

DIA 10/03/2017

Nesse dia houve uma interrupção no *datacenter* da COIN devido a um superaquecimento por conta de mau funcionamento dos aparelhos de ar condicionado. Boa parte dos sistemas ficaram inacessíveis, pois, os equipamentos desligaram automaticamente ao alcançar a temperatura máxima de funcionamento. Ainda pela manhã do mesmo dia os serviços foram restabelecidos e uma manutenção dos equipamentos de ar condicionado foi solicitada. A manutenção dos aparelhos foi realizada e até a presente data não voltaram a apresentar mau funcionamento, outrossim, há a necessidade de substituição de 2 dos 4 os equipamentos de ar condicionado do *datacenter*, isso ainda está sob análise de qual tipo de equipamento solicitaremos, considerando o fato que esses equipamentos nunca são desligados.

DIA 20/03/2017

Por volta das 10h a Seção de Segurança recebeu um comunicado da Divisão de Desenvolvimento, relatando sobre uma lentidão anormal nos sistemas administrativos. No diagnóstico, foi identificado uma utilização anormal dos recursos de processamento do *Firewall*, que é o equipamento concentrador de toda a rede da UFGD.

A partir desse momento foram realizados procedimentos que finalizariam o grande número de conexões que o equipamento estava recebendo e causando a lentidão. Foram realizadas várias configurações a fim de impedir que tais conexões exaurissem todos os recursos do equipamento, porém o único método que surtiu efeito, mesmo que por muito pouco tempo, foi sua reinicialização, essa ação foi repetida por 3 vezes.

Verificado que a instabilidade persistia mesmo ao utilizarmos configurações alternativas com o objetivo amenizar o problema, a Seção de Redes iniciou uma verificação do estado da rede nos outros equipamentos responsáveis pela transmissão aos blocos (*switches*). A UFGD possui um *Switch Core* de grande capacidade, sendo que o mesmo não demonstrou alteração em seu funcionamento no período de instabilidade, assim descartamos como um possível problema na rede e retornamos a investigação do *Firewall*.

Entramos em contato com o Suporte da empresa que realizou a venda do equipamento, esta por sua vez, após algum tempo de análise, julgou melhor passar o Chamado da UFGD para o suporte oficial da fabricante do equipamento (SonicWall). O Suporte oficial realizou uma série de testes, procedimento padrão para situações como esta.

Após um bom tempo realizando testes, que causavam grande instabilidade na rede, continuamos sem sucesso na reconfiguração do equipamento, nesse período retornamos a varredura de possíveis

problemas na rede, isolando rede a rede das diversas localidades da UFGD (todos os blocos/setores foram totalmente desconectados, não simultaneamente, por alguns minutos) a fim de eliminar a possibilidade de *loop* na rede (problema gerado quando se fecha uma espécie de “curto-circuito” em equipamentos de rede que não possuem capacidade de prevenção desse tipo de problema). Vale ressaltar que o problema de adição de equipamentos não homologados na rede é recorrente e sempre causa problemas, como os que estavam ocorrendo na Unidade 1 nos últimos dias, geralmente graças à indiferença das chefias e displicência dos usuários quanto a esse problema (já que sempre que nos deparamos com problemas do tipo, tentamos conscientizar as pessoas, sem sucesso).

Felizmente, quando isolamos toda a rede Acadêmica, os demais equipamentos da rede voltaram a operar de forma normal, restaurando completamente a estabilidade da rede. Após isso, iniciamos a busca do local do problema que estava causando interferência no *Firewall*, nos blocos das faculdades e laboratórios.

Por meio de análises nas conexões do Switch Core e de alguns *Switches* de alguns blocos, notou-se que os Blocos CDOC, FCS e MULTIDISCIPLINAR possuíam um nível muito alto de processamento nos *switches* locais, o que poderia ser um indicador do problema.

Foram realizadas buscas nas salas dos blocos para encontrar equipamentos como HUBs e Roteadores não homologados (possíveis causadores do problema), porém não foi encontrado nada fora da normalidade, o que nos faz pensar que o usuário possivelmente trazia o equipamento de casa e usava o mesmo no seu horário de expediente e/ou aula.

Não é possível afirmar que o problema realmente foi esse, já que o impacto dessa vez foi maior do que o comum e porque não encontramos o equipamento durante nossa busca, entretanto, ainda é plausível já que o usuário pode ter suspeitado que seu equipamento era o causador do problema na rede e, por conta disso, não teria religado, mantendo assim a rede operacional.

Outra possibilidade é que, como a rede Acadêmica ficou desligada por alguns dias, o usuário pode ter desistido de utilizá-lo devido à indisponibilidade da rede acadêmica, onde o provável equipamento estava conectado.

Esse problema todo ocorreu em um período que a redundância do equipamento *Firewall* foi enviado para troca em garantia (a solução de *Firewall* é composta por dois equipamentos que trabalham em redundância, quando um apresenta qualquer tipo de problema o redundante assume toda a carga da rede de modo transparente para que não haja instabilidade na rede). Na falta da redundância, quando o *Firewall* travava e/ou reiniciava, todas as conexões de rede eram interrompidas.

No dia 23, após a chegada do equipamento de redundância da garantia, deu-se início à configuração que garantiria a estabilidade da rede mesmo em momentos onde houvesse um grande tráfego de rede causado na rede Acadêmica.

A configuração foi finalizada no dia 27, com a ajuda do suporte SonicWall e Altasnet. Desse dia em diante, não houve mais travamentos, mesmo sendo reestabelecida toda a comunicação de rede nos blocos que apresentaram o problema já mencionado. Até o dia de hoje (05/04/2017) não foi observado qualquer tipo de instabilidade.

O *Firewall* vem mantendo uma boa performance e estabilidade, de forma que toda a rede está operacional de forma consistente. Porém ainda é preciso reestabelecer alguns recursos que foram desabilitados enquanto se buscava a fonte do problema que ocorreu.

Um destes recursos é a autenticação, que é usada para registrar os acessos de todos usuários da rede da UFGD, registro este que é exigido pelo Marco Civil da Internet.

Recursos como a Autenticação serão reestabelecidos conforme for observada a total estabilidade da rede, de forma que isso não comprometa os sistemas institucionais e o acesso à internet por parte dos usuários. Esse recurso já foi causa de vários problemas de instabilidade no ano de 2016, entretanto, o fabricante nos enviou algumas atualizações de software que reduziram consideravelmente esses problemas. Já fomos informados de uma nova atualização que promete otimizar ainda mais o recurso de autenticação, essa atualização será aplicada nos próximos dias.

Seguimos monitorando os recursos de rede e possuímos um processo de aquisição de algumas licenças de software que nos permitirão monitorar e detectar possíveis problemas de rede em tempo real. Ao mesmo tempo, estamos em contato direto com o Suporte Oficial do fabricante do equipamento para que sejam aplicadas medidas que possam impedir que tal instabilidade ocorra novamente.

Dia 30/03/2017

A UFGD possui quatro *storages* (equipamentos específicos para armazenamento de dados que são utilizados nos servidores dos sistemas hospedados no *datacenter*) em produção, três desses equipamentos são bem antigos, com mais de 8 anos de uso ininterruptos. Duas *storages* são do modelo Dell PS6000, nesse dia uma delas apresentou instabilidade em seu funcionamento, os volumes de armazenamento nela alocados foram desligados, ficando inacessíveis. Algumas máquinas virtuais, o servidor de arquivos Zeus e outros serviços da UFGD dependem de acesso a estes volumes para seu correto funcionamento. A equipe buscou descobrir o que estava causando esse desligamento dos volumes da *storage*, entretanto, o problema não ficou nos registros de erro do equipamento. Como esse é um equipamento antigo, com diversos discos danificados, a possibilidade de a placa controladora do equipamento estar danificada é alta. Para sanar este erro a solução encontrada foi desligar todo o equipamento e religá-lo novamente (isso foi realizado pelo menos 3 vezes), dessa forma os volumes do equipamento ficaram disponíveis novamente. Com os volumes novamente acessíveis, as máquinas virtuais precisam ser reiniciadas para que o acesso seja restabelecido, o que nos leva a outro problema: O SVM1, um dos servidores de máquinas virtuais (Virtual Machines – VMs), quando desligado, não volta a ligar de imediato podendo levar mais de horas para voltar a funcionar, provavelmente devido a um defeito em sua placa-mãe (já realizamos troca de outras peças mas o problema persiste), pois, assim como a *storage* PS6000, esse servidor é um equipamento muito antigo. Ações para migração destes serviços para os novos equipamentos instalados em 2016 já estão em curso, mas a pequena quantidade de licenças do software VMWare nos limita na utilização desses equipamentos mais novos (já encaminhamos a solicitação de mais licenças), devido a este tempo que o servidor de VMs demora para voltar, as máquinas nele alocadas, bem como os sistemas ali instalados, ficam indisponíveis durante todo esse tempo.

Dia 05/04/2017

A *storage* voltou a apresentar o mesmo defeito. A mantivemos desligada por alguns minutos e ao religarmos os dados voltaram a ficar acessíveis novamente. Realizamos várias ações para evitar reinicializar o servidor SVM1 por causa do problema informado anteriormente. Alguns sistemas voltaram a funcionar no mesmo dia, entretanto o acesso aos dados na *storage* problemática está sensivelmente mais lento, dessa forma estamos acelerando o possível para concluir a migração dos sistemas para outra estrutura. Como esse equipamento se mostrou totalmente não confiável, estamos avançando um processo de compras que expandirá a *storage* instalada em 2016 para que possamos armazenar essas informações no equipamento mais novo e que ainda possui contrato de garantia.

Infelizmente todos esses problemas ocorreram sucessivamente e se somaram, causando um efeito para quem observa de fora como se fosse um único problema. Conseguimos solucionar alguns desses problemas e estamos concluindo outros alocando pessoal de equipes diferentes para auxiliar na aplicação de uma solução de cada vez, pois, não conseguimos atuar em todas as áreas simultaneamente devido à característica do nosso quadro de pessoal. Essas ocorrências devem atrasar um pouco mais o cronograma de implantação da solução de rede *wifi*, já que é essa mesma equipe mista que está alocada para essa tarefa.