



FlexVision EventsManager

DESAFIO

Enormes volumes de eventos de sistemas que são gerados diariamente, são uma valiosa fonte de informações para os administradores de redes.

Estas informações ajuda os administradores a fazer mudanças nos ambientes, tomar ações administrativas e identificar erros nos sistemas. Isto é entretanto, uma tarefa quase impossível sem ferramentas apropriadas.

Em uma grande rede você precisa de uma solução que permita a monitorar, gerenciar e arquivar os milhares de eventos que são gerados pelos dispositivos e aplicações.

SOLUÇÃO

FlexVision EventsManager é uma módulo que monitora, gerencia e arquiva um grande número de tipos de eventos como Windows Event Log, Syslogs e traps SNMPs que são gerados por firewalls, roteadores, servidores, etc.

Permite receber estes eventos, transformá-los em alarmes (se necessário) e armazená-los de forma centralizada para análise.

BENEFÍCIOS

- Centraliza Syslog, eventos Windows e traps SNMP gerados por firewalls, servidores, roteadores, switches, telefones IP, etc.
- Incrementa o uptime da rede e notifica problemas através de alertas em real-time
- Rápida implementação e gerenciamento na rede
- Capacidade de receber grandes volumes de eventos

Características

Log de eventos centralizado:

Logs de eventos são constantemente e automaticamente gerados pelo usuário ou por processos automatizados e estes logs são armazenados em diferentes locais. FlexVision EventsManager armazena todos os eventos de logs recebidos e capturados em um único local, ou seja, no próprio FlexVision.

Automaticamente estes eventos são correlacionados aos dispositivos/aplicações cadastrados no FlexVision, tendo assim um console geral e um console específico para cada elemento.

Análise de logs:

Como administrador de redes, você passa pela experiência de examinar enormes logs, o que faz deste trabalho um complexo processo. FlexVision EventsManager proporciona a facilidade de consulta destes logs de maneira centralizada, recebendo e capturando os dados das várias origens que estes partem na rede.

FlexVision EventManager inclui recebimento e capturas dos logs:

- Windows Event Log;
- Syslogs;
- Traps SNMP;
- Oracle Alert Log;
- MSSQL Error Log;
- Captura de logs armazenados em arquivos nos servidores em real-time.

Detalhamento e controle de eventos:

FlexVision EventsManager ajuda você a monitorar uma gama de sistemas e dispositivos através de uma interface centralizada dos mais variados tipos de logs, incluindo eventos de Windows, Syslog, Trap SNMP, MSSQL ErrorLog, Oracle AlertLog dentre outros gerados pelos recursos existentes no ambiente operacional.

Administradores poderão ter informações de diversos tipos de eventos a partir de servidores Windows e dispositivos diversos, podendo associá-los à base de conhecimento do FlexVision, ajudando assim na tomada de decisões e também no auxílio da equipe de suporte a efetuar procedimentos mediante um evento ocorrido.

Ajudando você manter a vantagem

FlexVision Professional Services ajuda sua empresa a manter a vantagem competitiva por uma suite de serviços que incluem consultoria, instalação, implementação, configuração e customização. FlexVision Professional Services oferece subsídios para assegurar disponibilidade das aplicações de negócios críticas, maximizar o potencial do produto, reduzir o risco do projeto, entregar valor agregado para seu negócio e melhorar sua operação. Para mais informações, visite o site <http://www.flexvision.com.br>.

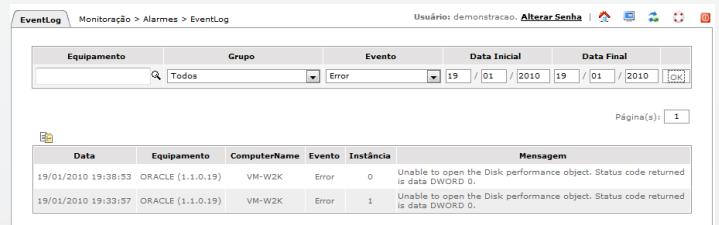
Suporte a novos dispositivos:

Gerenciar traps SNMP requer habilidade para entender a "linguagem" de cada fabricante que confecciona suas mibs (Manage Information Base) para definir os eventos que ocorrerão em seus equipamentos.

FlexVision EventsManager possui uma base de dados de traps SNMP para os principais fabricantes do mercado e também é capaz de importar MIBs de qualquer fabricante possibilitando assim editá-las e até traduzir os traps importados.

Conclusão

De uma forma inteligente e eficiente, FlexVision EventsManager centraliza e armazena todos os eventos do ambiente operacional. Se integra à base de conhecimento do FlexVision facilitando a operação do dia a dia.



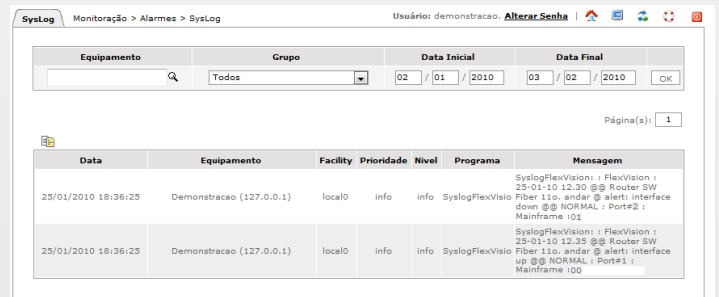
EventLog

Equipamento	Grupo	Evento	Data Inicial	Data Final
Equipamento: Todos				
Evento: Error				
Data Inicial: 19 / 01 / 2010				
Data Final: 19 / 01 / 2010				

Página(s): 1

Data	Equipamento	ComputerName	Evento	Instância	Mensagem
19/01/2010 19:38:53	ORACLE (1.1.0.19)	VM-W2K	Error	0	Unable to open the Disk performance object. Status code returned is data DWORD 0.
19/01/2010 19:33:57	ORACLE (1.1.0.19)	VM-W2K	Error	1	Unable to open the Disk performance object. Status code returned is data DWORD 0.

Consulta de Windows Event Log.



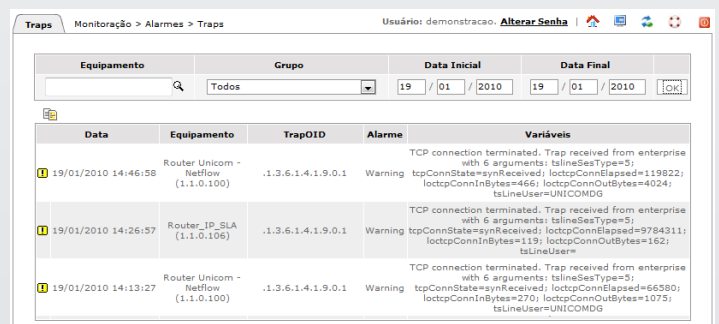
Syslog

Equipamento	Grupo	Data Inicial	Data Final
Equipamento: Todos			
Data Inicial: 02 / 01 / 2010			
Data Final: 03 / 02 / 2010			

Página(s): 1

Data	Equipamento	Facility	Prioridade	Nível	Programa	Mensagem
25/01/2010 18:36:25	Demonstracao (127.0.0.1)	local0	info	info	SyslogFlexVisio	SyslogFlexVisio : FlexVision : 25-01-10 12.30 @ Router SW Fiber 11o. and@ alert: interface down @ NORMAL : Porte2 : Mainframe 103
25/01/2010 18:36:25	Demonstracao (127.0.0.1)	local0	info	info	SyslogFlexVisio	SyslogFlexVisio : FlexVision : 25-01-10 12.30 @ Router SW Fiber 11o. and@ alert: interface up @ NORMAL : Porte1 : Mainframe 100

Consulta de Syslog.



Traps

Equipamento	Grupo	Data Inicial	Data Final
Equipamento: Todos			
Data Inicial: 19 / 01 / 2010			
Data Final: 19 / 01 / 2010			

Página(s): 1

Data	Equipamento	TrapOID	Alarme	Variáveis
19/01/2010 14:46:58	Router Unicom - Netflow (1.1.0.100)	.1.3.6.1.4.1.9.0.1	Warning	TCP connection terminated. Trap received from enterprise with 6 arguments: tslineSesType=5; tcpConnState=synReceived; loctcpConnElapsed=119822; loctcpConnInBytes=466; loctcpConnOutBytes=4024; tslineUser=UNICOMDG
19/01/2010 14:26:57	Router_IP_SLA (1.1.0.196)	.1.3.6.1.4.1.9.0.1	Warning	TCP connection terminated. Trap received from enterprise with 6 arguments: tslineSesType=5; tcpConnState=synReceived; loctcpConnElapsed=9784311; loctcpConnInBytes=119; loctcpConnOutBytes=162; tslineUser=
19/01/2010 14:13:27	Router Unicom - Netflow (1.1.0.100)	.1.3.6.1.4.1.9.0.1	Warning	TCP connection terminated. Trap received from enterprise with 6 arguments: tslineSesType=5; tcpConnState=synReceived; loctcpConnElapsed=66280; loctcpConnInBytes=570; loctcpConnOutBytes=1075; tslineUser=UNICOMDG

Consulta Recebimento de Traps SNMP.

(11) 5105-7500 www.flexvision.com.br falecom@flexvision.com.br

(11) 5105-7500

Av. das Nações Unidas, 11.857
2º andar - Brooklin
São Paulo - SP



FlexVision
UNIVERSAL MANAGEMENT