Implantação do Núcleo de Operação e Controle - NOC na UFSM

Luciano A. Cassol[1], **Eduardo Speroni**[1], **Lucimara Dallaporta**[1]

[1]Centro de Processamento de Dados – Universidade Federal de Santa Maria (UFSM)
Av. Roraima, 1000 – Prédio 48. Bairro Camobi
CEP 97105-900 – Santa Maria, RS

{lcassol, speroni, lucimara}@ufsm.br

Resumo. *Com a crescente dependência das pessoas e organizações em relação ao uso de recursos de Tecnologia da Informação (TI), a importância do monitoramento e o gerenciamento de incidentes nos serviços e na infraestrutura de TI torna-se cada vez mais indispensável. Esse trabalho apresenta o processo de implantação e operação do Núcleo de Operação e Controle - NOC no Centro de Processamento de Dados da Universidade Federal de Santa Maria e os resultados obtidos em um ano de operação.*
Palavras-chave: *Monitoramento, Gerenciamento de Incidentes, Zabbix, OTRS, ITIL*

Abstract. *As the dependency on IT resources by the people and organizations increases, the importance of monitoring and incident management of those resources is becoming increasingly indispensable. This paper presents the implementation process of a Núcleo de Operação e Controle - NOC on the Centro de Processamento de Dados of the Universidade Federal de Santa Maria and the results of a year of operation.*
Keywords: *Monitoring, Incident Management, Zabbix, OTRS, ITIL*

1. Introdução

O Centro de Processamento de Dados (CPD) da Universidade Federal de Santa Maria (UFSM) presta serviços de tecnologia da informação a toda comunidade universitária. Desde 2013 iniciou-se um processo de melhoria nos processos internos do CPD como também a reestruturação dos setores. Em 2014 iniciou-se com a organização da gestão de projetos, em específico os projetos de desenvolvimento de software, em 2015 iniciou a utilização do software OTRS (*Open Ticket Request System*) [5]. O OTRS é uma ferramenta *open-source* para a gestão de serviços de TI implementado conforme o *framework* ITIL[1], tendo sido certificado pela entidade `PinkVERIFY`[3] como um software que atende os processos do ITIL, como por exemplo: gerenciamento de incidentes, gerenciamento de mudanças, gerenciamento de nível de serviço (SLA), gerenciamento de itens de configuração, gerenciamento do conhecimento, melhoria contínua de serviço através de pesquisas de satisfação, definição de papéis entre outros. A ferramenta possui diversos módulos e extensões, que expandem suas funcionalidades.

O OTRS começou a ser utilizado pelo CPD em setembro de 2015. A implantação do OTRS foi feita separando as requisições de serviço dos registros e tratamento de incidentes. O registro e tratamento de incidentes foi mapeado através de um processo específico.

Para que o tratamento de incidentes e a posterior prevenção dos mesmos tivesse um efeito prático e positivo foi criado no início de 2016 um setor que seria responsável por esse tratamento de incidentes como também o monitoramento de toda a infraestrutura de TI da instituição. Em Abril de 2016 entrou em operação o Núcleo de Operação e Controle - NOC, que é responsável pelo monitoramento da infraestrutura dos ativos de rede, *datacenter* e os sistemas institucionais.

O Núcleo de Operação e Controle foi implantado com três pessoas, dois analistas de TI e um técnico em TI. O objetivo do núcleo é monitorar toda a infraestrutura de TI e realizar a gestão de incidentes de TI. O monitoramento é realizado através do software Zabbix [4] e o gerenciamento de incidentes é feito através do software OTRS [5].

2. Metodologia

Os incidentes gerados na instituição ficam, em sua maioria, sob responsabilidade do NOC. A Figura 1 mostra o processo de gestão de incidentes que foi implementado no OTRS. Através desse processo é feito o registro do incidente que é encaminhado para tratamento no NOC onde é realizada a classificação de impacto, criticalidade e prioridade. A partir dessa classificação a resolução do incidente é direcionada ao setor específico. Caso seja necessário são outros criados chamados de serviços para resolver o incidente, mantendo os dois registros, tanto o incidente como o novo serviço gerado.

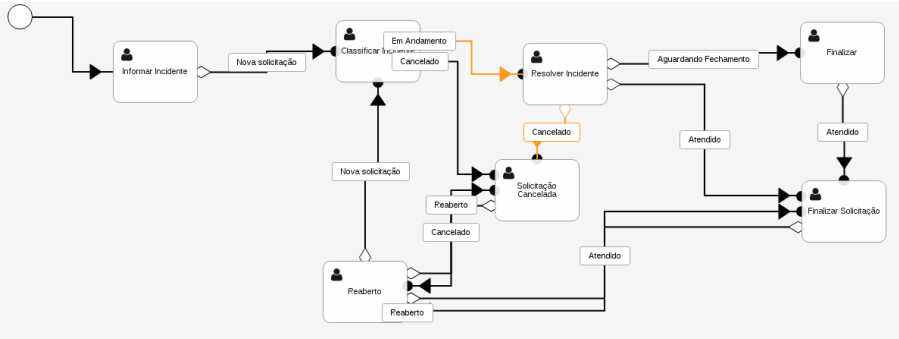

Figura 1. Processo de gestão de incidentes no OTRS

O software Zabbix é utilizado para o monitoramento dos principais ativos de rede, servidores e sistemas. A escolha do Zabbix ocorreu devido ao conjunto de recursos que esse software dispõe como capacidade de auditoria, controle de permissões e facilidade de uso.

Os principais *switches* são monitorados através do protocolo SNMP (*Simple Network Management Protocol* onde é possível obter informações como o estado e banda utilizada em cada porta, informações de temperatura, processamento entre outras. Os *switches* de menor importância tem seu estado verificado por requisições de ICMP Ping, com sua performance medida pela perda de pacotes destas requisições. A Figura 2 apresenta o mapa do *backbone* da instituição e os principais *switches* que estão ligados ao *backbone*. Nesta Figura é possível observar as diversas ligações que a infraestrutura de rede da UFSM tem. Quando ocorre um dos ativos de rede fica inoperante é possível graficamente visualizar a quantidade de unidades da instituição que estão ”fora do ar”.

Além dessa visualização gráfica tendo como base o mapa da instituição uma outra visualização também é importante que é a lista de incidentes que estão ocorrendo no momento. A Figura 3 mostra esse formato de visualização onde é possível verificar quais elementos (*switch*, sistemas, *hosts*) estão com problema e qual o problema detectado.

Foram implantados 3810 gatilhos no Zabbix para alertarem sobre incidentes nos principais *switches*, nos servidores, nos sistemas institucionais e nos serviços oferecidos para a comunidade universitária. A instituição utiliza o sistema de gestão educacional SIE. Esse sistema é desenvolvido em dois ambientes: a parte *Desktop* em Delphi e a parte WEB em Java. Para monitorar os servidores de aplicação do ambiente Delphi foi necessário desenvolver uma aplicação em C# que monitora as aplicações COM+ [2] que são enviadas ao servidor Zabbix. Com essa implementação e o constante

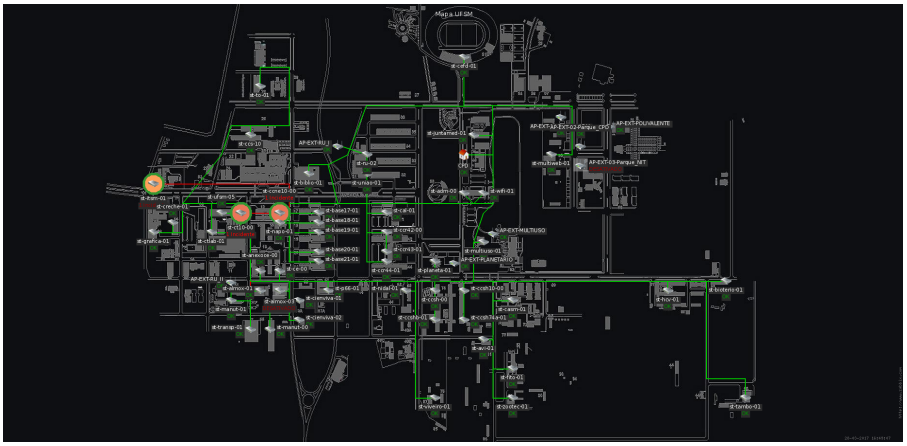

Figura 2. Mapa de monitoramento do backbone da UFSM

monitoramento é possível reiniciar os serviços em caso de travamento, inclusive automaticamente baseado nos dados coletados pelo agente.

Incidentes do grupo de hosts

Host	Assunto ▾	Última alteração	Idade
st-ccne10-00	st-ct10-00 port is down on st-ccne10-00	03-03-2017 13:42:02	23d 20h 10m
st-ct10-00	st-ccne10-00 port is down on st-ct10-00	03-03-2017 13:38:04	23d 20h 14m
st-ccr44-12 (desativado pois desligam na sala)	st-ccr44-12 (desativado pois desligam na sala) is unavailable by ICMP	24-03-2017 09:23:50	3d 28m
st-ccr44-10 (desligam na sala)	st-ccr44-10 (desligam na sala) is unavailable by ICMP	24-03-2017 09:23:48	3d 28m
st-ceu1-4a	st-ceu1-4a is unavailable by ICMP	21-03-2017 22:58:39	5d 10h 54m
Controladora-CISCO_5508	AP-245016-CE is unavailable	07-03-2017 12:17:52	19d 21h 34m
srv-voip-02.net.ufsm.br	TCP 5432 service is down on srv-voip-02.net.ufsm.br	14-02-2017 12:03:01	1m 10d 22h
srv-voip-02.net.ufsm.br	TCP 389 service is down on srv-voip-02.net.ufsm.br	14-02-2017 12:03:00	1m 10d 22h
rd-horta-st	rd-horta-st is unavailable by ICMP	13-02-2017 11:55:56	1m 11d 22h
rd-horta-ap	rd-horta-ap is unavailable by ICMP	13-02-2017 11:55:55	1m 11d 22h
cruzeira.cpd.ufsm.br	HTTP service is down on cruzeira.cpd.ufsm.br	09-02-2017 11:18:36	1m 15d 23h
st-ctlab-12	st-ctlab-12 is unavailable by ICMP	17-01-2017 16:06:31	2m 8d 18h
st-politec-12	Response time is too high on st-politec-12	27-03-2017 09:51:59	47s
rtufsm_interface_externa	Ping loss is too high on rtufsm_interface_externa	27-03-2017 09:51:39	1m 7s
st-ceu2-40	Ping loss is too high on st-ceu2-40	27-03-2017 09:40:25	12m 21s
coralx.ufsm.br	Disk I/O is overloaded on coralx.ufsm.br	27-03-2017 09:32:13	20m 33s
st-ceu2-313	Ping loss is too high on st-ceu2-313	27-03-2017 09:22:23	30m 23s
chimango.si.ufsm.br	Free disk space is less than 20% on volume F:	16-03-2017 16:29:05	10d 17h 23m
cruzeira.cpd.ufsm.br	Ping loss is too high on cruzeira.cpd.ufsm.br	20-02-2017 11:51:43	1m 4d 22h

Figura 3. Lista de Incidentes gerado pelo Zabbix

Além da implementação descrita anteriormente também foi necessário implementar uma aplicação em Python para realizar a coleta de dados do banco de dados institucional IBM DB2. Um serviço em execução no servidor Zabbix mantém um pool de conexões com o banco de dados e monitora a saúde do banco de dados e as operações que são realizadas nele. Para os servidores que necessitam de monitoramento mais fino foi instalado um agente do Zabbix para que seja possível reportar informações de desempenho, como uso de CPU e memória, além de informações de serviços, como operações por segundo de bancos MySQL, se um serviço está sendo executado ou não, ou informações de log. A combinação de monitoramento via agente e monitoramento via servidor possibilita medir com precisão o estado e performance de um serviço, e um gatilho pode ser criado para identificar momentos de instabilidade ou indisponibilidade de serviço.

Com a utilização do software OTRS para o gerenciamento de incidentes e o software Zabbix para o monitoramento foi necessário interligar os dois sistemas. Quando um incidente é identificado no Zabbix o mesmo chama um *web service* do OTRS registrando um *ticket* com as informações do incidente ocorrido. Quando esse incidente é resolvido e o Zabbix não o identifica mais como incidente também é comunicado ao mesmo *ticket* do OTRS gerado anteriormente que o incidente já foi resolvido e o *ticket* do OTRS é fechado. Em algumas situações ocorre que o incidente gerado

através do Zabbix é encaminhado para uma das equipes que irá tratar o incidente e nesse intervalo de tempo o incidente é resolvido. Nesse caso o Zabbix não realiza o fechamento automático do *ticket* mas adiciona informações ao mesmo para que a equipe de tratamento saiba que o incidente já está resolvido.

3. Resultados

A implantação do Núcleo de Operação e Controle - NOC no CPD da UFSM iniciou em abril de 2016, nesse um ano ocorreram avanços significativos no processo de resposta a incidentes. Antes da implantação do NOC os incidentes de TI eram muitas vezes informados e respondidos a partir de notificações do usuário o que acarretava um desgaste desnecessário da imagem dos serviços prestados pelo CPD. Com a implantação do NOC o processo de resposta a incidentes foi sistematizado e não é mais reativo a notificação do usuário.

A Figura 4 apresenta o gráfico de incidentes gerados automaticamente pelo software Zabbix e os incidentes tratados via OTRS pela equipe por mês. É possível notar um número muito maior de incidentes gerados pelo Zabbix do que a quantidade de incidentes tratados via OTRS.

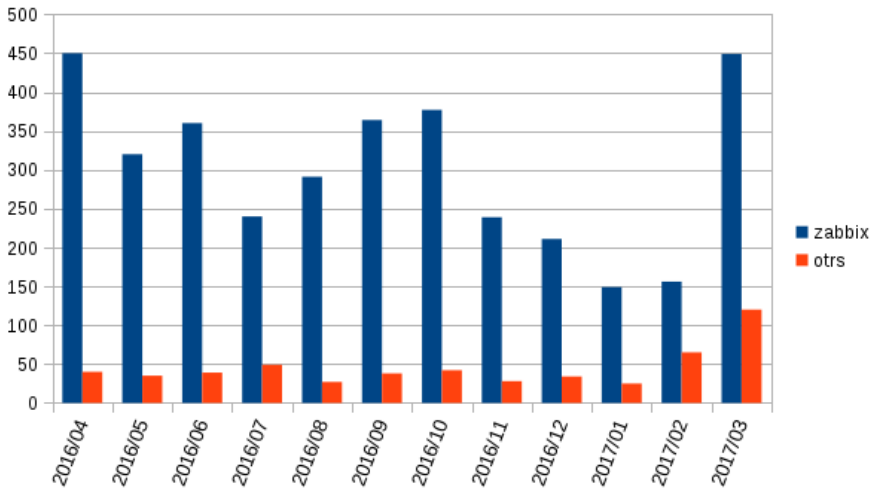

Figura 4. Quantidade de Incidentes tratados via Zabbix x OTRS

Essa diferença ocorre por dois motivos, o primeiro deles é que muitos incidentes relacionados a conectividade são falhas momentâneas e retornam a operação sem intervenção direta. Um outro número são incidentes gerados a partir de um incidente tratado, como por exemplo uma queda em um *switch* do *backbone* ou um travamento de banco de dados. Qualquer um desses dois exemplos gera um conjunto de outros incidentes relacionados a eles.

A Figura 5 apresenta a quantidade de incidentes agrupados por causa raiz. É possível observar que a maior causa de incidentes ocorre devido a inoperância de *switch*. Essa causa tem vinculada a ela diferentes situações como: manutenções não programadas, problemas elétricos, configurações equivocadas entre outros. Para reduzir esse tipo de incidente foi normatizado o processo de manutenção desses equipamentos como também da rede de maneira geral. Um outro incidente que tem uma quantidade significativa é relacionado a problemas de configuração de impressora. Ele ocorre devido a diversidade de impressoras existentes na instituição. Para minimizar esses problemas foram definidas marcas e modelos de impressora que podem ser adquiridos e que tendem a causar uma menor quantidade de incidentes.

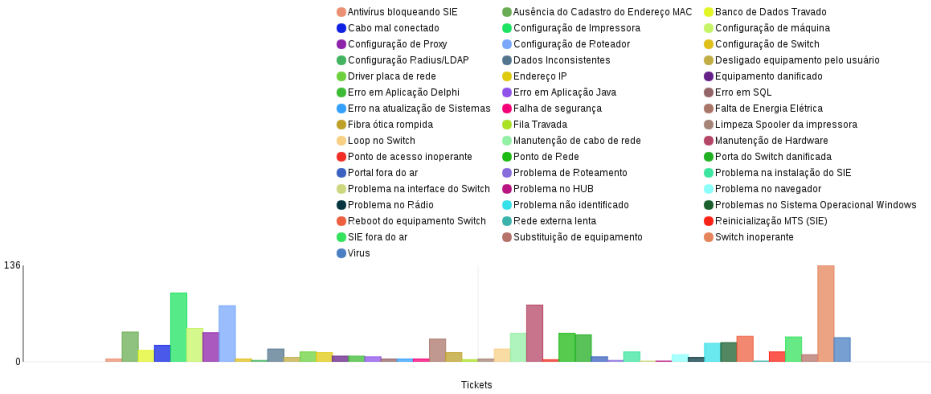

Figura 5. Quantidade de Incidentes tratados por causa raiz

4. Considerações Finais

Atualmente o monitoramento e o gerenciamento de incidentes de TI está sob responsabilidade do Núcleo de Operação e Controle - NOC. Essa responsabilização tem trazido grandes benefícios para o CPD devido a agilidade que o setor tem no processo de gestão e acompanhamento dos incidentes e no monitoramento de incidentes, essas práticas eram antes realizadas de forma *ad hoc* e hoje estão sistematizadas com software e processos adequados para essas ações. A utilização das ferramentas *Zabbix* e *OTRS* permitiu que praticamente qualquer serviço da instituição possa ser monitorado, e novas soluções são desenvolvidas de acordo com a demanda em caso de recursos não nativos.

Alguns desafios ainda se impõe como o aculturamento da importância do gerenciamento de incidentes, do atendimento aos acordos de nível de serviço, mas os dois maiores desafios são relacionados a implantação do processo de gestão de mudanças para a infraestrutura de TI e para os sistemas institucionais e o comprometimento e apoio de toda a unidade em reduzir o número de causas de incidentes e tratar os incidentes de forma rápida e ágil.

Referências

[1] CANNON, D., WHEELDON, D., LACY, S., AND HANNA, A. *ITIL V3.0 - Service Strategy*, 2nd ed. TSO (The Stationery Office), 2011.

[2] CORPORATION, M. Com+ component services. http://msdn.microsoft.com/en-us/library/windows/desktop/ms685978(v=vs.85).aspx, 2017. ”acessado em 18/03/2017”.

[3] ELEPHANT’S, P. Pinkverify toolsets. http://www.pinkelephant.com, 2017. ”acessado em 18/03/2017”.

[4] LLC, Z. Zabbix - the enterprise - class monitoring solution for everyone. http://www.zabbix.com, 2017. ”acessado em 18/03/2017”.

[5] OTRS. Otrs - open tecnology real service. http://www.otrs.com, 2017. ”acessado em 18/04/2017”.