# Sistema de Suporte às Atividades de Administração de Redes de Computadores Unix - Unix Operation Center (UOC)

Larissa Tiemi Kato de Oliveira[1], Saymmo Roberto Orlandini[2], Eduardo S. Forbici[3]

[1]Dep. Acadêmico de Informática, Cefet/Pr, Av. Sete de Setembro, 3165, Centro, Curitiba, PR, Brasil
ltkoliveira@yahoo.com.br
[2]Dep. Acadêmico de Informática, Cefet/Pr, Av. Sete de Setembro, 3165, Centro, Curitiba, PR, Brasil
saymmo@yahoo.com.br
[3]Faculdade Cenecista Presidente Kennedy, Rua Rui Barbosa 541, Centro, Campo Largo, PR, Brasil
eduardo@presidentekennedy.br

**Resumo** - O desenvolvimento acelerado das redes de computadores, aliado a importância que as mesmas têm assumido dentro das organizações, tem exigido uma administração mais ampla e complexa. Tal administração, além de cobrar profissionais com mais capacitação e experiência, tem requerido novas ferramentas capazes de suportar as atividades administrativas com eficiência, eficácia e baixo custo. Diante deste contexto, este trabalho visa o estudo e o desenvolvimento de uma ferramenta capaz de auxiliar a monitoração e a gerência de serviços e servidores em um ambiente Unix.

Palavras-chave: Administração de Redes de Computadores, Redes de Computadores, Unix.

**Abstract -** The intense development of computer networks, alied to their importance in organisations, has been demanding an ampler and more complex administration which requires low cost new tools that are able to stand administrative activities with efficiency and effectiveness, besides enabled and experinced employees. In this context, this paper aims at the study and development of a tool able to monitor and manage services and servers in an Unix environment.

Keywords: Computer Network Administration, Computer Networks, Unix.

## Introdução

A complexidade da atividade de Administração e Gerenciamento de Redes de Computadores [1] cresce na medida em que se aumenta a quantidade de estações de processamento na rede. Com o crescimento das redes de computadores aumenta também a dependência das organizações pelas mesmas.

Na administração atual não se considera apenas a monitoração dos elementos e equipamentos de rede, mas também dos serviços e aplicações. Assim na administração moderna há um número crescente de monitorações e análises das ocorrências.

Com o crescimento da Internet [2], as redes de computadores tornaram-se maiores e mais complexas, exigindo ferramentas mais poderosas para monitorar e analisar ocorrências. Muitas ferramentas para a administração de redes surgiram desde então. Elas são muitos úteis, porém a grande maioria apresenta um custo bastante elevado.

O UOC (Unix Operation Center) é uma ferramenta projetada para ambientes Unix [3], que auxiliam os administradores de redes de computadores nas monitorações e análise de ocorrências das estações de trabalho. Seu principal atrativo está no seu baixo custo, uma vez que é totalmente baseado em aplicações gratuitas (software free), e na simplicidade de operação.

O desenvolvimento do UOC tem como principal objetivo monitorar e gerenciar aplicações e recursos de computadores em um ambiente Unix. O UOC permite a monitoração de processos, utilização de memória, consumo de CPU, percentual de utilização de filesystem e verificação de arquivos de Log. Ele permite que o Usuário execute atividades de monitoração comuns ao ambiente Unix, e também específicas, através da criação de scripts personalizados.

## Arquitetura do Sistema UOC

Atualmente a administração de redes de computadores constitui-se em uma atividade complexa e, ao mesmo tempo exigente quanto à qualificação e experiência dos profissionais da área. Assim o administrador de rede necessita de ferramentas automatizadas que possam auxiliar em suas atividades. O UOC visa ser uma ferramenta para suportar e auxiliar essas atividades a um custo reduzido.

A arquitetura do UOC inspira-se nos

conceitos clássicos de Gerência de Redes [4]. Os elementos que constituem a arquitetura do UOC são o Servidor Central e os Servidores Monitorados. O Servidor Central atua como um processo gerente solicitando informações e enviando scripts de monitoração aos Servidores Monitorados. O papel de processo agente é exercido pelos Servidores Monitorados, que além de atender às requisições do Servidor Central, monitoram as aplicações e recursos da estação de trabalho em que executam. A figura 1 ilustra o relacionamento entre o Servidor Central e os Servidores Monitorados.

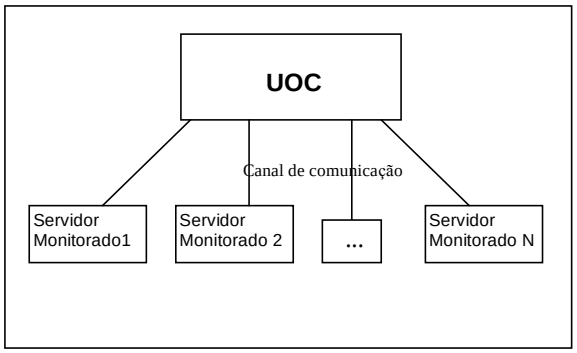


**Figura 1** - Arquitetura do Sistema UOC.

**Servidor Central**

Uma das funções do Servidor Central é verificar o estado do processo crond nos Servidores Monitorados. Através deste processo o sistema operacional do Servidor Monitorado executa periodicamente outros processos que realizam a monitoração da estação de trabalho.

No Servidor Central são cadastrados todos os Servidores Monitorados e também os seus recursos e/ou serviços a serem monitorados. Estas informações são armazenadas em um banco de dados no Servidor Central. A partir delas são gerados arquivos executáveis (scripts), os quais são armazenados no Servidor Central e enviados para os Servidores Monitorados. O Servidor Central atualiza uma monitoração em um Servidor Monitorado, copiando (RCP) o arquivo cron deste Servidor Monitorado. Em seguida este arquivo é atualizado e reenviado juntamente com os scripts para o Servidor Monitorado. No arquivo cron são inseridos scripts de monitoração e também os respectivos horários de execução.

O Servidor Central verifica, a cada 30 segundos, a existência de novas mensagens de monitorações enviadas pelos Servidores Monitorados. Estas mensagens de monitorações são armazenadas na base de dados e em seguida apresentadas ao usuário.

Sempre que uma monitoração for incluída ou alterada, o arquivo cron do Servidor Monitorado deverá ser atualizado e os seus scripts deverão ser substituídos.

Basicamente o Servidor Central tem como atribuições:

- Testar periodicamente (a cada sessenta segundos) o canal de comunicação com os Servidores Monitorados através do comando ping (ICMP);
- Verificar se o processo crond está ativo nos Servidores Monitorados;
- Verificar se o processo inetd está ativo no Servidor Central e nos Servidores Monitorados.

**Servidor Monitorado**

A função de um Servidor Monitorado é monitorar os serviços e recursos de uma estação de trabalho. Estas monitorações devem ser previamente cadastradas no Servidor Central. Quando uma monitoração detectar uma ocorrência, o Servidor Monitorado deverá informar ao Servidor Central.

Todos os sistemas operacionais baseados no Unix possuem o processo crond. Este processo coordena a execução de scripts cadastrados pelo Usuário do UOC. Se este processo não estiver ativo o sistema UOC não funcionará corretamente, pois não será possível executar as monitorações.

Quando um Servidor Monitorado recebe o arquivo cron atualizado (inserção/remoção de scripts) do Servidor Central, este último, através do comando rsh, reinicia o processo crond. A partir deste momento, as atividades de monitorações iniciam e todos as ocorrências detectadas serão gravadas em arquivos Log, e em seguida transmitidas para o Servidor Central.

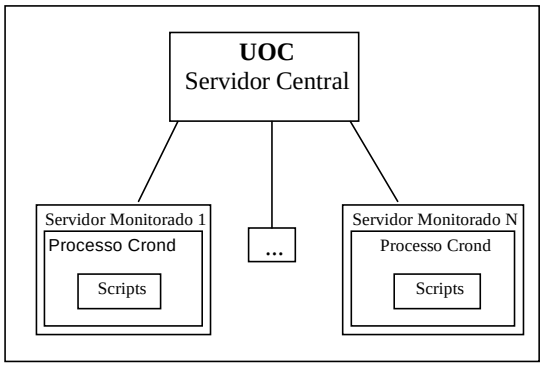


**Figura 2** - Detalhes da Arquitetura do UOC.

A Figura 2 ilustra os scripts agendados nos Servidores Monitorados.

**Mensagens de Monitoração**

No sistema UOC uma mensagem de monitoração é gerada sempre que uma

ocorrência de um determinado evento for verificada por um script. Esta mensagem de monitoração consiste em um arquivo texto que contém dados sobre a monitoração. Estes dados consistem na identificação da monitoração, a hora e data da ocorrência e uma mensagem que será apresentada ao Usuário do UOC.

No momento em que uma ocorrência é detectada, o script "envio.sh" [5] gera uma mensagem de monitoração através da criação de um arquivo no diretório "/usr/uoc/transferencia" do Servidor Monitorado. O nome deste arquivo será o número de identificação da monitoração. Em seguida o script "envio.sh" envia todos os arquivos que estão no diretório "/usr/uoc/transferencia" para o diretório "/usr/uoc/arquivos" no Servidor Central. Se durante a detecção da ocorrência a comunicação com o Servidor Central não estiver disponível, o arquivo criado não poderá ser transmitido. Quando acontecer a próxima ocorrência, e se a comunicação estiver disponível, todos os arquivos do diretório "/usr/uoc/transferencia" serão enviados ao Servidor Central.

**Scripts do Sistema UOC**

Para cada monitoração cadastrada, existe um script, gerado pelo sistema UOC, a partir de informações fornecidas pelo Usuário do UOC. Há dois tipos de geração de scripts: automático e personalizada.

Na geração de scripts automática, o usuário pode selecionar as ações que deverão ser executadas pelo script quando a ocorrência no Servidor Monitorado for detectada. Por exemplo, ao cadastrar a monitoração de "filesystem full" o usuário pode informar o nome dos arquivos que terão o seu conteúdo removido. Nesta situação os arquivos permanecerão apenas com o nome, ou seja, arquivos ficarão com zero bytes de tamanho. Neste caso, a mensagem apresentada ao usuário (via browser) será informativa. Deve-se ressaltar que a geração automática será apenas para monitorações definidas como padrões pelo UOC, tais como: consumo de CPU e memória, utilização de filesystem, processos ativos e mensagens em arquivos de Logs.

Na geração personalizada, o Usuário pode desenvolver um script de monitoração específica para uma determinada monitoração. O usuário deve indicar no script, quais as mensagens a serem exibidas no browser do Servidor Central. Estas mensagens são enviadas através de um script padrão ("envio.sh"). O usuário também deve informar a localização ("PATH") do script personalizado. Assim o UOC poderá carregar este script e enviá-lo para o Servidor Monitorado.

**Base de Dados**

O Servidor Central necessita de uma base de dados para armazenar os dados usados para a criação dos scripts, cadastro de usuários, e também para armazenar as mensagens de monitorações.

Entre as várias opções disponíveis de banco de dados, o MYSQL [6] se destaca pela sua flexibilidade, facilidade de uso, suporte on-line, consistência e confiabilidade. O MYSQL é um banco de dados adotado por várias organizações, sendo que a sua presença alcança milhões de instalações para WebSites, Datawarehouses, Aplicações de Negócios, etc.

Como o UOC é centrado para sistemas operacionais baseados no Unix, o MYSQL interage facilmente com várias linguagens deste ambiente, como por exemplo, a linguagem C, Java, Perl, Python, PHP, Tcl e outras.

**Interface do Sistema UOC**

A interface do sistema UOC com os usuários é implementada via WEB, ou seja, através de um browser. O servidor de WorldWideWeb Apache, foi selecionado pela sua simplicidade, velocidade e facilidade de conexão com a linguagem de programação PHP [7]. A linguagem PHP é amplamente utilizada e foi desenvolvida especialmente para a Internet. Um conjunto de instruções de linguagem PHP pode ser inserido facilmente em código HTML.

**Aspectos de Segurança**

O UOC previne acessos não autorizados às páginas do sistema. Assim os acessos são validados através de um login inicial.

Utilizando os recursos da linguagem de programação PHP, o UOC usa o mecanismo de sessão. Na linguagem PHP, uma sessão é uma diretiva capaz de registrar e consultar variáveis da sessão. Se os valores do processo login não forem registrados pela sessão o acesso não será permitido. Um processo de login validado é registrado em uma variável de sessão. Esta variável será testada sempre que o usuário tentar acessar alguma página do sistema UOC.

A variável de sessão permanecerá registrada até o fim do UOC (seleção da opção "Sair" do Menu ou fechamento da página do browser do UOC). Quando uma página do sistema UOC permanece inativa por mais de cento e oitenta segundos, a variável de sessão expira fechando a sessão. Uma vez fechada, a sessão o acesso ao sistema exige um novo processo de login. O valor de cento e oitenta segundos é determinado pela linguagem PHP durante a sua instalação. No entanto este valor pode ser alterado no arquivo "php.ini".

O UOC utiliza-se de alguns serviços como,

por exemplo, o RSH e o RCP para a transmissão de mensagens de monitoração. Se estes serviços forem mal configurados podem ocasionar falhas de segurança. Cabe ao administrador da rede de computadores, adotar medidas preventivas que evitem problemas de segurança, como por exemplo, ataques de spoofing [8].

A figura 3 ilustra a página inicial do sistema onde ocorre o processo de login.

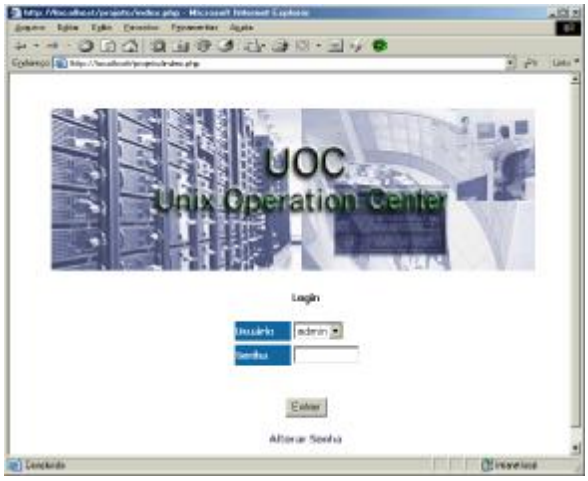


**Figura 3** – Página Inicial do Sistema UOC.

**Comunicação entre os Servidores**

A comunicação entre os componentes do sistema ocorre através de acessos remotos. Esses acessos remotos são viabilizados pelos comandos RSH e RCP. O RSH (Remote Shell) é usado pelo Servidor Central para executar comandos nos servidores Monitorados como, por exemplo, reinicializar o processo crond. O RCP é utilizado tanto pelo Servidor Central como pelos Servidores Monitorados para a transmissão de arquivos. O comando RSH (Remote Shell Daemon) e o comando RCP são viabilizados pelo processo INETD.

Na utilização dos serviços "telnet" e "ftp", os scripts de gerenciamento do sistema UOC conteriam os dados de autenticação (senha e login). Isto facilitaria o acesso não autorizado ao sistema UOC, uma vez que o conteúdo destes arquivos podem ser facilmente visualizados. Os comandos RSH e RCP não exigem que os seus dados de autenticação sejam armazenados no próprio script, no entanto, é necessário o uso do comando "SUDO[1]". Este comando emula a execução de qualquer comando como se ele for executado por um usuário "root". Assim o acesso aos servidores é liberado ao sistema com privilégios de usuário "root".

**Operações do Sistema UOC**

A administração e gerenciamento do UOC são realizados pelo Administrador do UOC. Todas as informações de monitoração devem ser cadastradas no Servidor Central pelo Administrador do UOC. As ocorrências conseqüentes da monitoração serão exibidas pelo browser para a supervisão dos usuários do UOC.

Portanto, no sistema UOC, há dois tipos de Usuários: administradores e não administradores. As ações dos usuários são validadas durante o processo de login no sistema.

No processo de login a variável de sessão registra "admin" ou "nao_admin". Os dois tipos de Usuários possuem acesso às páginas de "Ajuda", permissão para fechar mensagens e visualizar as mensagens do dia já fechadas.

Na Página Principal há um menu que apresenta mensagens abertas e mensagens fechadas. As mensagens abertas são mensagens que ainda estão pendentes para verificação. Cada mensagem possui as seguintes informações: severidade, nome do servidor que enviou a mensagem, data e hora da ocorrência e detalhes da mensagem. A severidade (importância) da mensagem é escolhida no momento do cadastro da monitoração. Para cada tipo de severidade (Informação, Atenção, Crítica e Fatal) há uma cor correspondente à sua importância.

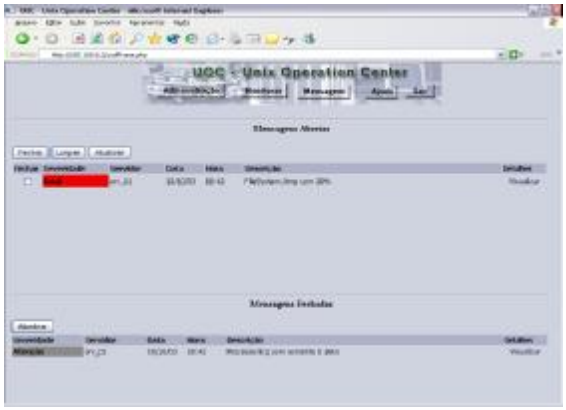


**Figura 4** – Página Principal do sistema UOC.

A Figura 4 corresponde à Página principal do sistema UOC e é composta por um menu com mensagens abertas e outro com mensagens fechadas.

**Questões Relevantes**

Há quatro processos que devem estar sempre ativos no Servidor Central: inetd, crond, httpd, mysqld.

A monitoração dos processos inetd e crond

[1] Sudo é um recurso do sistema operacional que permite um usuário do sistema operacional executar um script ou comando com permissão de root . Ex: sudo ls , o comando ls será executado como root.

no Servidor Central foi implementada de maneira diferente da implementação dos mesmos processos nos Servidores Monitorados. Para garantir uma maior eficácia na monitoração destes serviços, os principais serviços para o UOC, os scripts de monitoração do inetd e crond no Servidor Central não são executados pelo serviço inetd. Pois, se o serviço estiver inativo, as monitorações não ocorrem. Portanto, para evitar que a queda deste serviço no Servidor Central interrompa o funcionamento do UOC, estes processos são monitorados através do script "inetd_timestamp.sh" [5] para o Servidor Central e "inetd_nomedoservidormonitorado_timestamp.sh" para os Servidores Monitorados.

O httpd e mysqld, processos referentes ao Apache e ao banco de dados MYSQL respectivamente, são os serviços primários do UOC, portanto, a não ativação de um deles irá causar o não funcionamento do UOC. Pois não haverá mais acesso ao banco e nem ao browser.

**Conclusão**

O desenvolvimento de novas ferramentas que possam auxiliar os administradores de redes de computadores é de suma importância. A complexidade e a importância que as redes vêm assumindo dentro das organizações é inquestionável. Uma rede fora de operação acarreta enormes custos e transtornos para a organização.

Há muitas ferramentas para auxiliar na administração de redes de computadores. No entanto, a grande maioria apresenta elevados custos tanto para a aquisição quanto para a manutenção. Assim este trabalho propõe o desenvolvimento de uma ferramenta inspirada na ferramenta Tivoli [9] da IBM. No entanto a ferramenta proposta neste trabalho, apresenta um custo reduzido devido à utilização de softwares gratuitos, além da simplicidade de operação.

Após a conclusão do projeto e analisando a sua operação e abrangência, observou-se os seguintes pontos:

Pontos positivos da Ferramenta:

- As monitorações permitem, aos Usuários do UOC, realizar diagnósticos rápidos e confiáveis sobre a utilização e disponibilidade de recursos do ambiente;
- Utilização de softwares gratuitos, o que acarreta um baixo custo se comparado a sistemas similares.
- Flexibilidade para monitoração de recursos e aplicações;
- Os scripts e o arquivo Cron dos Servidores Monitorados são armazenados (backup) no Servidor Central, podendo a qualquer momento ser restaurados;
- Com a queda no Servidor Central, as informações de monitoração podem ser obtidas diretamente nos Servidores Monitorados, através dos arquivos de Log;
- Processamento distribuído.

Pontos negativos da ferramenta:

- Suporta apenas aplicativos Unix;
- O Servidor Central deve constantemente verificar a situação do Canal de Comunicação;
- Quando o processo HTTPD, do servidor WEB Apache, estiver fora de operação, o acesso ao UOC via browser ficará impossibilitado. Nesta situação somente os arquivos Logs estarão disponíveis. A indisponibilidade deste processo compromete o sistema;
- Caso o processo mysqld, do servidor de banco de dados MYSQL, estiver fora de operação, não será possível à apresentação de mensagens para os Usuários do UOC, além da inacessibilidade do bando de dados. A indisponibilidade deste processo também compromete o sistema;
- Administração centralizada no Servidor Central;
- Exige que o Administrador do UOC adote algumas medidas de segurança, como por exemplo, para evitar Spoofing de IP;
- O sistema UOC foi testado somente com os sistemas operacionais Linus RedHat e Linux Conectiva, HP-UX e AIX;

Pré-requisitos para a operação da Ferramenta:

- Conhecimentos de scripts Shell;
- Conhecimentos básicos de ambientes Unix (crond, inetd, ...);
- Conhecimentos de Internet.

Como continuação do trabalho aqui apresentado, fica a sugestão para a implementação de novas funcionalidades para o sistema UOC. Por exemplo, a ferramenta poderia permitir que o Usuário definisse outras monitorações como sendo padrões. Também poderia ser possível que o Servidor Central pudesse interagir com outros Servidores Centrais. Isso iria permitir uma contigência do sistema, o que seria bastante útil no caso de falha do Servidor Central.

**Referências Bibliográficas**


1. Frisch, Aeleen. Essential System Administration. Segunda edição. Editado por O'Reilly & Associates.
2. Barry L. M.. A Brief History of the Internet – Research Institute for Advanced Computer Sciense. Disponível em :<http://www.isoc.org/internet-history/brief.html>
3. Molay, Bruce. Undestanding Unix/Linux Programming. PRENTICE HALL. 2002.

4. Subramanian, Mani. Network Management – Principles an Practice. Addison Wesley, 2000.
5. Oliveira, Larissa T. K.; Orlandini, Saymmo R.; Sistema de Suporte às Atividades de Administração de Redes de Computadores Unix - Unix Operation Center (UOC); Trabalho de Diplomação, Curso Superior de Tecnologia em Informática - Modalidade Teleinformática, Dainf, Cefet/Pr, 2003.
6. MYSQL.net. Disponível em: <http://www.mysql.com> Acesso em:Agosto 2003.
7. PHP.net. Diponível em: < http://www.php.net> /Acesso em: todo período.
8. Kiewie S., Figueiredo E. F., Segurança Máxima. Rj Editora Campus, 2001.
9. IBM-Tivoli. Disponível em: < http://www.ibm.com > Acesso em: Agosto 2003.