Differenze tra log e debug su appliance di sicurezza adattive

Sommario

Introduzione

In questo documento viene fornita una descrizione semplice della funzionalità di debug delle appliance ASA (Adaptive Security Appliance) con versione 8.4 e successive. Alcune funzionalità sono tuttavia disponibili solo nella versione 9.5(2) e successive.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ASA 5506-X con software ASA versione 9.5(2)
- Cisco Adaptive Security Device Manager (ASDM) versione 7.5.2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Funzionalità di registrazione di base

Le appliance ASA gestiscono i messaggi di debug in modo diverso dai dispositivi Cisco IOS®. Per impostazione predefinita (a meno che non si utilizzi "logging debug-trace", come descritto più avanti), le tracce vengono visualizzate sullo schermo quando si è connessi tramite la porta della

console o tramite telnet/Secure Shell (SSH), ma sono completamente indipendenti. Quando si utilizza la console, queste vengono visualizzate immediatamente dopo l'immissione del comando debug. La stessa azione viene eseguita anche con una sessione SSH.

Indipendenza significa che quando si abilitano i debug sulla porta console e si è connessi tramite SSH, i debug non vengono visualizzati sul protocollo SSH. È necessario riattivarle manualmente. Inoltre, se i debug sono abilitati su una sessione SSH, non verranno visualizzati sull'altra sessione. È possibile farvi riferimento come **per il debug della sessione.**

Inoltre, non è necessario usare il comando **terminal monitor** sull'appliance ASA per visualizzare i debug, in quanto i debug abilitati sul protocollo SSH o su una sessione telnet vengono visualizzati indipendentemente dal comando. Lo scopo di questo comando è molto diverso rispetto ai dispositivi Cisco IOS e l'esempio di configurazione del syslog dell'ASA descrive in dettaglio questa funzione.

Differenza tra i messaggi di syslog e di debug

I debug sono messaggi specificati per un determinato protocollo o funzione delle appliance ASA. Non esiste alcun livello di debug, ma il livello di dettaglio può essere modificato. Possono inoltre non disporre di un timestamp, di un codice messaggio o di un livello di gravità. Dipende dal debug specifico.

Nell'esempio viene mostrata la differenza tra i messaggi di debug e i messaggi syslog relativi alla stessa richiesta ping.

Questo è un esempio di output del comando debug dopo l'immissione del 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
```

Questo è un esempio di messaggio **syslog** relativo alla stessa richiesta 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
```

Raccogli debug

Il timeout predefinito per SSH o telnet è di cinque minuti e la sessione viene disconnessa dopo questo periodo di inattività. Il timeout predefinito per la connessione alla console è 0, che indica che l'utente ha eseguito l'accesso fino alla disconnessione manuale.

Sfortunatamente, la funzione di registrazione è limitata dal timeout impostato su un particolare metodo di gestione, quindi quando la sessione SSH termina anche i debug vengono interrotti.

Per continuare a raccogliere i debug per un periodo di tempo esteso, è necessario usare la connessione alla console e quindi reindirizzarli al server syslog con il comando **log debug-trace**. Verranno reindirizzati come messaggi syslog 711001 emessi con un livello di gravità pari a 7. Per

interrompere l'invio dei messaggi ai log, è possibile utilizzare il comando insert "no" prima di eseguire il comando.

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

Dalla versione 9.5.2, l'ASA consente di continuare a inviare i debug come messaggi syslog dopo un timeout o una disconnessione da SSH/telnet/console. Se si immette il comando **debug-trace persistent**, è possibile cancellare in modo selettivo i debug abilitati in una sessione da un'altra sessione e mantenerli attivi in background. Per disabilitare questa funzione, inserire "no" prima del comando.

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

Per impostazione predefinita, tutti i messaggi di debug hanno un livello di gravità pari a 7. Per filtrarli dai messaggi indesiderati, è possibile aumentare a 3 il livello di gravità del messaggio in modo da raccogliere solo i messaggi di errore accanto ai debug. Inserire "no" per disabilitare il reindirizzamento.

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

Esempio di configurazione

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

Questi comandi consentono di inviare messaggi di errore e debug ICMP (Internet Control Message Protocol) contrassegnati anche come errori al server 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
```

Informazioni correlate

- Esempio di configurazione del syslog ASA
- Documentazione e supporto tecnico – Cisco Systems