Accesso ai registri protetti di Web Appliance

Sommario

Introduzione

In questo documento vengono descritti i metodi per visualizzare i log di Secure Web Appliance (SWA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- SWA fisico o virtuale installato.
- Licenza attivata o installata.
- Client Secure Shell (SSH).
- Installazione guidata completata.
- Accesso amministrativo all'SWA.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Tipi di log SWA

Secure Web Appliance registra le proprie attività di gestione del traffico e del sistema scrivendo tali attività in file di registro. Gli amministratori possono consultare questi file di registro per monitorare e risolvere i problemi dell'accessorio.

In questa tabella vengono descritti i tipi di file di log di Secure Web Appliance.

Tipo file registro	Descrizione	Supporta Syslog Push?	Attivato per impostazione predefinita?
Log di Access Control Engine	Registra i messaggi correlati al motore di valutazione ACL (Access Control List) del proxy Web.	No	No
Registri Secure Endpoint Engine	Registra informazioni sulla scansione della reputazione e l'analisi dei file (Secure Endpoint).	Sì	Sì
Registri di controllo	Registra gli eventi AAA (Authentication, Authorization, and Accounting). Registra tutte le interazioni utente con l'applicazione e le interfacce della riga di comando e acquisisce le modifiche di cui è stato eseguito il commit. Di seguito sono riportati alcuni dettagli del registro di controllo: • Utente - Accesso • Utente - Password non corretta per l'accesso • Utente - Accesso non riuscito nome utente sconosciuto • Utente - Account accesso non riuscito scaduto • Utente - Disconnessione • Utente - Blocco • Utente - Attivato • Utente - Modifica password • Utente - Reimpostazione password • Utente - Impostazioni protezione/modifica profilo	Sì	Sì

Tipo file registro	Descrizione	Supporta Syslog Push?	Attivato per impostazione predefinita?
	• Utente - Creato • Utente - Eliminato/modificato • Gruppo/Ruolo - Eliminazione/Modificato • Gruppo /Ruolo - Modifica autorizzazioni		
Log degli accessi	Registra la cronologia del client proxy Web.	Sì	Sì
Registri framework motore ADC	Registra i messaggi relativi alla comunicazione tra il proxy Web e il motore ADC.	No	No
Registri motore ADC	Registra i messaggi di debug dal motore ADC.	Sì	Sì
Log di Authentication Framework	Registra la cronologia di autenticazione e i messaggi.	No	Sì
Registri framework motore AVC	Registra i messaggi relativi alla comunicazione tra il proxy Web e il motore AVC.	No	No
Registri motore AVC	Registra i messaggi di debug dal motore AVC.	Sì	Sì
Log di controllo CLI	Registra un controllo cronologico dell'attività dell'interfaccia della riga di comando.	Sì	Sì
Log di configurazione	Registra i messaggi correlati al sistema di gestione della configurazione del proxy Web.	No	No
Log di gestione connessione	Registra i messaggi correlati al sistema di gestione delle connessioni del proxy Web.	No	No

Tipo file registro	Descrizione	Supporta Syslog Push?	Attivato per impostazione predefinita?
Registri sicurezza dati	Registra la cronologia dei client per le richieste di caricamento valutate dai filtri di sicurezza dei dati Cisco.	Sì	Sì
Registri del modulo di sicurezza dati	Registra i messaggi relativi ai filtri di sicurezza dei dati Cisco.	No	No
Registri framework motore DCA (Analisi dinamica dei contenuti)	Registra i messaggi relativi alla comunicazione tra il proxy Web e il motore di analisi dei contenuti dinamici dei controlli di utilizzo Web di Cisco.	No	No
Registri motore DCA (Analisi dinamica dei contenuti)	Registra i messaggi correlati al motore di analisi dinamica dei contenuti dei controlli di utilizzo Web di Cisco.	Sì	Sì
Registri proxy predefiniti	Registra gli errori correlati al proxy Web. Si tratta del log più semplice di tutti i log relativi al proxy Web. Per risolvere problemi più specifici relativi al proxy Web, creare una sottoscrizione di registro per il modulo del proxy Web applicabile.	Sì	Sì
Registri di Gestione disco	Registra su disco i messaggi proxy Web correlati alla scrittura nella cache.	No	No
Log di autenticazione esterni	Registra i messaggi relativi all'utilizzo della funzionalità di autenticazione esterna, ad esempio le comunicazioni riuscite o non riuscite con il server di autenticazione esterno. Anche se l'autenticazione esterna è disattivata, questo registro contiene messaggi relativi all'esito	No	Sì

Tipo file registro	Descrizione	Supporta Syslog Push?	Attivato per impostazione predefinita?
	positivo o negativo dell'accesso degli utenti locali.		
Log commenti	Registra gli utenti Web che segnalano le pagine classificate in modo erroneo.	Sì	Sì
Registri proxy FTP	Registra i messaggi di errore e di avviso correlati al proxy FTP.	No	No
Registri server FTP	Registra tutti i file caricati e scaricati da Secure Web Appliance tramite FTP.	Sì	Sì
Log GUI (Interfaccia grafica dell'utente)	Registra la cronologia degli aggiornamenti della pagina nell'interfaccia Web. I log GUI includono inoltre informazioni sulle transazioni SMTP, ad esempio informazioni sui report pianificati inviati tramite e-mail dall'accessorio.	Sì	Sì
Log Haystack	I registri Haystack registrano l'elaborazione dei dati di tracciabilità delle transazioni Web.	Sì	Sì
Log HTTPS	Registra i messaggi proxy Web specifici per il proxy HTTPS (quando il proxy HTTPS è abilitato).	No	No
Log del server ISE	Registra le informazioni sulla connessione e sul funzionamento dei server ISE.	Sì	Sì
Log dei moduli delle licenze	Registra i messaggi relativi alla licenza del proxy Web e al sistema di gestione delle chiavi di funzionalità.	No	No
Log di Framework	Registra i messaggi correlati al sistema di registrazione del proxy Web.	No	No
Log	Registra gli errori correlati alla gestione dei registri.	Sì	Sì

Tipo file registro	Descrizione	Supporta Syslog Push?	Attivato per impostazione predefinita?
Registri di McAfee Integration Framework	Registra i messaggi relativi alla comunicazione tra il proxy Web e il motore di scansione McAfee.	No	No
Registri McAfee	Registra lo stato dell'attività di scansione antimalware dal motore di scansione McAfee.	Sì	Sì
Registri di Gestione memoria	Registra i messaggi proxy Web correlati alla gestione di tutta la memoria, inclusa la cache in memoria per il processo proxy Web.	No	No
Registri vari moduli proxy	Registra i messaggi proxy Web utilizzati principalmente dagli sviluppatori o dal supporto tecnico.	No	No
Log di AnyConnect Secure Mobility	Registra l'interazione tra l'appliance Web sicura e il client AnyConnect, incluso il controllo dello stato.	Sì	Sì
Registri NTP (Protocollo orario di rete)	Registra le modifiche apportate all'ora di sistema dal protocollo Network Time Protocol.	Sì	Sì
Log del daemon di hosting file PAC	Registra l'utilizzo del file PAC da parte dei client.	Sì	Sì
Log di bypass proxy	Registra le transazioni che ignorano il proxy Web.	No	Sì
Log di report	Registra una cronologia della generazione del report.	Sì	Sì
Report log query	Registra gli errori correlati alla generazione del	Sì	Sì

Tipo file registro	Descrizione	Supporta Syslog Push?	Attivato per impostazione predefinita?
	report.		
Richiedi log di debug	Registra informazioni di debug molto dettagliate su una transazione HTTP specifica da tutti i tipi di log del modulo Proxy Web. Si consiglia di creare questa sottoscrizione di log per risolvere un problema del proxy con una determinata transazione senza creare tutte le altre sottoscrizioni di log del proxy. Nota:è possibile creare questa sottoscrizione di log solo nella CLI.	No	No
Registri autenticazione	Registra i messaggi correlati alla funzionalità Controllo di accesso.	Sì	Sì
Registri SHD (Daemon di stato del sistema)	Registra una cronologia dello stato dei servizi di sistema e una cronologia di riavvii imprevisti del daemon.	Sì	Sì
Log SNMP	Registra i messaggi di debug correlati al motore di gestione della rete SNMP.	Sì	Sì
Registri del modulo SNMP	Registra i messaggi proxy Web relativi all'interazione con il sistema di monitoraggio SNMP.	No	No
Registri Sophos Integration Framework	Registra i messaggi relativi alla comunicazione tra il proxy Web e il motore di scansione Sophos.	No	No
Registri Sophos	Registra lo stato dell'attività di scansione antimalware dal motore di scansione Sophos.	Sì	Sì
Log di stato	Registra le informazioni correlate al sistema, ad esempio i download delle chiavi delle funzionalità.	Sì	Sì

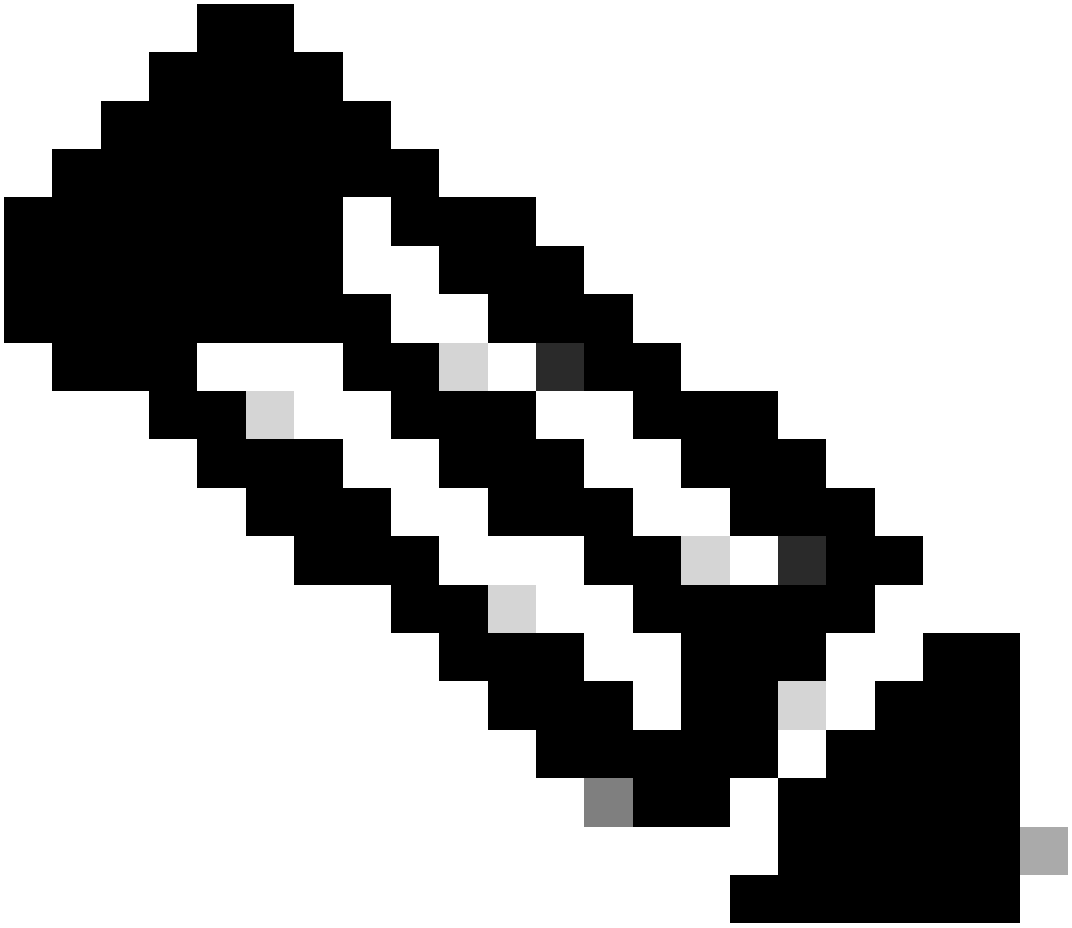
Tipo file registro	Descrizione	Supporta Syslog Push?	Attivato per impostazione predefinita?
Log di sistema	Registra le attività DNS, di errore e di commit.	Sì	Sì
Registri errori di Monitoraggio traffico	Registra l'interfaccia L4TM e gli errori di acquisizione.	Sì	Sì
Registri di Traffic Monitor	Registra i siti aggiunti al blocco L4TM e gli elenchi degli indirizzi consentiti.	No	Sì
Registri UDS (Servizio di individuazione utenti)	Registra i dati relativi al modo in cui il proxy Web individua il nome utente senza eseguire l'autenticazione effettiva. Include informazioni sull'interazione con Cisco Adaptive Security Appliance per Secure Mobility e sull'integrazione con il server Novell eDirectory per un'identificazione trasparente degli utenti.	Sì	Sì
Registri Updater	Registra una cronologia di WBRS e altri aggiornamenti.	Sì	Sì
Registri W3C	Registra la cronologia del client proxy Web in un formato compatibile con W3C. Ulteriori informazioni.	Sì	No
Registri WBNP (partecipazione alla rete SensorBase)	registra una cronologia delle partecipazioni di Cisco SensorBase Network caricate sulla rete SensorBase.	No	Sì
Registri framework WBRS (punteggio Web Reputation)	Registra i messaggi relativi alla comunicazione tra il proxy Web e i filtri reputazione Web.	No	No

Tipo file registro	Descrizione	Supporta Syslog Push?	Attivato per impostazione predefinita?
Registri modulo WCCP	Registra i messaggi proxy Web correlati all'implementazione di WCCP.	No	No
Registri di WebCat Integration Framework	Registra i messaggi relativi alla comunicazione tra il proxy Web e il motore di filtro URL associato ai controlli dell'utilizzo Web di Cisco.	No	No
Log di WebRoot Integration Framework	Registra i messaggi relativi alla comunicazione tra il proxy Web e il motore di scansione Webroot.	No	No
Log Webroot	Registra lo stato dell'attività di analisi antimalware dal motore di analisi Webroot.	Sì	Sì
Log di conferma della pagina di benvenuto	Registra una cronologia dei client Web che fanno clic sul pulsante Accetto nella pagina di conferma dell'utente finale.	Sì	Sì

Visualizza registri

Per impostazione predefinita, i log vengono archiviati localmente nell'SWA, è possibile scaricare i file di log archiviati localmente tramite la GUI o visualizzarli dalla CLI.

Download dei file di log tramite GUI



Nota: sull'accessorio deve essere attivato l'FTP. Per abilitare l'FTP, fare riferimento a Abilita FTP su Secure Web Appliance in questo articolo.

È possibile scaricare i file di log dalla GUI:

Passaggio 1. Login alla GUI

Passaggio 2. Passare a Amministrazione sistema

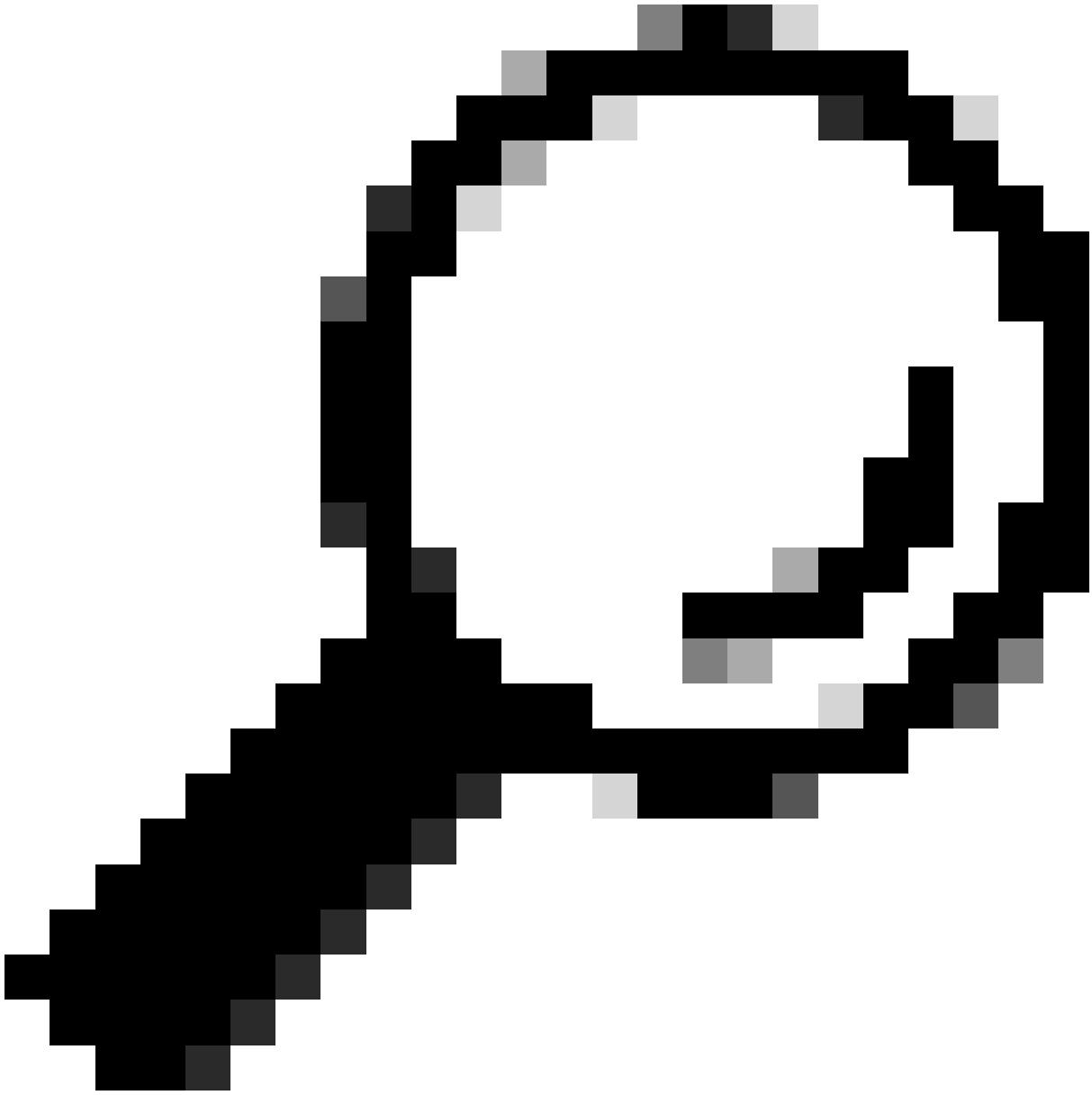
Passaggio 3. Scegli sottoscrizioni log

Passaggio 4. Fare clic sul nome della sottoscrizione di log nella colonna File di log dell'elenco delle sottoscrizioni di log.

Passaggio 5. Quando richiesto, immettere il nome utente e la password amministratore per accedere all'accessorio.

Passaggio 6.Una volta eseguito l'accesso, fare clic su uno dei file di registro per visualizzarlo nel

browser o per salvarlo su disco.



Suggerimento: aggiornare il browser per visualizzare i risultati aggiornati.

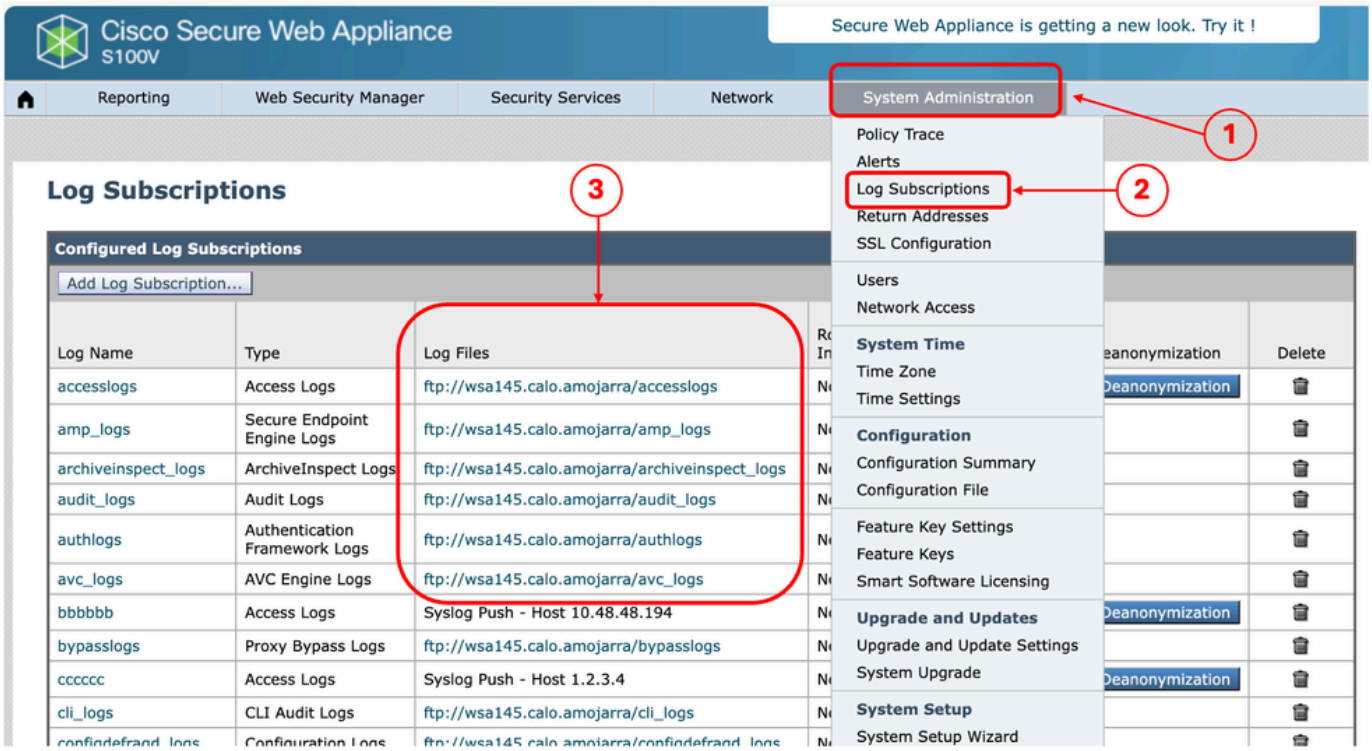
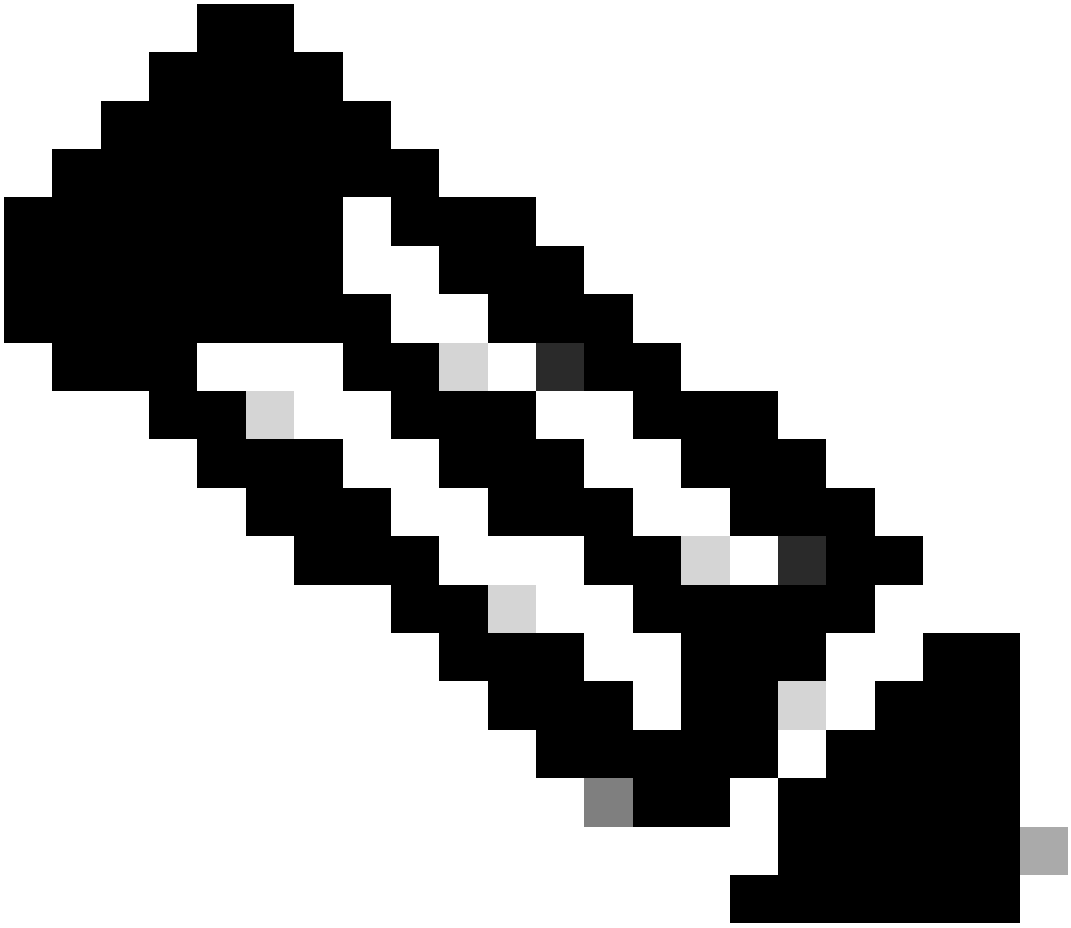


Immagine - Scarica file di log



Nota: se una sottoscrizione di log è compressa, scaricarla, decomprimerla e quindi aprirla.

Visualizza log dalla CLI

È possibile visualizzare i log dalla CLI. in questo caso, è possibile accedere ai log attivi o filtrare una parola chiave nei log.

Passaggio 1. Connetti alla CLI

Passaggio 2. Digitare grep e premere Invio.

Passaggio 3. Immettere il numero del registro da visualizzare

Passaggio 4. (Facoltativo) è possibile filtrare l'output definendo un'espressione regolare o una parola, altrimenti premere Invio

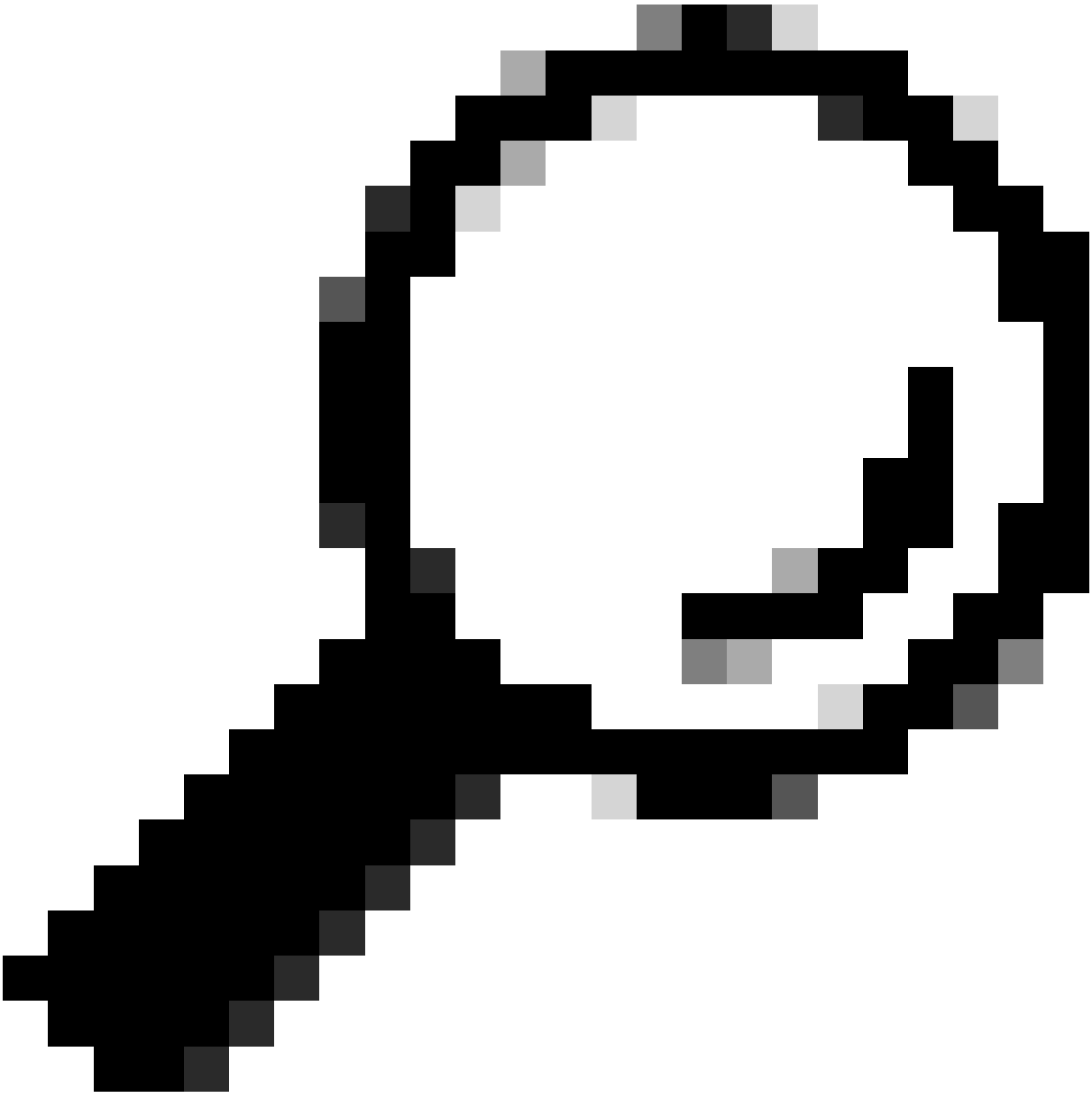
Passaggio 5. Se è necessario eseguire la ricerca della parola chiave immessa nel passaggio 4, per non fare distinzione tra maiuscole e minuscole, premere Invio in "Si desidera che la ricerca

non faccia distinzione tra maiuscole e minuscole? [Y]>", digitare "N" e premere Invio.

Passaggio 6. Se è necessario escludere la parola chiave dalla ricerca, digitare "Y" in "Cercare righe non corrispondenti? [N]>", altrimenti premere Invio.

Passaggio 7. Per visualizzare i log attivi, digitare "Y" in "Eseguire la coda dei log? [N]>", altrimenti premere Invio.

Passaggio 8. Se si desidera impaginare i log per visualizzarli pagina per pagina, digitare "Y" in "Impaginare l'output? [N]>" , altrimenti premere Invio.



Suggerimento: se si sceglie di impaginare, è possibile uscire dai log premendo "q"

Di seguito è riportato un esempio di output in cui sono mostrate tutte le righe contenenti un messaggio di avvertenza:

```
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]>
```

Abilita FTP su Secure Web Appliance

Per impostazione predefinita, l'FTP non è abilitato sull'SWA. Per abilitare l'FTP:

Passaggio 1. Login alla GUI

Passaggio 2. Passa alla rete

Passaggio 3. Scegli interfacce

Passaggio 4. Fare clic su Modifica impostazioni.

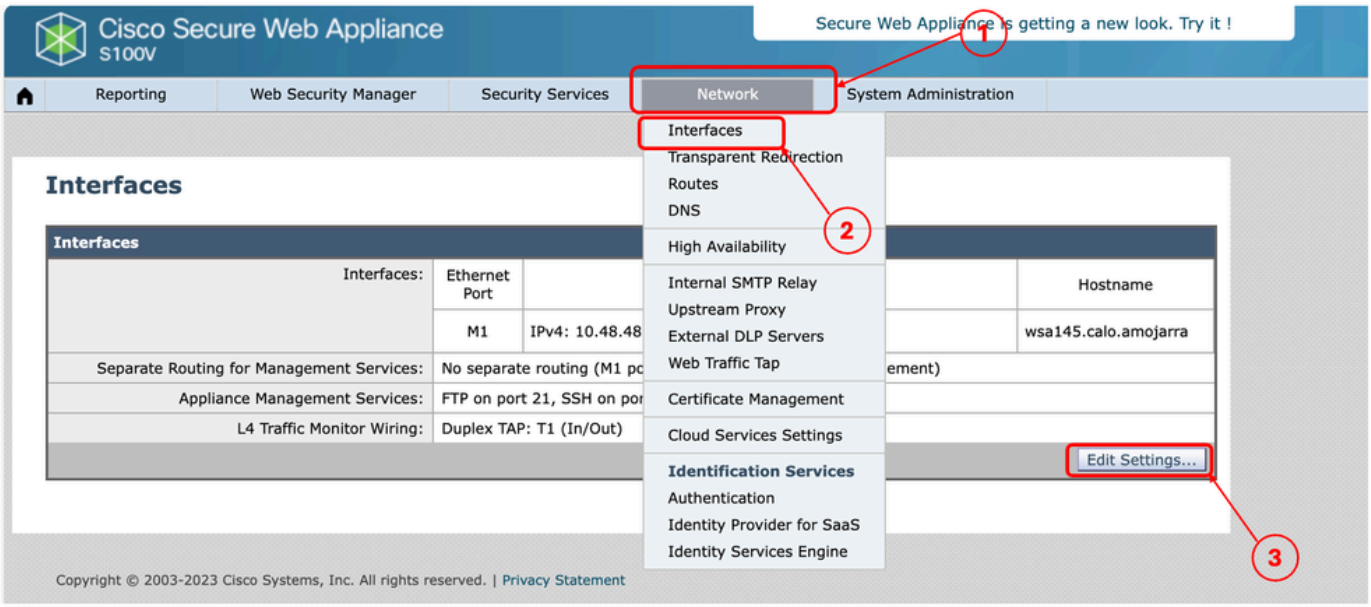


Immagine - Abilita FTP su SWA

Passaggio 5. Selezionare la casella di controllo FTP

Passaggio 6. Specificare il numero della porta TCP per l'FTP (la porta FTP predefinita è 21)

Passaggio 7. Invia e conferma modifiche

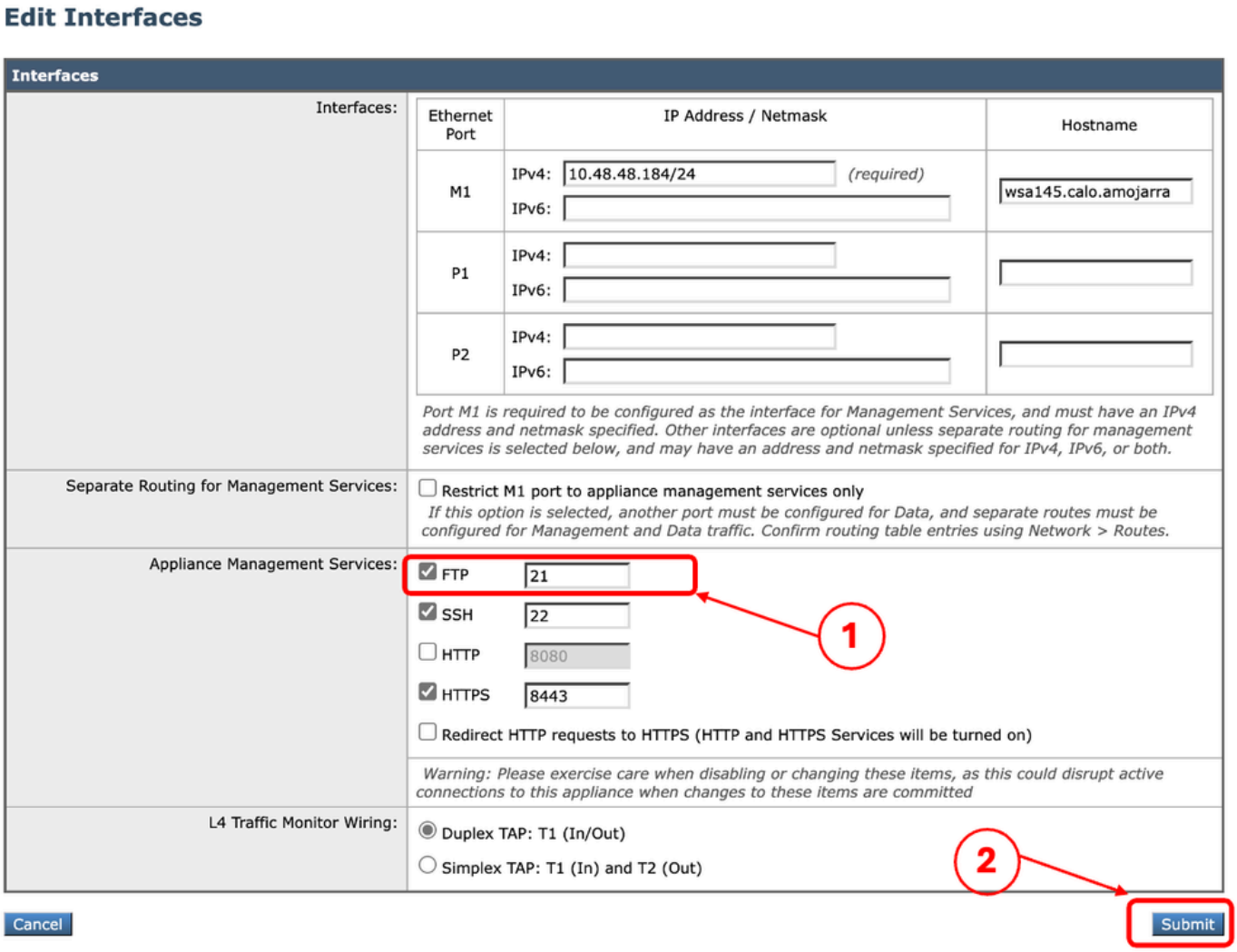


Immagine - Configura parametro FTP in SWA

Informazioni correlate

- [Guida per l'utente di AsyncOS 15.0 for Cisco Secure Web Appliance - LD (installazione limitata) - Risoluzione dei problemi...]
- [Configurazione dei log di push SCP in Secure Web Appliance con Microsoft Server - Cisco]

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).