Diferenças entre registros e depurações em dispositivos de segurança adaptáveis

Contents

Introduction

Este documento fornece uma descrição simples para a funcionalidade de depuração em Adaptive Security Appliances (ASAs) que executam a versão 8.4 e posterior. Entretanto, alguns dos recursos estão disponíveis somente na versão 9.5(2) e posterior.

Prerequisites

Requirements

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 software ASA versão 9.5(2)
- Cisco Adaptive Security Device Manager (ASDM) versão 7.5.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Funcionalidade básica de registro

Os ASAs lidam com mensagens de depuração de forma diferente dos dispositivos do Cisco IOS®. Por padrão (a menos que seja usado o "logging debug-trace", que é descrito mais adiante), eles são exibidos na tela quando você está conectado através da porta do console ou através do telnet/Secure Shell (SSH), mas eles são completamente independentes. Quando você usa o console, eles aparecem imediatamente depois que você digita o comando debug. A mesma ação

também acontece com uma sessão SSH.

Independência significa que quando você habilita depurações na porta do console e está conectado por SSH, as depurações não aparecem no SSH. Você precisa ativá-los manualmente novamente. Além disso, se as depurações forem ativadas em uma sessão SSH, elas não aparecerão de todo na outra sessão. Você pode fazer referência a ele como **depuração por sessão.**

Também não há necessidade de inserir o comando **terminal monitor** em um ASA para mostrar depurações, pois as depurações ativadas em SSH ou uma sessão telnet aparecem independentemente desse comando. A finalidade deste comando é muito diferente da dos dispositivos Cisco IOS e o Exemplo de Configuração de Syslog ASA descreve esse recurso em profundidade.

Diferença entre mensagens de syslog e depuração

As depurações são mensagens especificadas para um determinado protocolo ou recurso dos ASAs. Não há nenhum nível de depuração; em vez disso, eles são muito detalhados e o nível de detalhes pode ser alterado. Eles também podem não ter um carimbo de data/hora, código de mensagem ou nível de gravidade. Isso depende da depuração específica.

Este exemplo mostra a diferença entre depurações e mensagens de syslog em relação à mesma solicitação de ping.

Este é um exemplo de saída de depuração após você inserir 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 uma mensagem **syslog** em relação à mesma solicitação 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
```

Coletar depurações

O tempo limite padrão para SSH ou telnet é de cinco minutos e a sessão é desconectada após esse tempo de inatividade. O tempo limite padrão para a conexão do console é 0, o que significa que o usuário está conectado até que o usuário faça logoff manualmente.

Infelizmente, o recurso de registro é limitado pelo tempo limite definido em um método de gerenciamento específico, de modo que quando a sessão SSH encerra as depurações também é interrompida.

Para continuar a coletar as depurações por um tempo estendido, você precisa usar a conexão do console e, em seguida, pode redirecioná-las para o Servidor syslog com o comando **logging debug-trace**. Eles serão redirecionados como mensagem de syslog 711001 emitida no nível de gravidade 7. Para parar de enviar essas mensagens aos registros, você pode usar inserir "não"

antes do comando.

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

Na versão 9.5.2, o ASA permite que você continue a enviar depurações como mensagens de syslog após um tempo limite ou fazer logoff em uma conexão SSH/telnet/console. Se você inserir o comando **debug-trace persistent**, será possível limpar seletivamente as depurações habilitadas em uma sessão de uma sessão diferente e elas permanecerão ativas em segundo plano. Para desabilitar esse recurso, insira "não" antes do comando.

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

Por padrão, todas as mensagens de depuração têm uma gravidade de nível 7. Para filtrá-los de mensagens indesejadas, você pode aumentar a gravidade desta mensagem para 3, de modo que coletará somente mensagens de erro ao lado das depurações. Insira "no" para desabilitar esse redirecionamento.

```
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
```

Esses comandos permitem que você envie mensagens de erro e depurações do Internet Control Message Protocol (ICMP) marcadas também como erros para o Servidor 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 da configuração de syslog do ASA
- Suporte Técnico e Documentação - Cisco Systems