Guia de Troubleshooting ASA: Logs faltantes em destinos do Syslog

Índice

Introdução

Este documento descreve como pesquisar defeitos o problema com a capacidade da ferramenta de segurança adaptável (ASA) de enviar Syslog aos vários destinos, e, mais especificamente, as edições onde os sintomas tais como estes são observados:

- Tempo real lento que entra o Security Device Manager adaptável (ASDM).
- Syslog intermitentes que faltam em uns ou vários destinos do Syslog.

Antes de Começar

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada em Cisco ASA e não é limitado a uma versão de software específica ASA.

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas

técnicas Cisco.

Caracterize a informação

Os ASA, como a maioria outros de dispositivos Cisco, são capazes de enviar Syslog aos destinos múltiplos do Syslog. Alguns dos destinos mais de uso geral são ilustrados aqui:

O número de destinos possíveis é umas vantagens reais. Se escolhidos com cuidado, e como ilustrado aqui, podem amplamente ser classificados em duas categorias principal baseadas na finalidade que servem:

- Arquivístico
- Debugging em tempo real/Troubleshooting

Na maioria de redes, é suficiente ter apenas os destinos arquivísticos permitidos a menos que uns ou vários dos destinos da eliminação de erros forem necessários. Ao mesmo tempo, e bastante frequentemente, os problemas resultam de permitir destinos múltiplos do Syslog simultaneamente a níveis de registro altos tais como informativo (nível 6) ou acima.

Metodologia de Troubleshooting

Sempre que as edições ocorrem onde há uma perda de informação de syslog em uns ou vários destinos, há duas coisas que você deve verificar:

- Reveja a configuração da informações de syslog (saída do **registro executado mostra**).
- Olhe a saída da **fila de registro da mostra**.

Análise de dados

Reveja a configuração da informações de syslog

Conclua estes passos:

1. Certifique-se de que o mensagem do syslog que você está procurando não está desabilitado por **nenhum** comando do **mensagem de registro** *<ID>*.
2. Uma vez que confirmado, olhe o número de destinos do Syslog permitidos e do nível em que cada log é enviado a cada um. Este é um exemplo de tal configuração:
```
logging enable
logging timestamp
logging standby
logging console informational
logging buffered informational
logging trap informational
logging asdm informational
logging device-id hostname
logging host inside 172.16.110.32
```

Neste exemplo, o ASA está enviando Syslog a 4 destinos diferentes a nível informacional (nível 6).

Saída da fila de registro da mostra

Com uma configuração tal como o acima, onde os destinos múltiplos estão recebendo grandes quantidades de mensagens de registro, você pode ser executado em uma situação onde os mensagens do syslog das gotas ASA devido a um excesso da fila de registro. Nesses casos, a saída parecerá similar a esta:

```
ciscoasa# show logging queue Logging Queue length limit : 512 msg(s) 2352325 msg(s) discarded due to queue overflow 0 msg(s) discarded due to memory allocation failure Current 512 msg on queue, 512 msgs most on queue
```

Àrevelia, a fila de registro guarda 512 mensagens.

Problemas comuns

Ao ser executado nas edições onde os mensagens do syslog não estão sendo gravados, considere estas opções:

- Desabilite o logging de console. Entrar ao console **não deve** ser permitida para a operação normal. O logging de console deve ser usado somente para o Troubleshooting em tempo real, com baixo nível de registro ou tráfego baixo. Entrar ao console em uma taxa alta causará ao taxa-limite de registro do processo severamente as mensagens. O console é somente capaz dos mensagens de registro em 9600 bps, e não toma a dos logs antes que comece tentar despejar mais ao console do que o console pode output à tela. Nesta situação, os logs começarão ser protegidos na fila de registro. Uma vez que a fila de registro se enche acima, as mensagens Tail-estarão deixadas cair.
- Aumente o tamanho da fila de registro além de 512. A fila de registro do máximo é 1024 no ASA-5505, 2048 no ASA-5510, e 8192 em todas Plataformas restantes. Nota: A fila de registro é usada para “explosões” dos Syslog. Se a taxa mantida dos Syslog é mais rápida do que o ASA pode os transmitir aos vários destinos, nenhum limite de fila de registro será grande bastante.
- Desabilite mensagens do syslog individuais que você não está interessado na arquivística. Emita o *comando no logging message <syslog_id>* a fim desabilitar Syslog individuais.
- Seja cuidadoso dos mensagens de registro ao disco (flash) do ASA. Escrever ao flash é uma operação muito lenta. O registro excessivo a piscar fará com que o ASA proteja os arquivos do Syslog acima na memória, esgotando eventualmente toda a memória disponível (RAM). Adicionalmente, as grandes quantidades de registro de mensagens do syslog a piscar podem elevar o CPU. Recomenda-se registrar somente as mensagens do nível 1 para piscar (que cobrem eventos de sistema crítico).

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems