

Evolução do Serviço de Monitoramento da RNP

Emmanuel Gomes Sanches, Paulo Maurício Júnior,

Rede Nacional de Ensino e Pesquisa, R. Lauro Muller 116 / 1103, 22290-906 - Rio de Janeiro, Brasil
emmanuel.sanches@rnp.br, paulo.junior@rnp.br

Resumo: Este trabalho tem por objetivo compartilhar a experiência da RNP na promoção da evolução do seu serviço de monitoramento que teve como principal motivação estabelecer um maior controle da operação e melhor gestão da infraestrutura de comunicação da rede acadêmica brasileira, assim como de seus serviços agregados de comunicação e colaboração. Em uma mudança na sua filosofia de trabalho a RNP decide ampliar significativamente sua responsabilidade de suporte e monitoramento, incluindo as conexões de clientes com a rede acadêmica no seu escopo de monitoramento, trabalho que antes ficava a cargo das equipes de cada um dos seus pontos de presença nacional. Portanto descreve as necessidades de melhoria identificadas, a estratégia adotada, seu plano de ação ao longo de 2 anos, suas dificuldades, as soluções encontradas e os benefícios que essa evolução do serviço de monitoramento proporcionou para a gestão de infraestrutura da RNP e conseqüentemente para seus clientes. Finalmente aponta quais deverão ser os próximos passos já definidos que a RNP está seguindo na continuidade da melhoria.

Palavras chave: Gestão de redes, gestão de serviços, disponibilidade, monitoramento de rede, monitoramento de serviços, monitoramento de datacenter, arquitetura distribuída

Eixo temático: Infraestrutura e desenvolvimento de software

1. Introdução

1.1. Sobre a RNP

A Rede Nacional de Ensino e Pesquisa (RNP) [1] foi criada em 1989, pelo Ministério da Ciência, Tecnologia e Inovação (MCTI) [2], para construir uma infraestrutura de internet acadêmica. Desde então, participa do desenvolvimento da internet no Brasil, com a introdução de novas tecnologias e a implantação da primeira rede óptica acadêmica da América Latina, em 2005, batizada de Rede Ipê. Portanto a RNP é a *National Research and Education Network* (NREN) brasileira, que proporciona à comunidade acadêmica do país serviços de conectividade e de comunicação e colaboração, disponibilizados através de uma infraestrutura de rede predominantemente sobre TCP/IP.

1.2. Sobre a Rede Ipê

A rede da RNP (Rede Ipê) é composta por um conjunto de enlaces que interconectam 27 PoPs (Pontos de Presença), formando uma malha óptica, espelhados por todo o país (Figura 1). As instituições clientes da RNP se conectam nacionalmente à Rede Ipê através dos PoPs, através de redes metropolitanas próprias existentes ou através de circuitos contratados de provedores de Internet.

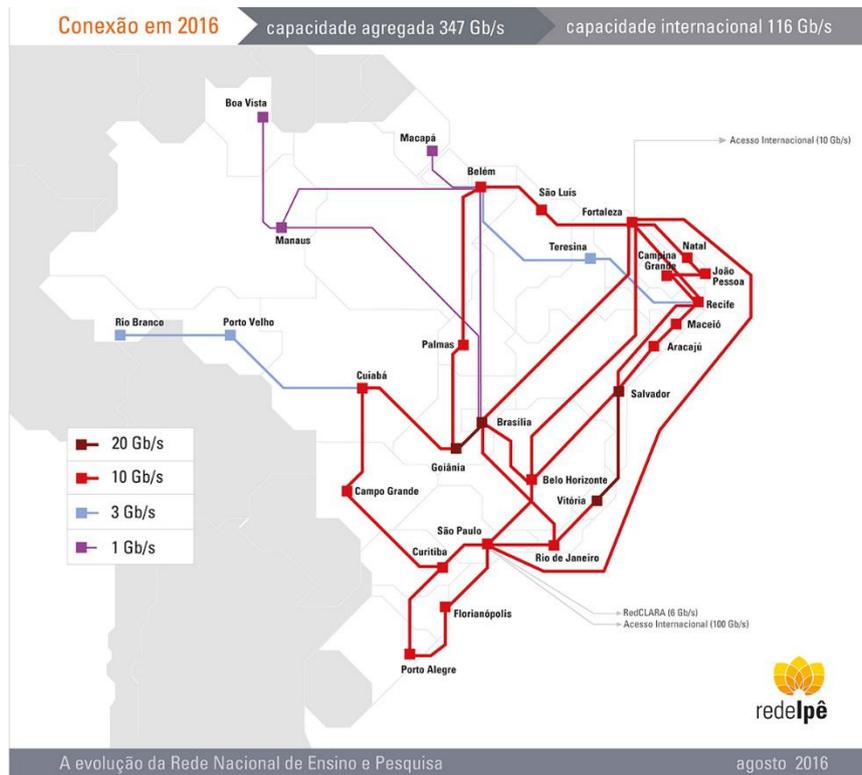


Fig. 1. Cenário de topologia da rede Ipê e seus 27 PoPs em dezembro de 2016

1.3. Sobre o NOC

O Núcleo de Operações de Redes da RNP ou *Network Operation Center* (NOC) tem por objetivo fazer todo o monitoramento de interesse da RNP através de ferramentas especializadas e equipe em regime 24x7. Sua missão primária é monitorar os enlaces que formam o *backbone* da Rede Ipê, acompanhando os seus estados e o correto funcionamento de importantes serviços disponibilizados aos clientes da RNP. A gestão de suas atividades assim como o planejamento e implementação de sua evolução são feitos pela Gerência de Tecnologia da Informação (GTI), uma das

gerências da Diretoria de Engenharia e Operações (DEO), da RNP. Além do monitoramento e análise de falsos positivos para acionamento das equipes técnicas responsáveis pela recuperação, a equipe do NOC faz ainda a operação de primeiro nível dos enlaces da Rede Ipê (*backbone*). A partir da identificação de uma falha ou incidente a equipe de operadores do NOC aciona o analista responsável pela disciplina afetada para a recuperação do serviço (Figura 2).

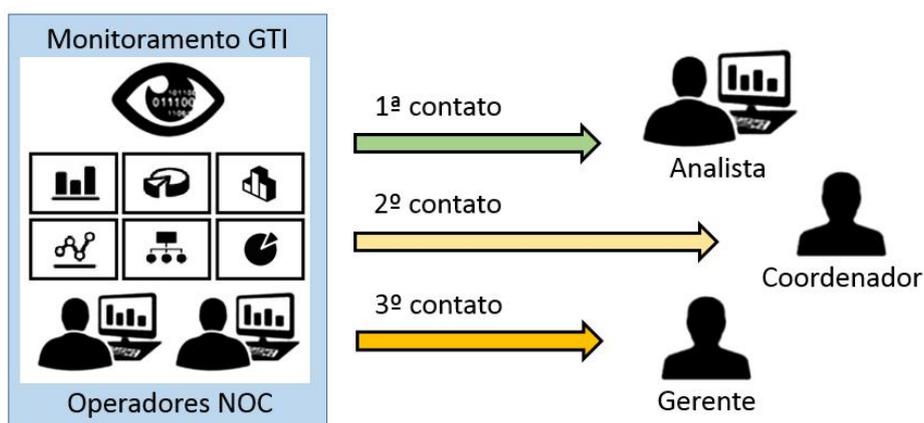


Fig. 2. Processo de monitoramento e escalonamento a cada 10 minutos

2. Cenário inicial

Até 2014 o NOC da RNP fazia o monitoramento da conectividade da rede e do status da infraestrutura de TI residente em seu datacenter principal (IDC) em Brasília, DF, com ferramentas como NAGIOS [3] e [4], CACTI [5] e OpManager [6], através de protocolo SNMP. Dessa forma, uma eventual falha na rede de comunicação ou na infraestrutura que comporta seus serviços avançados podia ser identificada rapidamente. Apesar do serviço regular de monitoramento estabelecido, a RNP continuava sendo surpreendida eventualmente com algumas dificuldades:

- Atuação reativa em situações de falha na recuperação da conectividade dos clientes com os PoPs
- Falta de visibilidade na identificação de serviços afetados em caso de falha na infraestrutura de TI
- Ausência de estatísticas de disponibilidade dos seus serviços
- Dependência de relatórios das equipes dos PoPs para acompanhamento da saúde da conectividade das instituições usuárias
- Falta de padronização e qualidade (variável) nas informações para a gestão do serviço de conectividade

3. Objetivo

A partir deste cenário a GTI decidiu elaborar um plano para promover a evolução do monitoramento para melhoria da qualidade da sua gestão, através da inserção de novas ferramentas, ampliação do seu escopo de atuação e readequação de sua equipe, alinhada com as demais gerências da DEO. Com isso esperava-se ter uma atuação mais proativa, diminuir o tempo de recuperação, aumentar a disponibilidade dos seus serviços e elevar a satisfação de seus clientes.

4. Estratégia

Para a construção do plano de evolução do monitoramento foi adotada a seguinte abordagem:

Identificar possibilidades de melhoria no serviço. Para tal definimos as seguintes ações:

- Observar anseios das áreas clientes
- Reavaliar ferramentas de monitoramento
- Redefinir o escopo de monitoramento

Estabelecer *roadmap* para evolução do escopo. Os seguintes tipos de monitoramento foram identificados como necessários para melhoria da gestão:

- Monitoramento da Disponibilidade
- Monitoramento da Performance
- Monitoramento da Qualidade

O NOC já fazia monitoramento da disponibilidade de diversos ativos e serviços da RNP, entretanto poderia ser melhorado. Após este trabalho melhoria deveremos avaliar a performance dos objetos monitorados para em seguida definir métricas de qualidade e avaliar o cumprimento das mesmas.

Iniciando pela análise do monitoramento da disponibilidade, estabelecemos o seguinte escopo:

- Melhoria do monitoramento da Conectividade
- Melhoria do monitoramento da Infraestrutura de TI
- Estabelecer o monitoramento dos Serviços Avançados para clientes
- Estabelecer o monitoramento dos Serviços Internos (corporativos)

5. Nova arquitetura de monitoramento

No modelo adotado anteriormente, todas as ferramentas utilizadas faziam o monitoramento da rede de forma centralizada, geralmente em um servidor localizado no seu datacenter principal (IDC), estabelecendo um ponto de falha no serviço. Por exemplo, em uma situação onde ocorresse uma falha na comunicação de um dos PoPs com a Rede Ipê, a RNP perdia a informação de funcionamento do datacenter do PoP e da comunicação desse com todas as suas instituições clientes, sem possibilidade de recuperar o histórico desse monitoramento (Figura 3).

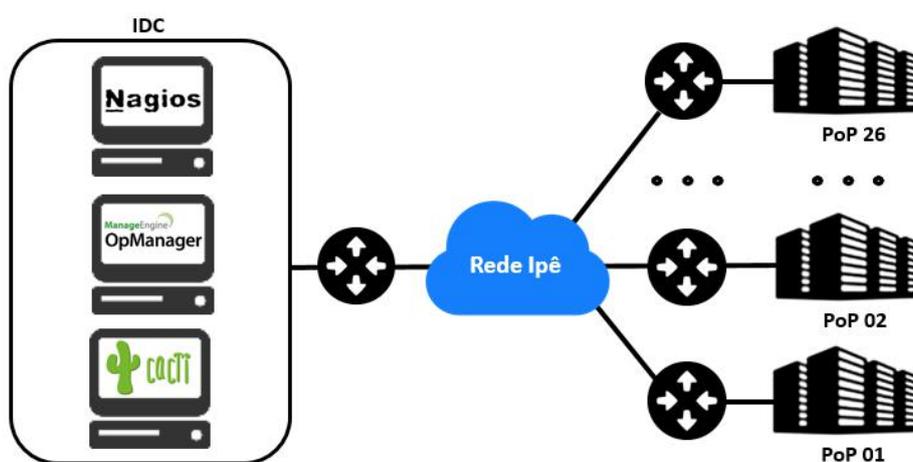


Fig. 3. Arquitetura da solução anterior com monitoramento centralizado

Em 2015 a GTI iniciou estudo para avaliação de outras soluções para monitoramento de sistemas distribuídos [7] de forma atender seu cenário de infraestrutura distribuída geograficamente e em sua conclusão optou por adotar uma nova ferramenta de monitoramento denominada Centreon [8] ainda neste mesmo ano.

Ao contrário da solução anterior, esta nova solução possui arquitetura distribuída, com desenvolvimento baseado no código do Nagios, onde elementos distribuídos (*pollers*) coletam informações de monitoramento e encaminham para um servidor central fazer a consolidação (Figura 4).

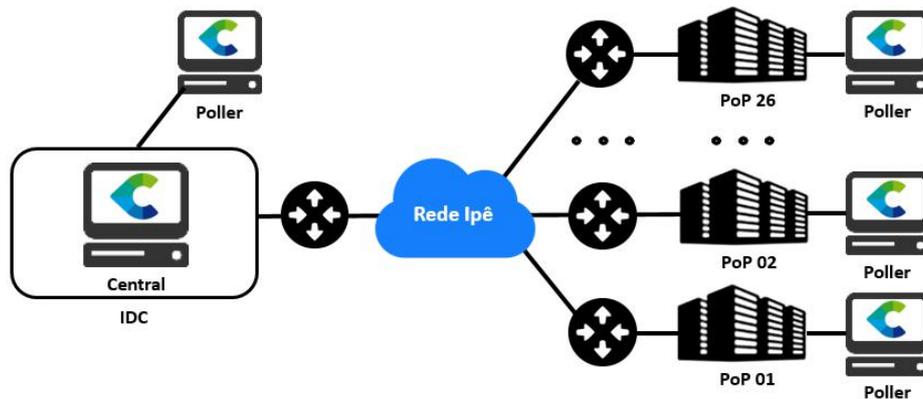


Fig. 4. Arquitetura da nova solução adotada com monitores (*pollers*) distribuídos

Esta solução provê maior disponibilidade ao serviço de monitoramento, se tornando resiliente (capacidade de recuperação) a falhas de comunicação com sites e/ou ambientes remotos a serem monitorados. Em caso de perda de comunicação com um dos hosts a serem monitorados, o elemento remoto (*poller*) da arquitetura distribuída continua coletando estatísticas locais de monitoramento (Figura 5). Ao reestabelecer a comunicação o *poller* local atualiza o servidor Central e o sistema não perde o cenário geral de monitoramento.

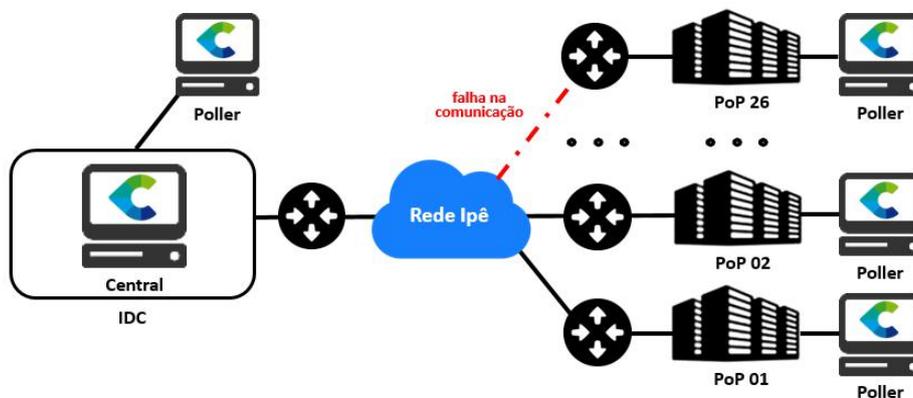


Fig. 5. Exemplo do modelo de alta resiliência onde serviços no datacenter do PoP 26 continuam sendo monitorados durante situação de falha na comunicação

A GTI já instalou até o momento 21 servidores *pollers* e está atualmente monitorando 1.037 hosts com um total de 3.012 elementos. Desta forma as ferramentas de monitoramento do NOC estão sendo gradativamente substituídas por uma solução mais robusta e com maior capacidade de monitoramento. Isso sem necessidade de aumento do orçamento, conforme a mesma possui código aberto.

6. Escopo do monitoramento

A partir da avaliação de atuação do NOC na contribuição com a gestão da rede e dos serviços da RNP, foi definido o seguinte conjunto de objetos a serem monitorados a ser estabelecido (Figura 6):

- | | | |
|---|---|--------------|
| ○ Monitoramento da Rede Ipê monitorado | - | Já |
| ○ Monitoramento de clientes das Redes Metropolitanas monitorado | - | Já |
| ○ Monitoramento da Infraestrutura de TI monitorado | - | Já |
| ○ Monitoramento dos Serviços corporativos da RNP | - | Implementar |
| ○ Monitoramento dos Serviços avançados para clientes | - | Implementar |
| ○ Monitoramento dos circuitos internacionais | - | Internalizar |
| ○ Monitoramento dos circuitos nacionais <i>Out of Band</i> | - | Implementar |
| ○ Monitoramento da conectividade dos clientes | - | Implementar |

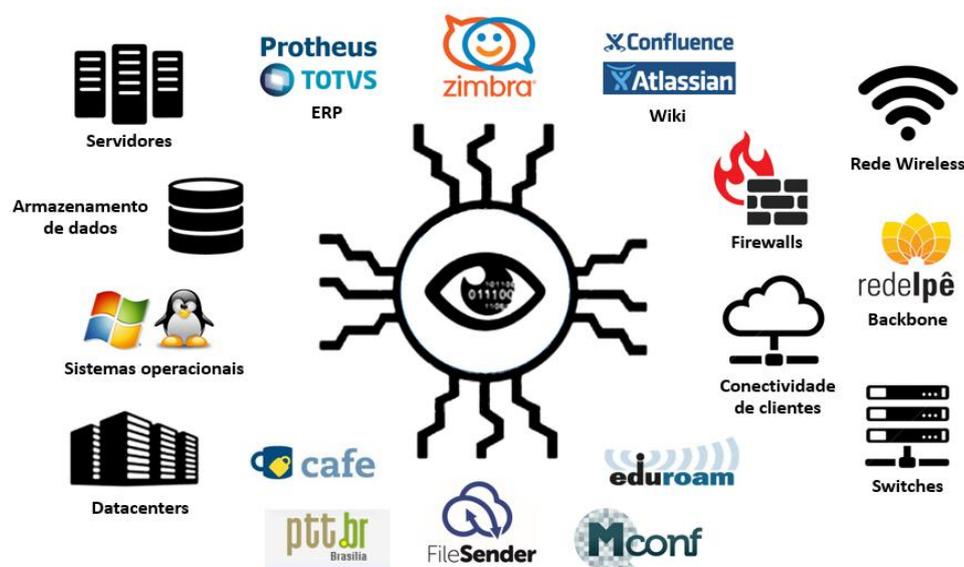


Fig. 6. Exemplos de objetos de monitoramento da RNP, tais como infraestrutura de rede, TI, datacenter, serviços avançados, corporativos e etc.

6.1. Sobre os Serviços Avançados

A RNP possui um conjunto de serviços oferecidos através da sua Rede Ipê, que são disponibilizados para todos os seus clientes, contribuindo com seus processos e

reduzindo custos para essa comunidade. Os serviços disponíveis atualmente podem ser agrupados nas seguintes categorias:

- Serviços de colaboração e comunicação
 - Webconferência
 - fone@RNP
 - Telepresença
 - Videoconferência
- Serviços de Conteúdo Digital
 - Transmissão de vídeo ao vivo
 - Transmissão de sinal de TV
 - Vídeo sob demanda
 - Videoaula@RNP
 - FileSender@RNP
- Serviços de Gestão de Identidade
 - Comunidade Acadêmica Federada (CAFe)
 - eduroam
 - Infraestrutura de Chave Pública para Pesquisa e Educação (ICPEdu)
- Serviços de Hosting Estratégico
 - Internet Data Center

No escopo da ação de evolução do monitoramento da RNP, com a introdução da nova ferramenta (Centreon) o NOC passou a ter visibilidade específica da disponibilidade de todos esses serviços e não apenas identificar problemas na infraestrutura de TI dos mesmos para ter que concluir sobre a indisponibilidade de um serviço.

Para tal foi feito o levantamento do conjunto de todos os componentes que formam um serviço e construído um mapa de interdependência entre esses componentes para que o diagnóstico do problema seja mais facilmente identificado, permitindo o acionamento mais acertado da equipe responsável técnica por recuperar tal componente.

6.2. Sobre os datacenters da RNP

A RNP possui atualmente 3 datacenters próprios, conforme descrito a seguir:

- IDC-DF: Internet Data Center, localizado em Brasília
- CDC-AM: Container Data Center, localizado em Manaus
- CDC-PE: Container Data Center, localizado em Recife

Desta forma a RNP estabelece presença estratégica distribuída em regiões do Brasil de forma a atender demandas de processamento e armazenamento de seus clientes com melhor performance.

Para monitorar a infraestrutura de seus datacenters, que é composta pelos sistemas de fornecimento de energia e climatização de precisão, a RNP utiliza uma ferramenta de DCIM (*Data Center Infrastructure Manager*) específica denominada DataFaz [9].

Além de monitorar circuitos elétricos e acompanhar o consumo da infraestrutura de TI e refrigeração, coleta ainda dados de sensores de fumaça, temperatura, umidade e inundação.

6.3. Sobre a infraestrutura de TI

A infraestrutura de TI é composta por todos os equipamentos que implementam as redes locais da RNP e seus serviços (switches, servidores, blades, storages, firewalls e etc.). Os mesmos estão distribuídos atualmente em 5 localidades.

6.4. Sobre os serviços corporativos

Os chamados serviços corporativos (correio eletrônico, Intranet, wiki, VPN, ERP, etc.) são disponibilizados exclusivamente para usuários da RNP para apoiar na sua operação e produtividade.

6.5. Sobre a conectividade de instituições clientes

Entre as ações que compõem o esforço da RNP para evolução do seu serviço de monitoramento está o projeto denominado “Monitoramento Integrado” que tem como objetivo ampliar o escopo de monitoramento do NOC, que antes observava apenas a disponibilidade das conexões que formam o *backbone* da Rede Ipê e a infraestrutura dos serviços ofertados via rede. A partir deste trabalho, o NOC também passou a monitorar as conexões de cada um dos clientes da RNP com os respectivos PoPs.

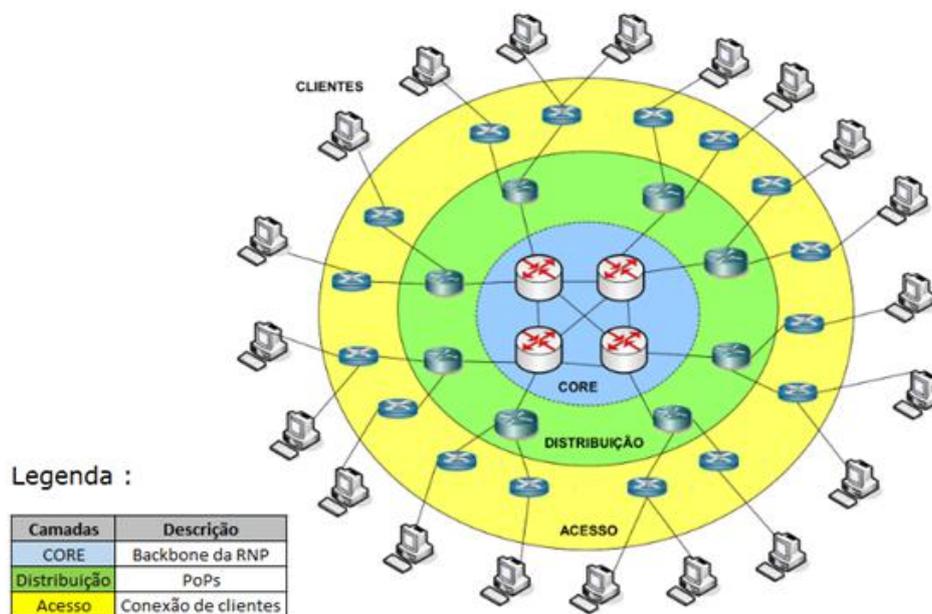


Fig. 7. Camadas de comunicação da Rede Ipê representando as fases de ampliação do escopo de monitoramento da RNP.

Após o levantamento dos elementos a serem monitorados em cada PoP a RNP implementou a infraestrutura de monitoramento de arquitetura distribuída, formada por servidores pollers em cada PoP. A partir daí passou a monitorar a saúde da comunicação de cada cliente com o respectivo PoP de acesso à Rede Ipê (Figura 7).

Ao longo da implementação deste projeto que iniciou em 2015, a RNP vai tendo uma maior visibilidade do estado geral da comunicação de todos os clientes da Rede Ipê. Esta ação tem objetivo de incluir seus 27 PoPs e cerca de 1.237 instituições no escopo de monitoramento do NOC.

Em 2017 a RNP está dando continuidade nesta ação, que dezembro de 2016 foram adicionados no monitoramento cerca de 497 roteadores (hosts), impactando num aumento de 1.627 elementos a serem monitorados pelo time do NOC. Nesta fase do projeto já foram incluídos 10 dos 27 PoPs operando neste novo modelo de gestão da rede:

- PoP-AL – 77 itens monitorados
- PoP-CE – 227 itens monitorados
- PoP-DF – 241 itens monitorados
- PoP-PA – 226 itens monitorados
- PoP-PR – 138 itens monitorados
- PoP-RJ – 171 itens monitorados
- PoP-RN – 148 itens monitorados
- PoP-SE – 72 itens monitorados

- PoP-SP – 257 itens monitorados
- PoP-TO – 70 itens monitorados

Com isso a RNP que antes monitorava apenas o seu *backbone* (vide camada core na figura acima) passa a monitorar também os PoPs (camada de distribuição) e todas as suas instituições clientes (camada de acesso). Isso já está permitindo a RNP fazer uma atuação pró ativa na gestão da conectividade das suas instituições clientes, identificando eventuais falhas antes que o cliente perceba, que regularmente passou a ser avisado do incidente.

7. A evolução do monitoramento no tempo

Até 2014 o NOC já realizava o monitoramento da Rede Ipê e Infraestrutura de TI, entretanto com a conclusão do estudo para avaliação de ferramentas em 2015, todo este escopo precisou ser reintroduzido, desta vez na nova ferramenta (Centreon).

Ainda em 2015 foram inseridos no escopo de monitoramento do NOC:

- Serviços Avançados, disponibilizados através da Rede Ipê para as instituições clientes da RNP
- Circuitos “*out of band*”, que fazem redundância da comunicação dos roteadores da Rede Ipê através de uma rota alternativa pela Internet

Outra mudança que ocorreu foi a iniciativa para ampliar o escopo do monitoramento da rede até alcançar a conectividade das suas instituições clientes. Esta ação iniciou em 2015, continuou a ser feita em 2016, está sendo feita em 2017 e terá prosseguimento até 2018 para conseguir incluir todas as 1.237 instituições clientes.

Anteriormente a RNP contratava um serviço de monitoramento para os links internacionais, mas em 2016 este trabalho acabou sendo internalizado pelo NOC. No mesmo ano a RNP implementou o monitoramento dos seus serviços corporativos (cerca de 40).

8. O monitoramento em números

Atualmente o NOC da RNP monitora somente através da ferramenta Centreon um total de 5.450 itens, sendo que 1.277 relativos a hosts (máquinas) e 4.223 elementos (memória, CPU, armazenamento, indicadores de banco de dados, componentes de serviços, aplicações e etc.). Observando alguns dos principais grupos monitorados pelo NOC, podemos destacar:

- Monitoramento da Rede Ipê com 191 itens, sendo 39 hosts e 152 elementos

- Monitoramento dos PoPs, inclui as conexões com as Redecomeps e todos as instituições cliente conectadas aos PoPs, totalizando 1.635 itens, sendo 508 hosts e 1.127 elementos
- Monitoramento dos serviços avançados da RNP para suas instituições clientes com 747 itens, sendo 83 hosts e 664 elementos
- Monitoramento dos serviços corporativos da RNP com 1.272 itens, sendo 126 hosts e 1.146 elementos
- Monitoramento da infraestrutura de datacenters, composta por sistemas de energia e climatização de precisão, com 84 itens

9. Impacto da evolução na demanda sobre o NOC

Com a ampliação do escopo de monitoramento do NOC estabelecido com a inserção dos serviços avançados e da conectividade das suas instituições clientes, tivemos um aumento significativo na demanda sobre o time, representando um incremento de 256% na quantidade de tíquetes abertos pelos operadores (Figura 8).

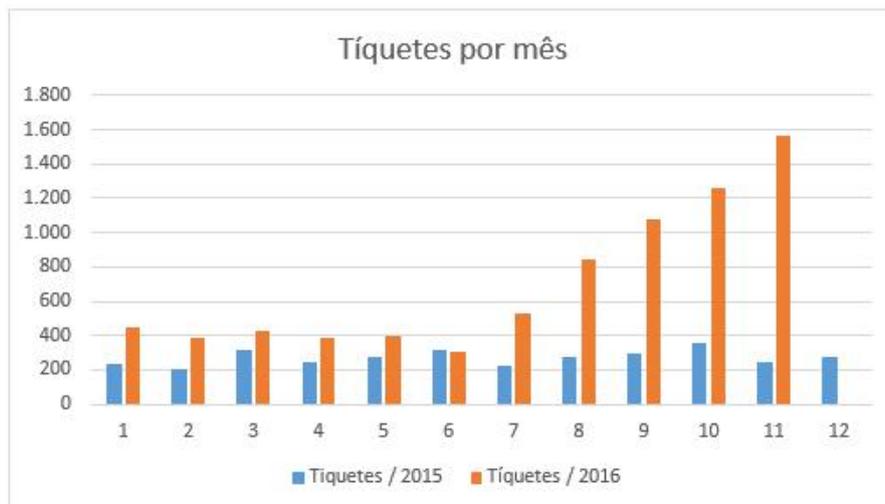


Fig. 8. Evolução da demanda sobre o time do NOC, mostrando aumento de 256%

Portanto observamos que existia uma demanda reprimida por monitoramento que exigiu uma readequação do time de operadores do NOC. Com isso foi necessário inserir mais um operador por turno na equipe.

10. Benefícios e conclusão

Após avaliarmos os resultados obtidos com a implementação do plano de evolução do monitoramento da RNP ao longo deste período de 2 anos, observamos os seguintes benefícios:

A adoção da nova ferramenta (Centreon) proporcionou uma maior disponibilidade e resiliência em caso de falhas, ao serviço de monitoramento da RNP, através de sua arquitetura distribuída onde agentes remotos (pollers) continuam o monitoramento dos ativos (hosts e elementos) de uma dada localidade, mesmo quando essa perde comunicação com o datacenter principal da RNP.

A nova ferramenta possibilitou ainda acrescentar capacidade ao NOC de monitorar não apenas a infraestrutura dos serviços, mas também de realizar testes funcionais para verificar a saúde dos serviços.

A inserção da visibilidade de serviços ao monitoramento da RNP possibilitou um melhor diagnóstico de problemas e maior acerto no encaminhamento dos incidentes para as equipes técnicas de suporte, evitando por exemplo acionar um analista de infraestrutura de TI numa situação onde a falha está sendo ocasionada por um mau comportamento da aplicação que deveria ser encaminhado para a equipe de sistemas.

O diagnóstico mais preciso através do monitoramento dos serviços avançados ocasionou uma maior disponibilidade dos mesmos, conforme diminuimos os seus tempos de recuperação.

A ampliação do escopo de monitoramento através da inserção da conectividade dos suas instituições clientes com os PoPs possibilitou a RNP ter uma atuação proativa na identificação e recuperação dos circuitos e elevar a satisfação geral dos seus clientes.

Todas estas ações possibilitaram que a RNP passasse a fazer um melhor controle, planejamento e suporte aos seus serviços, tanto de conectividade quanto serviços avançados para suas instituições clientes.

Finalmente consideramos que a iniciativa foi bem sucedida e deverá ter continuidade agora em 2017 para aumento da capacidade de gestão dos serviços [10] e [11] da RNP.

11. Próximos passos

Neste momento a RNP continua trabalhando na evolução do seu serviço de monitoramento, implementando as seguintes melhorias:

11.1. Status blog

A RNP deseja disponibilizar para seus clientes um *dashboard* que mostre um panorama instantâneo da saúde e funcionamento de todos os seus serviços, tanto de conectividade quanto sobre os serviços avançados.

11.2. Ferramenta de relatórios

Outra funcionalidade identificada como de interesse das suas instituições clientes é uma interface web que permita gerar relatórios de disponibilidade no tempo, conforme o período desejado, de todos os seus serviços e/ou componentes dos mesmos.

11.3. Monitoramento de performance

Após a conclusão do monitoramento da disponibilidade, a próxima modalidade de monitoramento a ser abordada será o de performance. Este deverá avaliar aspectos dos serviços como por exemplo o tempo de abertura de uma página web, tempo de resposta de um banco de dados, tempo para envio de uma mensagem, assim como o tempo de resposta de qualquer aplicação de interesse.

11.4. Monitoramento da qualidade

Um serviço pode estar disponível mas isso não significa que o mesmo está sendo ofertado com a qualidade esperada. Uma vez tendo os dados relativos a performance dos serviços da RNP, será feito um entendimento com seus clientes, para cada serviço, o que define que tal serviço seja de qualidade. A partir daí estabeleceremos o monitoramento de *thresholds* para avaliarmos se a qualidade desejada de um dado serviço está sendo alcançada. Isso vai permitir que a RNP identifique antes mesmo da ocorrência de um problema de indisponibilidade, que já é necessária uma atuação na melhoria do serviço.

Agradecimentos

Agradecemos à Rede Nacional de Ensino e Pesquisa (RNP) e ao Ministério da Ciência, Tecnologia e Inovação (MCTI) por viabilizarem a elaboração deste trabalho para contribuir com a melhoria da gestão da rede acadêmica e seus serviços para a comunidade.

Referências

1. Rede Nacional de Ensino e Pesquisa, <https://www.rnp.br/>

2. Ministério da Ciência, Tecnologia, Inovações e Comunicações, <http://www.mcti.gov.br/>
3. Josephsen, D., Galstad, E.: Nagios : Building Enterprise-Grade Monitoring Infrastructures for Systems and Networks. Prentice Hall (2013)
4. Barth, W.: Nagios : System and Network Monitoring. Open Source Press GmbH (2008)
5. Costa, F.: Ambiente de Rede Monitorado com Nagios e Cacti. Ciência Moderna (2013)
6. ManageEngine: OpManager, <https://www.manageengine.com/network-monitoring/>
7. Ewaschuk, R., Beyer, B.: Monitoring Distributed Systems: Case Studies from Google's SER Team. O'Reilly (2016)
8. Centreon Documentation, <https://documentation.centreon.com/>
9. DataFaz – DCIM para Data centers, <http://www.datafaz.com/>
10. Magalhães, IL., Walfrido, BP.: Gerenciamento de Serviços de TI na Prática: Uma Abordagem com Base na ITIL, Novatec (2006)
11. Freitas MA: Fundamentos do Gerenciamento de Serviços de TI: Preparatório para a certificação ITIL Foundation. Brasport (2011)