Accéder aux journaux de l'appliance Web sécurisée

Table des matières

Introduction

Ce document décrit les méthodes d'affichage des journaux de l'appareil Web sécurisé (SWA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- SWA physique ou virtuel installé.
- Licence activée ou installée.
- Client Secure Shell (SSH).
- L'Assistant de configuration est terminé.
- Accès administratif au SWA.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Types de journaux SWA

L'appliance Web sécurisée enregistre ses propres activités de gestion du système et du trafic en les consignant dans des fichiers journaux. Les administrateurs peuvent consulter ces fichiers journaux pour surveiller et dépanner l'appliance.

Ce tableau décrit les types de fichier journal de l'appliance Web sécurisée.

Type de fichier journal	Description	Prend en charge Syslog Push ?	Activé par défaut ?
Journaux du moteur de contrôle d'accès	Enregistre les messages liés au moteur d'évaluation de la liste de contrôle d'accès du proxy Web.	Non	Non
Journaux Secure Endpoint Engine	Enregistre des informations sur l'analyse de réputation et l'analyse des fichiers (Secure Endpoint).	Oui	Oui
Journaux d'audit	Enregistre les événements AAA (Authentication, Authorization, and Accounting). Enregistre toutes les interactions de l'utilisateur avec l'application et les interfaces de ligne de commande, et capture les modifications validées. Voici quelques-uns des détails du journal d'audit : • Utilisateur - Connexion • Utilisateur - Echec de la connexion - Mot de passe incorrect • Utilisateur - Echec de la connexion nom d'utilisateur inconnu • Utilisateur - Le compte de connexion a expiré • Utilisateur - Déconnexion • Utilisateur - Verrouillage • Utilisateur - Activé • Utilisateur - Modification du mot de passe • Utilisateur - Mot de passe réinitialisé • Utilisateur - Paramètres de sécurité/modification du	Oui	Oui

Type de fichier journal	Description	Prend en charge Syslog Push ?	Activé par défaut ?
	profil • Utilisateur - Créé • Utilisateur - Supprimé/modifié • Groupe/Rôle - Suppression/modification • Groupe/Rôle - Modification des autorisations		
Journaux d'accès	Enregistre l'historique du client proxy Web.	Oui	Oui
Journaux du framework du moteur ADC	Enregistre les messages liés à la communication entre le proxy Web et le moteur ADC.	Non	Non
Journaux du moteur ADC	Enregistre les messages de débogage du moteur ADC.	Oui	Oui
Journaux du cadre d'authentification	Enregistre l'historique et les messages d'authentification.	Non	Oui
Journaux du framework du moteur AVC	Enregistre les messages liés à la communication entre le proxy Web et le moteur AVC.	Non	Non
Journaux du moteur AVC	Enregistre les messages de débogage du moteur AVC.	Oui	Oui
Journaux d'audit CLI	Enregistre un audit historique de l’activité de l’interface de ligne de commande.	Oui	Oui
Journaux de configuration	Enregistre les messages relatifs au système de gestion de la configuration du proxy Web.	Non	Non

Type de fichier journal	Description	Prend en charge Syslog Push ?	Activé par défaut ?
Journaux de gestion des connexions	Enregistre les messages liés au système de gestion des connexions du proxy Web.	Non	Non
Journaux de sécurité des données	Enregistre l'historique du client pour les demandes de téléchargement évaluées par les filtres de sécurité des données Cisco.	Oui	Oui
Journaux du module de sécurité des données	Enregistre les messages relatifs aux filtres de sécurité des données Cisco.	Non	Non
Journaux du cadre du moteur DCA (Analyse dynamique du contenu)	Enregistre les messages liés à la communication entre le proxy Web et le moteur d'analyse dynamique du contenu des contrôles d'utilisation Web de Cisco.	Non	Non
Journaux du moteur DCA (Analyse dynamique du contenu)	Enregistre les messages liés au moteur d'analyse dynamique du contenu des contrôles d'utilisation Web de Cisco.	Oui	Oui
Journaux proxy par défaut	Enregistre les erreurs liées au proxy Web. Il s'agit du journal le plus basique de tous les journaux liés au proxy Web. Pour résoudre des problèmes plus spécifiques liés au proxy Web, créez un abonnement au journal pour le module de proxy Web concerné.	Oui	Oui
Journaux de Disk Manager	Enregistre les messages du proxy Web relatifs à l'écriture dans le cache sur le disque.	Non	Non

Type de fichier journal	Description	Prend en charge Syslog Push ?	Activé par défaut ?
Journaux d'authentification externes	Enregistre les messages relatifs à l'utilisation de la fonctionnalité d'authentification externe, tels que la réussite ou l'échec de la communication avec le serveur d'authentification externe. Même si l'authentification externe est désactivée, ce journal contient des messages sur les utilisateurs locaux qui se connectent avec succès ou qui échouent.	Non	Oui
Journaux des commentaires	Enregistre les utilisateurs Web signalant des pages mal classées.	Oui	Oui
Journaux du proxy FTP	Enregistre les messages d'erreur et d'avertissement relatifs au proxy FTP.	Non	Non
Journaux du serveur FTP	Enregistre tous les fichiers téléchargés vers et depuis l'appliance Web sécurisé via FTP.	Oui	Oui
Journaux GUI (Interface graphique utilisateur)	Enregistre l'historique des actualisations de page dans l'interface Web. Les journaux de l'interface utilisateur graphique contiennent également des informations sur les transactions SMTP, par exemple des informations sur les rapports planifiés envoyés par e-mail depuis l'appliance.	Oui	Oui
Journaux Haystack	Haystack enregistre le traitement des données de suivi des transactions Web.	Oui	Oui
Journaux HTTPS	Enregistre les messages du proxy Web spécifiques au proxy HTTPS (lorsque le proxy HTTPS est activé).	Non	Non
Journaux du serveur ISE	Enregistre les informations de connexion et de fonctionnement des serveurs ISE.	Oui	Oui
Journaux du module de licence	Enregistre les messages relatifs au système de gestion des clés de licence et de fonctionnalité du proxy Web.	Non	Non

Type de fichier journal	Description	Prend en charge Syslog Push ?	Activé par défaut ?
Journaux du cadre de journalisation	Enregistre les messages liés au système de journalisation du proxy Web.	Non	Non
Journaux de journalisation	Enregistre les erreurs liées à la gestion des journaux.	Oui	Oui
Journaux de McAfee Integration Framework	Enregistre les messages relatifs à la communication entre le proxy Web et le moteur d'analyse McAfee.	Non	Non
Journaux McAfee	Enregistre l'état de l'activité d'analyse anti-programme malveillant à partir du moteur d'analyse McAfee.	Oui	Oui
Journaux de Memory Manager	Enregistre les messages du proxy Web relatifs à la gestion de toute la mémoire, y compris le cache en mémoire pour le processus du proxy Web.	Non	Non
Journaux de modules proxy divers	Enregistre les messages de proxy Web qui sont principalement utilisés par les développeurs ou le support client.	Non	Non
Journaux des démons AnyConnect Secure Mobility	Enregistre l'interaction entre l'appliance Web sécurisé et le client AnyConnect, y compris la vérification de l'état.	Oui	Oui
Journaux NTP (Protocole d'Heure Réseau)	Enregistre les modifications apportées à l'heure système par le protocole NTP.	Oui	Oui
Journaux des démons d'hébergement de fichiers PAC	Enregistre l'utilisation du fichier de configuration automatique du proxy (PAC) par les clients.	Oui	Oui

Type de fichier journal	Description	Prend en charge Syslog Push ?	Activé par défaut ?
Journaux de contournement du proxy	Enregistre les transactions qui contournent le proxy Web.	Non	Oui
Journaux de rapports	Enregistre un historique de génération de rapports.	Oui	Oui
Journaux de requête de rapport	Enregistre les erreurs liées à la génération de rapports.	Oui	Oui
Demander les journaux de débogage	Enregistre des informations de débogage très détaillées sur une transaction HTTP spécifique à partir de tous les types de journaux du module Proxy Web. Il est conseillé de créer cet abonnement au journal pour résoudre un problème de proxy avec une transaction particulière sans créer tous les autres abonnements au journal de proxy. Remarque : vous ne pouvez créer cet abonnement au journal que dans l'interface de ligne de commande.	Non	Non
Journaux d'authentification	Enregistre les messages liés à la fonctionnalité de contrôle d'accès.	Oui	Oui
Journaux SHD (Démon d'intégrité système)	Enregistre un historique de l'état des services système et un historique des redémarrages inattendus du démon.	Oui	Oui
Journaux SNMP	Enregistre les messages de débogage relatifs au moteur de gestion de réseau SNMP.	Oui	Oui
Journaux du module SNMP	Enregistre les messages du proxy Web relatifs à l'interaction avec le système de surveillance SNMP.	Non	Non
Journaux Sophos Integration	Enregistre les messages relatifs à la communication entre le proxy Web et le moteur d'analyse Sophos.	Non	Non

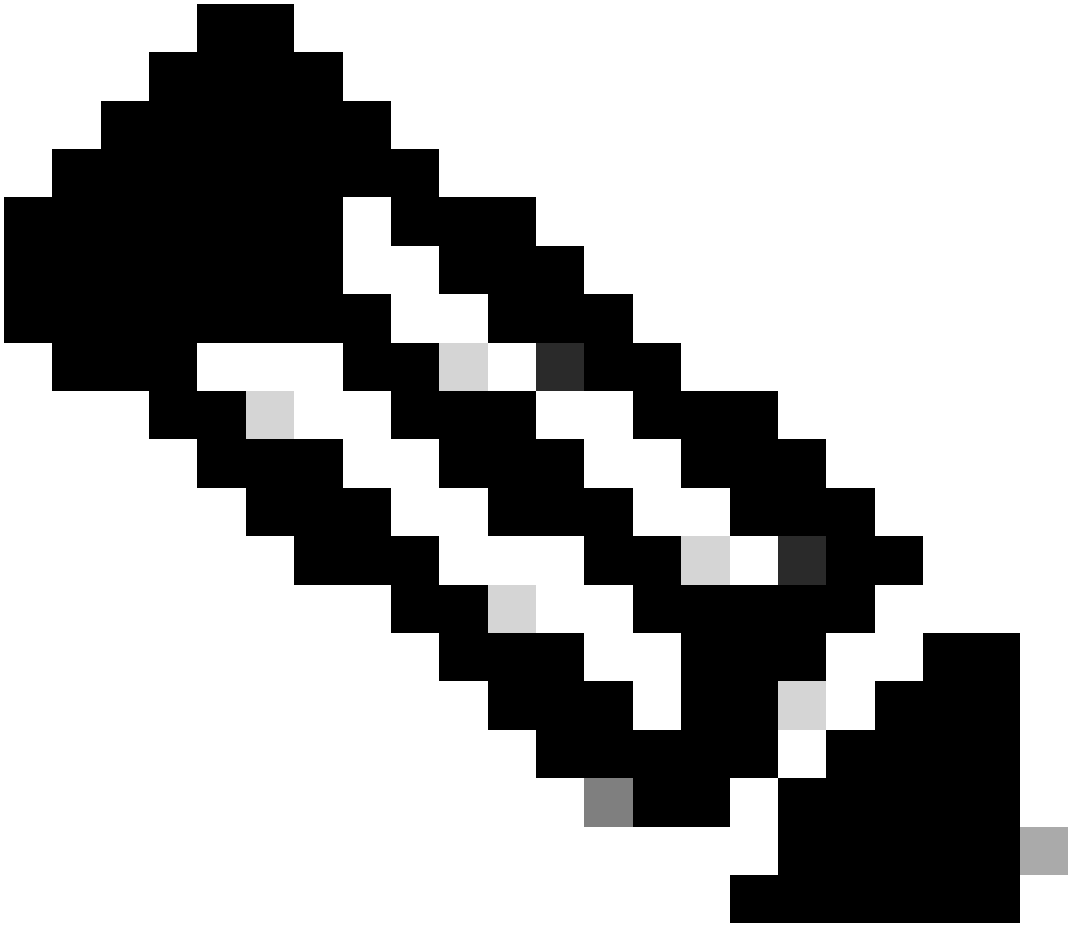
Type de fichier journal	Description	Prend en charge Syslog Push ?	Activé par défaut ?
Framework			
Journaux Sophos	Enregistre l'état de l'activité d'analyse anti-programme malveillant du moteur d'analyse Sophos.	Oui	Oui
Journaux d'état	Enregistre les informations relatives au système, telles que les téléchargements de clés de fonction.	Oui	Oui
Journaux du système	Enregistre les activités DNS, d'erreur et de validation.	Oui	Oui
Journaux des erreurs du Moniteur de trafic	Enregistre les erreurs d'interface L4TM et de capture.	Oui	Oui
Journaux du Moniteur de trafic	Enregistre les sites ajoutés au bloc L4TM et les listes d'autorisation.	Non	Oui
Journaux UDS (Service de découverte utilisateur)	Enregistre des données sur la façon dont le proxy Web découvre le nom d'utilisateur sans effectuer d'authentification réelle. Il inclut des informations sur l'interaction avec l'appliance de sécurité adaptative Cisco pour la mobilité sécurisée, ainsi que sur l'intégration avec le serveur Novell eDirectory pour une identification transparente des utilisateurs.	Oui	Oui
Journaux de mise à jour	Enregistre un historique de WBRS et d'autres mises à jour.	Oui	Oui
Journaux W3C	Enregistre l'historique du client de proxy Web dans un format compatible avec le W3C. Pour plus d'informations.	Oui	Non
Journaux WBNP	Enregistre un historique des téléchargements de	Non	Oui

Type de fichier journal	Description	Prend en charge Syslog Push ?	Activé par défaut ?
(Participation au réseau SensorBase)	participation à Cisco SensorBase Network vers le réseau SensorBase.		
Journaux de WBRS Framework (score de réputation Web)	Enregistre les messages liés à la communication entre le proxy Web et les filtres de réputation Web.	Non	Non
Journaux du module WCCP	Enregistre les messages de proxy Web liés à la mise en oeuvre de WCCP.	Non	Non
Journaux du cadre d'intégration Webcat	Enregistre les messages liés à la communication entre le proxy Web et le moteur de filtrage d'URL associé aux contrôles d'utilisation Web de Cisco.	Non	Non
Journaux de Webroot Integration Framework	Enregistre les messages liés à la communication entre le proxy Web et le moteur d'analyse Webroot.	Non	Non
Journaux Webroot	Enregistre l'état de l'activité d'analyse anti-programme malveillant du moteur d'analyse Webroot.	Oui	Oui
Journaux d'accusé de réception	Enregistre l'historique des clients Web qui cliquent sur le bouton Accepter de la page d'accusé de réception de l'utilisateur final.	Oui	Oui

Afficher les journaux

Par défaut, les journaux sont stockés localement dans le SWA, vous pouvez télécharger les fichiers journaux stockés localement via l'interface utilisateur graphique ou afficher les journaux à partir de l'interface de ligne de commande.

Télécharger les fichiers journaux via l'interface utilisateur graphique



Remarque : le protocole FTP doit être activé sur l'appliance. Pour activer le protocole FTP, reportez-vous à la section Activer le protocole FTP sur l'appareil Web sécurisé dans cet article.

Vous pouvez télécharger les fichiers journaux à partir de l'interface utilisateur graphique :

Étape 1. Connexion à l'interface utilisateur graphique

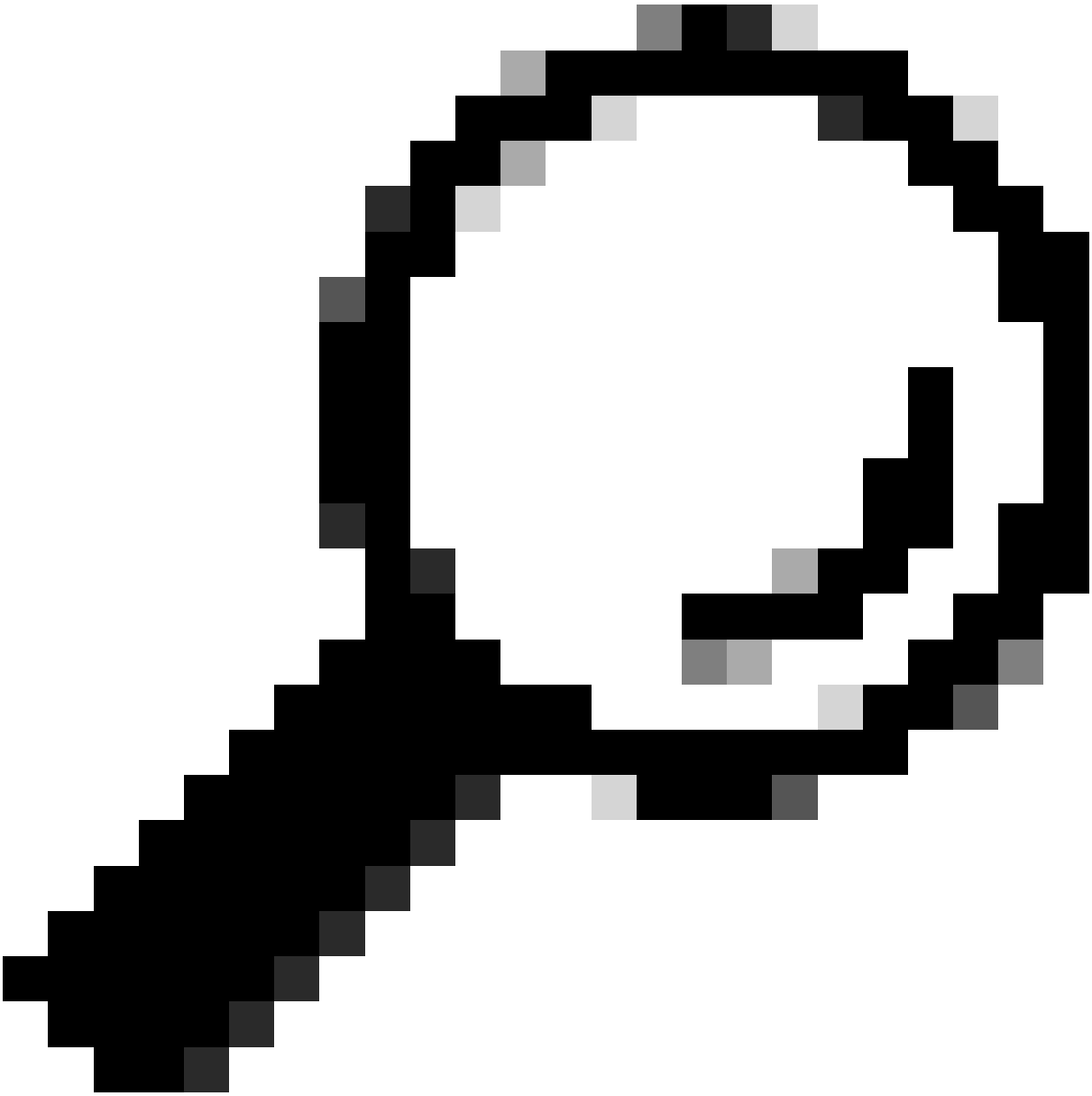
Étape 2. Accédez à Administration système

Étape 3. Choisir les abonnements au journal

Étape 4.Cliquez sur le nom de l'abonnement au journal dans la colonne Fichiers journaux de la liste des abonnements au journal.

Étape 5.Lorsque vous y êtes invité, entrez le nom d'utilisateur et le mot de passe de l'administrateur pour accéder à l'appliance.

Étape 6.Lorsque vous êtes connecté, cliquez sur l’un des fichiers journaux pour l’afficher dans votre navigateur ou l’enregistrer sur le disque.



Conseil : actualisez le navigateur pour obtenir des résultats mis à jour.

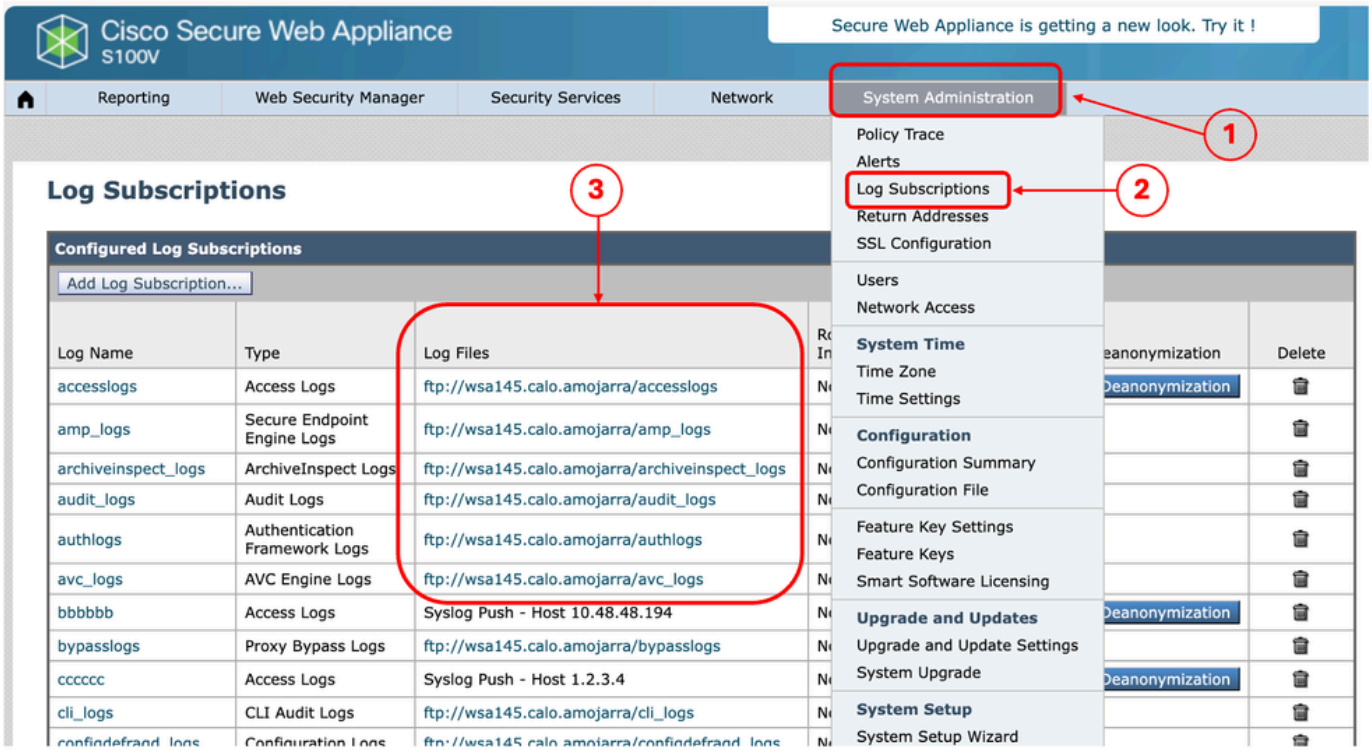
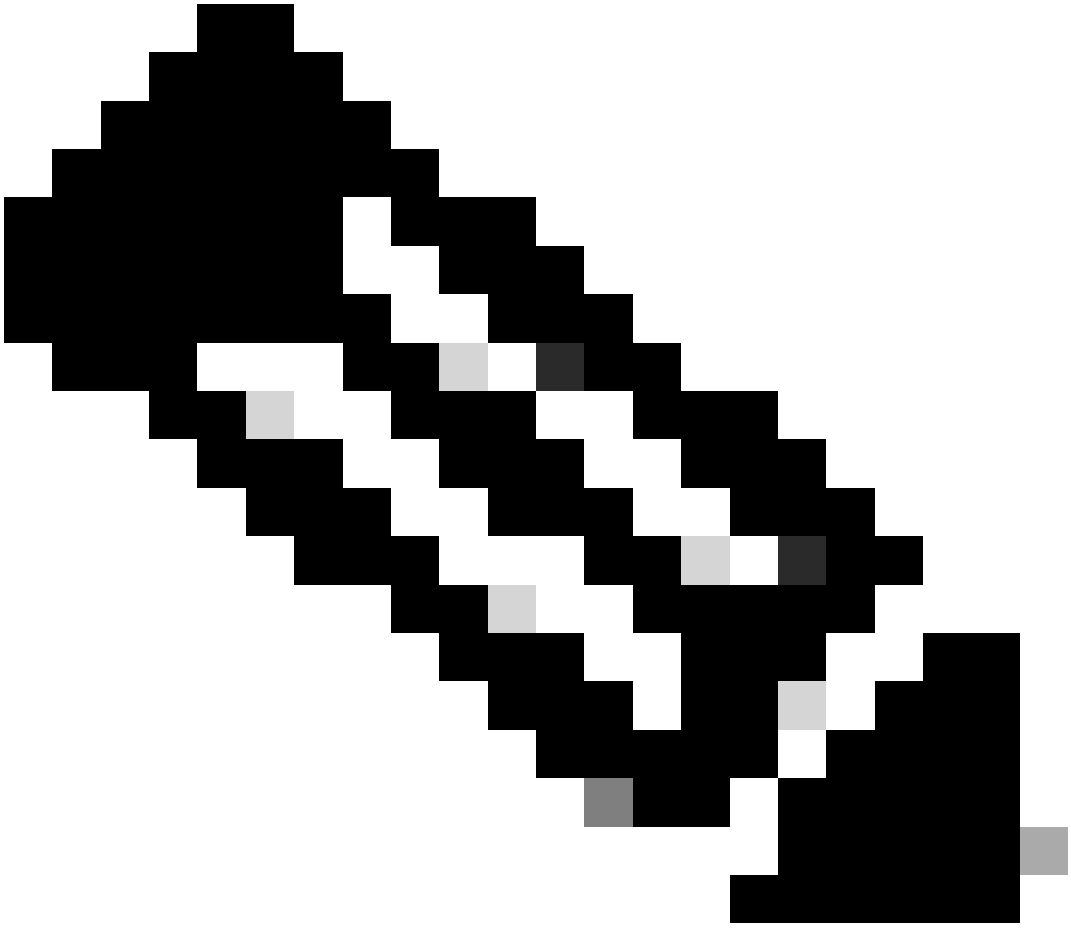


Image - Télécharger les fichiers journaux



Remarque : si un abonnement au journal est compressé, téléchargez, décompressez, puis ouvrez-le.

Afficher les journaux depuis CLI

Vous pouvez afficher les journaux à partir de l'interface de ligne de commande. Dans ce cas, vous pouvez accéder aux journaux actifs ou filtrer un mot clé dans les journaux.

Étape 1. Connexion à CLI

Étape 2. Tapez grep et appuyez sur Entrée.

Étape 3. Saisissez le numéro du journal que vous souhaitez afficher

Étape 4. (Facultatif) vous pouvez filtrer la sortie en définissant une expression régulière ou un mot, sinon appuyez sur Entrée

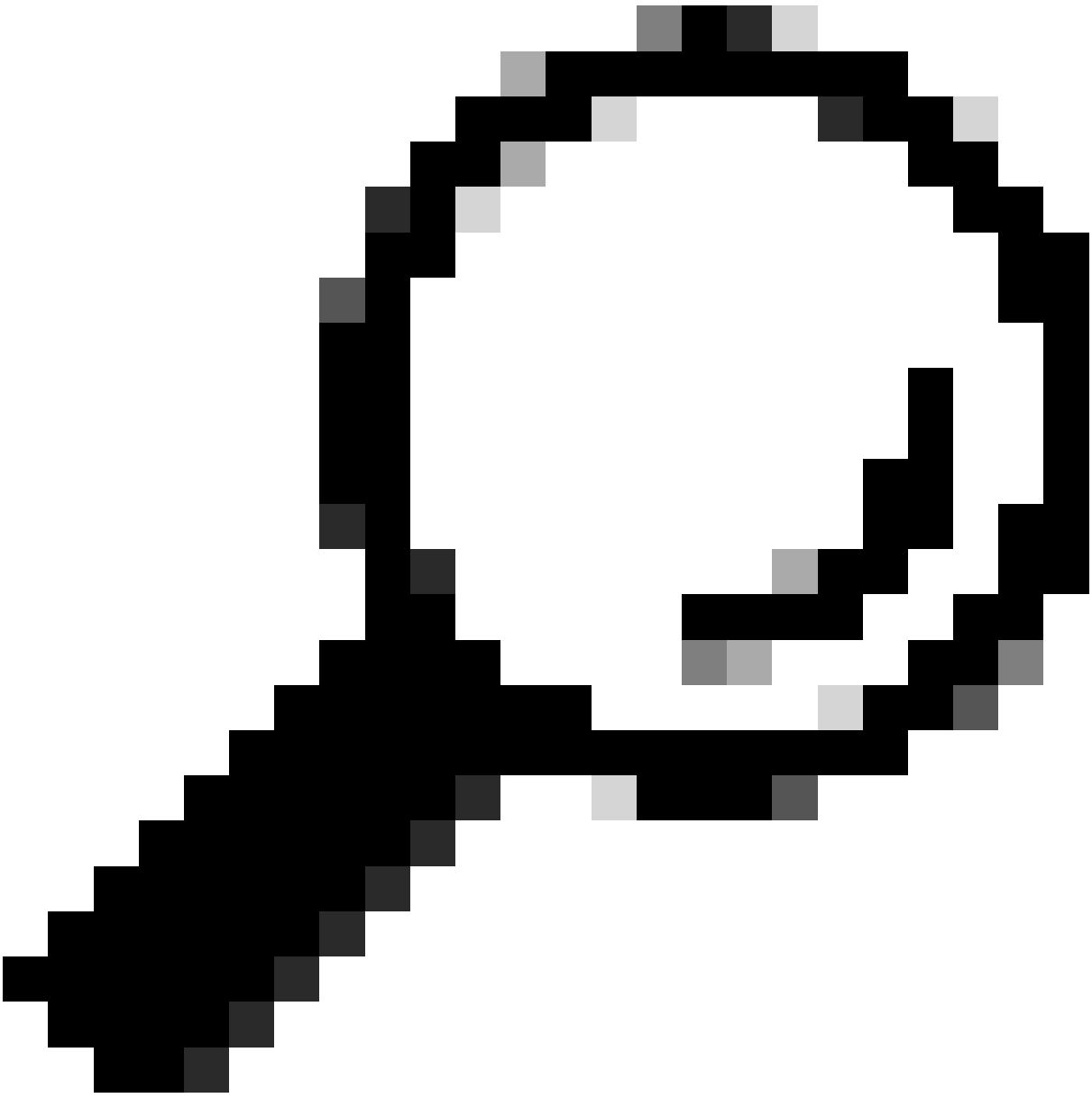
Étape 5. Si vous souhaitez que la recherche du mot clé entré à l'étape 4 ne respecte pas la casse,

appuyez sur Entrée dans « Voulez-vous que cette recherche respecte la casse ? [Y]>" sinon tapez "N" et appuyez sur Entrée.

Étape 6. Si vous devez exclure votre mot clé de la recherche, tapez « Y » dans « Voulez-vous rechercher des lignes sans correspondance ? [N]>" sinon, appuyez sur Entrée.

Étape 7. Si vous devez afficher les journaux en direct, tapez « Y » dans « Voulez-vous suivre les journaux ? [N]>", sinon appuyez sur Entrée.

Étape 8. Si vous voulez paginer les journaux pour les afficher page par page, tapez "Y" dans "Voulez-vous paginer le résultat ? [N]>" , sinon appuyez sur Entrée.



Conseil : si vous choisissez de paginer, vous pouvez quitter les journaux en appuyant sur "q"

Voici un exemple de résultat montrant toutes les lignes qui ont "Warning" en elles :

```
SWA_CLI> grep

Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "amp_logs" Type: "Secure Endpoint Engine Logs" Retrieval: FTP Poll
3. "archiveinspect_logs" Type: "ArchiveInspect Logs" Retrieval: FTP Poll
4. "audit_logs" Type: "Audit Logs" Retrieval: FTP Poll
5. "authlogs" Type: "Authentication Framework Logs" Retrieval: FTP Poll
6. "avc_logs" Type: "AVC Engine Logs" Retrieval: FTP Poll
7. "bypasslogs" Type: "Proxy Bypass Logs" Retrieval: FTP Poll
8. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
...
45. "upgrade_logs" Type: "Upgrade Logs" Retrieval: FTP Poll
46. "wbnp_logs" Type: "WBNP Logs" Retrieval: FTP Poll
47. "webcat_logs" Type: "Web Categorization Logs" Retrieval: FTP Poll
48. "webrootlogs" Type: "Webroot Logs" Retrieval: FTP Poll
49. "webtapd_logs" Type: "Webtapd Logs" Retrieval: FTP Poll
50. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP Poll
Enter the number of the log you wish to grep.
[]> 40

Enter the regular expression to grep.
[]> Warning

Do you want this search to be case insensitive? [Y]>

Do you want to search for non-matching lines? [N]>

Do you want to tail the logs? [N]>

Do you want to paginate the output? [N]>
```

Activer FTP sur l'appareil Web sécurisé

Par défaut, FTP n'est pas activé sur le SWA. Pour activer le protocole FTP :

Étape 1. Connexion à l'interface utilisateur graphique

Étape 2. Accéder au réseau

Étape 3. Choisir des interfaces

Étape 4. Cliquez sur Modifier les paramètres.

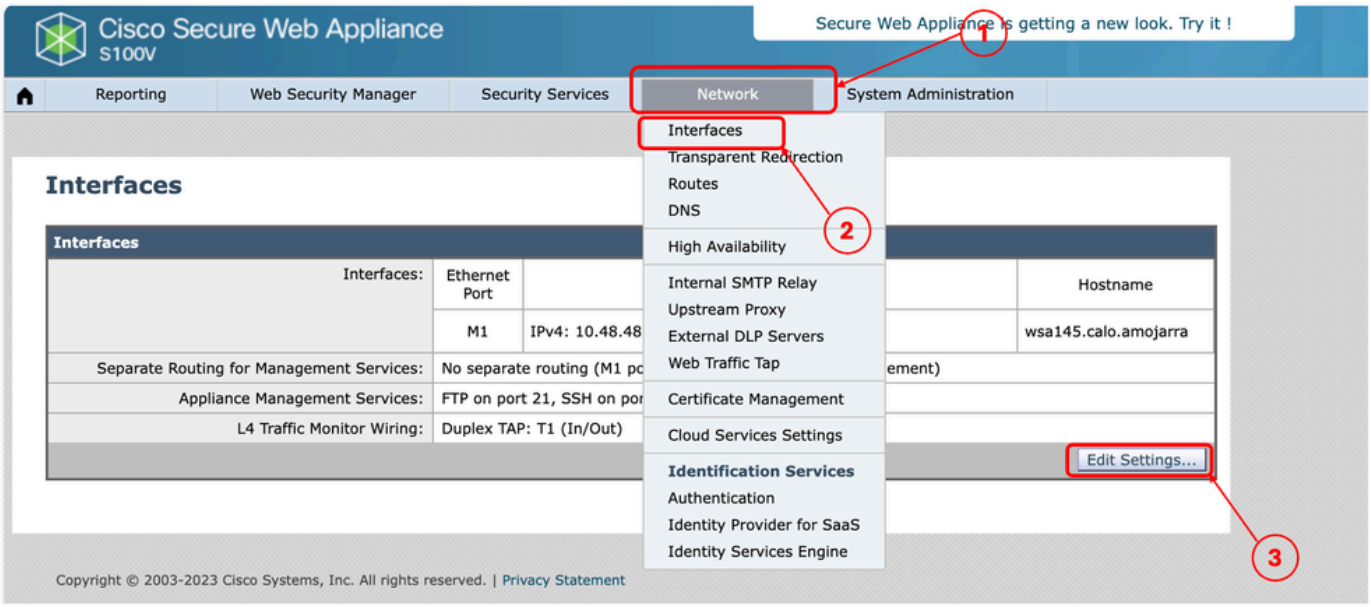


Image - Activer FTP sur SWA

Étape 5. Activez la case à cocher FTP

Étape 6. Indiquez le numéro de port TCP pour FTP (le port FTP par défaut est 21)

Étape 7. Envoyer et valider les modifications

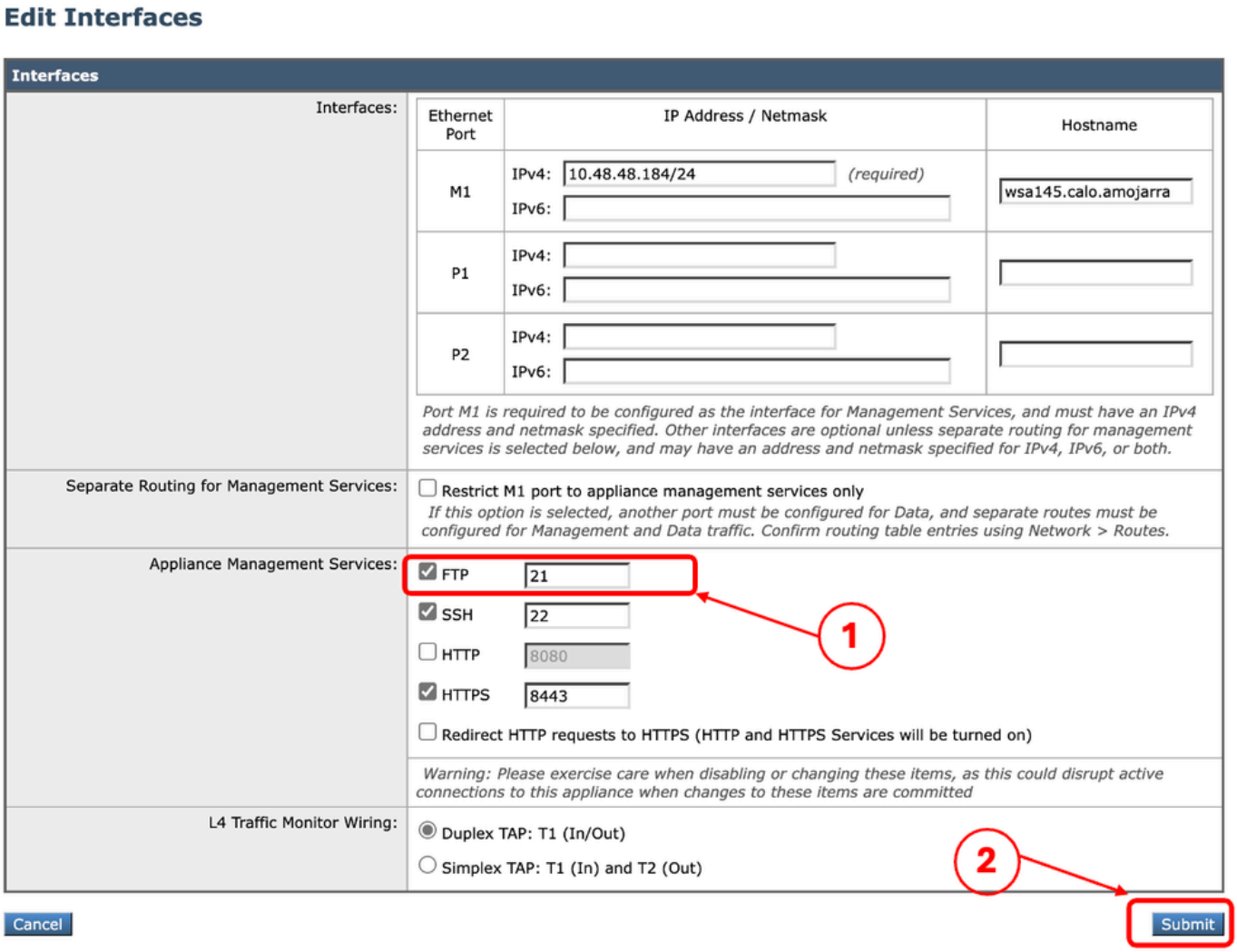


Image : configuration du paramètre FTP dans SWA

Informations connexes

- Guide de l'utilisateur d'AsyncOS 15.0 pour Cisco Secure Web Appliance - LD (Limited Deployment) - Troubleshooti...
- Configuration des journaux de transmission SCP dans l'appareil Web sécurisé avec Microsoft Server - Cisco

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.