Configuration des journaux de débogage des requêtes dans l'appliance Web sécurisée

Table des matières

Introduction

Ce document décrit les étapes à suivre pour demander des journaux de débogage dans l'appareil Web sécurisé (SWA).

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- Accès administratif à l'interface de ligne de commande (CLI) de SWA.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Demander les journaux de débogage

Les journaux de débogage des requêtes dans SWA sont un type de journal spécialisé conçu pour capturer des informations de débogage de bout en bout extrêmement détaillées et jusqu'au niveau de trace pour une transaction HTTP ou HTTPS spécifique unique ou une machine client. Contrairement aux journaux de proxy standard qui enregistrent des événements récapitulatifs sur de nombreuses demandes, les journaux de débogage des demandes regroupent les résultats de débogage de tous les modules de proxy Web impliqués dans le traitement d'une demande particulière (tels que l'authentification, le filtrage URL, le déchiffrement, l'analyse des programmes malveillants et les services de réputation) dans un flux de journal corrélé. Ce type de journal est destiné uniquement aux diagnostics approfondis et ne peut être créé que via l'interface de ligne de commande, et non via l'interface utilisateur graphique

Les journaux de débogage des demandes sont essentiels lors du dépannage de problèmes de proxy complexes ou intermittents lorsque les journaux standard manquent de détails. Ils permettent aux administrateurs et au centre d'assistance technique Cisco de suivre exactement comment une seule demande a été traitée à chaque étape du traitement, ce qui permet d'identifier les causes premières telles que les correspondances de stratégies inattendues, les retards d'analyse, les échecs d'authentification ou les verdicts incohérents entre les moteurs. Comme le journal se concentre sur une transaction, il offre une visibilité maximale sans la surcharge opérationnelle et l'impact sur les performances de l'activation de la journalisation de débogage sur tous les modules proxy à l'échelle du système. Cela fait des journaux de débogage des demandes un outil de diagnostic précis, efficace et à faible risque pendant les investigations avancées.

Configuration des journaux de débogage des demandes

Étape 1. Connectez-vous à l’interface de ligne de commande, exécutez logconfig et sélectionnez new.

Étape 2. Sélectionnez le numéro associé aux journaux de débogage des demandes et appuyez sur Entrée.

Étape 3. Entrez le nom du journal.

Étape 4. Sélectionnez Trace comme niveau de journalisation.

Étape 5. Choisissez les modules où vous le souhaitez pour collecter la journalisation avancée. Plusieurs sélections peuvent être effectuées sous la forme d’une liste séparée par des virgules ou d’une liste de plages (par exemple, 1, 3, 4 ou 3-7).

Conseil : Si aucun module spécifique n'est demandé par le centre d'assistance technique, il

---

est préférable de sélectionner tous les modules (par exemple, 1 à 30).

Étape 6. Spécifiez le nombre de demandes pour lesquelles la journalisation avancée doit être activée. Une fois ce nombre de requêtes capturé, la journalisation s'arrête automatiquement.

Remarque : Il est important de sélectionner une valeur raisonnable en fonction des conditions de trafic lors du dépannage. Par exemple, si une machine de test dédiée est utilisée et que le trafic en arrière-plan est minimal, un nombre inférieur de requêtes est suffisant. Cependant, dans les environnements où l'activité en arrière-plan est plus importante (comme les mises à jour du système d'exploitation, les requêtes en arrière-plan du navigateur ou les applications telles que Webex), le choix d'une valeur plus élevée garantit que la transaction concernée est capturée.

Étape 7. Définissez les critères de correspondance des demandes pour la journalisation avancée en sélectionnant l'adresse IP du client, l'adresse IP de destination ou le domaine de destination.

Remarque : Dans la plupart des cas, il est recommandé de sélectionner l'adresse IP du client, même lors du dépannage de l'accès à un site Web unique. Cette approche garantit que toutes les requêtes Web générées pendant le chargement de la page sont capturées, y compris les requêtes en arrière-plan vers des URL supplémentaires qui ne sont peut-être pas immédiatement visibles. Cependant, cette méthode est plus efficace lorsque vous utilisez une machine de test dédiée avec un trafic Internet en arrière-plan minimal. Dans les environnements où le client génère un trafic supplémentaire important (comme les mises à jour du système d'exploitation, les services de navigateur en arrière-plan ou les applications telles que Webex), il est préférable de filtrer par domaine de destination ou par adresse IP de destination.

Conseil : Si le point exact de défaillance est inconnu, les journaux HAR du navigateur peuvent être collectés pour identifier l'URL ou le domaine spécifique présentant des problèmes (par exemple, échecs de chargement de page ou latence élevée), et ce domaine peut ensuite être configuré dans les critères du journal de débogage de requête.

Étape 8. Choisissez la méthode de récupération des journaux. Si vous sélectionnez FTP Poll, les journaux sont stockés sur le SWA.

Étape 9. Définissez le nom de fichier à utiliser pour les fichiers journaux ou appuyez sur Entrée pour accepter le nom de fichier généré actuel.

Étape 10. Sélectionnez Non pour la substitution de fichiers journaux basée sur le temps, car la journalisation s'arrête une fois que le nombre défini de demandes a été atteint.

Étape 11. Définissez la taille de fichier maximale en octets ou appuyez sur Entrée pour accepter la valeur actuelle.

Conseil : La définition d'une taille de fichier journal plus importante peut rendre les journaux plus difficiles à télécharger et à consulter. Au lieu d'augmenter la taille des fichiers journaux individuels, il est recommandé d'augmenter le nombre de fichiers journaux (étape suivante). Cette approche améliore la gestion tout en garantissant que toutes les informations de débogage requises sont capturées sans créer de fichiers trop volumineux.

Étape 12. Configurez le nombre maximal de fichiers journaux en fonction du nombre de modules proxy sélectionnés pour la journalisation à l'étape 5 et des critères de correspondance des demandes définis à l'étape 7. La sélection d'une limite de fichier raisonnable est importante pour garantir que toutes les informations de débogage pertinentes sont capturées sans arrêter prématurément la journalisation, ce qui peut entraîner des journaux incomplets ou manquants.

Étape 13. Sélectionnez No lorsque vous y êtes invité avec Si une alerte doit être envoyée lorsque des fichiers sont supprimés en raison du nombre maximal de fichiers autorisés ? Cela évite les alertes inutiles pendant la rotation normale du journal, en particulier lorsque les journaux de débogage des demandes sont générés intentionnellement à des fins de dépannage.

Étape 14. Sélectionnez No lorsque vous êtes invité à indiquer Do you want to compress logs (yes/no)? (Voulez-vous compresser les journaux (oui/non) ?). Cela permet de conserver les fichiers journaux non compressés, ce qui facilite leur consultation et leur analyse lors du dépannage.

Étape 15. Appuyez sur Entrée pour quitter l'assistant

Étape 16. Tapez commit et appuyez sur Entrée pour enregistrer les modifications

```
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.
```

Informations connexes

- Guide de l'utilisateur d'AsyncOS 15.2 pour Cisco Secure Web Appliance
- Utilisation des meilleures pratiques de sécurisation des appliances Web

- Accéder aux journaux de l'appliance Web sécurisée
- Configuration des journaux de transmission SCP dans SWA avec Microsoft Server

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.