Aanvragen voor foutopsporing configureren in Secure Web Appliance

Inhoud

Inleiding

In dit document worden de stappen beschreven voor het aanvragen van foutopsporingslogboeken in Secure Web Appliance (SWA).

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:

- Administratieve toegang tot de Command Line Interface (CLI) van SWA.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Foutopsporingslogboeken aanvragen

Request Debug Logs in SWA zijn een gespecialiseerd logtype dat is ontworpen om uiterst gedetailleerde, end-to-end debug en tot op niveau informatie vast te leggen voor een enkele, specifieke HTTP- of HTTPS-transactie of een clientsysteem. In tegenstelling tot standaard proxy-logs die samengevatte gebeurtenissen in veel verzoeken registreren, verzamelen Request Debug Logs debug-uitvoer van alle Web Proxy-modules die betrokken zijn bij het verwerken van een bepaald verzoek (zoals authenticatie, URL-filtering, decodering, scannen van malware en reputatieservices) in één gecorreleerde logstream. Dit logtype is puur bedoeld voor diepe diagnostiek en kan alleen worden gemaakt via de CLI, niet via de GUI

Debug-logboeken voor aanvragen zijn essentieel bij het oplossen van complexe of intermitterende proxyproblemen waarbij standaardlogboeken onvoldoende details bevatten. Ze stellen beheerders en Cisco TAC in staat om precies te traceren hoe een enkel verzoek in elke verwerkingsfase werd afgehandeld, waardoor het mogelijk is om onderliggende oorzaken te identificeren, zoals onverwachte beleidsovereenkomsten, scanvertragingen, authenticatiefouten of inconsistente oordelen tussen engines. Omdat het logboek zich richt op één transactie, biedt het maximale zichtbaarheid zonder de operationele overhead en impact op de prestaties van het inschakelen van debug-logging voor alle proxymodules over het hele systeem. Dit maakt Request Debug Logs een nauwkeurige, efficiënte en laag risico diagnostische tool tijdens geavanceerde onderzoeken.

De logs voor foutopsporing bij aanvragen configureren

Stap 1. Meld u aan bij CLI, voer logconfig uit en kies nieuw.

Stap 2. Selecteer het nummer dat is gekoppeld aan logs voor foutopsporing aanvragen en druk op Enter.

Stap 3. Voer de naam voor het logboek in.

Stap 4. Kies Trace als logboekniveau.

Stap 5. Kies modules waar gevraagd om de verbeterde logboekregistratie te verzamelen. Meerdere selecties kunnen worden gemaakt in de vorm van een komma gescheiden of bereik lijst (zoals 1, 3, 4 of 3-7).

 Tip: Als de TAC geen specifieke module heeft aangevraagd, kunt u het beste alle modules

---

selecteren (zoals 1-30).

Stap 6. Geef het aantal aanvragen op waarvoor verbeterde logboekregistratie moet worden ingeschakeld. Zodra dit aantal aanvragen is vastgelegd, wordt de registratie automatisch gestopt.

Opmerking: Het is belangrijk om een redelijke waarde te selecteren op basis van de verkeersomstandigheden tijdens het oplossen van problemen. Als er bijvoorbeeld een speciale testmachine wordt gebruikt en het achtergrondverkeer minimaal is, is een lager aantal verzoeken voldoende. In omgevingen met een hogere achtergrondactiviteit (zoals updates van het besturingssysteem, achtergrondverzoeken van browsers of toepassingen zoals Webex) zorgt het kiezen van een hogere waarde er echter voor dat de relevante transactie wordt vastgelegd.

Stap 7. Definieer de criteria voor het matchen van verzoeken voor verbeterde logboekregistratie door het IP-adres van de client, het IP-adres van de bestemming of het bestemmingsdomein te selecteren.

Opmerking: In de meeste gevallen wordt aanbevolen om het IP-adres van de client te selecteren, zelfs bij het oplossen van problemen met de toegang tot één website. Deze aanpak zorgt ervoor dat alle webverzoeken die tijdens het laden van de pagina worden gegenereerd, worden vastgelegd, inclusief achtergrondverzoeken voor extra URL's die mogelijk niet onmiddellijk zichtbaar zijn. Deze methode is echter het meest effectief bij het gebruik van een speciale testmachine met minimaal achtergrondinternetverkeer. In omgevingen waar de client aanzienlijk extra verkeer genereert (zoals updates van het besturingssysteem, browserachtergrondservices of toepassingen zoals Webex), is het beter om te filteren op bestemmingsdomein of bestemmings-IP-adres.

Tip: Als het exacte punt van falen onbekend is, kunnen HAR-logs van de browser worden verzameld om de specifieke URL of het domein te identificeren dat problemen vertoont (bijvoorbeeld fouten in het laden van pagina's of hoge latentie), en dat domein kan vervolgens worden geconfigureerd in de criteria voor het debuglogboek voor aanvragen.

Stap 8. Kies de methode om de logs op te halen. Als u FTP Poll selecteert, worden de logboekbestanden op de SWA opgeslagen.

Stap 9. Definieer de bestandsnaam die u wilt gebruiken voor logbestanden of druk op Enter om de huidige gegenereerde bestandsnaam te accepteren.

Stap 10. Selecteer Nee voor de rollover van logbestanden op basis van tijd, omdat de logboekregistratie stopt nadat aan het gedefinieerde aantal verzoeken is voldaan.

Stap 11. Definieer de maximale bestandsgrootte in bytes of druk op Enter om de huidige waarde te accepteren.

Tip: Als u een grotere logboekbestandsgrootte definieert, kunnen logs moeilijker worden gedownload en beoordeeld. In plaats van de grootte van afzonderlijke logbestanden te vergroten, wordt aanbevolen het aantal logbestanden te verhogen (Volgende stap). Deze aanpak verbetert de beheerbaarheid en zorgt ervoor dat alle vereiste foutopsporingsinformatie wordt vastgelegd zonder al te grote bestanden te maken.

Stap 12. Configureer het maximale aantal logbestanden op basis van het aantal proxy-modules dat is geselecteerd voor aanmelding bij stap 5 en de criteria voor het matchen van aanvragen die zijn gedefinieerd in stap 7. Het selecteren van een redelijke bestandslimiet is belangrijk om ervoor te zorgen dat alle relevante foutopsporingsinformatie wordt vastgelegd zonder voortijdig de logboekregistratie te stoppen, wat kan resulteren in onvolledige of ontbrekende logs.

Stap 13. Selecteer Nee wanneer daarom wordt gevraagd Moet er een waarschuwing worden verzonden wanneer bestanden worden verwijderd vanwege het maximaal toegestane aantal bestanden? Dit voorkomt onnodige waarschuwingen tijdens de normale rotatie van het logboek, met name wanneer de logboeken voor het opsporen van fouten opzettelijk worden gegenereerd voor het oplossen van problemen.

Stap 14. Selecteer Nee wanneer u wordt gevraagd Wilt u logs comprimeren (ja/nee)? Hierdoor blijven de logbestanden ongecomprimeerd, waardoor ze gemakkelijker kunnen worden bekeken en geanalyseerd tijdens het oplossen van problemen.

Stap 15. Druk op Enter om de wizard af te sluiten

Stap 16. Typ commit en druk op Enter om de wijzigingen op te slaan

```
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.
```

Gerelateerde informatie

- Gebruikershandleiding voor AsyncOS 15.2 voor Cisco Secure Web Appliance
- Best practices voor veilige webapparaten gebruiken

- Toegang tot beveiligde logbestanden van webapparaten
- SCP-pushlogboeken configureren in SWA met Microsoft Server

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.