Dove e come posso accedere ai log archiviati su Cisco Email Security Appliance (ESA)?

Cisco Email Security Appliance (ESA) crea una directory per ciascuna sottoscrizione di log in base al nome della sottoscrizione di log.

Formato file registro ESA

Il nome effettivo del file di log nella directory è composto dal nome del file di log specificato dall'utente, dall'indicatore orario di avvio del file di log e da un codice di stato a carattere singolo.

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

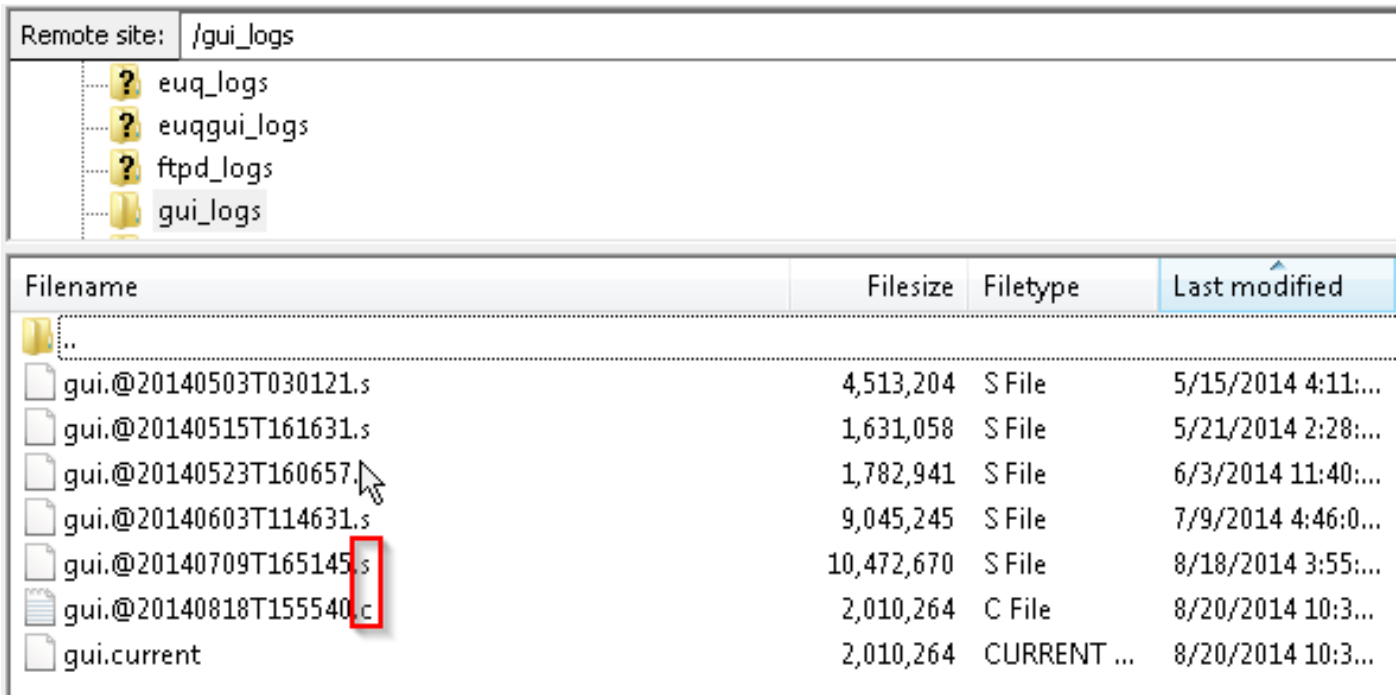
Per visualizzare LogSubscriptionNames, usare il comando **logconfig**:

```
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
```

Estensioni di file di log aggiuntive

I codici di stato possono avere l'estensione .c (che indica corrente) o .s (che indica salvato)



Come si accede ai registri?

Per impostazione predefinita, esistono due metodi per recuperare i log memorizzati nell'ESA: **FTP o SCP.**

Per il recupero dei log è necessario utilizzare le stesse credenziali di login utilizzate per autenticarsi all'ESA per l'amministrazione.

Log degli accessi tramite FTP

FTP: Riga di comando

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

FTP: Client GUI

Un client FTP GUI come Filezilla può essere utilizzato per "trascinare e rilasciare" dall'ESA al computer locale.

FTP: Browser Web

Èpossibile utilizzare anche qualsiasi browser Web FTP supportato, come Mozilla Firefox, Google Chrome o Microsoft Internet Explorer.

Copia dei log in un altro sistema tramite SCP

Uso di SCP:

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

Nota: Verificare di aver abilitato il servizio corretto (FTP o SCP) sull'ESA usando il comando **interfaceconfig** nella CLI.