Où sont stockés les journaux sur l'appliance de sécurité de la messagerie Cisco (ESA) et comment y accéder ?

L'appliance de sécurité de la messagerie Cisco (ESA) crée un répertoire pour chaque abonnement au journal en fonction du nom de l'abonnement au journal.

Format de fichier journal ESA

Le nom réel du fichier journal dans le répertoire est composé du nom de fichier journal que vous avez spécifié, de l'horodatage au démarrage du fichier journal et d'un code d'état à un caractère.

```
/LogSubscriptionName/LogFilename.@timestamp.statuscode
```

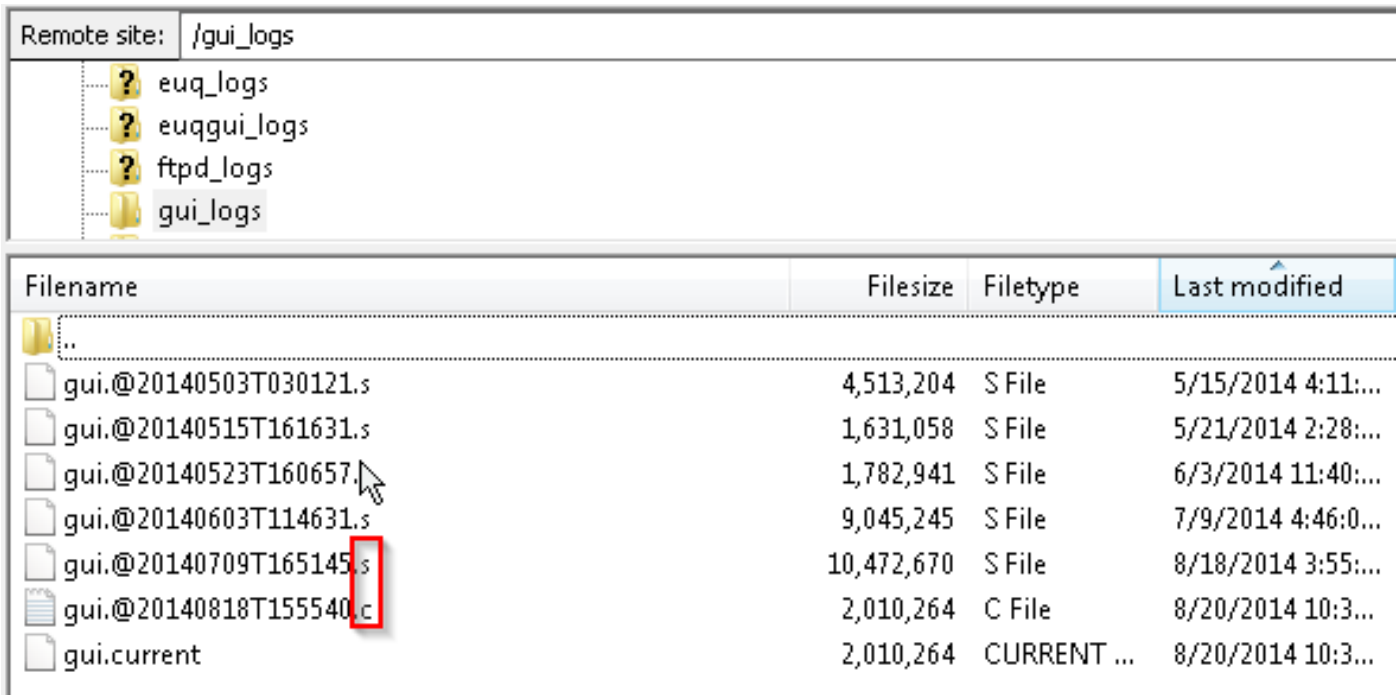
LogSubscriptionNames peut être vu via la commande **logconfig** :

```
esa.example.com> logconfig

Currently configured logs:
   Log Name            Log Type                      Retrieval           Interval
 ---------------------------------------------------------------------------------
 1. TLStest             Injection Debug Logs          Manual Download     None
 2. Test                Domain Debug Logs             Manual Download     None
 3. amp                 AMP Engine Logs               Manual Download     None
 4. amparchive          AMP Archive                   Manual Download     None
 5. antispam            Anti-Spam Logs                Manual Download     None
 6. antivirus           Anti-Virus Logs               Manual Download     None
 7. asarchive           Anti-Spam Archive             Manual Download     None
 8. authentication      Authentication Logs           Manual Download     None
 9. avarchive           Anti-Virus Archive            Manual Download     None
10. bounces             Bounce Logs                   Manual Download     None
11. cli_logs            CLI Audit Logs                Manual Download     None
12. encryption          Encryption Logs               Manual Download     None
13. error_logs          IronPort Text Mail Logs       Manual Download     None
```

Extensions de fichier journal supplémentaires

Les codes d'état peuvent afficher une extension de fichier telle que .c (courant signifiant) ou .s (signifiant enregistré)



Comment puis-je accéder aux journaux ?

Par défaut, il existe deux méthodes pour récupérer vos journaux qui sont stockés dans votre ESA : **FTP ou SCP.**

Vous devez utiliser les mêmes informations d'identification de connexion pour la récupération des journaux que pour l'authentification auprès de l'ESA pour l'administration.

Journaux d'accès par FTP

FTP: Ligne de commande

```
ftp hostname.example.com
cd /LogNameDirectory
get
```

FTP : client GUI

Un client FTP GUI tel que Filezilla peut être utilisé pour faire glisser-déplacer de l'ESA vers votre machine locale.

Utilisation de FTP : Navigateur Web

Tout navigateur Web pris en charge par FTP, tel que Mozilla Firefox, Google Chrome ou Microsoft Internet Explorer, peut également être utilisé.

Copier les journaux vers un autre système via SCP

Utilisation de SCP :

```
scp admin@mail3.example.com:/LogNameDirectory/LogFilename
```

Note: Assurez-vous que le service approprié (FTP ou SCP) est activé sur votre ESA à l'aide de la commande **interfaceconfig** dans l'interface de ligne de commande.