Uma Arquitetura para Correlação de Alarmes Baseada em Políticas e Web Services

Evandro Della Vecchia Pereira, Lisandro Zambenedetti Granville

Instituto de Informática – Universidade Federal do Rio Grande do Sul
Caixa Postal 15064 – 90501-970 Porto Alegre, RS

edvpereira@inf.ufrgs.br, granville@inf.ufrgs.br

Resumo. *No gerenciamento de redes de computadores, alarmes são fundamentais para a percepção de erros ou falhas. Com a utilização de SNMP, agentes são configurados para enviarem traps aos gerentes, alertando sobre a constatação de alguma anormalidade em dispositivos ou na própria rede. Porém, vários agentes em uma mesma rede podem constatar a mesma falha e enviarem o mesmo alerta ao gerente. Ou ainda, se a mesma falha não é resolvida em determinado tempo, inúmeros alertas são gerados. Quando há apenas um gerente ou apenas um nível de gerentes, não há como eliminar alertas repetidos ou considerados inúteis para o administrador, mas quando há mais de um nível de gerentes, uma correlação de alarmes pode ser feita. Esta correlação faz com que o número de alarmes seja reduzido, o que ajuda o administrador na visualização das falhas em seu software de gerenciamento. Este trabalho propõe uma arquitetura onde é feita uma correlação dos alarmes e a comunicação entre gerentes é feita através de Web Services.*

1. Introdução

Alarmes são muito úteis no gerenciamento de redes de computadores, pois a iniciativa é do dispositivo, avisando ao gerente que há algum problema. Dessa forma o gerente não precisa consultar todos os dispositivos da rede em um intervalo de tempo muito pequeno. Além disso, o alarme é disparado seguindo limiares definidos pelo administrador, como por exemplo, em determinado momento o administrador define que um determinado percentual de colisões de pacotes na rede é muito alto e deve ser gerado um alarme, e, em outro momento o administrador decide baixar esse percentual.

Os alarmes mais utilizados são os *traps*, transportados pelo SNMP. Cada alarme é transportado em uma mensagem, não havendo correlação entre alarmes. Esta possível correlação poderia reduzir o número de mensagens. Se um problema persiste por muito tempo, os alarmes são gerados continuamente, relatando o mesmo problema, o que pode ”inundar”a rede com tráfego desnecessário. Outro problema é que determinadas falhas ocasionam outras, se não forem corrigidos os problemas. Como não há correlação levando-se em consideração determinado intervalo de tempo, todas falhas geram alarmes, o que ”inunda”mais ainda a rede.

A partir do SNMPv2, a comunicação entre gerentes se tornou possível, porém os alarmes são repassados sem nenhuma correlação, e o tráfego continua sem ser reduzido.

Para tal correlação, é necessário que algum sistema de gerência analise os alarmes vindos dos dispositivos, verifique regras de correlação definidas pelo administrador em uma base de dados e repasse ao gerente do nível superior menos mensagens de alarme, reduzindo o tráfego e melhorando a visualização de alarmes pelo administrador, sem nenhum prejuízo à possível resolução das falhas acusadas pelos alarmes.

Muitas vezes, a comunicação entre gerentes é realizada em uma rede de longa distância. Como mensagens SNMP são transportadas sobre UDP, corre-se o risco da perda de alarmes. Uma solução para este problema é a utilização da tecnologia Web Service. Além de serem orientados à conexão, os Web Services são componentes independentes de software capazes de oferecer mecanismos de chamadas de procedimento remoto. Web Services utilizam como protocolo de transporte o SOAP, que pode ser encapsulado em HTTP, FTP, SMTP entre outros. O mais aconselhado, para não ter problemas em filtros de *firewalls*, é o HTTP.

Na seção 2 será mostrado o conceito de Web Services, na seção 3 o conceito de correlação de alarmes. A arquitetura proposta será apresentada na seção 4 e por fim, na seção 5 serão mostradas as conclusões.

2. Web Services

Web Services são componentes independentes de aplicações que são disponibilizados na Web de tal maneira que outras aplicações Web possam achá-los e utilizá-los. Variam de simples a complexos e trazem a promessa de flexibilidade e de computação distribuída na Internet [Roy and Ramanujan, 2001].

Os Web Services, considerados sucessores de CORBA e DCOM, são um dos principais passos na evolução da Web. Eles permitem que objetos ativos sejam colocados em Web sites para fornecer serviços distribuídos a clientes. Os Web Services têm sido utilizados em *e-commerce*, no gerenciamento de informações distribuídas, já que sistemas de bancos de dados distribuídos têm dificuldades com compatibilidade de plataformas e softwares [Abiteboul et al., 2000]. Também podem ser descritos como aplicações capazes de executar transações na Internet. Eles podem ser acessados tanto pelos clientes (ex.: browsers) como por outros Web Services [Sahai et al., 2001].

Os Web Services podem ser vistos como integradores de computadores, dispositivos, bancos de dados e redes em um único sistema virtual, onde os usuários podem trabalhar utilizando browsers [Vaughan-Nichols, 2002].

Uma das principais utilidades dos Web Services são as chamadas de procedimento remoto: usuários ativam determinadas tarefas em um dispositivo/máquina remoto [Preece and Decker, 2002].

Uma definição mais completa para Web Service seria: um serviço disponível na Internet que utiliza um sistema de mensagens XML, e não depende de sistema operacional nem linguagem específica. Na figura 1 é mostrado como é feita a comunicação de um Web Service básico em alto nível [Cerami, 2002].

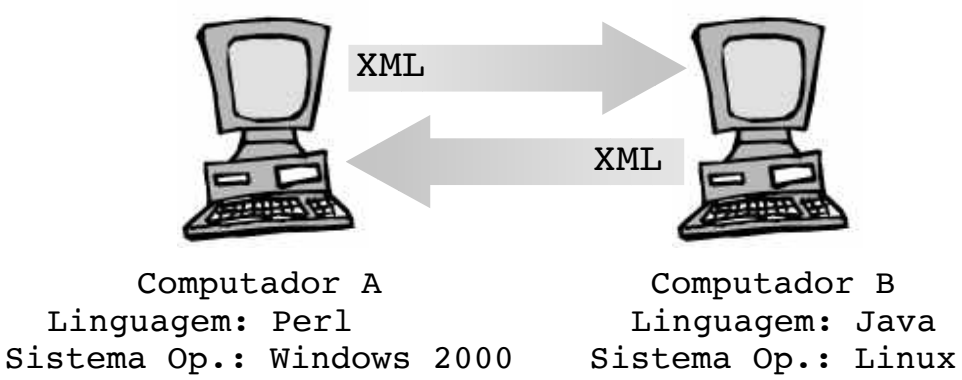

Figura 1: Web Service básico

3. Correlação de Alarmes

Alarmes gerados por dispositivos de redes de computadores e enviados ao(s) gerente(s) são essenciais para ajudar o administrador à verificar e, se possível, solucionar problemas. Porém, muitas vezes, alarmes relatando o mesmo problema são gerados porque o intervalo de tempo definido para geração de alarmes é pequeno. Isso faz com que a visualização do administrador que utiliza um software gerente seja prejudicada. Outra situação que ocasiona uma quantidade maior de alarmes é que algumas falhas fazem com que vários dispositivos gerem o mesmo alarme, sendo que na verdade há apenas uma falha.

Um alarme é a notificação de um evento considerado anormal, que pode ou não representar um erro (ou falha). Como mencionado anteriormente, um único incidente pode causar a geração de vários alarmes. Abaixo são listados alguns fatores relacionados a estes fatos [de Castro and Nogueira, 1998]:

- um agente pode gerar vários alarmes em conseqüência de uma única falha;
- uma falha pode ser intermitente, o que resulta em um novo alarme para cada ocorrência da falha;
- uma falha em um item pode ocasionar a geração de alarmes cada vez que o dispositivo for solicitado (uma consulta por exemplo);
- uma única falha pode ser detectada por diferentes itens na rede;
- uma falha em um item pode afetar outros itens na rede.

Como pode ser visto, uma redução das mensagens de alarme pode ser necessária, para agilizar o processo de análise e solução de problemas, pelo administrador. Essa redução de mensagens pode ser realizada através da correlação de alarmes. A correlação deve levar em conta os fatores mencionados anteriormente. Ou seja, além de serem correlacionados os alarmes originados por agentes diferentes relatando a mesma falha, alarmes devem ser correlacionados também em relação ao tempo. Mensagens contendo o mesmo alarme em instantes de tempo diferentes devem ser analisadas para que seja feita a verificação se eles estão relatando a mesma falha (quando a falha não foi solucionada). Essas mensagens também podem significar uma falha atuando de forma intermitente ou ainda, a falha pode ter sido solucionada e o item voltou a apresentar problemas.

Algumas técnicas de correlação de alarmes são comumente utilizadas em *softwares* comerciais. São elas [Zupan and Medhi, 2003]:

- raciocínio baseado em regras;

- raciocínio baseado em modelos;
- raciocínio baseado em casos;
- codebook;
- modelo de grafo de transição de estados;
- modelo de máquina de estados finita.

Além de utilizar técnicas de correlação de alarmes, é necessário conhecer o comportamento de eventos presentes em uma rede. Segundo [Melo et al., 2000], os seguintes tipos de comportamento de eventos estão presentes em redes IP gerenciadas através de SNMP:

- *start*/*stop*: eventos que se apresentam aos pares. Um dos eventos indica quando certa condição se torna válida e outro indica quando esta não é mais válida. Como exemplo tem-se *traps* RMON [Waldbusser et al., 2003], *traps* SNMP de mudança de estados e eventos de monitoração do próprio gerente SNMP;
- *storm*: seqüência de vários eventos do mesmo tipo, em um determinado período;
- fluxo de eventos correlatos: quando a ocorrência de um evento está associada com a ocorrência de outro;
- fluxo de eventos independente: não tem relação significativa com outros eventos.

4. Arquitetura Proposta

Nesta seção será mostrada uma arquitetura que tem como objetivo correlacionar alarmes de forma hierárquica (figura 2). Os alarmes são gerados nos dispositivos de rede através de *traps* SNMP ou RMON, estes são correlacionados em um gerente de primeiro nível e repassados ao gerente de nível superior. Ou seja, a arquitetura prevê pelo menos dois níveis de gerente e teoricamente não há limite nos níveis gerenciais.

O envio das mensagens de alarmes já correlacionados é feito com o uso de Web Services. O processo de correlação de alarmes e envio ao nível superior se repete até que os alarmes cheguem ao gerente do último nível. Cada gerente deverá ter uma base de dados contendo as regras necessárias para que a correlação seja feita. Estas regras devem permitir tanto a correlação de alarmes originados em dispositivos diferentes como a correlação de alarmes originados no mesmo dispositivo, porém em instantes diferentes. Isso porque em determinadas falhas, o mesmo alarme pode ser originado de tempo em tempo, conforme mencionado anteriormente.

A correlação será feita com o auxílio de políticas (regras) armazenadas em bases de dados que os gerentes tenham acesso. O administrador alimentará as bases de dados com as regras de correlação, de acordo com as técnicas de correlação e tipos de comportamento de eventos apresentados na seção 3. O uso de gerenciamento baseado em políticas [Westerinen et al., 2001] permite que a árvore de correlação de alarmes seja dinâmica. Um exemplo do dinamismo da árvore de correlação seria o caso de um gerente, seguindo as políticas definidas pelo administrador, enviar suas correlações a um gerente X no período das 7h às 8h, e ao gerente Y, no período das 8h às 9h. Dessa forma o gerente de nível superior muda conforme o horário em questão.

Com a utilização de Web Services na comunicação entre gerentes, há a possibilidade destes se encontrarem em domínios administrativos diferentes, visto que os Web

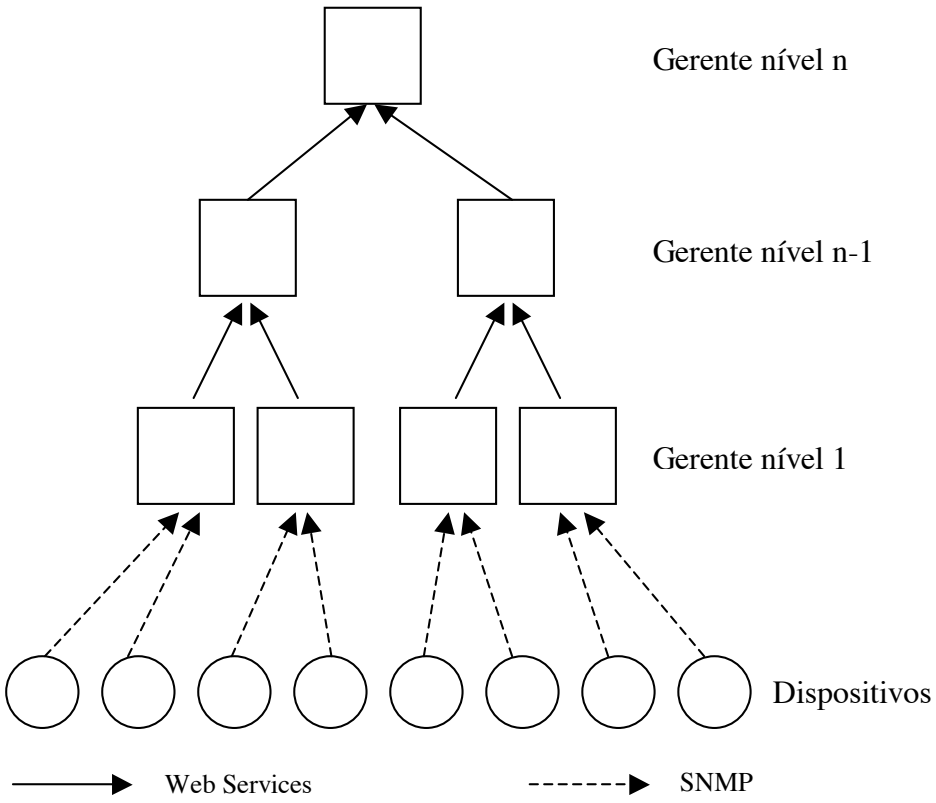

Figura 2: Arquitetura Proposta

Services podem ser encapsulados em HTTP, SMTP, entre outros. Protocolos como o HTTP e SMTP geralmente tem acesso livre em *firewalls*, evitando ter que solicitar ao administrador de determinado domínio administrativo uma liberação de tráfego em certas portas.

Outra vantagem na utilização dos Web Services na comunicação entre gerentes, utilizando HTTP ou SMTP é que estes são orientados à conexão. Desta forma há garantia na entrega das mensagens. Para evitar problemas como servidor indisponível por alguns instantes, por exemplo, optou-se pelo uso de Web Services baseados em SMTP. Assim, se o servidor estiver indisponível por alguns instantes, não haverá problema no envio das mensagens, ao contrário do HTTP que não permite uma comunicação *off-line*. A utilização de Web Services sobre SMTP é totalmente inexplorado, o que requer pesquisa para que seja comparado com soluções que utilizam Web Services sobre HTTP ou outro protocolo.

5. Conclusões

A partir dos estudos realizados, foi constatado que correlação de alarmes é um assunto não muito explorado e que a utilização da tecnologia Web Service para realizar a correlação aparentemente não é utilizada. Um aspecto importante na utilização de Web Services é a facilidade de implementação e manutenção, sem contar a fácil interoperabilidade que esta tecnologia propicia. Outro aspecto importante é a garantia de entrega das mensagens de alarme, tornando o sistema confiável (no caso da utilização de SMTP para entrega das

mensagens, deve-se levar em consideração o *timeout* definido para servidores SMTP e se uma rede ou servidor ficar inoperante por mais tempo que o *timeout*, a garantia de entrega deixa de existir).

A alimentação das bases de dados pelo administrador, com regras de correlação, torna o sistema flexível. Com isso, novos agentes podem ser implementados, com novos *traps* e mesmo assim o gerente poderá realizar as correlações.

Um estudo sobre ferramentas comerciais deve ser feita para que se possa comparar resultados. A idéia deste trabalho é implementar a arquitetura proposta e verificar se esta solução é melhor ou não do que soluções que não utilizam Web Services. Para isto, testes de desempenho deverão ser realizados após a implementação completa da arquitetura.

Referências

Abiteboul, S., Benjelloun, O., and Milo, T. (2000). Web services and data integration. In *Proceedings INTERNATIONAL CONFERENCE ON WEB INFORMATION SYSTEMS ENGINEERING (WISE)*.

Cerami, E. (2002). *Web Services Essentials*. O'Reilly.

de Castro, T. and Nogueira, J. (1998). An alarm correlation system for sdh networks. In *Proceedings Telecommunications Symposium - SBT/IEEE International ITS '98*. Pages 492 - 497, Vol. 2.

Melo, E., Vieira, E., and Sari, S. (2000). Tratamento de eventos. *Boletim bimestral sobre tecnologia de redes*, 4(4). Disponível em <http://www.rnp.br/newsgen/0007/art10.html>. Acesso em 08 Jun.

Preece, A. and Decker, S. (2002). Intelligent web services. *IEEE Intelligent Systems*, pages 15–17.

Roy, J. and Ramanujan, A. (2001). Understanding web services. *IEEE Computer Society - ITPro*, pages 69–73.

Sahai, A., Machiraju, V., Ouyang, J., and Wurster, K. (2001). Message tracking in soap-based web services. *Technical Reports Hewlett-Packard Laboratories*.

Vaughan-Nichols, S. J. (2002). Web services: Beyond the hype. *Industry Trends*, pages 18–21.

Waldbusser, S., Kalbfleisch, C., and Romascanu, D. (2003). *Introduction to the Remote Monitoring (RMON) Family of MIB Modules: RFC 3577*. IETF.

Westerinen, A. et al. (2001). *Terminology for Policy-Based Management: RFC 3198*. IETF.

Zupan, J. and Medhi, D. (2003). An alarm management approach in the management of multi-layered networks. In *Proceedings 3rd IEEE Workshop on IP Operations and Management (IPOM)*. Pages 77 - 84.