The Price of Freedom is the Eternal Vigilance
Um Arcabouço de Autenticação e Auditoria para Ativos na Rede do Campus AC. Simões da UFAL

Erivaldo L. Mariano[1], **Raul S. C. Vieira**[1],
Marcelo Q. A. Oliveira[1], **Kleymerson P. Lins**[1], **Fabrício F. Carvalho**[1]

[1]Núcleo de Tecnologia da Informação – Universidade Federal de Alagoas (UFAL)
Av. Lourival Melo Mota, S/N – Tabuleiro do Martins – 57072-970, Maceió – Alagoas – Brasil

{erivaldo.mariano, raul.vieira, marcelo, kleymerson, fabricio.carvalho}

@nti.ufal.br

Resumo. *Este trabalho aborda o processo de implantação de ferramentas de AAA no acesso aos ativos na rede do Campus AC. Simóes da Universidade Federal de Alagoas, cujos objetivos são realizar a Autenticação em uma base única e compartilhada com os diversos sistemas da universidade; Autorização diferenciada para diversos perfis de usuários (lotação e permissão de escrita); Auditoria de todo acesso e operação executada em qualquer ativo na rede.*

1. Introdução

Na área da segurança dos ativos da redes, uma prática incentivada por vários autores de material sobre assunto é a utilização de mecanismos de AAA (Autenticação, Autorização e Auditoria/Contabilização[1]).

O atual trabalho traz a experiência da equipe de Redes e Infra-estrutura da UFAL, que não diferente de outras instituições por ser pequena e lida com uma grande demanda de sustentação, de implantar e gerenciar um sistema composto pela coleta de *logs*, e pela autenticação e autorização de usuários nos ativos. O desafio da manutenção de uma rede do porte da UFAL, descrito na Seção 2, está no gerenciamento de acesso, operações e auditoria dos ativos. A segunda motivação está na rotatividade das pessoas que integram a equipe de redes, tornando inviável alterar a senha de todos os *ativos* quando uma usuário sai da equipe, e o terceiro e último é a permissão de acesso e modificação somente para usuários específicos do local onde o ativo está instalado.

O texto é dividido em 5 seções, a 2^a descreve o cenário em que o projeto foi aplicado, a 3^a traz os objetivos da abordagem do projeto, a 4^a a metodologia e os resultados obtidos, e na 5^a seção as considerações finais e trabalhos futuros.

2. Cenário

O cenário encontrado é uma rede de 24 unidades e 3 campi interligados por meio de aproximadamente 150 *Switchs* fabricados pela *Extreme Networks*[2] executando versões do EXOs[3] entre 12.X e 16.X acessados e configurados por meio do Console[4] e SSH[5].

[1]Do inglês: Authentication, Authorizing e Accounting

[2]Fabricante de soluções para redes de computadores. Acessível por `https://www.extremenetworks.com/`.

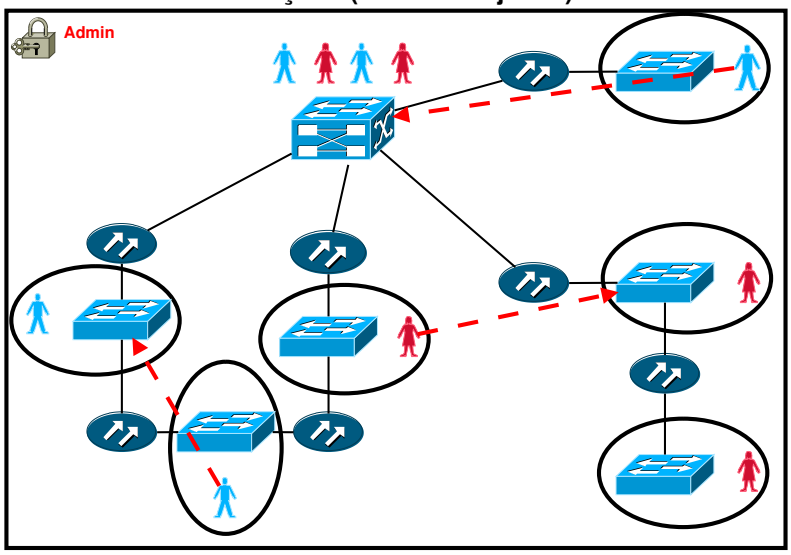
[3]Sistema operacional dos ativos da *Extreme Networks*

[4]Interface de configuração de um ativo acessada por meio de porta serial.

[5]Interface de configuração executada por uma conexão segura, criptografada, que pode ocorrer sobre uma rede não segura.

As alterações eram realizadas por meio de uma credencial padrão[6], o **admin** dos *switchs*, no entanto, a senha era de conhecimento de todos na equipe de redes, como exemplificado na figura 1. Consequentemente, as mudanças e os acessos não eram auditáveis.

Figura 1. Cenário onde todos os ativos possuem a mesma credencial (admin) e os responsáveis (bonecos) por lugares específicos (elipses) podem acessar dispositivos em outras localizações (setas tracejadas).



3. Objetivos

- Autenticar o acesso aos ativos de rede (promoção da irretratabilidade[7]);
- Registrar a entrada e a saída das credencias aos ativos;
- Autorizar o acesso de acordo com o perfil:
  - local do usuário - O técnico do local, previamente cadastrado na base de autenticação, poderá acessar o ativo, porém não poderá acessar ativos de outros lugares.
  - tipo de usuário:
    - **Leitura** - Para usuários que podem identificar um problema na configuração ou na rede, porém não possuem a opção de alterar a configuração do equipamento;
    - **Escrita** - Para usuários que podem realizar a tarefa de **leitura**, porém podem realizar alterações na configuração do equipamento.
- Auditar as alterações executadas na configuração do ativo por meio dos registros de acesso e *logs* de operação.

4. Metodologia

No intuito de atingir os objetivos, duas linhas de frente foram adotadas: o registro de (*logs*), e a autenticação e autorização dos usuários nos ativos.

[6]Apesar de usar a credencial **admin**, que é padrão, a troca da senha era realizada antes da inserção do ativo na rede.

[7]Também conhecido como ”Não repúdio”.

4.1. Registros de *log*

Inicialmente, a equipe determinou a ferramenta de captação de log seria utilizada para receber, armazenar e exibir os *logs* e identificar as *streams*[8] a serem enviadas pelo sistema operacional dos *switchs*.

4.1.1. Escolha do servidor

Duas ferramentas *open-source* foram analisadas: o LogAnalyzer[Adiscon and Community] e o Graylog [Graylog, Inc]. O LogAnalyzer, na versão 3.6.6, é um *frontend* para rsyslog[Rainer Gerhards and Community] que suporta autenticação de acessos, depende de bibliotecas de terceiros para gerar gráficos e não dispõe da completa configuração via interface para configurar o serviço de recebimento de *log* . O GrayLog, na versão 2.3.1, também permite autenticação de acessos, possui ferramentas de gráficos próprias e tem uma maior usabilidade em virtude da configuração ser realizada pela interface *WEB*. Além disso, é capaz de associar outros servidores *Graylog* no intuito de instituir um cluster de processamento de mensagens. A limitação da versão aberta é receber ”somente”5 GB de *logs* por dia.

A melhor usabilidade, a facilidade na configuração e a capacidade de escalabilidade oferecidas pelo *Graylog*, motivou a escolha por esta solução.

4.1.2. Configuração dos ativos Extreme

Nos *switchs* gerenciáveis, foi criado um filtro para enviar, no padrão syslog, as mensagens de *log* correspondentes às *streams* selecionadas. No filtro abaixo, as mensagens de CLI[9], linhas de comando, e AAA, autenticação/autorização/auditoria do acesso do usuário, serão enviadas.

```
create log filter GraylogFilter
configure log filter GraylogFilter add  events cli
configure log filter GraylogFilter add  events AAA
```

Após criação a aplicação do filtro no ativos, é necessário configurá-lo para enviar o *log* ao Graylog, para que o mesmo possa processar e indexar a mensagem. Este procedimento é executado com o seguinte comando:

```
configure syslog add #IP_SERVIDOR_LOG:#PORTA_SERVICO_LOG vr #ROTA local0
enable log target syslog #IP_SERVIDOR_LOG:#PORTA_SERVICO_LOG vr #ROTA local0
configure log target syslog #IP_SERVIDOR_LOG:#PORTA_SERVICO_LOG vr #ROTA local0 \
  filter GraylogFilter severity debug-summary
configure log target syslog #IP_SERVIDOR_LOG:#PORTA_SERVICO_LOG vr #ROTA local0 match Any
configure log target syslog #IP_SERVIDOR_LOG:#PORTA_SERVICO_LOG vr #ROTA local0 format \
  timestamp seconds date Mmm-dd event-name none priority tag-name
```

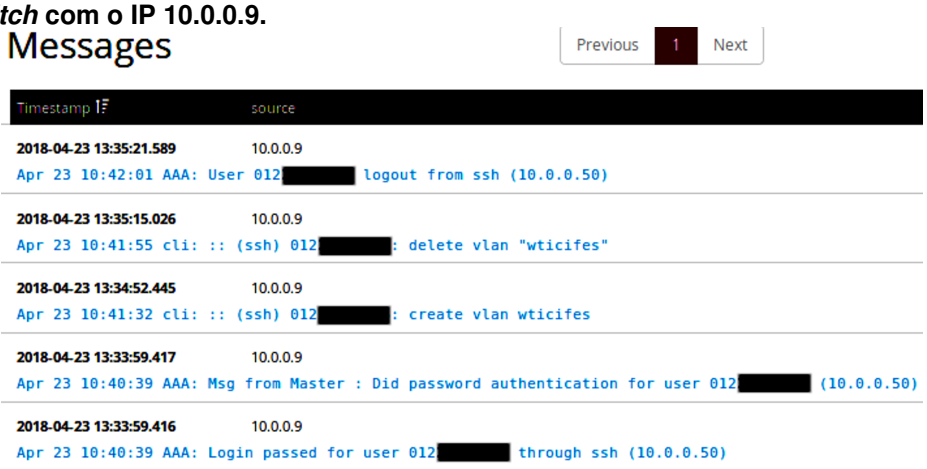
O resultado da registro de *logs* em um consulta a um ativo pode ser verificado na figura 2.

---

[8]Cada fabricante possui uma lista de *streams* especificando o que será enviado para o *log*. Por exemplo, a *stream* POE envia as informações sobre a alimentação de equipamentos pela rede. POE (*Power Over Ethernet*).

[9]Do inglês: Command Line Interface (Interface de Linha de Comando)

Figura 2. Graylog - Mensagens recebidas pelo servidor de *logs* enviadas pelo *switch* com o IP 10.0.0.9.



4.2. Autenticação e Autorização de Usuários

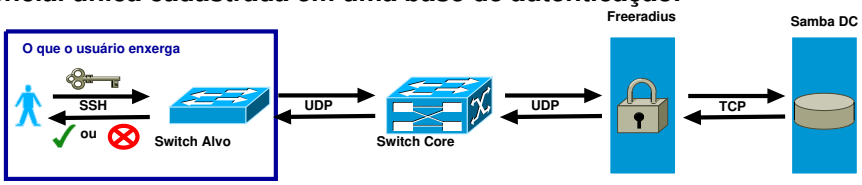
Para a autenticação e autorização dos ativos foram utilizados o FreeRadius[FreeRADIUS Server Project and Contributors], versão 3, também *open-source* e a base de usuários provida por um controlador de domínio SAMBA [Community], já utilizada como autenticação de sistemas utilizados na instituição.

Em um *switch Extreme*, para utilizar o serviço de autenticação, precisa ser configurado com os seguinte comandos:

```
configure radius mgmt-access primary server #IP_SERVIDOR_FREERADIUS #PORTA_SERVICO \
  client-ip #IP_SWITCH vr #ROTA
configure radius mgmt-access primary shared-secret #CHAVE_RADIUS
enable radius mgmt-access
```

Após a configuração, o usuário pode acessar um ativo por meio de um cliente de terminal remoto, preferencialmente SSH, com a credencial pessoal definida no controlador de domínio *samba*. É importante salientar que não é necessário que o usuário configure o seu cliente SSH para poder se autenticar em qualquer equipamento já configurado, ver Figura 3.

Figura 3. Processo de autenticação utilizando o *Freeradius*. O usuário não precisa configurar para ter acesso ao ativo, basta acessar o ativo por meio de sua credencial única cadastrada em uma base de autenticação.



A autorização (permissão) dada ao usuário é definida na configuração do *Freeradius* e na estrutura da árvore do domínio, se baseando na ideia da tupla: (**local do ativo**, **permissão de escrita**). **O local do ativo** representa a localização física de um grupo de ativos e a **permissão de escrita** representa as permissões de leitura (não pode realizar alterações) ou escrita (pode realizar modificações na configuração). Desta forma, é possível designar quais usuários podem acessar/administrar os ativos de um local específico, evitando o cenário proposto na Figura 1.

4.3. Infraestrutura

A especificação descrita na tabela 1 é referente aos servidores virtualizados em produção para cada serviço.

Tabela 1. Especificações de Hardware usada em cada servidor. *Valores de pico baseados em um dia sem incidentes.

Hardware	Autenticação e autorização (FreeRadius)	Registro de log de acesso (Graylog)
VCPUs*	1 (aproximadamente $< 2\%$ de uso)	4 (aproximadamente $< 4\%$ de uso)
Memória*	1024MB (aproximadamente 100MB de uso)	8 GB (aproximadamente 1.52GB de uso)
Armazenamento	30 GB	120 GB

5. Conclusão

Este documento aborda o processo de implantação de AAA nos ativos de redes da Universidade Federal de Alagoas e a partir deste projetos, alguns pontos são considerados como desafios futuros: a aplicação da autenticação 802.1x nos *uplinks*[10] e *downlinks*[11], restringindo acessos à rede não permitidos; no intuito de adicionar confidencialidade ao *log* enviado pela rede e apesar do tráfego destes passar por uma VLAN específica de gerenciamento, é necessário buscar criptografar o envio; implantar tabelas de tempo e permissão por demanda, as quais permitirão um usuário logar em um ativo somente se estiver com a tarefa atribuída e uma data e hora específica; mudar a cultura dos funcionários que ainda usam uma senha padrão, pois é comum a afirmação que a senha da credencial própria ”é muito longa”e torna o acesso/trabalho ”lento”.

No entanto, foi notado que o uso da credencial própria gera segurança profissional, pois os usuários que a usam incentivam outros com o argumento que não serão envolvidos em problemas relacionados a credencial ”padrão”. Portanto, levando em consideração a experiência positiva adquirida, conclui-se que implantar um mecanismo de autenticação, autorização e auditoria nos ativos de rede é uma boa prática.

Referências

Adiscon and Community. Adiscon LogAnalyzer - syslog web viewer, analysis and reporting tool. `http://loganalyzer.adiscon.com/`. Acessado: 2017-12-22.

Community, S. SAMBA - opening windows to a wider world. `https://www.samba.org/`. Acessado: 2017-12-22.

FreeRADIUS Server Project and Contributors. Freeradius. `https://freeradius.org/`. Acessado: 2018-03-16.

Graylog, Inc. Graylog open source log management. `https://www.graylog.org/`. Acessado: 2017-12-22.

Rainer Gerhards and Community. RSYSLOG - the rocket-fast system for log processing. `https://www.rsyslog.com/`. Acessado: 2017-12-22.

[10]Uplinks são enlace entre os `Switchs` que propagam a rede na direção do *switch* núcleo.

[11]Downlinks são enlaces que não caminham na direção do *switch* núcleo.