Abilita registrazione di debug massima per il modulo SWG

Sommario

- Introduzione
- Casi di utilizzo per l'abilitazione della registrazione di massimo debug
- Abilitazione della registrazione di debug massima su AnyConnect 4.10 MR7, CSC 5.0 MR2 o versioni precedenti
  - Posizione di SWGConfig.json
  - Rendi permanente la registrazione di debug
    - Creazione del file dei flag
    - Copia e modifica del contenuto
    - Riavvia servizio
- Verifica e fornitura del numero massimo di log di debug
  - Verifica di Windows
  - Verifica macOS
  - Note aggiuntive
- Abilita registrazione di debug massima su CSC 5.0 MR3 e AC 4.10 MR8 o versioni successive
  - Panoramica
    - Modifiche
  - Abilita registrazione debug
- Note operative e di configurazione
- Informazioni correlate

Introduzione

Questo documento descrive come abilitare la registrazione massima del debug sul modulo Secure Web Gateway (SWG) per AnyConnect e Cisco Secure Client (CSC).

Casi di utilizzo per l'abilitazione della registrazione di massimo debug

Abilitare la registrazione di debug massima sul modulo SWG durante la risoluzione di problemi quali:

- Problemi di hotspot tramite Captive Portal
- L'elenco di esclusione del dominio esterno non viene applicato
- Problemi intermittenti di prestazioni DNS o Web

Abilitazione della registrazione di debug massima su AnyConnect

4.10 MR7, CSC 5.0 MR2 o versioni precedenti

Se si usa AnyConnect 4.10 MR7, CSC 5.0 MR2 o una versione precedente, attenersi alla seguente procedura. Per impostazione predefinita, la registrazione massima del debug non è abilitata e la configurazione non è consentita tramite il dashboard Umbrella o l'ASA. È necessario aggiungere manualmente `"logLevel": "1"` all`orgConfig`'oggetto nel `SWGConfig.json` file. Se si usa la versione più recente di AnyConnect o Cisco Secure Client, saltare questa sezione.

Posizione di SWGConfig.json

- Windows (AnyConnect):

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

- Windows (Secure Client):

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

- macOS (AnyConnect):

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

- macOS (client protetto):

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

Rendi permanente la registrazione di debug

Il file modificato `SWGConfig.json` rimane solo fino alla successiva sincronizzazione API da parte del modulo Cisco AnyConnect Umbrella. Per rendere persistente la configurazione e impedire che venga sovrascritta dalla sincronizzazione API, distribuire un `swg_org_config.flag` file nella `Umbrella/data` cartella.

1. Creazione del file dei flag

    - Creare un nuovo file denominato **`swg_org_config.flag`** nella cartella Dati ombrello. L'estensione del file deve essere `.flag`.

    - Windows (AnyConnect):

-

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

- Windows (Secure Client):

-

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

- macOS (AnyConnect):

-

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

- macOS (client protetto):

-

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

2. Copia e modifica del contenuto

- Copiare il contenuto dell**orgConfig**'oggetto dal SWGConfig.json file al swg_org_config.flag file.
- Aggiungi con "logLevel": "1".
- Ad esempio:

```
{
"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"
}
```

- Assicurarsi che il file di flag inizi con { "exceptionList": [...] e termini con **"SWGEchoService": "http://www.msftconecttest.com/connecttest.txt"}**.
- Evitare di copiare righe in eccesso prima o dopo l'oggetto.
- La copia non corretta di linee quali identity, deviceIdo adUserIDpuò compromettere la funzionalità SWG.

Esempio non corretto: Il file di contrassegno contiene chiavi quali **identity**, deviceIdo dUserID precedenti

Esempio corretto: Il file di contrassegno inizia con { "exceptionList":

14970100184724

3. Riavvia servizio
   - Riavviare il servizio Cisco AnyConnect Secure Mobility Agent/Secure Client, riavviare il computer o connettere e disconnettere la VPN.
4. Verifica della configurazione
   - Dopo il riavvio o la connessione/disconnessione VPN, aprire il file per SWGConfig.json confermare l'impostazione del livello massimo del registro di debug SWG. Una volta configurata, questa voce viene visualizzata nel file:

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

Verifica e fornitura del numero massimo di log di debug

Verifica di Windows

1. Aprire il Visualizzatore eventi di Windows.
2. Cercare righe di registro simili a quelle illustrate negli esempi seguenti. Ciò indica che la registrazione di Max Debug è stata abilitata.

   Esempio 1:

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

Esempio 2: Tutte le richieste Web in fase di inoltro vengono registrate. Le richieste Web che ignorano AnyConnect SWG in base all'elenco dei domini interni/esterni non vengono registrate.

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

3. Utilizzare il comando PowerShell per convertire il numero massimo di registri eventi di debug (.evtx) in txt:

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

Verifica macOS

In Mac OSX, la registrazione di debug può essere visualizzata con questo comando (è possibile utilizzare il comando grep o scriverlo in txt).

1. Eseguire il comando:

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

   - Output di esempio durante l'esplorazione di purple.com mentre è attivata la registrazione di Max Debug:

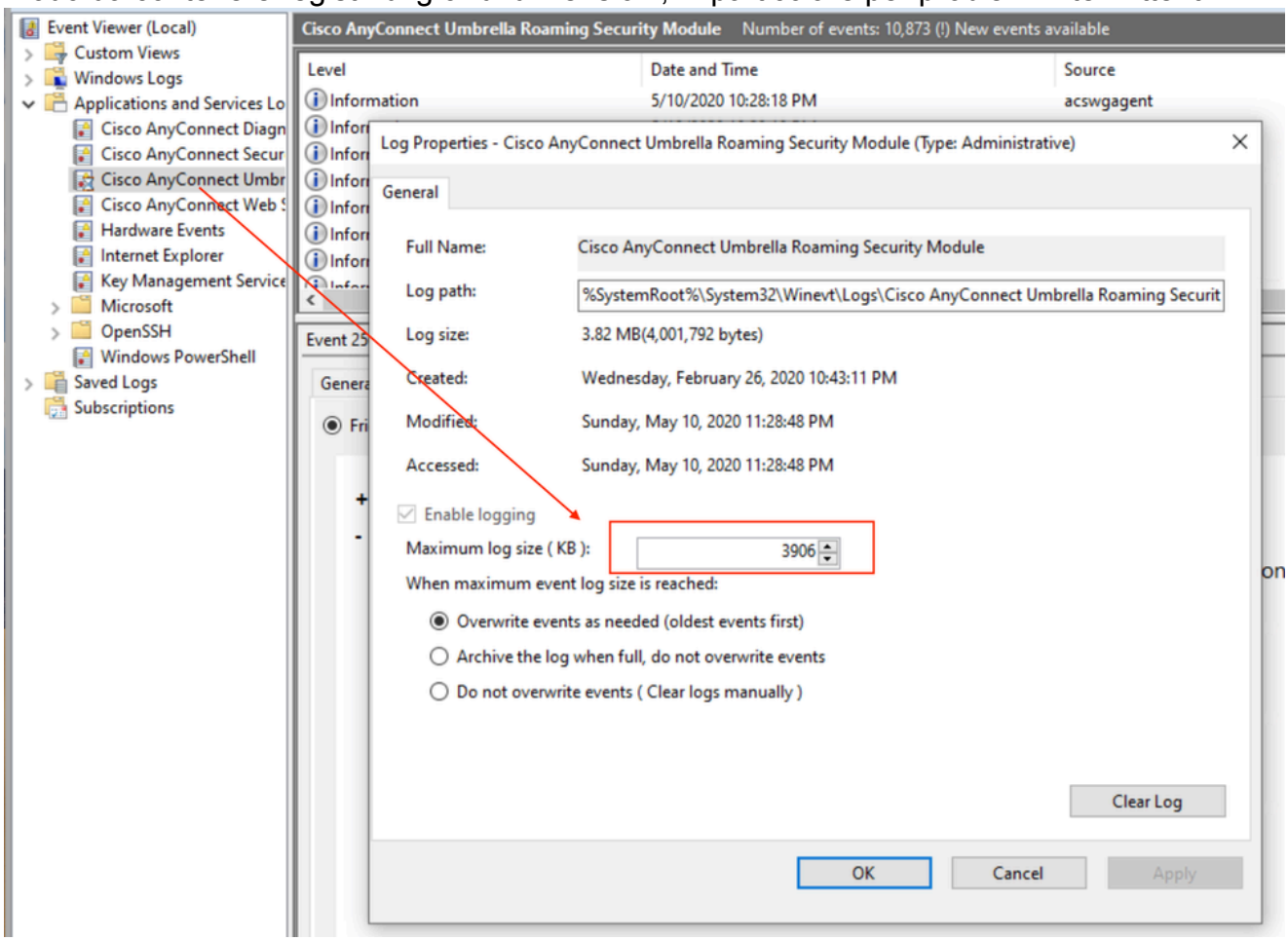
```
2022-09-19 10:51:15.627229+1000 0x16b121 Default 0x0 98970 0 acswgagent: Connection : Hostna
```

2. Il bundle DART di AnyConnect include il numero massimo di log di debug. Dopo aver verificato l'abilitazione, ricreare il problema, registrare l'indicatore orario, l'esperienza utente e il dominio in questione e fornire queste informazioni insieme al pacchetto DART da supportare.

Note aggiuntive

- La registrazione di debug massima genera registri dettagliati. Configurare le dimensioni del registro del modulo di sicurezza Umbrella Roaming nel Visualizzatore eventi di Windows in

modo da contenere registri di grandi dimensioni, in particolare per problemi intermittenti.



360056784112

- Rimuovere o rinominare il file per swg_org_config.flag disattivare la registrazione di Max Debug al termine della risoluzione dei problemi.

Abilita registrazione di debug massima su CSC 5.0 MR3 e AC 4.10 MR8 o versioni successive

Panoramica

A partire da CSC 5.0 MR3 e AC 4.10 MR8, l'abilitazione della registrazione del debug utilizza un processo più semplice.

Modifiche

- Copiare il file (con contenuto statico) nella SWGConfigOverride.json cartella SWG per abilitare la registrazione di debug.
- Non è necessario copiare o modificare l' orgConfig da SWGConfig.json. Il contenuto di questo file non cambierà org in org.
- Nessuna dipendenza dal modulo DNS per eseguire la sincronizzazione della configurazione o la lettura dal file di flag. Il file non SWGConfig.json viene modificato.

Abilita registrazione debug

Il valore config in **SWGConfigOverride.json** ha la precedenza sul valore (se presente) in SWGConfig.json. The **SWGConfigOverride.json** può contenere ed eseguire l'override solo di due configurazioni: logLevel (per abilitare/disabilitare il log di debug) e autotuning (per abilitare/disabilitare l'autotuning del buffer di invio).

1. Per abilitare la registrazione del debug, copiareSWGConfigOverride.jsonil contenuto:

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

   - Per abilitare sia il log di debug che il tuning automatico, utilizzare:

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

2. Posizionate **SWGConfigOverride.json** nella cartella SWG:

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

3. Riavviare il servizio SWG o Umbrella oppure riavviare il sistema.

- macOS: Arrestare e avviare l'agente AnyConnect o Secure Client.
- Windows: Riavviare, arrestare o avviare il servizio Gateway Web sicuro (acswgagent in 4.10.x build /csc_swgagent in 5.x build) tramite lo snap-in MMC Servizi (Start > Esegui > Servizi.msc).

Nota: Il metodo precedente per l'abilitazione della registrazione del debug è ancora supportato e può ancora essere seguito ed è l'unica opzione disponibile per i client con più di 5.0 MR3 o 4.10 MR8.

Note operative e di configurazione

- Nel file `SWGConfig.json` viene fatta distinzione tra maiuscole e minuscole. Utilizzare `"logLevel": "1"` tra virgolette.
- Il`logLevel`valore è una stringa 1, non un intero, quindi deve essere "1" con virgolette doppie.
- Il file `swg_org_config.flag` deve avere un'`.flag`estensione, non `.txt`un'estensione.
- Il log di debug massimo genera log estremamente dettagliati. Abilitare la registrazione massima del debug solo se richiesto da un tecnico del supporto Umbrella.
- `swg_org_config.flag`Il file contiene un elenco statico dei domini ignorati e non viene sincronizzato con i domini esterni elencati in Dashboard > Distribuzioni > Gestione dominio.

Informazioni correlate

- Supporto tecnico Cisco e download
- Cisco Secure Access Help Center
- Guida alla progettazione di Cisco BASE

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).