Configurazione dei log di debug delle richieste in Secure Web Appliance

Sommario

Introduzione

In questo documento viene descritto come richiedere i log di debug in Secure Web Appliance (SWA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso amministrativo all'interfaccia della riga di comando (CLI) dell'SWA.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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.

Richiedi log di debug

I log di debug delle richieste in SWA sono un tipo di log specializzato progettato per acquisire informazioni estremamente dettagliate, end-to-end di debug e fino al livello di traccia per una singola transazione HTTP o HTTPS specifica o un computer client. A differenza dei log proxy standard che registrano gli eventi di riepilogo in molte richieste, i log di debug delle richieste aggregano l'output di debug da tutti i moduli proxy Web coinvolti nell'elaborazione di una richiesta specifica (ad esempio autenticazione, filtro URL, decrittografia, scansione di malware e servizi di reputazione) in un unico flusso di log correlato. Questo tipo di log è progettato esclusivamente per la diagnostica approfondita e può essere creato solo tramite la CLI, non tramite la GUI

I log di debug delle richieste sono essenziali per la risoluzione di problemi complessi o intermittenti relativi ai proxy in cui i log standard non sono sufficientemente dettagliati. Consentono agli amministratori e a Cisco TAC di tracciare esattamente il modo in cui una singola richiesta è stata gestita in ogni fase di elaborazione, consentendo di individuare le cause principali, ad esempio corrispondenze di policy impreviste, ritardi di scansione, errori di autenticazione o verdetti incoerenti tra i motori. Poiché il log è incentrato su una transazione, fornisce la massima visibilità senza il sovraccarico operativo e l'impatto sulle prestazioni dell'abilitazione del log di debug su tutti i moduli proxy a livello di sistema. In questo modo, i log di debug delle richieste diventano uno strumento di diagnostica preciso, efficiente e a basso rischio durante le indagini avanzate.

Configurazione dei log di debug delle richieste

Passaggio 1. Accedere alla CLI, eseguire logconfig e scegliere new.

Passaggio 2. Selezionare il numero associato ai log di debug delle richieste e premere Invio.

Passaggio 3. Immettere il nome del log.

Passaggio 4. Scegliere Traccia come livello di log.

Passaggio 5. Scegliere i moduli in cui viene richiesto di raccogliere il log avanzato. È possibile effettuare più selezioni sotto forma di elenco separato da virgole o di intervalli (ad esempio 1, 3, 4 o 3-7).

Suggerimento: Se il TAC non richiede alcun modulo specifico, è consigliabile selezionare tutti i moduli (ad esempio 1-30).

Passaggio 6. Specificare il numero di richieste per le quali deve essere abilitata la registrazione avanzata. Una volta acquisito questo numero di richieste, la registrazione si interrompe automaticamente.

Nota: È importante selezionare un valore ragionevole in base alle condizioni del traffico durante la risoluzione dei problemi. Se ad esempio si utilizza un computer di prova dedicato e il traffico in background è minimo, è sufficiente un numero di richieste inferiore. Tuttavia, in ambienti con attività in background più elevate (come gli aggiornamenti del sistema operativo, le richieste in background dei browser o applicazioni quali Webex), la scelta di un valore più alto assicura che la transazione rilevante venga acquisita.

Passaggio 7. Definire i criteri di corrispondenza richiesta per la registrazione avanzata selezionando l'indirizzo IP del client, l'indirizzo IP di destinazione o il dominio di destinazione.

Nota: Nella maggior parte dei casi, si consiglia di selezionare l'indirizzo IP del client, anche quando si risolvono problemi di accesso a un singolo sito Web. Questo approccio assicura che tutte le richieste Web generate durante il caricamento della pagina vengano acquisite, incluse le richieste in background ad altri URL che potrebbero non essere immediatamente visibili. Tuttavia, questo metodo è più efficace quando si utilizza un computer di test dedicato con un traffico Internet in background minimo. Negli ambienti in cui il client genera traffico aggiuntivo significativo (ad esempio, aggiornamenti del sistema operativo, servizi di background del browser o applicazioni quali Webex), è preferibile filtrare in base al dominio di destinazione o all'indirizzo IP di destinazione.

Suggerimento: Se non si conosce il punto esatto dell'errore, è possibile raccogliere i log HAR del browser per identificare l'URL specifico o il dominio che presenta problemi (ad esempio, errori di caricamento della pagina o latenza elevata) e configurare il dominio nei criteri del log di debug della richiesta.

Passaggio 8. Scegliere il metodo per il recupero dei log. Se si seleziona FTP Poll, i log vengono memorizzati sull'SWA.

Passaggio 9. Definire il nome file da utilizzare per i file di log oppure premere Invio per accettare il nome file generato corrente.

Passaggio 10. Selezionare No per il rollover dei file di log basati sul tempo, poiché il log si interrompe dopo che è stato raggiunto il numero definito di richieste.

Passaggio 11. Definire le dimensioni massime del file in byte o premere Invio per accettare il valore corrente.

Suggerimento: La definizione di un file di registro di dimensioni maggiori può rendere più difficile il download e l'analisi dei registri. Anziché aumentare le dimensioni dei singoli file di registro, si consiglia di aumentare il numero di file di registro (passaggio successivo). Questo approccio migliora la gestibilità e garantisce che tutte le informazioni di debug necessarie vengano acquisite senza creare file di dimensioni eccessive.

Passaggio 12. Configurare il numero massimo di file di log in base al numero di moduli proxy selezionati per l'accesso al passaggio 5 e ai criteri di corrispondenza alle richieste definiti nel passaggio 7. La selezione di un limite di file ragionevole è importante per garantire che tutte le informazioni di debug pertinenti vengano acquisite senza interrompere prematuramente la registrazione, il che potrebbe determinare registri incompleti o mancanti.

Passaggio 13. Selezionare No quando viene richiesto se deve essere inviato un avviso quando i file vengono rimossi a causa del numero massimo di file consentiti. In questo modo si evitano avvisi non necessari durante la normale rotazione del log, in particolare quando i log di debug delle richieste vengono generati intenzionalmente a scopo di risoluzione dei problemi.

Passaggio 14. Selezionare No quando richiesto con Comprimere i log (sì/no)? In questo modo i file di log non vengono compressi, per facilitarne la revisione e l'analisi durante la risoluzione dei problemi.

Passaggio 15. Premere Invio per uscire dalla procedura guidata

Passaggio 16. Digitare commit e premere Invio per salvare le modifiche

```
SWA_CLI> logconfig

Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "adc_logs" Type: "ADC Engine Logs" Retrieval: FTP Poll
...
[Output removed to simplify readability]
...
55. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP Poll

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- HOSTKEYCONFIG - Configure SSH host keys.
- AUDITLOGCONFIG - Adjust settings for audit logging.
[]> new

Choose the log file type for this subscription:
1. ADC Engine Framework Logs
2. ADC Engine Logs
...
```

```
[Output removed to simplify readability]
...
53. Request Debug Logs
...
[Output removed to simplify readability]
...
[1]> 53

Please enter the name for the log:
[]> Request_Debug_Logs

Log level:
1. Critical
2. Warning
3. Information
4. Debug
5. Trace
[3]> 5

Choose modules where enhanced request logging is to be performed.
Multiple selections can be made in the form of a comma separated or range list (e.g. 1,3,4 or 3-7)
Choosing the Default Proxy will enable enhanced logging across modules:
1. Default Proxy
2. Access Control Engine
3. Proxy Configuration
4. Disk Manager
5. Memory Manager
6. McAfee Integration Framework
7. Sophos Integration Framework
8. Webroot Integration Framework
9. Webcat Integration Framework
10. Connection Management
11. Authentication Framework
12. HTTPS
13. FTP proxy
14. WCCP Module
15. License Module
16. SNMP Module
17. WBRS Integration Framework
18. Logging Framework
19. Data Security Module
20. Miscellaneous Proxy Modules
21. DCA Engine Framework
22. AVC Engine Framework
23. Cloud Connector
24. SOCKS Proxy
25. Advanced Malware Protection
26. ArchiveScan module in proxy
27. Web Traffic Tap module in proxy
28. Bandwidth Control
29. Http2 proxy
30. ADC Engine Framework
[1]> 1-30

Please enter the number of requests for which to perform enhanced logging:
[1]> 100

Choose the request criteria for logging:
1. Client IP Address
2. Destination Domain
3. Destination IP Address
[1]> 1
```

```
Specify source IP address
[]> 10.20.3.15

Choose the method to retrieve the logs:
1. FTP Poll
2. FTP Push
3. SCP Push
[1]> 1

Filename to use for log files:
[Request_Debug_Logs.text]>

Do you want to configure time-based log files rollover? [N]>

Please enter the maximum file size:
[10485760]>

Please enter the maximum number of files:
[10]> 50

Should an alert be sent when files are removed due to the maximum number of files allowed? [N]>

Do you want to compress logs (yes/no)
[n]>

Currently configured logs:
1. "Request_Debug_Logs" Type: "Request Debug Logs" Retrieval: FTP Poll
2. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
3. "adc_logs" Type: "ADC Engine Logs" Retrieval: FTP Poll
...
[Output removed to simplify readability]
...
56. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP Poll


SWA_LIC> commit

Warning: In order to process these changes, the proxy
process will restart after Commit. This will cause a brief
interruption in service. Additionally, the authentication
cache will be cleared, which might require some users to
authenticate again.
```

Informazioni correlate

- Guida per l'utente di AsyncOS 15.2 per Cisco Secure Web Appliance
- Utilizzare le procedure ottimali per Secure Web Appliance
- Accesso ai registri protetti di Web Appliance
- Configurazione dei log push SCP in SWA con Microsoft Server

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).