Téléchargez les journaux depuis l'interface graphique de votre ESA CES et de votre CMD

Table des matières

Introduction

Ce document décrit comment télécharger des journaux à partir de l'interface graphique utilisateur (GUI) de votre passerelle de cloud de messagerie sécurisée (CES) via la ligne de commande (CMD).

Conditions préalables

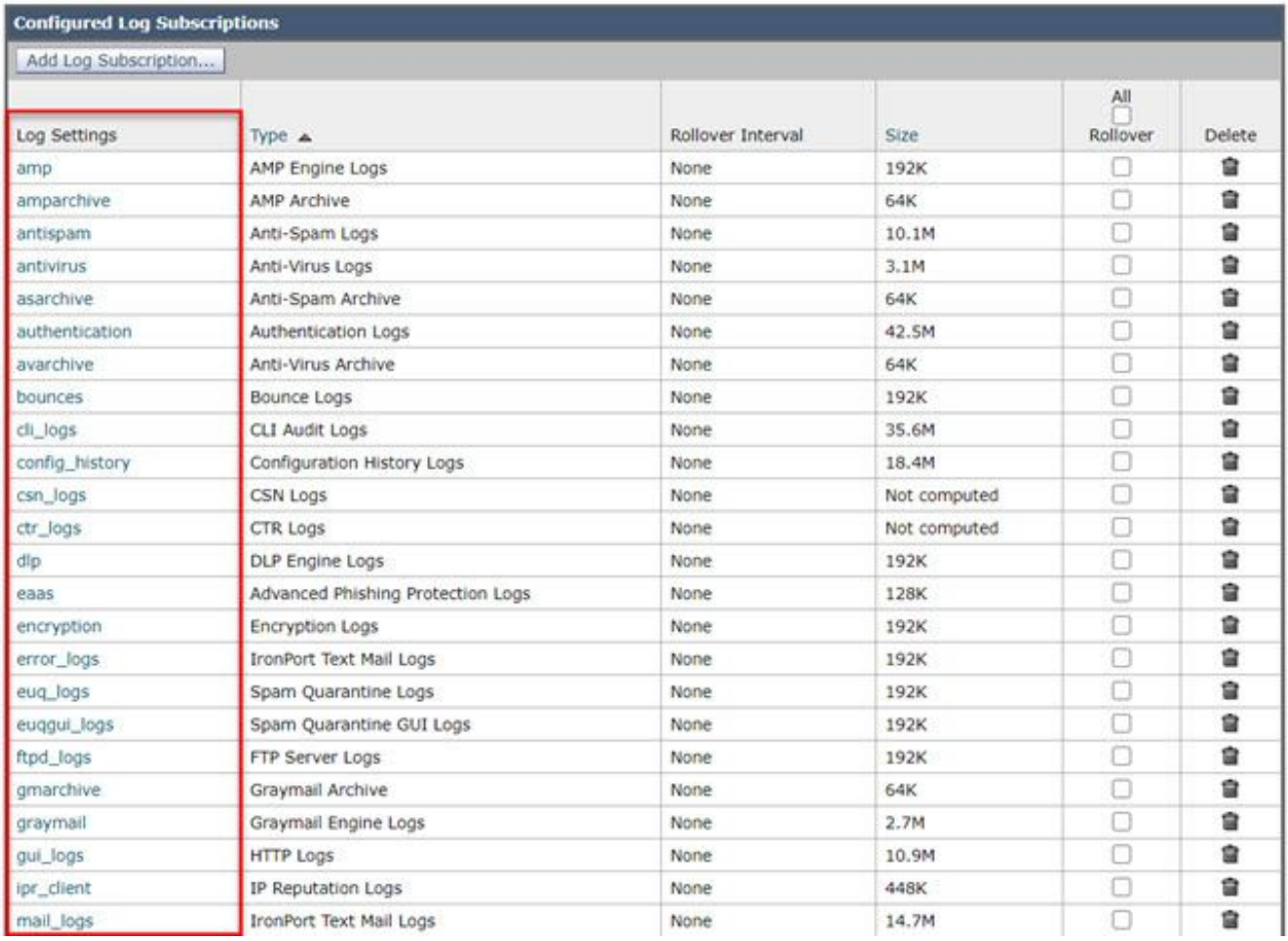
Un compte d'utilisateur avec l'autorisation Administrateur ou Administrateur cloud.

Télécharger les journaux depuis l'interface graphique

1. Connectez-vous à l'interface utilisateur graphique de votre instance ESA (Email Security Appliance) CES et accédez à **Administration système > Inscriptions au journal.**

2. Notez l'URL affichée dans votre navigateur (Exemple : [Abonnements au journal d'administration du système](#))

3. Ensuite, vous devez passer en revue la colonne **Log Settings** et trouver un journal que vous souhaitez télécharger. Pour cet exemple, utilisez **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. Prenez l'URL de l'étape deux et effectuez les modifications suivantes :

a. Supprimez /log_subscriptions.

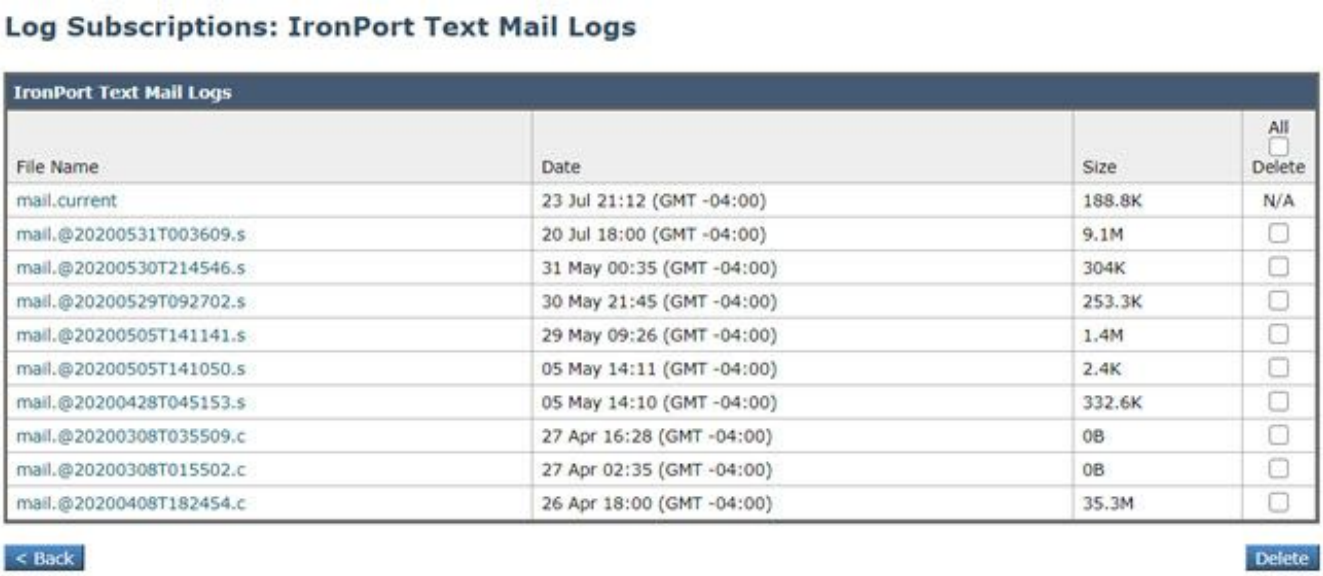
b. Ajoutez /log_list?log_type=<nom_journal> à la fin de l'URL, où <nom_journal> est remplacé par ce qui est affiché sous les **paramètres de journal**

colonne.

c. Remplacez dhXXXX-esa1.iphmx.com par le nom de domaine complet (FQDN) de votre ESA.

Remarque : pour utiliser mail_logs comme exemple, System Administration Log Subscriptions devient System Administration Log List.

5. Enfin, accédez à l'URL modifiée et connectez-vous. Vous accédez à une page similaire à celle de l'image, où vous pouvez cliquer sur un fichier, le télécharger et l'enregistrer.

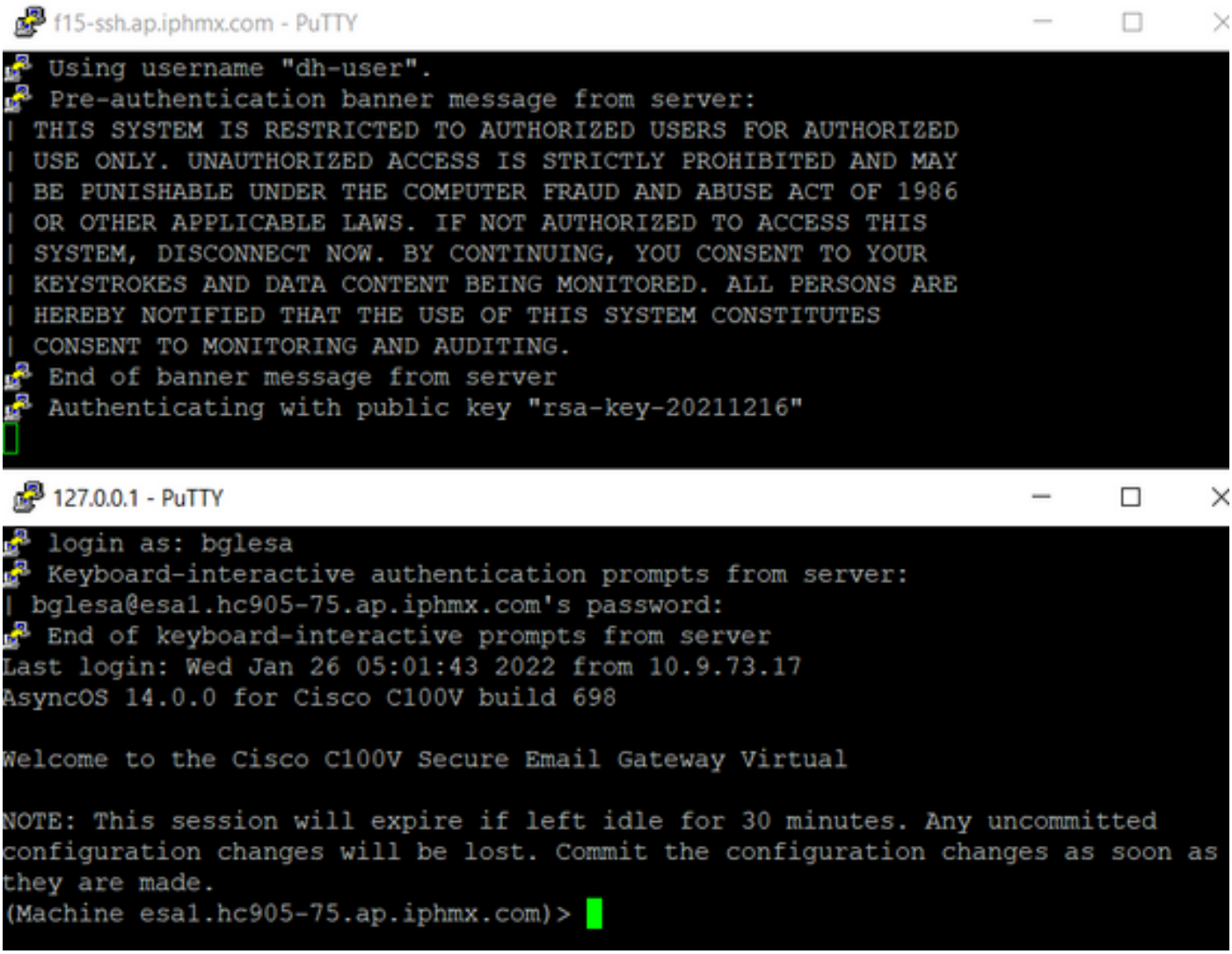


Télécharger les journaux depuis CMD

Assurez-vous que vous disposez de l'accès CLI de l'ESA CES. Pour connaître les étapes à suivre pour demander un accès à l'interface de ligne de commande, consultez l'article Accès à l'interface de ligne de commande client.

Il est recommandé d'utiliser Putty SCP (PSCP) pour avoir un accès SSH afin d'extraire les journaux :

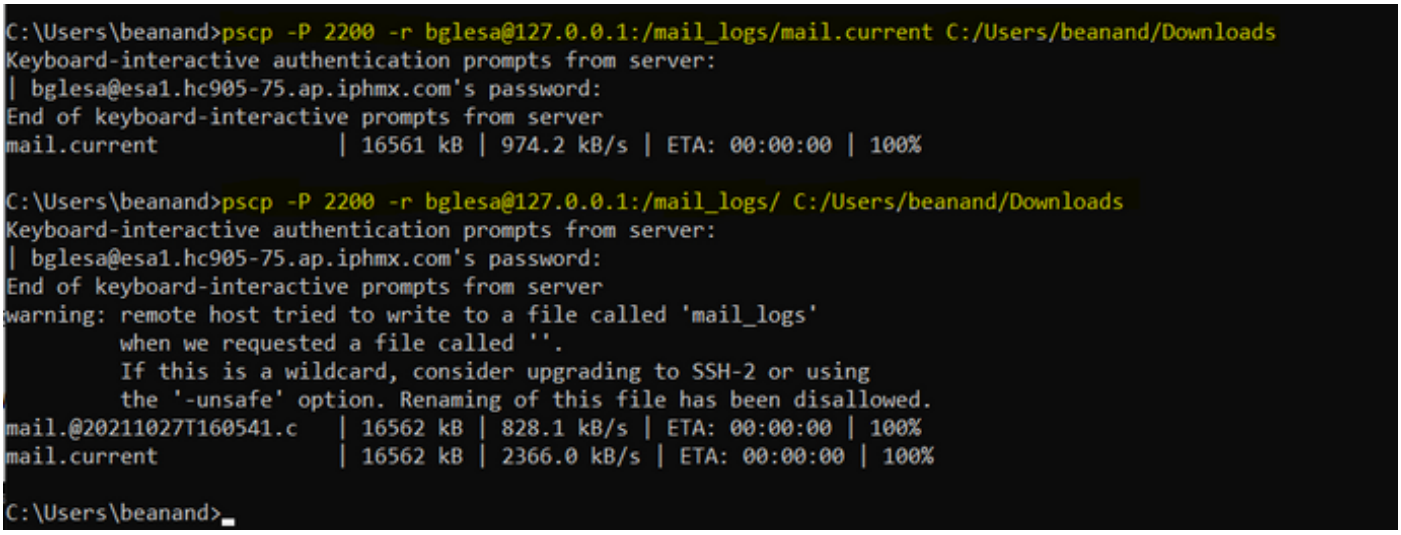
1. Télécharger PSCP Télécharger PuTTY
2. Ouvrez la configuration de proxy activée sur ESA et laissez le proxy ouvert.



3. Exécutez CMD et tapez : **pscp -P port -r <user>@localhost:/mail_logs/* /path/on/local/system**

1. Le port est celui qui est précédemment configuré pour l'accès CLI.
2. /mail_logs/ signifie qu'il télécharge tous les fichiers sous ce dossier particulier.
3. Si seul le fichier actuel doit être téléchargé, tapez /mail_logs/mail.current ou le journal requis.
4. Entrez le mot de passe lorsque vous y êtes invité une fois la commande entrée.

Exemple de commande : **pscp -P 2200 -r admin@127.0.0.1:/mail_logs/ C:/Users/beanand/Downloads**



Informations connexes

- Appliance de sécurisation de la messagerie Cisco - Guides de l'utilisateur final

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.