Activer la journalisation de débogage maximale pour le module SWG

Table des matières

Introduction

Exemples d'utilisation pour activer la consignation maximale du débogage

Activer la consignation de débogage maximale sur AnyConnect 4.10 MR7, CSC 5.0 MR2 ou version antérieure

- Emplacement de SWGConfig.json
- Rendre la journalisation de débogage persistante
  - Créer le fichier d'indicateur
  - Copier et modifier le contenu
  - Redémarrer le service

Vérification et fourniture de journaux de débogage maximum

- Vérification Windows
- Vérification macOS
- Notes supplémentaires

Activer la journalisation de débogage maximale sur CSC 5.0 MR3 et AC 4.10 MR8 ou version ultérieure

- Aperçu
  - Modifications
- Activer la consignation du débogage

Notes de configuration et de fonctionnement

Informations connexes

Introduction

Ce document décrit comment activer la journalisation de débogage maximale sur le module Secure Web Gateway (SWG) pour AnyConnect et Cisco Secure Client (CSC).

Exemples d'utilisation pour activer la consignation maximale du débogage

Activez la journalisation de débogage maximale sur le module SWG lors de la résolution de problèmes tels que :

- Problèmes de hotspot via Captive Portal
- Liste de contournement de domaine externe non applicable
- Problèmes de performances DNS ou Web intermittents

Activer la consignation de débogage maximale sur AnyConnect

4.10 MR7, CSC 5.0 MR2 ou version antérieure

Si vous utilisez AnyConnect 4.10 MR7, CSC 5.0 MR2 ou une version antérieure, procédez comme suit. Par défaut, la journalisation de débogage maximale n'est pas activée et la configuration n'est pas possible via le tableau de bord Umbrella ou ASA. Vous devez ajouter manuellement "logLevel": "1" à l'objet orgConfig dans le SWGConfig.json fichier. Si vous utilisez la dernière version d'AnyConnect ou de Cisco Secure Client, ignorez cette section.

Emplacement de SWGConfig.json

- Windows (AnyConnect) :

```
C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella\SWG\
```

- Windows (client sécurisé) :

```
C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\SWG\
```

- macOS (AnyConnect) :

```
/opt/cisco/anyconnect/umbrella/swg/
```

- macOS (Secure Client) :

```
/opt/cisco/secureclient/umbrella/swg/
```

Rendre la journalisation de débogage persistante

Le fichier modifié SWGConfig.json reste uniquement jusqu'à la prochaine synchronisation de l'API par le module Cisco AnyConnect Umbrella. Pour conserver cette configuration et l'empêcher d'être écrasée par la synchronisation API, déployez un fichier swg_org_config.flag dans le dossier Umbrella/data.

1. Créer le fichier d'indicateur

    - Créez un nouveau fichier nommé **swg_org_config.flag** dans le dossier Umbrella Data. L'extension de fichier doit être .flag.

    - Windows (AnyConnect) :

- `C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella\data\swg_org_config.fl`

- Windows (client sécurisé) :

- `C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\data\swg_org_config.flag`

- macOS (AnyConnect) :

- `/opt/cisco/anyconnect/umbrella/data/swg_org_config.flag`

- macOS (Secure Client) :

- `/opt/cisco/secureclient/umbrella/data/swg_org_config.flag`

2. Copier et modifier le contenu

- Copiez le contenu de l' **orgConfig** objet du fichier SWGConfig.json vers le fichier swg_org_config.flag.
- Ajouter avec "logLevel": "1".
- Exemple :

```
{
"exceptionList": [
"www.example.com",
"smh.com.au",
"*.smh.com.au",
"www.blue.com",
"*.www.blue.com",
"146.112.133.72"
// ...additional entries...
],
"failOpen": 1,
"logLevel": "1",
"swgAnycast": "146.112.255.50",
"swgDomain": "swg-url-proxy-https.sigproxy.qq.opendns.com",
"swgEchoService": "http://www.msftconnecttest.com/connecttest.txt"
}
```

- Assurez-vous que le fichier d'indicateur commence par { "exceptionList": [...] et se termine par **"SWGEchoService": "http://www.msftconecttest.com/connecttest.txt"}.**
- Évitez de copier des lignes supplémentaires avant ou après l'objet.
- La copie incorrecte de lignes telles que identity, deviceId, ou adUserIDpeut interrompre la fonctionnalité SWG.

Exemple incorrect : Le fichier d'indicateur contient des clés telles que **identity**, deviceId, ou dUserID antérieures à

Exemple correct : Le fichier indicateur commence par { "exceptionList":



14970100184724

3. Redémarrer le service
   - Redémarrez le service Cisco AnyConnect Secure Mobility Agent/Secure Client, redémarrez la machine ou connectez et déconnectez le VPN.
4. Vérifier la configuration
   - Après le redémarrage ou la connexion/déconnexion VPN, ouvrez le fichier pour confirmer que le niveau maximal du journal de débogage SWG SWGConfig.json est défini. Une fois configurée, cette entrée apparaît dans le fichier :

```
"logLevel": "1"
```

Vérification et fourniture de journaux de débogage maximum

Vérification Windows

1. Ouvrez l'Observateur d'événements Windows.
2. Recherchez des lignes de journal similaires à ces exemples. Cela indique que la journalisation de débogage max. a été activée.

   Exemple 1 :

```
BRIDGE | Thread 1d18 | Connection : Resolved IP from 'swg-url-proxy-https.sigproxy.qq.opendns.com'
THREAD | Thread 1d18 | SetGUID '959bfe4d6fba87a65b433321c6748d761d9492cb'
```

Exemple 2 : Toute requête Web en cours de proxy est consignée. Les requêtes Web contournant AnyConnect SWG conformément à la liste des domaines internes/externes ne sont pas consignées.

```
LISTEN | Thread 1d18 | Connection : Hostnames from KDF are login.live.com
```

3. Utilisez la commande PowerShell pour convertir le nombre maximal de journaux d'événements de débogage (.evtx) en texte :

```
Get-WinEvent -Path C:\Desktop\Umbrella.evtx | Format-Table -AutoSize | Out-File C:\Desktop\Umbrell
```

Vérification macOS

Sur Mac OSX, la journalisation de débogage peut être visualisée avec cette commande (vous pouvez les grep ou les écrire en texte).

1. Exécutez la commande :

```
>log show --predicate 'subsystem contains "com.cisco.anyconnect.swg" || senderImagePath endswith "
```

   - Exemple de résultat lors de la navigation dans purple.com alors que la journalisation de débogage max est activée :

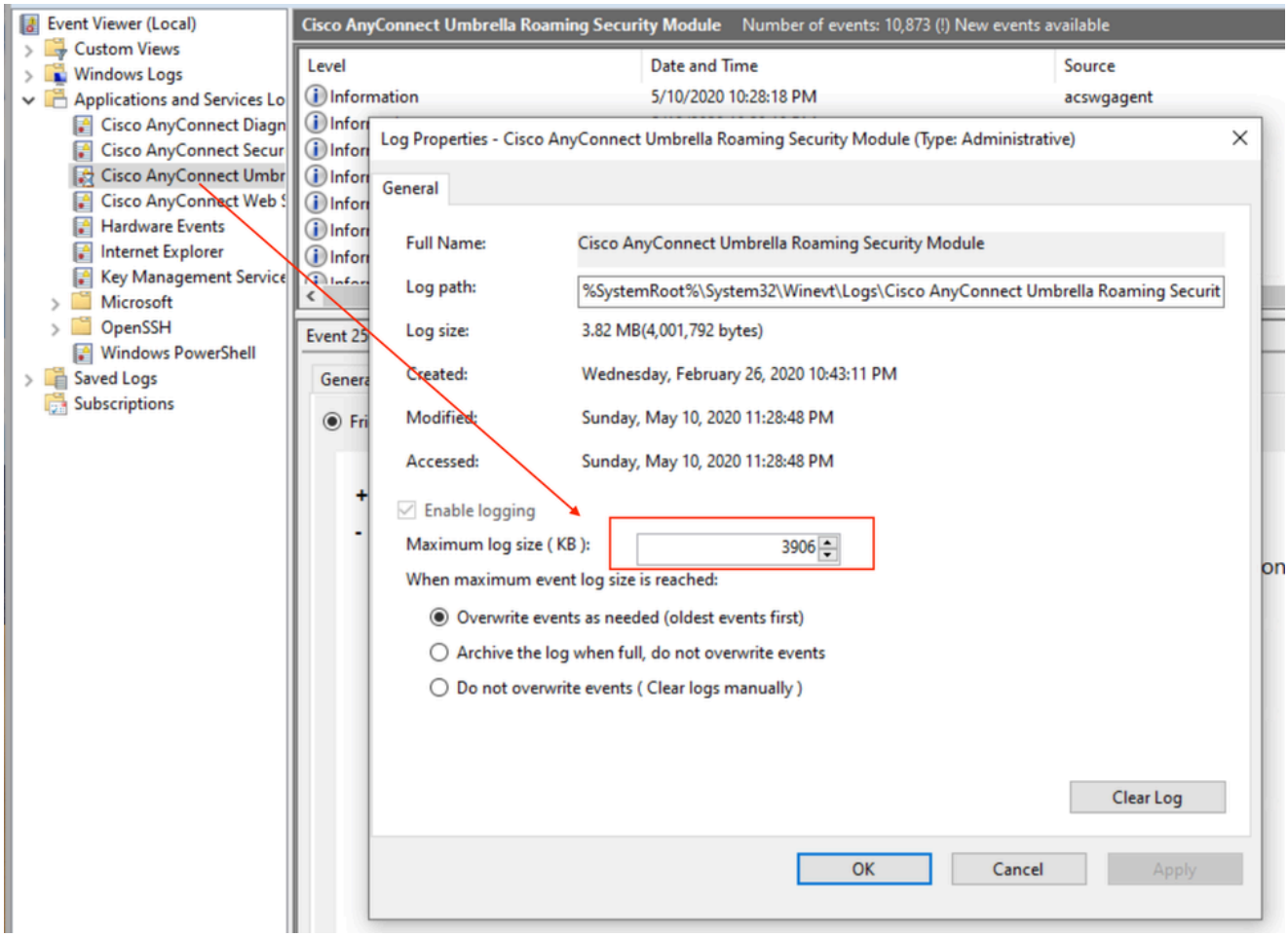
```
2022-09-19 10:51:15.627229+1000 0x16b121 Default 0x0 98970 0 acswgagent: Connection : Hostna
```

2. Le bundle DART AnyConnect inclut des journaux de débogage maximum. Après avoir vérifié l'activation, recréez le problème, enregistrez l'horodatage, l'expérience utilisateur et le domaine en question, et fournissez ces informations avec l'offre DART à prendre en charge.

Notes supplémentaires

- La journalisation de débogage maximale génère des journaux détaillés. Configurez la taille

du journal du module de sécurité d'itinérance Umbrella dans l'Observateur d'événements Windows pour prendre en charge les journaux volumineux, en particulier pour les problèmes intermittents.



360056784112

- Supprimez ou renommez le fichier swg_org_config.flag pour désactiver la journalisation de débogage maximale lorsque le dépannage est terminé.

Activer la journalisation de débogage maximale sur CSC 5.0 MR3 et AC 4.10 MR8 ou version ultérieure

Aperçu

À partir de CSC 5.0 MR3 et AC 4.10 MR8, l'activation de la journalisation de débogage utilise un processus plus simple.

Modifications

- Copiez le fichier SWGConfigOverride.json (avec le contenu statique) dans le dossier SWG pour activer la journalisation du débogage.
- Il n'est pas nécessaire de copier ou de modifier le orgConfig de SWGConfig.json. Le contenu de ce fichier ne changera pas org en org.

- Aucune dépendance sur le module DNS pour effectuer la synchronisation de la configuration ou la lecture à partir du fichier d'indicateur. Le fichier SWGConfig.json reste intact.

Activer la consignation du débogage

La valeur de configuration dans **SWGConfigOverride.json** est prioritaire sur la valeur (si elle est présente) dans ne SWGConfig.json. The **SWGConfigOverride.json** peut contenir et remplacer que deux configurations - logLevel (pour activer/désactiver la journalisation de débogage) et autotuning (pour activer/désactiver l'autotuning de la mémoire tampon d'envoi).

1. Pour activer la journalisation du débogage, copiezSWGConfigOverride.jsonavec le contenu :

```
{"logLevel": "1"}
```

   - Pour activer la journalisation du débogage et le réglage automatique, utilisez :

```
{"logLevel": "1", "autotuning": "1"}
```

2. Placez-le **SWGConfigOverride.json** dans le dossier SWG :

- Windows (AnyConnect) :
  `C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella\SWG\`
- Windows (client sécurisé) :
  `C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\SWG\`
- macOS (AnyConnect) :
  `/opt/cisco/anyconnect/umbrella/swg/`
- macOS (Secure Client) :
  `/opt/cisco/secureclient/umbrella/swg/`

3. Redémarrez le service SWG ou Umbrella, ou redémarrez le système.

- macOS : Arrêtez et démarrez l'agent AnyConnect ou Secure Client.
- Fenêtres: Redémarrez ou arrêtez/démarrez le service Secure Web Gateway (acswgagent dans 4.10.x builds /csc_swgagent dans 5.x builds) via le composant logiciel enfichable

Services MMC (Démarrer > Exécuter > Services.msc).



Remarque : L'ancienne méthode d'activation de la journalisation de débogage est toujours prise en charge et peut toujours être suivie. C'est la seule option pour les clients antérieurs à 5.0 MR3 ou 4.10 MR8.

Notes de configuration et de fonctionnement

- Le fichier est `SWGConfig.json` sensible à la casse. Utilisez `"logLevel": "1"` des guillemets doubles.
- La`logLevel`valeur est une chaîne 1, pas un entier, par conséquent elle doit être "1" avec des guillemets doubles.
- Le fichier `swg_org_config.flag` doit avoir une `.flag` extension, pas `.txt`.
- La journalisation de débogage maximale génère des journaux extrêmement détaillés. Activez la journalisation de débogage maximale uniquement si un ingénieur du support Umbrella le demande.
- Le fichier`swg_org_config.flag`contient une liste statique de domaines contournés et n'est pas synchronisé avec les domaines externes répertoriés dans Tableau de bord > Déploiements > Gestion des domaines.

Informations connexes

- Assistance technique de Cisco et téléchargements
- Centre d'aide Cisco Secure Access
- Guide de conception Cisco SASE

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.