Documentação Técnica

Olá! Meu nome é Nilo Trigueiro e, ao longo dos últimos dias, tenho trabalhado em algumas documentações importantes para o nosso ambiente. Gostaria de compartilhar com vocês algumas orientações e insights que podem ser úteis, baseados nas minhas experiências.

Servidor Hypervisor

Sempre que realizarmos qualquer alteração no arquivo `zabbix_agentd.conf` em um servidor Windows, é crucial lembrar que o serviço do Zabbix precisará ser reiniciado para que as mudanças sejam aplicadas. Este é um passo fundamental para garantir que as configurações atualizadas entrem em vigor.

Grafana: Ajustes na Política de Segurança (CSP)

Com as versões mais recentes do Grafana (a partir da 9.x e 10.x), a política de segurança de conteúdo (CSP - Content Security Policy) tornou-se significativamente mais rigorosa. Isso impacta diretamente a execução de scripts e estilos embutidos em painéis HTML (como os de Texto ou Gráficos HTML), que são frequentemente bloqueados por padrão.

Em ambientes específicos, como o meu, que é de acesso restrito e local, pode ser necessário flexibilizar ou até mesmo desativar a `content_security_policy`. Essa ação permite a execução de JavaScript inline, CSS e até mesmo a inclusão de links externos dentro do HTML dos painéis, o que pode ser essencial para certas funcionalidades.

Como Realizar o Ajuste

Para ajustar essa configuração, você precisará localizar a linha `content_security_policy = true` no arquivo de configuração do Grafana, que geralmente está localizado em `/etc/grafana/grafana.ini`, e alterá-la para `content_security_policy = false`.

Você pode editar o arquivo usando o comando `vim /etc/grafana/grafana.ini`.

```
content_security_policy = true
```

```
content_security_policy = false
```

Após realizar essa alteração, salve o arquivo e reinicie o serviço do Grafana. No Linux, você pode fazer isso com o seguinte comando:

```
sudo systemctl restart grafana-server
```

Considerações Importantes e Riscos de Segurança

ATENÇÃO: Esta alteração deve ser feita por sua conta e risco.

É fundamental compreender que desabilitar ou flexibilizar a Content Security Policy pode introduzir riscos de segurança, como vulnerabilidades de Cross-Site Scripting (XSS), caso um usuário mal-intencionado obtenha acesso aos seus dashboards. Por essa razão, **recomendo que esta modificação seja aplicada apenas se o seu ambiente Grafana for estritamente interno e controlado, ou se você tiver total confiança nos usuários que possuem permissão para editar painéis.** No meu caso, essa foi a solução adotada devido ao ambiente ser de acesso restrito e local, minimizando os riscos associados.

Espero que estas informações sejam úteis para vocês! Qualquer dúvida, estou à disposição.

Atenciosamente, Nilo Trigueiro www.linkedin.com/in/nilotrigueiro