As diferenças entre logs e debugam em ferramentas de segurança adaptáveis

Índice

[Introdução](#)
[Pré-requisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Funcionalidade de registro básica](#)
[Diferença entre mensagens do syslog e debug](#)
[Recolha debuga](#)
[Configuração de exemplo](#)
[Informações Relacionadas](#)

Introdução

Este documento fornece uma descrição simples para a funcionalidade da eliminação de erros nas ferramentas de segurança adaptáveis (ASA) essa versão 8.4 e mais recente da corrida. Contudo, algumas das características estão disponíveis somente na versão 9.5(2) e mais recente.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- ASA 5506-X com versão de software ASA 9.5(2)
- Versão 7.5.2 do Cisco Adaptive Security Device Manager (ASDM)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Funcionalidade de registro básica

Os ASA seguram debugam mensagens diferentemente do que dispositivos do ® do Cisco IOS. À revelia (a menos que “o debugar-traço de registro”, que está descrito mais tarde, é usado), está indicado na tela qualquer um quando você é conectado através da porta de Console ou com o telnet/Shell Seguro (ssh), mas é completamente independente. Quando você usa o console,

aparecem imediatamente depois que você inscreve o comando debug. A mesma ação igualmente acontece com uma sessão SSH.

A independência significa que quando você permite debuga na porta de Console e você é conectado com o SSH, debuga não aparece no SSH. Você tem que manualmente permiti-los outra vez. Também, se debuga são permitidos em uma sessão SSH que não aparecerão de todo na outra sessão. Você pode referir-lhe conforme a **eliminação de erros da sessão.**

Não há igualmente nenhuma necessidade de inscrever o **comando terminal monitor em um** ASA a fim mostrar debuga, porque debuga permitido no SSH ou uma sessão de Telnet aparece apesar deste comando. A finalidade deste comando é muito diferente do que no exemplo de configuração dos dispositivos IOS Cisco e do Syslog ASA descreve essa característica detalhada.

Diferença entre mensagens do syslog e debug

Debuga são mensagens especificadas para um determinada protocolo ou característica dos ASA. Não há nenhum nível de debuga, em lugar de são muito detalhados e o nível do detalhe pode ser mudado. Igualmente não puderam ter um timestamp, um código da mensagem, ou um nível de seriedade. Isto é dependente do detalhe debuga.

Este exemplo mostra que a diferença no meio debuga e mensagens do syslog com respeito à mesma solicitação de ping.

Este é um exemplo do resultado do debug depois que você inscreve o **comando debug icmp trace**:

```
ICMP echo request from 10.229.24.48 to 10.48.67.75 ID=1 seq=29 len=32

ICMP echo reply from 10.48.67.75 to 10.229.24.48 ID=1 seq=29 len=32
```

Este é um exemplo de um **mensagem do syslog** com respeito ao mesmo pedido ICMP:

```
Jan 01 2016 13:29:22: %ASA-6-302020: Built inbound ICMP connection for faddr 10.229.24.48/1
 gaddr 10.48.67.75/0 laddr 10.48.67.75/0

Jan 01 2016 13:29:22: %ASA-6-302021: Teardown ICMP connection for faddr 10.229.24.48/1
 gaddr 10.48.67.75/0 laddr 10.48.67.75/0
```

Recolha debuga

O timeout padrão para o SSH ou o telnet é cinco minutos e a sessão é desligada após esta época da inatividade. O timeout padrão para a conexão de console é 0, assim que significa que o usuário está entrado até os log de usuário para fora manualmente.

Os recursos de registro são limitados infelizmente pelo intervalo ajustado em um método de Gerenciamento particular, assim que quando a sessão SSH termina debugam igualmente a parada.

A fim continuar a recolher debuga por um tempo prolongado, você tem que usar a conexão de console e então você pode reorientá-lo ao servidor de SYSLOG com o comando de **registro do debugar-traço**. Serão reorientados como o mensagem do syslog 711001 emitido a nível de seriedade 7. a fim parar de enviar a isto mensagens aos logs, você podem usar a inserção “não”

antes do comando.

```
logging debug-trace
no logging debug-trace
```

Da versão 9.5.2, o ASA permite que você continue a enviar debuga como mensagens do syslog após um intervalo ou uma saída em uma conexão SSH/telnet/console. Se você inscreve o **comando persistent que do debugar-traço** você será seletivamente claro capaz debuga permitido em uma sessão de uma sessão diferente e ficarão ativos no fundo. A fim desabilitar esta característica, introduza “não” antes do comando.

```
logging debug-trace persistent
no logging debug-trace persistent
```

Àrevelia, todos debugam mensagens têm uma severidade do nível 7. a fim filtrá-las dos mensagens não desejada que você pode levantar a severidade desta mensagem para 3 assim que você recolherá somente Mensagens de Erro ao lado do debuga. Introduza “não” a fim desabilitar esta reorientação.

```
logging message 711001 level 3
no logging message 711001 level 3
```

Configuração de exemplo

```
logging enable
logging host 10.0.0.1
logging trap errors
logging debug-trace persistent
logging message 711001 level errors
debug icmp trace
```

Estes comandos enable você enviar Mensagens de Erro e Internet Control Message Protocol (ICMP) debuga marcado igualmente como erros ao servidor de SYSLOG:

```
Jan 01 2016 13:30:22: %ASA-3-711001: ICMP echo request from 10.229.24.48 to 10.48.67.75 ID=1
 seq=29 len=32

Jan 01 2016 13:30:22: %ASA-3-711001: ICMP echo reply from 10.48.67.75 to 10.229.24.48 ID=1
 seq=29 len=32
```

Informações Relacionadas

- Exemplo de configuração do Syslog ASA
- Suporte Técnico e Documentação - Cisco Systems