- Uptime;

- Desenvolvimento de agentes customizados.

POSTGRES:

- autovac_freeze;
- backends;
- bloat;
- checkpoint;
- connection;
- custom_query;
- database_size;
- dbstats;
- fetch;
- disk_space;
- fsm_pages / fsm_relations;
- relation_size;
- index_size;
- last_vacuum;
- last_autovacuum;
- last_analyze;
- last_autoanalyze;
- listener;
- locks;
- logfile;
- query_runtime;
- query_time;
- sequence;
- replicate_row;
- txn_time;
- txn_idle;
- settings_checksum;
- timesync;
- wal_files;

SYBASE:

- Availability;
- Number of Transactions;
- Number of Transactions per Minute;
- Number of User Tables;
- Number of User Tables per Minute;
- Number of Active Locks;
- Number of Active Page Locks;
- Number of Active Table Locks;
- Number of Servers;
- Number of Active Users;
- Number of Local Transactions;
- Number of Local Transactions per Minute;
- Number of External Transactions;
- Number of External Transactions per Minute;
- Instance Used Space;
- Instance Free Space;
- Instance Total Space;
- Up Time;
- Number of Indexes;

- Number of Tx Logs;
- Deadlocks;
- Avg Lock Contention;
- TDS Packets Sent;
- TDS Packets Received;
- Total Cache Misses Ratio;
- Total Cache Hits Ratio.

Access, Interbase, Informix, Progress:

- Conexão com banco e execução de qualquer query/select/SQL.

MONITORAMENTO DE SISTEMAS OPERACIONAIS

- Windows XP, 7, 8 ou superior e seus Services Packs;
- Windows 2008, 2012 ou superior e seus Services Packs;
- VMWare e Services Packs.

MONITORAMENTO DE SERVIDORES

Servidores Microsoft:

- CPU (porcentagem de uso, tempo de processamento privilegiado, filas de instruções no processador);
- Memória física e virtual utilizada;
- Serviços (in)ativos;
- Processos (in)ativos;
- Espaço em disco;
- Tempo de Uptime e detecção de “reboots”;
- I/O (DiskQueue, Disk Time, Disk Write, Disk Read, etc., geral ou por disco físico);
- Análise de entradas específicas de log no “Event Viewer”;
- Qualquer item disponível no “Performance Monitor”;
- Identificação dos processos responsáveis pelo consumo em cada recurso dentro dos percentuais de memória física, virtual e CPU.

Servidores Web:

Métricas com execução em ambiente de Balanceamento de Carga (Load Balance):

- Microsoft IIS 5 e superior;
- Apache Coyote/Tomcat 3.x ou superior;
- Métricas de FTP:
 - Número de bytes recebidos e enviados pelo serviço de FTP;
 - Total de arquivos transferidos pelo serviço de FTP.
- Métricas de Web Service:
 - Total de hits de um determinado domínio;
 - Percentual de page hits;
 - Taxa de bytes recebidos e enviados por segundo no Web Service;
 - Acessos anônimos, não anônimos e número máximo de usuários que estabeleceram conexões anônimas usando Web Service;
 - Conexões;
 - Tipos de método HTTP;
 - Erros HTTP.
- Microsoft COM+;
- Tomcat 3.x ou superior;

- .NET Framework;

AS/400:

- CPU e DB CPU;
- Login;
- User Messages;
- Outq Files, Writer & Status;
- Storage;
- Subsystems;
- Active & Running Jobs;
- Qualquer métrica provida por SNMP ou emulação de terminal.

HP-UX, AIX, SUN SOLARIS, UNIX TRU64, LINUX (todas as distribuições):

- Load e uso de CPU (sys, wait, idle);
- Memória física e virtual disponível e utilizada;
- Espaço livre/utilizado nos mountpoints;
- I/O de disco;
- Swap;
- Uptime;
- Número mínimo/máximo de processos;
- Tempo máximo de execução de processos;
- Detecção de processos zombies ou defunct;
- Tamanho virtual dos processos;
- Cotas de usuários;
- Análise de logs, buscando ocorrências específicas de erro;
- Tempo de uptime e detecção de reboots;
- Restart de serviços, em caso de queda;
- Agentes customizáveis para necessidades específicas de infraestrutura ou de processos de negócio;
- Identificação dos recursos consumidos para cada processo;
- Nos percentuais de memória física, virtual e CPU, a solução deve permitir a identificação dos processos responsáveis pelo consumo em cada recurso citado.

Novell:

- Abended-Threads;
- Buffer-Counts;
- CPU-Load-15min;
- DS-DB;
- Dirty-Buffers;
- LRU-Sitting-Time;
- Licensed-Connections;
- Logins;
- Long-Term-Cache-Hits;
- NLMs Loaded;
- Open-Files;
- Pct-Max-Used-Pckt-Rcv-Buff;
- Pct-Non-Purgable-VOLs;
- Pct-Purgable-VOLs;
- Used-Pckt-Rcv-Buff;
- VOLs utilization.

Mainframe Unisys:

- Monitoração de indicadores do sistema operacional OS2200, no ambiente Unisys DORADO 380, através de SNMP (UNISYS.MIB, VISINET.MIB, UNISYS-TIMEPLEX.MIB, etc.) e da utilização de softwares de emulação de terminais para a execução de comandos e tratamento das informações obtidas;
- Monitoração do banco de dados Unisys RDMS via emulação de terminais ou por acesso ODBC/JDBC.

Mainframe IBM:

- Monitoração de indicadores do sistema operacional através de SNMP, e da utilização de softwares de emulação de terminais para a execução de comandos e tratamento das informações obtidas.

MONITORAMENTO DE APLICAÇÕES

Monitora qualquer tipo de aplicação e seus componentes desde que seja possível ter acesso à informação. Alguns exemplos:

Java Virtual Machine:

- Java Virtual Machine;
- Garbage Collector;
- Threads;
- Memory;
- CPU;
- Uptime.

Websphere:

- JVM;
- System Metrics;
- Transaction Service;
- JDBC Provider;
- Thread Pool;
- EJB Module;
- StatelessSessionBean / StatefulSessionBean / MessageDrivenBean;
- Session Manager;
- Web Module;
- Servlet / JSP.

Weblogic:

- EJBModule;
- ThreadPool;
- JDBC Connection;
- JVM;
- Servlet.

IBOSS:

- Connection Pool;
- JMS;

- EJB.

TomCat:

- Thread Pool;
- Requests;
- Servlets;
- Web Modules.

Monitoração COM+:

- Métricas de consumo de recursos dos componentes;
- E-mail.

MONITORAMENTO DE E-MAIL

- Roteamento de mensagens:
 - Total de mensagens enviadas;
 - Total de mensagens web não enviadas;
 - Total de mensagens enfileiradas aguardando tratamento.
- Utilização do servidor:
 - Número de sessões ativas;
 - Número de sessões “interrompidas”;
 - Número de tarefas em execução.
- Disponibilidade:
 - Percentual de tempo que a aplicação esteve disponível;
 - Número de mensagens não enviadas (“dead mail”);
 - Número de requisições aguardando replicação.
- Desempenho:
 - Replicações completadas, aguardando replicação e falhas de replicação.
- Monitoração e análise de aplicações J2EE e .NET:
 - Representação gráfica, em tempo real, dos componentes com detalhamento do desempenho;
 - Possibilidade de selecionar aplicação ou servidor desejado e desabilitar visualização de outros servidores durante a execução;
 - Monitoramento, em tempo real, das aplicações dos usuários, incluindo os componentes que estão sendo executados;
 - Visão gráfica das informações sobre componentes executados dentro do servidor de aplicação J2EE ou .NET e os comandos SQL invocados por estes:
 - Nomes dos componentes e seus métodos, ou comandos SQL, sendo executados;
 - Tempo total de execução destes;
 - Percentual de utilização de CPU destas execuções;
 - Número de execuções de cada método ou comando SQL.

Microsoft Exchange (objetos de contadores):

- DSAccess Domain Controllers
- DSAccess Caches
- ActiveSync Notify
- Address List
- Sender ID
- Intelligent Message Filter
- OleDB Events
- OleDB Resource
- Transport Store Driver

- Transport Filter Sink
- MTA
- MTA Connections
- ISIS Transport Driver
- IS Public
- IS Mailbox
- ES
- SA – NSPI Proxy
- SRS
- OMA

Servidor QMAIL/POSTFIX:

- Availability
- Messages In Queue
- Messages Awaiting Preprocessing
- Process Resident Memory Size
- Process CPU Usage
- SMTP Availability
- SMTP Inbound Connections
- POP3 Availability
- POP3 Inbound Connections

MONITORAMENTO DE VIRTUALIZAÇÃO

- Gerenciamento de todos os níveis em um ambiente virtual. Uma visão única exibe todos os dados relevantes de sua estrutura de toda a rede com integração entre infraestrutura física e virtual;
- Monitoramento de VMware, Xen, KVM RHEL e mais;
- Define as expectativas de nível de serviço com limites preditivos;
- Monitora serviços e aplicações rodando em servidores virtuais;
- Análise de causa raiz, o que significa reduzir tempo de reparação e serviço de interrupções;
- A integração perfeita entre o monitoramento de infraestrutura física e virtual;
- Identifica gargalos de desempenho relacionados com armazenamento afetam os usuários finais;
- Relatórios e visualização de dados;
- Abordagem dinâmica para o planejamento de atualizações;
- Planejamento de capacidade proativa;
- KVM: planejamento de capacidade de KVM através de provisionamento adequado de uso de recursos como: armazenamento, CPU e memória. Estes três componentes permitem uma forma dinâmica para planejar proativamente atualizações de uma organização de uma forma eficaz.
- VMware vSphere: monitoramento, mapas, métricas e visualização das plataformas VMware e os aplicativos em execução no hypervisors fornecendo visibilidade de ponta a ponta, desde saúde e desempenho até a disponibilidade. Os alertas, a solução de problemas e as automações simplificam diariamente as operações de TI e todas as informações do seu VMware são exibido em uma visão unificada.
- Citrix Xen: monitoramento recursos para o Citrix Xen hypervisor, Xen infraestrutura virtual de lado físico, ambiente virtual e em nuvem através de uma visão unificada.

MONITORAMENTO SAP

- Monitoramento realizado através da conexão ao CCMS (Computing Center Management System) via interface RFC SDK da SAP disponível em <http://service.sap.com>;
- O OpMon possui uma vasta biblioteca de KPIs de monitoração da plataforma SAP, além de permitir a customização de itens a serem monitorados;

- A customização retorna quaisquer tabelas de valores críticas ao negócio;
- Os valores utilizados para warning e critical são configurados diretamente no SAP e o OpMon realiza a leitura destes dados;
- A exibição de KPIs de negócio, obtidas diretamente do ERP, permite a construção de dashboards de negócios com uma visão em tempo real na plataforma OpMon;
- Desenvolvimento de funções ABAP customizadas, que retornam quaisquer tabelas de valores críticas ao negócio:
 - Dialog Response Time;
 - GUI Callback time;
 - Dialog Front End Net Time;
 - Load Gen Time;
 - Monitoring Time;
 - DB Request Time;
 - Função ABAP Rstoque mínimo;
 - Background Aborted Jobs;
 - Backup Archiving Last Succeed;
 - Buffers Table Definition Net Radio;
 - Client 100 Response Time;
 - Gateway Reader;
 - Gateway Clients;
 - OpSys CPUS;
 - Oracle Tablespace PSAPSTABI;
 - Roll MEM Heap Peak;
 - Spool QUEUE Lenght.

MONITORAMENTO ERP DATA SUL

- Servidores e execuções RPW;
- Trans Log e Agents Busy;
- Simulações dos itens do Datasul Web Access;
- Entre outros itens customizáveis do banco de dados ou de processos de negócio.

MONITORAMENTO BAAN

- Desenvolvimento de agentes customizados.

MONITORAMENTO SPB – Sistema de Pagamentos Brasileiro (MQSeries)

- Monitoração das filas entre servidores;
- Monitoração das dead queues.

MONITORAMENTO CCMS

- Operating;
- System (CPU, I/O, Pages/Sec, etc.);
- Background (Aborted Jobs, Number Of WpBTC, etc.);
- Dialog times (DBReqTime, FrontEndRespTime, LoadGenTime, QueueTime, etc.);
- Spool (% de utilização, jobs, etc.);
- Oracle (Buffers, Segments, Tablespaces, Messages, Profile Parameters, etc.);
- Buffers (TableDenifition-DirUsed, TableDefinition-HitRatio, etc.);
- Gateway Reader (GatewayClients, GatewayConnections, etc.);

- Backup (LastBrArchiveRun, LastBackupRun, etc.);
- SM-50 (tempos de resposta), PerfU1 e PerfU2 (tempos de resposta);
- Roll-Mem-Mgmt (dados gerenciamento de memória);
- Qualquer item da CCMS;
- Sem a necessidade de instalação de client específico.

MONITORAMENTO FTP – SIMULADORES DE TRANSAÇÃO

- Efetua as transações como se fosse um usuário FTP, fornecendo tempos de resposta e retorno sobre falha ou sucesso na conclusão do processo;
- Número de bytes recebidos e enviados pelo serviço FTP;
- Total de arquivos transferidos pelo serviço FTP.

MONITORAMENTO DO TRÁFEGO DE REDE

- Suporte ao protocolo NetFLOW 5;
- TOP traffic utilization Dashboard;
- Drill down de diferentes combinações dos campos de NetFLOW e Probes;
- Alertas e relatórios em tempo real;
- Integração completa com o OpMon para alarmes e capacity planning;
- Integração com o OpMon para customização de alertas e relatórios via interface;
- Identificação automática de portas conhecidas através da RFC 6335 (acessível em iana.org);
- Inclusão e customização de novas portas fora do padrão de reconhecimento automático;
- Disponibilização de API para gerar relatórios customizados através de outras ferramentas;
- Dashboard automático com os maiores utilizadores de tráfego por **IP de origem**;
- Dashboard automático com os maiores utilizadores de tráfego por **IP de destino**;
- Dashboard automático com os maiores utilizadores de tráfego por **protocolos de aplicação**;
- Dashboard automático com os maiores utilizadores de tráfego por **protocolos de rede**;
- Combinação de filtros no dashboard de monitoramento de rede:
 - Protocolo de aplicação;
 - Endereço IP.
 - Sonda/Coletor de tráfego de rede;
 - Período de tempo;
 - Protocolo de rede.
- Dashboard de protocolos de rede detalhado;
- Dashboard de protocolos de aplicação detalhado;
- Dashboard de endereços IP de origem detalhado;
- Dashboard de endereços IP de destino detalhado;
- **Monitoração ilimitada de sondas ou probes**;
- Armazenamento **ilimitado** de histórico de dados de tráfego;
- Tecnologias suportadas:
 - Ethernet, Fast Ethernet, Gigabit Ethernet, Wireless
 - MPLS, X25, Frame Relay (RFC1490), PPP, Cisco HDLC
 - PPP, TCP/IP, TCP/IP v6, NetBios
- Links:
 - Checagem de tempo de latência e perda de pacotes, possibilitando % de disponibilidade mensal
 - Gráficos de utilização quantitativa e qualitativa
 - Módulo de coleta de tráfego de rede LAN e WAN, identificando tipos de protocolos que trafegam e a que aplicativos pertencem
 - Coleta de informações sem que o processo cause indisponibilidade ou interrupção nos links Wans ou na rede local

- Internet:
 - Checagem dos sites mais acessados internamente, via proxy e diretamente
 - Checagem dos sites corporativos, a partir do site externo do cliente ou da OpServices (opcional)
 - Checagem do tráfego de e-mails, garantido que o ciclo SMTP/POP esteja operando adequadamente
- Portas:
 - SMTP, POP3, HTTP, SNMP, etc. e seu tempo de resposta
 - Monitoração de portas indevidamente abertas
- SMNP:
 - Para roteadores, switches e appliances de rede, como wireless
 - Detecção de quedas de interfaces
 - % de utilização de interfaces, % erros in/out, % de pacotes descartados in/out
 - Qualquer item disponível nas MIBs standard e ambientais, como % de load do processador, temperatura do dispositivo, velocidade do cooler, etc.
- Simuladores de transações:
 - Logins em portais e sistemas web, efetuando as transações como se fosse um usuário comum, fornecendo os tempos de resposta e apontando falha/sucesso na conclusão do processo;
 - Tempos de processamento das aplicações, mostrando o tempo utilizado no processamento de usuário (cliente), rede de comunicação e servidor. Ajuda a identificar a origem de eventual problema de desempenho.

CONTROLE DE VERSIONAMENTO DE ARQUIVOS

- Controle de versionamento de arquivos para sistema operacional Windows;
- Especificação da listagem de arquivos que deverão ter o conteúdo monitorado;
- Armazenamento de arquivo toda vez o monitoramento apresentar quaisquer mudanças em seu conteúdo;
- Disponibilização de todas as versões armazenadas dos arquivos para download;
- Ferramenta de comparação gráfica das versões dos arquivos com indicação das diferenças entre duas versões selecionadas.

BACKUP AUTOMÁTICO DE SWITCHES OU ROTEADORES

- Recurso para acessar facilmente a configuração de um roteador ou verificar log de alterações realizadas (data, usuário e configuração modificada);
- A realização do backup possibilita aumento de produtividade, principalmente das empresas que precisam administrar uma quantidade grande deste tipo de equipamentos.

AGENTES

- Os agentes utilizados pelo OpMon não consomem mais que 0,5% de uso de processador, 15,0 MB de espaço em disco e 4,0 MB de memória do sistema operacional;
- O OpMon possui recurso de monitoração de seus agentes quando estes forem utilizados a fim de garantir a sua operacionalidade.

MONITORAMENTO CONFORME DESVIO DO COMPORTAMENTO PADRÃO

Criação automática de linhas de base ou “baselines”, a partir da análise dos dados coletados e padrões de comportamento, de modo a estabelecer uma linha de base que represente o comportamento normal e esperado, ao longo do período de amostragem, do ambiente de TI, a fim de permitir a identificação automática e em tempo real de mudanças no comportamento de um componente em relação ao valor basal (linha de base);

- Criação automática de linhas de base ou “baselines”, a partir da análise dos dados coletados e padrões de comportamento, de modo a estabelecer uma linha de base que represente o comportamento normal e esperado, ao longo do período de amostragem, do ambiente de TI, a fim de permitir a identificação automática e em tempo real de mudanças no comportamento de um componente em relação ao valor basal (linha de base);
- Período de amostragem das linhas de base configurável por IC (semana, mês, ano), podendo ser aferida a sazonalidade de um serviço sendo monitorado.
 - Ex: no monitoramento de transações bancárias pode ser necessário identificar através do baseline um comportamento diferente nos inícios de cada mês (volume maior de transações);
- Frequência de amostragem das linhas de base configurável por IC (a partir de 5 minutos);
- Notificações automáticas aos responsáveis para detecção de comportamentos anômalos mesmo que não tenha se configurado thresholds.

EVENTOS E ALARMES

- Monitoramento da disponibilidade, capacidade, performance e diversas métricas do ambiente de TI a partir das coletas de informação por:
 - SNMP;
 - WMI;
 - Agentes do próprio sistema;
 - Agentes de outras fontes;
 - Consultas em bases de dados;
 - Desenvolvimento de subagentes customizados.
- Em caso de alerta em um IC, os ICs hierarquicamente dependentes não gerarão alertas;
- Escalamento (crescente hierarquicamente) de incidentes a partir de prazos pré-determinados para a resolução de problemas. O escalonamento pode ser configurado por pessoa, equipe, ou nível de suporte e poderá “subir” de nível de acordo com a não resolução do problema ou identificação de gravidade;
- As notificações, eventos e alertas configurados a partir das regras da operação podem ser pelos seguintes meios:
 - E-mail (correio eletrônico)
 - SMS (através de modem GSM ou via gateway);
 - Interface com sistemas de Help Desk/Service Desk;
 - Mensagens instantâneas.
- Integração com softwares de gerenciamento de hardwares específicos (exemplo: Dell DRAC, HP iLO) para alertar pontos específicos de falha;
- Diferenciação entre indisponibilidade física do hardware ou falha de comunicação entre o agente e o sistema operacional;
- Alertas/alarmes a partir da detecção de mudanças na configuração de ICs:
 - Visualização do momento real do acontecimento de um comportamento anormal a partir da seleção de período em uma linha do tempo, trazendo indicadores de performance e histórico em tempo real;
 - Coleta de dados históricos otimizada para garantir alta escalabilidade e preservação do consumo de banda através da não utilização de operações em polling.

- Criação de condições para gerar alarmes quando da detecção de palavras ou padrões, pré estabelecidos em logs do tipo Syslog ou Windows Event Log.

ANÁLISE DE IMPACTO

Capacidade de análise do impacto de eventos, mostrando quais serviços de infraestrutura, serviços de TI, unidades e usuários dependentes do IC foram impactados.

RELATÓRIOS E APRESENTAÇÃO DOS DADOS

- A apresentação dos dados e os relatórios podem ser definidos de acordo com os intervalos de tempo: (1) totais: a partir de todo o período de registro; (2) pré-definidos: anuais, mensais, semanais e diários e (3) arbitrários: especificados pelo usuário entre qualquer ponto dos registros existentes.
- Recurso de customização de relatórios para medir quaisquer recursos gerenciados;
- Configuração de thresholds para visualização de indicadores de nível de serviços contratados;
- Agendamento de relatórios em períodos recorrentes e envio automático por e-mail para um ou múltiplos destinatários;
- Mecanismo de “drill-down” para explorar diferentes níveis de detalhamento das informações coletadas a partir de um relatório consolidado;
- Classificação e ordenação de dados e resultados para geração dos relatórios;
- Apresentação dentro de períodos analisados de valores mínimos, médios e máximos;
- Relatórios de disponibilidade dos elementos gerenciados com indicadores de MTTF, MTTR, e MTBF/MTBSI;
- Relatórios de disponibilidade com recurso de exclusão de períodos parada agendada e filtro “95th percentile”;
- Relatório de capacidade dos indicadores gerenciados com gráficos das suas performances;
- Ferramenta de zoom em séries de dados escolhida;
- Relatórios de disponibilidade e capacidade com opções de 24x7, 8x5 ou período customizável;
- Recurso de exportar relatórios em formato PDF, XML ou imagem (possibilitando sua inserção em outros documentos);
- Relatórios de SLM (Gerenciamento do Nível de Serviço), com visualização de nível de serviço definido, alcançado e cálculo de desvio;
- Relatórios de sumário de alertas com filtro por tipo de eventos, IC, conjuntos de IC e seleção de intervalos de tempo para o acompanhamento, por exemplo, dos maiores geradores de alertas do ambiente;
- Relatório de projeção futura para planejamento baseado no seu comportamento histórico;
- Customização de relatórios através de integração o software construtor de relatórios Jasper Reports via interface da solução e com recurso de importação de relatórios construídos na ferramenta.

DASHBOARDS (PAINÉIS VISUAIS)

- Recursos para a construção, edição e visualização de dashboards (painéis visuais) para a centralização de informações importantes através de combinação de um ou mais indicadores ou gráficos;
- Atualização automática do status, em tempo real ou de acordo com o tempo de checagem configurado, de cada um dos itens monitorados;
- Exemplos de componentes editáveis: gráficos do tipo linha, área, barra e disco; containers (podendo representar estados agrupados de um conjunto de IC da infraestrutura); área de texto,

- permitindo customizar, escolher e representar em tempo real os últimos valores coletados dos itens monitorados; mostradores (relógio e similares) e elementos do tipo gauges;
- Os componentes da construção de dashboards deverão exibir dados a partir da associação com itens gerenciados na solução de monitoramento e também dados de fontes externas através de integração com webservices;
 - Recurso para apresentação de dados agrupados de um ou mais itens gerenciados nos componentes a partir do OpMon ou de fontes de dados externos;
 - Recurso para criação de links de compartilhamento para visualização de dashboards nos navegadores Google Chrome, Mozilla Firefox e Internet Explorer sem a necessidade de realizar o Login dentro da plataforma;
 - Recurso para criação automática de código do tipo “embeded” podendo inserir o código gerado em outras ferramentas, sites ou intranet sem a necessidade de realizar o Login dentro da plataforma;
 - Recurso para selecionar os níveis de usuários que visualizarão o dashboard (ou disponível a todos);
 - Recurso para importação de imagens para utilização das mesmas como componentes dos dashboards e com possibilidade de associação de elementos a ela para sensibilização de estado do item monitorado;
 - Recurso de importação de imagens para utilização como plano de fundo dos dashboards
 - Recurso para modificação de imagens importados como planos de fundo dos dashboards como estender, repetir, preencher, transparência, entre outros;
 - Recurso de slide-show com seleção de telas, seleção de efeitos e tempo de transição automática entre as telas selecionadas para apresentação;
 - Interface ilimitada para a criação e definição de novos indicadores.

MONITORAÇÃO DA PERCEPÇÃO DO USUÁRIO

- Ferramenta para a criação e edição de robôs que simulam a experiência de usuários através da execução de rotinas análogas às dos usuários, a fim de medir seu tempo de resposta, a taxa de sucesso/falha das rotinas, identificação de erros e bugs em aplicações, dentre outras a serem customizadas dentro do módulo;
- Verificação/simulação dos seguintes itens: velocidade, correção de cada etapa, disponibilidade de links e serviços, situações em que erros ocorrem, real dimensão do problema, impacto, identificação de causa raiz de um problema de desempenho;
- Os robôs podem ser de três tipos: (1) web puros (GETs/POSTs); (2) web híbridos e (3) pixel a pixel (Terminal Services);
- Os robôs podem ser executados de forma local, remota (dentro da rede do cliente) ou externamente (servidores web);
- Exemplos de simulações com tempo de resposta e taxa de falha/sucesso: transações web, acessos a áreas restritas, caminho de um usuário para executar rotinas, testes de software, emissão de nota fiscal eletrônica, emissão de segundas-vias de boletos, entre outras;
- Integração com outros sistemas de monitoramento para envio das informações coletadas como Zabbix e Nagios, por exemplo;
- Rotinas de simulação a partir de: reconhecimento de imagens, clique, inserção de texto e execução de atalhos de teclado;
- Criação de ciclos de repetições de rotinas, onde uma rotina é testada após a execução da anterior;
- Clonagem de rotinas para reaproveitamento através de pequenas alterações;
- Backup de rotinas.

DOCUMENTAÇÃO DOS ITENS DE CONFIGURAÇÃO

- Repositório de documentações para todos os ICs e AICs;

- Elementos disponíveis para a documentação dos ICS e serviços:
 - Imagens (PNG, JPG, etc.);
 - URL;
 - Documentos (Word, PDF, etc.);
 - Dados de cadastro físico dos elementos;
 - Dados específicos para links de dados;
 - Dados de contato para fins de suporte/manutenção.
- Recurso para colocar prazos de expiração na documentação, o que permite garantir alertas para caso um analista cadastre um ação na documentação do dispositivo e não resolva o problema;
- Possibilidades de inserção de “flags” em documentações completas e incompletas para alimentação de gerência de continuidade.

CORRELACIONADOR DE EVENTOS

- Ferramenta para correlação de eventos através da automação e otimização de operações de TI;
- O módulo de correlação de eventos do OpMon provê uma interface gráfica com conectores drag-and-drop para a criação de regras para realizar processos automatizados, a partir dos eventos de TI;
- Os algoritmos de correlação possibilitam identificar, categorizar, filtrar e reduzir os volumes elevados de eventos de infraestrutura e aplicações em alertas acionáveis;
- Não necessita de programação para gerar as correlações;
- Lista de recursos disponíveis para a **criação de regras e configuração de alarmes**:
 1. **Pares de eventos**: criação de regras para eventos onde se espera que ocorram em pares. Exemplo: um evento deve ocorrer junto com outro e caso não ocorra pode ser configurado um alarme para uma ação responsiva ou preditiva;
 2. **Sequência de eventos**: criação de regras para identificação de uma ordem ou sequencia específica de eventos. Possibilita a identificar problemas ou padrões a partir de eventos que em uma ordem específica têm significado dentro da infraestrutura;
 3. **Combinação de eventos**: criação de regras para o acontecimento de alguns eventos específicos sem a necessidade de que ocorram em uma ordem específica;
 4. **Taxa de eventos**: criação de regras para quando a ocorrência de um evento se repetir dentro de um período específico de tempo;
 5. **Condiciona**: criação de regras para quando uma condição específica (e/ou mais de uma) for satisfeita. Caso um evento ocorra, outro evento deve acontecer.
- Outros eventos podem ocorrer paralelamente aos programados sem alterar a regra de pares de eventos, sequencia de eventos, combinação de eventos, taxa de eventos e condicional.

GERENCIADOR DE TRAPS SNMP

- Repositório central de SNMP-TRAPS gerados por qualquer sistema que envie traps no formato SNMP;
- Configuração de alarmes baseados em conteúdos de SNMP-TRAPS recebidos ou gerados;
- Correlação de TRAPS;
- Armazenamento em tabelas de banco de dados da aplicação principal de todas as mensagens geradas;
- Armazenamento de todas as SNMP-TRAPS recebidas;
- Consulta a todas as SNMP-TRAPS geradas, a qualquer momento.

GERENCIADOR DE LOGS

- Repositório central de logs gerados por diferentes sistemas e plataformas, como, por exemplo:
 - Solaris;

- AIX;
- Cisco;
- Linux;
- Windows;
- HP-UX.
- Armazenamento em banco de dados da aplicação principal de todas as mensagens geradas nestes sistemas;
- Consultas e mensagens de erros geradas pelas plataformas com o conteúdo completo delas;
- Configuração de alarmes baseados em conteúdos de LOGS (mensagens recebidas pelos sistemas);
- Correlação de LOGS.



RESUMO DAS PRINCIPAIS FUNCIONALIDADES
Gráficos e monitoração em tempo real
Não utiliza dados sumarizados para garantir dados e históricos reais
Alta performance e escalabilidade para gerenciamento
Interface multi-linguagem
Gerenciamento de disponibilidade (SLA/ANS) e nível de serviço (SLM/GNS)
Console gráfica para configuração e documentação
Topologia de redes
Ativação de estado de manutenção
Checagens de monitoração ativas e passivas e escala de notificações
Análise de impacto
Catálogo de Serviços
Níveis de dependência/parentesco de serviços e hosts
Monitoração com linhas de tendências (trendlines)
Gerenciamento de capacidade (CP/capacity planning) com previsão de esgotamento
Alarmes a partir de linhas de base (baseline)
Alertas via SMS e E-mail
Agendamento e envio automático de relatórios por e-mail
Relatório de sumário de alertas, desempenho, disponibilidade, impacto estrutural e financeiro
Dashboards (editáveis) que apresentam toda a informação relevante em uma única tela
Ferramenta intuitiva para desenho/customização de dashboards
Visualizador de dashboards para dispositivos móveis
Repositório de Logs e SNMP Traps
Monitoração qualitativa do tráfego de redes via Netflow
Correlação de eventos através de interface gráfica (drag-and-drop)
Compatibilidade com biblioteca de plugins e extensões do Nagios Exchange

REQUISITOS PARA INSTALAÇÃO E CONFIGURAÇÃO DO OPMON

A informação abaixo é destinada a fornecer orientações gerais sobre os requisitos de hardware necessários para executar o OpMon. À medida que cada cliente difere em infraestrutura, os requisitos de hardware para monitoramento também podem variar.

A tabela abaixo usa uma recomendação baseado na proporção de device por serviços estimada em 1:10, ou seja, para cada device monitorado temos até 10 serviços para este dispositivo, obedecendo um intervalo de checagem de 5 minutos em cada serviço monitorado.

O cliente disponibilizará um (1) servidor físico ou virtual atendendo os requisitos mínimos aceitáveis para instalação do OpMon, conforme abaixo:

Devices Monitorados	Serviços Monitorados	Disco Rígido	Processador	Memória
Até 100	1000	300 GB	1 a 2 Dual Core 2 GHz	2 a 4 GB
De 101 a 200	2000	500 GB	1 a 2 Quad Core 2 GHz	4 a 8 GB
De 201 a 300	3000	1 TB	1 a 2 Xeon Six Core 2 GHz	8 a 16 GB

Observações:

- É importante considerar que estas especificações foram estabelecidas para equipamentos físicos. O uso de máquinas virtuais causa degradação de performance quando - no mesmo host - outras máquinas virtuais também são hospedadas, consumindo recursos compartilhados (como processador, memória e disco), invalidando estas especificações;
- Por causa dos recursos de hardware compartilhados as máquinas virtuais podem não ser capazes de atender às necessidades de grandes ambientes de hardware mesmo com melhorias de desempenho, assim recomendamos a instalação em um servidor físico em detrimento a uma máquina virtual;
- Para instalações com monitoração acima de 300 devices ou 3000 serviços, ou havendo a necessidade de atividades não contempladas, realizamos um anteprojeto;
- Os requisitos acima são os considerados mínimos, podendo haver necessidade de incremento caso exista necessidade de aumentar o desempenho do sistema.