Scaricare i log dalla GUI di CES ESA e CMD

Sommario

Introduzione

In questo documento viene descritto come scaricare i log dall'interfaccia grafica utente (GUI) del Secure Email Cloud Gateway (CES) tramite la riga di comando (CMD).

Prerequisiti

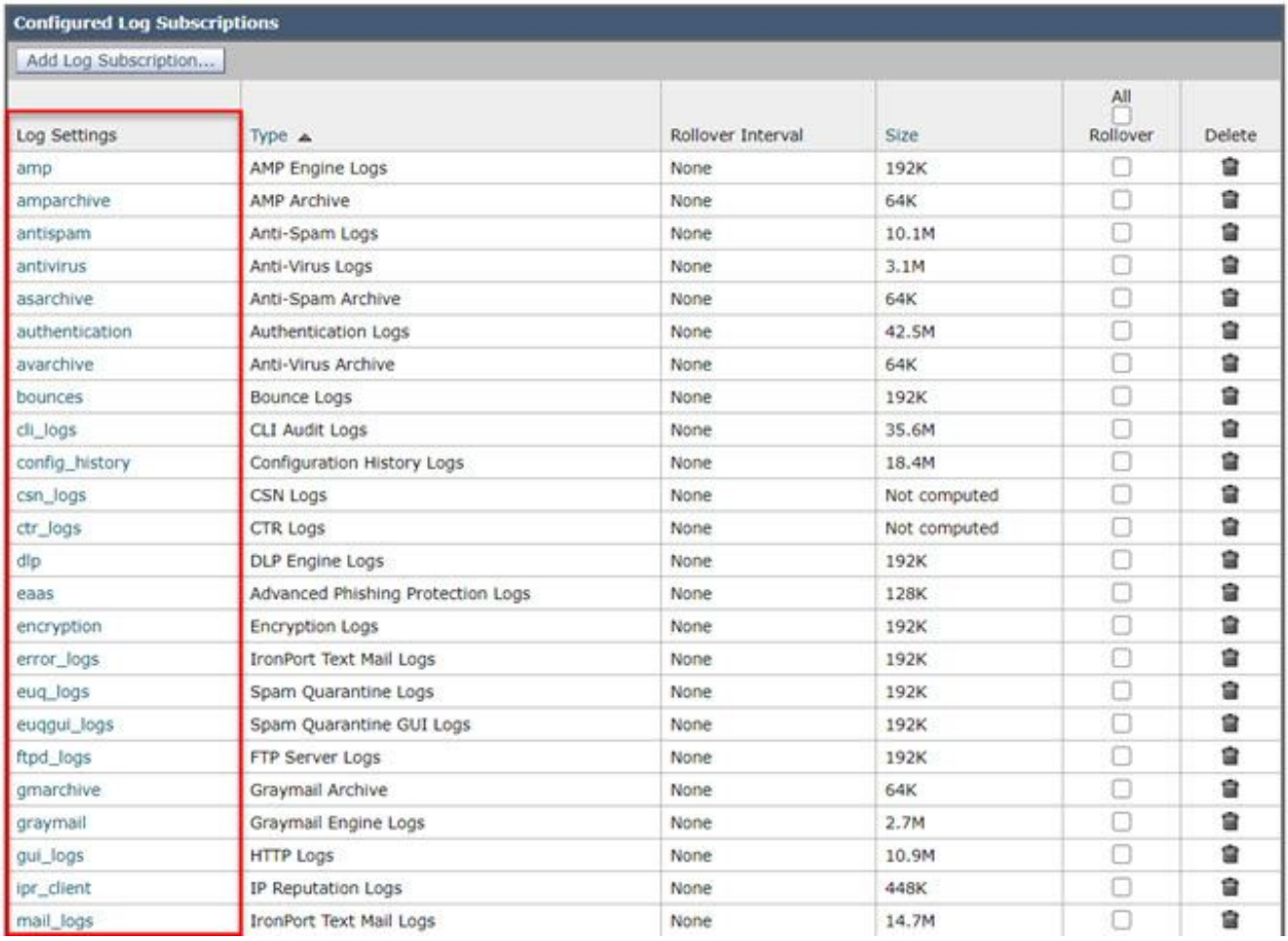
Account utente con autorizzazione Amministratore o Amministratore cloud.

Download dei log dalla GUI

1. Accedere alla GUI dell'istanza di CES Email Security Appliance (ESA) e selezionare **Amministrazione sistema > Registra sottoscrizioni.**

2. Si noti l'URL visualizzato nel browser (ad esempio: Sottoscrizioni ai log di amministrazione del sistema)

3. Quindi, è necessario rivedere la colonna **Impostazioni log** e trovare un log che si desidera scaricare. Per questo esempio, utilizzare **mail_logs**.



Configured Log Subscriptions

Add Log Subscription...

Log Settings	Type	Rollover Interval	Size	All Rollover	Delete
amp	AMP Engine Logs	None	192K		
amparchive	AMP Archive	None	64K		
antispam	Anti-Spam Logs	None	10.1M		
antivirus	Anti-Virus Logs	None	3.1M		
asarchive	Anti-Spam Archive	None	64K		
authentication	Authentication Logs	None	42.5M		
avarchive	Anti-Virus Archive	None	64K		
bounces	Bounce Logs	None	192K		
cli_logs	CLI Audit Logs	None	35.6M		
config_history	Configuration History Logs	None	18.4M		
csn_logs	CSN Logs	None	Not computed		
ctr_logs	CTR Logs	None	Not computed		
dlp	DLP Engine Logs	None	192K		
eaas	Advanced Phishing Protection Logs	None	128K		
encryption	Encryption Logs	None	192K		
error_logs	IronPort Text Mail Logs	None	192K		
euq_logs	Spam Quarantine Logs	None	192K		
euqgui_logs	Spam Quarantine GUI Logs	None	192K		
ftpd_logs	FTP Server Logs	None	192K		
gmarchive	Graymail Archive	None	64K		
graymail	Graymail Engine Logs	None	2.7M		
gui_logs	HTTP Logs	None	10.9M		
ipr_client	IP Reputation Logs	None	448K		
mail_logs	IronPort Text Mail Logs	None	14.7M		

4. Prendere l'URL dal secondo passaggio e apportare le modifiche:

r. Rimuovere /log_subscriptions.

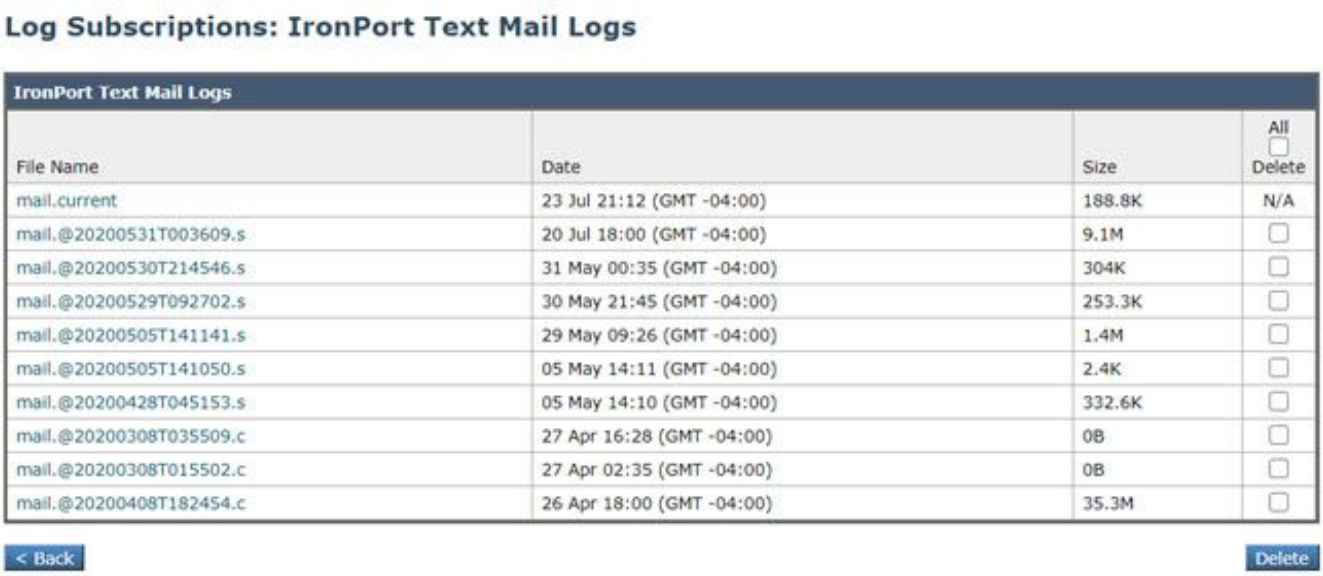
b. Aggiungere /log_list?log_type=<logname> alla fine dell'URL, dove <logname> viene sostituito con quanto visualizzato in **Impostazioni registro**

colonna.

c. Sostituire dhXXXX-esa1.iphmx.com con il nome di dominio completo (FQDN) dell'ESA.

Nota: per utilizzare mail_logs come esempio, le sottoscrizioni dei log di amministrazione del sistema diventano elenco dei log di amministrazione del sistema.

5. Infine, selezionare l'URL modificato e accedere. Viene visualizzata una pagina simile a quella mostrata nell'immagine in cui è possibile fare clic su un file, scaricarlo e salvarlo.

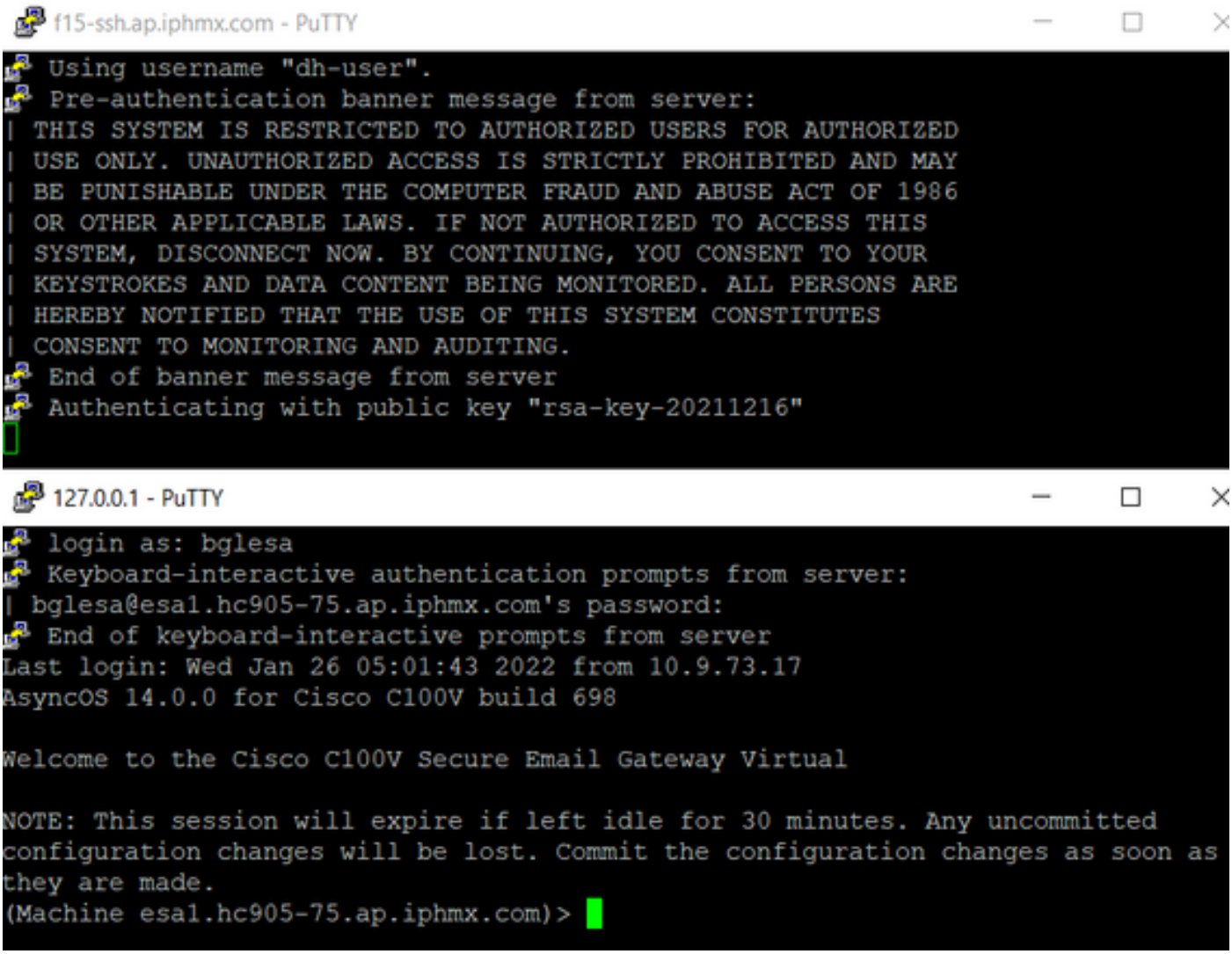


Download dei log da CMD

accertarsi di disporre dell'accesso CLI di CES ESA. Per la procedura di richiesta dell'accesso alla CLI, fare riferimento all'articolo Accesso alla CLI del cliente.

Si consiglia di utilizzare Putty SCP (PSCP) deve avere accesso SSH per estrarre i log:

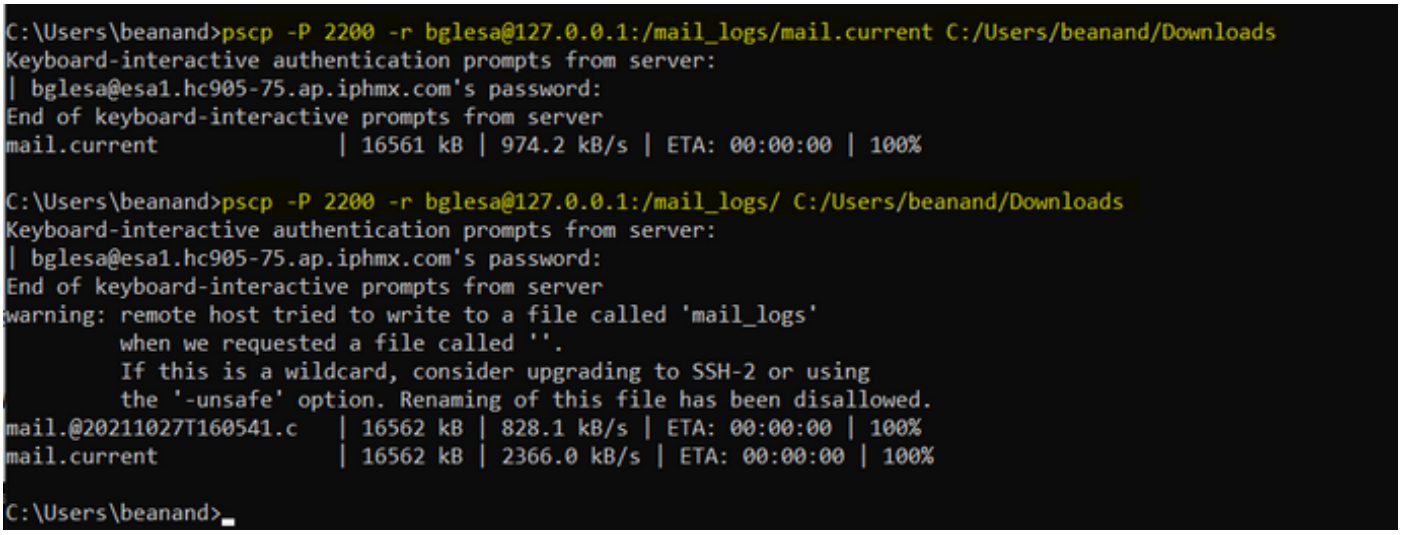
1. Scarica PSCP Scarica PuTTY
2. Aprire la configurazione proxy abilitata su ESA, quindi lasciare il proxy aperto.



3. Eseguire CMD e digitare: **pscp -P porta -r <utente>@localhost:/mail_logs/* /path/on/local/system**

1. La porta è quella precedentemente configurata per l'accesso dalla CLI.
2. /mail_logs/ indica che verranno scaricati tutti i file contenuti nella cartella specificata.
3. Se è necessario scaricare solo il file corrente, digitare /mail_logs/mail.current o il registro necessario.
4. Immettere la password quando richiesto dopo l'immissione del comando.

Comando di esempio: **pscp -P 2200 -r admin@127.0.0.1:/mail_logs/ C:/Users/band/Downloads**



Informazioni correlate

- [Cisco Email Security Appliance - Guide per l'utente]

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).