Pesquisa de LOG

Gráficos

Os gráficos podem monitorar o desempenho atual de objetos e contadores selecionados; por exemplo, o uso da CPU ou E/S em disco. É possível adicionar diversas combinações de objetos e contadores a um gráfico do Monitor do Sistema. Também é possível adicionar objetos e contadores do Microsoft Windows a um gráfico.

Cada gráfico representa um subconjunto de informações a monitorar. Por exemplo, um gráfico pode rastrear estatísticas de uso de memória e um outro gráfico pode rastrear estatísticas de E/S em disco.

* Usar um gráfico pode ser útil para as seguintes tarefas:
* Investigar por que um computador ou aplicativo está lento ou ineficiente.
* Monitorar continuamente os sistemas para localizar problemas de desempenho intermitentes.
* Descobrir por que a capacidade precisa ser aumentada.
* Exibir uma tendência na forma de um gráfico de linhas.
* Exibir uma comparação na forma de um gráfico de histograma.
* Gráficos são úteis para o monitoramento de curto prazo em tempo real de um computador local ou remoto (por exemplo, quando se deseja monitorar um evento enquanto ele ocorre).

Alertas

Usando alertas, o Monitor do Sistema rastreia eventos específicos e emite notificações a seu respeito conforme solicitado. Um log de alertas pode monitorar o desempenho atual de contadores e instâncias de objetos selecionados no SQL Server. Quando um contador excede um determinado valor, o log registra a data e a hora do evento. Um evento também pode gerar um alerta de rede. Você pode fazer com que um programa especificado seja executado na primeira vez ou em todas as vezes que o evento ocorrer. Por exemplo, um alerta pode enviar uma mensagem de rede a todos os administradores do sistema avisando que a instância do SQL Server está ficando com pouco espaço em disco.

Logs

Os logs permitem registrar informações sobre a atividade atual de objetos e computadores selecionados para visualização e análise posteriores. É possível coletar dados de vários sistemas em um mesmo arquivo de log. Por exemplo, é possível criar logs diferentes que coletem informações sobre o desempenho de objetos selecionados em diversos computadores para análise futura. Você pode salvar essas seleções sob um nome de arquivo e reutilizá-las quando quiser criar um outro log de informações similares para comparação.

Arquivos de log fornecem informações preciosas para a solução de problemas ou planejamento. Enquanto que gráficos, alertas e relatórios sobre a atividade atual propiciam um feedback instantâneo, os arquivos de log permitem rastrear os contadores por um longo intervalo de tempo. Assim, você pode examinar as informações mais minuciosamente e documentar o desempenho do sistema.

Relatórios

Os relatórios permitem exibir valores de instâncias e contadores de objetos selecionados que mudam constantemente. Os valores aparecem em colunas para cada instância. É possível ajustar os intervalos do relatório, imprimir instantâneos e exportar dados. Use relatórios quando precisar exibir os números brutos.

Para obter mais informações sobre como criar gráficos, alertas, logs e relatórios ou sobre objetos e contadores do Windows, consulte a documentação do Windows.

PRINCIPAIS FERRAMENTAS DE MONITORAMENTO DE LOGS

investigar incidentes de segurança, localizar um erro de aplicativo ou isolar um componente de baixo desempenho, as informações necessárias para facilitar sua vida estão em seus registros

Você acha que sua única opção para monitoramento de dados de log é o Splunk? Pense de novo

O gerenciamento de logs é vital para DevOps e equipes de aplicativos que procuram simplificar e acelerar as tarefas de triagem e resolução de problemas. Por exemplo, com o Gerenciador de Log do Site24x7, você pode coletar, consolidar, indexar, pesquisar e solucionar automaticamente os logs de seus servidores rapidamente, usando um *Web Client* intuitivo e unificado, tudo a partir da nuvem

Da mesma forma, o SIEM (Security Information and Event Management) é a prática de coletar, monitorar e analisar automaticamente dados relacionados à segurança de eventos e logs, incluindo software antivírus, sistemas de arquivos, firewalls, servidores, roteadores, comutadores, aplicativos e sistemas IDS e IPS. Você tem opções acessíveis, desde sistemas comerciais completos como o ManageEngine Log360 (uma solução completa para todos os desafios de gerenciamento de log e segurança de rede) ou sua contraparte baseada na nuvem, ManageEngine Log 360 Cloud, para alternativas open source OSSIM e PreludeIDS

Ao se preparar para aumentar seu monitoramento, adicionando recursos de gerenciamento de log ao seu arsenal, aqui estão algumas dicas e ferramentas para ajudá-lo a criar a abordagem de gerenciamento de log correta, ideal para você e sua organização.

**IDENTIFIQUE QUAIS LOGS DEVEM SER MONITORADOS**

Cada dispositivo e aplicativo em sua rede está registrando informações. Um acidente de aplicativo? Um OUTRAS OPÇÕES DE MONITORAMENTO DE LOG:

Loggly Serviço de gerenciamento de logs baseado em nuvem com análise e monitoramento de logs unificados e acesso com um clique ao código-fonte para agilizar o DevOps.

SumoLogic. Serviço de análise de dados de máquina nativa da nuvem para gerenciamento de logs e métricas de séries temporais.

Logentries por Rapid7. Gerenciamento de log e análise ao vivo para equipes de DevOps, TI e segurança.

XPL. Descoberta de log automatizada, pacotes de análise predefinidos e informações automatizadas para ajudar a dominar os dados de TI.

Logmatic.io. Registre a centralização, a análise e a visualização para melhorar o desempenho de TI e de negócios.

Bugfender Armazenamento em nuvem para os arquivos de registro dos aplicativos nos dispositivos dos usuários para ajudar a depurar mais rapidamente.

LogDNA. Capture instantaneamente, pesquise e faça o gráfico de logs a partir de qualquer plataforma com uma velocidade de pesquisa rápida para identificar a causa raiz.

Logz.io. Elasticsearch, Logstash e Kibana na nuvem com alertas, escalabilidade ilimitada e aprendizado de máquina e análise preditiva para que os usuários possam indexar, pesquisar e visualizar dados.

Escamosa Plataforma SaaS para gerenciamento de log de alta velocidade e monitoramento de servidores.

Sistemas de tear. Solução de alerta e análise de log com tecnologia AI para DevOps e gerentes de TI.

Humio Gerenciamento de log para desenvolvedores e DevOps para que eles possam analisar, armazenar, consultar e compartilhar painéis para encontrar padrões comportamentais ocultos e depurar falhas

Madeira. Log Management e sistema de agregação com retenção de dados, pesquisa avançada e relatórios de conformidade para engenheiros de software.

Log Correlation Engine. Solução de gerenciamento de logs projetada para analisar log, detectar anomalias, monitorar e correlacionar eventos

LogFusion. Projetado para monitoramento de logs em tempo real com filtragem de texto, realce de linha, colunas personalizadas, rolagem automática e muito mais para administradores e desenvolvedores de sistemas

LogSanctuary. Registra a plataforma de dados que fornece total transparência sobre logs de TI e notificação de ameaças e anomalias.servidor IIS sobrecarregado? Uma falha de chamada de banco de dados externo? Todos logados. Considere atribuir prioridades e começar pequeno à medida que você desenvolve sua estratégia de gerenciamento de log. Por exemplo, você poderia se concentrar primeiro nos dispositivos (dispositivos Windows, Linux e Unix, switches, firewalls, roteadores …) e aplicativos (Cassandra, Java, IIS, Apache, aplicativos personalizados, etc.) pelos quais sua equipe é responsável, aqueles mais críticos para os negócios, ou sistemas mais propensos a erros. Você sempre pode expandir e gerenciar mais registros mais tarde.

**COLETE E AGREGUE REGISTROS AUTOMATICAMENTE**

Centralize e unifique todos os dados de registro em um único local para facilitar o acesso e o consumo em todas as funções e equipes. Aqui você pode explorar ferramentas de código aberto como o Logstash (um pipeline de processamento de dados do servidor que insere dados de várias fontes simultaneamente, transforma e envia para um “stash” ou outras saídas), Fluentd (arquitetura conectável para coletar e rotear registra-se em big data, data warehouses, sistemas de notificação e muito mais) ou Syslog-ng, que também coleta logs de qualquer fonte, processa-os em tempo real e os entrega a uma grande variedade de destinos. Você também pode se inscrever para uma conta gratuita de avaliação de gerenciamento de log Site24x7 com recursos avançados de detecção automática para reconhecer automaticamente o formato de mais de 20 logs relacionados a aplicativos e começar a coletar registros com o clique de um botão.

**ARQUIVAR, ARMAZENAR E RETER**

A retenção de dados de log é importante para a solução de problemas em tempo real e a análise de incidentes e eventos históricos, além de basear e comparar o desempenho do aplicativo e do sistema. Deseja transmitir dados para o Hadoop para análise e armazenamento adicionais? Você precisa manter seus registros para provas forenses ou comparações históricas? Confira as ferramentas de fontes abertas, como o Apache Flume, o Logalyze ou a versão gratuita do NXLog Community Edition. Com o ManageEngine Log360, você também pode arquivar logs de dispositivos syslog, dispositivos de segurança de perímetro, servidores Linux / UNIX / Windows, aplicativos e muito mais para atender aos rígidos requisitos de armazenamento de vários anos de exigências regulatórias como PCI DSS, FISMA, HIPAA, SOX, GLBA, GPG 13

e mais.

### OUTRAS OPÇÕES DE MONITORAMENTO DE LOG:

Loggly Serviço de gerenciamento de logs baseado em nuvem com análise e monitoramento de logs unificados e acesso com um clique ao código-fonte para agilizar o DevOps.

SumoLogic. Serviço de análise de dados de máquina nativa da nuvem para gerenciamento de logs e métricas de séries temporais.

Logentries por Rapid7. Gerenciamento de log e análise ao vivo para equipes de DevOps, TI e segurança.

XPL. Descoberta de log automatizada, pacotes de análise predefinidos e informações automatizadas para ajudar a dominar os dados de TI.

Logmatic.io. Registre a centralização, a análise e a visualização para melhorar o desempenho de TI e de negócios.

Bugfender Armazenamento em nuvem para os arquivos de registro dos aplicativos nos dispositivos dos usuários para ajudar a depurar mais rapidamente.

LogDNA. Capture instantaneamente, pesqOUTRAS OPÇÕES DE MONITORAMENTO DE LOG:

Loggly Serviço de gerenciamento de logs baseado em nuvem com análise e monitoramento de logs unificados e acesso com um clique ao código-fonte para agilizar o DevOps.

SumoLogic. Serviço de análise de dados de máquina nativa da nuvem para gerenciamento de logs e métricas de séries temporais.

Logentries por Rapid7. Gerenciamento de log e análise ao vivo para equipes de DevOps, TI e segurança.

XPL. Descoberta de log automatizada, pacotes de análise predefinidos e informações automatizadas para ajudar a dominar os dados de TI.

Logmatic.io. Registre a centralização, a análise e a visualização para melhorar o desempenho de TI e de negócios.

Bugfender Armazenamento em nuvem para os arquivos de registro dos aplicativos nos dispositivos dos usuários para ajudar a depurar mais rapidamente.

LogDNA. Capture instantaneamente, pesquise e faça o gráfico de logs a partir de qualquer plataforma com uma velocidade de pesquisa rápida para identificar a causa raiz.

Logz.io. Elasticsearch, Logstash e Kibana na nuvem com alertas, escalabilidade ilimitada e aprendizado de máquina e análise preditiva para que os usuários possam indexar, pesquisar e visualizar dados.

Escamosa Plataforma SaaS para gerenciamento de log de alta velocidade e monitoramento de servidores.

Sistemas de tear. Solução de alerta e análise de log com tecnologia AI para DevOps e gerentes de TI.

Humio Gerenciamento de log para desenvolvedores e DevOps para que eles possam analisar, armazenar, consultar e compartilhar painéis para encontrar padrões comportamentais ocultos e depurar falhas

Madeira. Log Management e sistema de agregação com retenção de dados, pesquisa avançada e relatórios de conformidade para engenheiros de software.

Log Correlation Engine. Solução de gerenciamento de logs projetada para analisar log, detectar anomalias, monitorar e correlacionar eventos

LogFusion. Projetado para monitoramento de logs em tempo real com filtragem de texto, realce de linha, colunas personalizadas, rolagem automática e muito mais para administradores e desenvolvedores de sistemas

LogSanctuary. Registra a plataforma de dados que fornece total transparência sobre logs de TI e notificação de ameaças e anomalias.uise e faça o gráfico de logs a partir de qualquer plataforma com uma velocidade de pesquisa rápida para identificar a causa raiz.

Logz.io. Elasticsearch, Logstash e Kibana na nuvem com alertas, escalabilidade ilimitada e aprendizado de máquina e análise preditiva para que os usuários possam indexar, pesquisar e visualizar dados.

Escamosa Plataforma SaaS para gerenciamento de log de alta velocidade e monitoramento de servidores.

Sistemas de tear. Solução de alerta e análise de log com tecnologia AI para DevOps e gerentes de TI.

Humio Gerenciamento de log para desenvolvedores e DevOps para que eles possam analisar, armazenar, consultar e compartilhar painéis para encontrar padrões comportamentais ocultos e depurar falhas

Madeira. Log Management e sistema de agregação com retenção de dados, pesquisa avançada e relatórios de conformidade para engenheiros de software.

Log Correlation Engine. Solução de gerenciamento de logs projetada para analisar log, detectar anomalias, monitorar e correlacionar eventos

LogFusion. Projetado para monitoramento de logs em tempo real com filtragem de texto, realce de linha, colunas personalizadas, rolagem automática e muito mais para administradores e desenvolvedores de sistemas

LogSanctuary. Registra a plataforma de dados que fornece total transparência sobre logs de TI e notificação de ameaças e anomalias.