Konfigurieren von Debug-Anforderungsprotokollen in der sicheren Web-Appliance

Inhalt

Einleitung

In diesem Dokument werden die Schritte zum Anfordern von Debug-Protokollen in der sicheren Web-Appliance (SWA) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Administratorzugriff auf die Kommandozeile von SWA

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Debugprotokolle anfordern

Request Debug Logs in SWA sind ein spezieller Protokolltyp, der entwickelt wurde, um extrem detaillierte End-to-End-Debugging- und bis zu Ablaufverfolgungsebeneninformationen für eine einzelne, spezifische HTTP- oder HTTPS-Transaktion oder einen Client-Computer zu erfassen. Im Gegensatz zu Standard-Proxy-Protokollen, die zusammengefasste Ereignisse für eine Vielzahl von Anforderungen aufzeichnen, bündeln Request Debug Logs die Debug-Ausgabe aller Webproxy-Module, die an der Verarbeitung einer bestimmten Anforderung beteiligt sind (z. B. Authentifizierung, URL-Filterung, Entschlüsselung, Malware-Scanning und Reputations-Services), in einem korrelierten Log-Stream. Dieser Protokolltyp ist ausschließlich für die Detaildiagnose vorgesehen und kann nur über die CLI und nicht über die GUI erstellt werden.

Anfordern von Debug-Protokollen ist für die Behebung komplexer oder zeitweiliger Proxy-Probleme, bei denen die Standardprotokolle keine ausreichenden Details enthalten, von entscheidender Bedeutung. Administratoren und das Cisco TAC können in jeder Verarbeitungsphase genau verfolgen, wie eine einzelne Anforderung behandelt wurde. So können Ursachen wie unerwartete Richtlinienübereinstimmungen, Scanverzögerungen, Authentifizierungsfehler oder inkonsistente Verdicts zwischen Engines genau ermittelt werden. Da sich das Protokoll auf eine Transaktion konzentriert, bietet es maximale Transparenz ohne die betrieblichen Gemeinkosten und die Auswirkungen auf die Leistung, die die Aktivierung der Debugprotokollierung über alle Proxymodule hinweg systemweit mit sich bringt. Dies macht Request Debug Logs zu einem präzisen, effizienten und risikoarmen Diagnosetool bei erweiterten Untersuchungen.

Konfigurieren der Anforderungsdebugprotokolle

Schritt 1: Melden Sie sich bei CLI an, führen Sie logconfig aus, und wählen Sie new.

Schritt 2: Wählen Sie die Nummer aus, die den Request Debug Logs zugeordnet ist, und drücken Sie die Eingabetaste.

Schritt 3: Geben Sie den Namen für das Protokoll ein.

Schritt 4: Wählen Sie Trace als Protokollierungsebene aus.

Schritt 5. Wählen Sie die Module aus, für die Sie die erweiterte Protokollierung anfordern. Sie können mehrere Module in Form einer kommagetrennten Liste oder einer Bereichsliste (z. B. 1, 3, 4 oder 3-7) auswählen.

Tipp: Wenn vom TAC kein bestimmtes Modul angefordert wird, sollten Sie alle Module (z. B. 1-30) auswählen.

Schritt 6: Geben Sie die Anzahl der Anforderungen an, für die die erweiterte Protokollierung aktiviert werden soll. Sobald diese Anzahl von Anforderungen erfasst wurde, wird die Protokollierung automatisch beendet.

Anmerkung: Es ist wichtig, bei der Fehlerbehebung einen angemessenen Wert auf Basis der Datenverkehrsbedingungen auszuwählen. Wenn beispielsweise ein dedizierter Testrechner verwendet wird und der Hintergrundverkehr minimal ist, reicht eine geringere Anzahl von Anfragen aus. In Umgebungen mit höherer Hintergrundaktivität (z. B. Betriebssystem-Updates, Browser-Hintergrundanforderungen oder Anwendungen wie WebEx) stellt die Auswahl eines höheren Werts jedoch sicher, dass die betreffende Transaktion erfasst wird.

Schritt 7: Definieren Sie die Kriterien für die Anforderungszuordnung für eine verbesserte Protokollierung, indem Sie entweder die Client-IP-Adresse, die Ziel-IP-Adresse oder die Zieldomäne auswählen.

Anmerkung: In den meisten Fällen wird empfohlen, die Client-IP-Adresse auszuwählen, selbst wenn der Zugriff auf eine einzige Website gestört wird. Dieser Ansatz stellt sicher, dass alle beim Laden der Seite generierten Webanforderungen erfasst werden, einschließlich Hintergrundanforderungen an zusätzliche URLs, die möglicherweise nicht sofort sichtbar sind. Diese Methode ist jedoch am effektivsten, wenn ein dedizierter Testcomputer mit minimalem Internet-Hintergrundverkehr verwendet wird. In Umgebungen, in denen der Client erheblichen zusätzlichen Datenverkehr generiert (z. B. Betriebssystem-Updates, Browser-Hintergrunddienste oder Anwendungen wie WebEx), ist es besser, nach Zieldomäne oder Ziel-IP-Adresse zu filtern.

Tipp: Wenn der genaue Fehlerpunkt unbekannt ist, können HAR-Protokolle des Browsers erfasst werden, um die spezifische URL oder Domäne zu identifizieren, die Probleme aufweist (z. B. Fehler beim Laden von Seiten oder hohe Latenz). Diese Domäne kann dann in den Kriterien für das Anforderungsdebugprotokoll konfiguriert werden.

Schritt 8: Wählen Sie die Methode zum Abrufen der Protokolle aus. Wenn Sie "FTP Poll" (FTP-Abfrage) auswählen, werden die Protokollspeicher auf dem SWA abgefragt.

Schritt 9: Legen Sie den für Protokolldateien zu verwendenden Dateinamen fest, oder drücken Sie die Eingabetaste, um den aktuell generierten Dateinamen zu akzeptieren.

Schritt 10. Wählen Sie Nein für das zeitbasierte Rollover von Protokolldateien, da die

Protokollierung beendet wird, nachdem die festgelegte Anzahl von Anforderungen erfüllt wurde.

Schritt 11: Legen Sie die maximale Dateigröße in Byte fest, oder drücken Sie die Eingabetaste, um den aktuellen Wert zu übernehmen.

Tipp: Wenn Sie eine größere Protokolldatei definieren, können Sie Protokolle nur schwer herunterladen und überprüfen. Anstatt die Größe einzelner Protokolldateien zu erhöhen, wird empfohlen, die Anzahl der Protokolldateien zu erhöhen (nächster Schritt). Dieser Ansatz verbessert die Verwaltbarkeit und stellt gleichzeitig sicher, dass alle erforderlichen Debuginformationen erfasst werden, ohne dass übermäßig große Dateien erstellt werden.

Schritt 12. Konfigurieren Sie die maximale Anzahl von Protokolldateien auf der Grundlage der Anzahl von Proxymodulen, die für die Protokollierung in Schritt 5 ausgewählt wurden, und der in Schritt 7 definierten Anforderungsvergleichskriterien. Wählen Sie eine angemessene Dateibeschränkung aus, um sicherzustellen, dass alle relevanten Debuginformationen erfasst werden, ohne die Protokollierung vorzeitig zu beenden, was zu unvollständigen oder fehlenden Protokollen führen kann.

Schritt 13. Wählen Sie Nein, wenn Sie dazu aufgefordert werden. Soll eine Warnung gesendet werden, wenn Dateien aufgrund der maximal zulässigen Anzahl von Dateien entfernt werden? Dadurch werden unnötige Warnungen während der normalen Protokollrotation vermieden, insbesondere wenn Request Debug Logs absichtlich für die Fehlerbehebung generiert werden.

Schritt 14. Wählen Sie Nein, wenn Sie dazu aufgefordert werden Möchten Sie Protokolle komprimieren (ja/nein)? Dadurch bleiben die Protokolldateien unkomprimiert, was die Überprüfung und Analyse während der Fehlerbehebung vereinfacht.

Schritt 15. Drücken Sie die Eingabetaste, um den Assistenten zu beenden.

Schritt 16. Geben Sie commit ein und drücken Sie Enter, um die Änderungen zu speichern

```
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.
```

Zugehörige Informationen

- Bedienungsanleitung für AsyncOS 15.2 für Cisco Secure Web Appliance

- Best Practices für sichere Web-Appliances

- Zugreifen auf Protokolle der sicheren Web-Appliance
- Konfigurieren von SCP-Push-Protokollen in SWA mit Microsoft Server

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.