Superviser l'activité du système au moyen de journaux

Cette rubrique contient les sections suivantes :

Survol de la journalisation

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

L'appliance divise les différents types d'activités en différents types de journalisation pour simplifier la recherche d'informations sur des activités spécifiques. La plupart d'entre eux sont activés automatiquement par défaut, mais certains doivent être activés manuellement selon les besoins.

Vous activez et gérez les fichiers journaux par le biais d'abonnements aux fichiers journaux. Les abonnements vous permettent de définir les paramètres de création, de personnalisation et de gestion des fichiers journaux.

Les deux principaux types de fichiers journaux généralement utilisés par les administrateurs sont les suivants :

- **Journal d'accès.** Ce journal enregistre toutes les activités de filtrage et d'analyse des proxy Web.

- **Journal de supervision de trafic** Ce journal enregistre toute l'activité du processus de supervision du trafic de la couche 4.

Vous pouvez afficher l'activité actuelle et passée de l'appliance à l'aide de ces types de journaux et d'autres. Des tableaux de référence sont disponibles pour vous aider à interpréter les entrées des fichiers journaux.

Thèmes connexes

- Tâches courantes de journalisation, on page 2
- Types de fichiers journaux, on page 3

Tâches courantes de journalisation

Tâche	Liens vers des rubriques et des procédures connexes
Ajouter et modifier des abonnements aux journaux	Ajout et modification d'abonnements aux journaux, on page 9
Afficher les fichiers journaux	Affichage des fichiers journaux, on page 17
Interpréter les fichiers journaux	Interprétation des entrées de verdict d'analyse des journaux d'accès, on page 31
Personnaliser les fichiers journaux	Personnalisation des journaux d'accès, on page 41
Envoyer les fichiers journaux vers un autre serveur	Transmission des fichiers journaux à un autre serveur, on page 15
Archivage des fichiers journaux	Archivage des fichiers journaux, on page 16

Bonnes pratiques en matière de journalisation

- La réduction du nombre d'abonnements aux journaux améliorera les performances du système.
- La journalisation de moins de détails améliorera les performances du système.

Résolution de problèmes de proxy Web en utilisant les journaux

Par défaut, Secure Web Appliance a un abonnement au journal créé pour les messages de journalisation du proxy Web, appelé « journaux de proxy par défaut ». Cela capture des informations de base sur tous les modules de proxy Web. L'appliance comprend également des types de fichiers journaux pour chaque module de proxy Web afin que vous puissiez lire des informations de débogage plus spécifiques pour chaque module sans encombrer les journaux de proxy par défaut.

Suivez les étapes ci-dessous pour résoudre les problèmes de proxy Web à l'aide des différents journaux disponibles.

Étape 1 Lisez les journaux de proxy par défaut.

Étape 2 Si vous voyez une entrée qui pourrait être liée au problème mais qu'il n'y a pas suffisamment d'informations pour le résoudre, créez un abonnement au journal pour le module de proxy Web spécifique concerné. Les types de journaux de module de proxy Web suivants sont disponibles :

Journaux du moteur de contrôle d'accès	Journaux relatifs à l'environnement de journalisation
Journaux relatifs à l'environnement du moteur AVC	Journaux relatifs à l'environnement d'intégration de McAfee
Journaux de configuration	Journaux du gestionnaire de mémoire
Journaux de gestion des connexions	Journaux de divers modules de proxy
Journaux du module de sécurité des données	Journaux de débogage des demandes
Journaux relatifs à l'environnement du moteur DCA	Journaux du module SNMP
Journaux du gestionnaire de disque	Journaux relatifs à l'environnement d'intégration Sophos
FireAMP	Journaux relatifs à l'environnement WBRS
Journaux de proxy FTP	Journaux du module WCCP
HTTPS Logs (Journaux HTTPS)	Journaux relatifs à l'environnement d'intégration Webcat
Journaux du module de licence	Journaux relatifs à l'environnement d'intégration Webroot

Étape 3 Recréez le problème et lisez le journal du nouveau module de proxy Web pour repérer les entrées pertinentes.

Étape 4 Répétez l'opération au besoin avec les autres journaux du module de proxy Web.

Étape 5 Supprimez les abonnements qui ne sont plus nécessaires.

What to do next

Thèmes connexes

- Types de fichiers journaux, on page 3
- Ajout et modification d'abonnements aux journaux, on page 9

Types de fichiers journaux

Certains types de journaux liés au composant proxy Web ne sont pas activés. Le type de journal principal du proxy Web, appelé « journaux de proxy par défaut », est activé par défaut et capture des informations élémentaires sur tous les modules de proxy Web. Chaque module de proxy Web possède son propre type de journal que vous pouvez activer manuellement au besoin.

Le tableau suivant décrit les types de fichiers journaux Secure Web Appliance.

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 (ACL) du proxy Web.	Non	Non

Type de fichier journal	Description	Prend en charge Syslog Push?	Activé par défaut?
Journaux du moteur Cisco Secure Endpoint	Enregistre des informations sur le contrôle de réputation des fichiers et l'analyse des fichiers (Cisco Secure Endpoint). Voir aussi Fichiers de journalisation.	Oui	Oui
Journaux d'audit	Enregistre les événements AAA (Authentication, Authorization et Accounting ou Authentification, Autorisation et Comptabilité). Enregistre toutes les interactions de l'utilisateur avec l'application et les interfaces de ligne de commande, et capture les modifications validées. Voici quelques détails du journal d'audit : • Utilisateur – Connexion • Utilisateur – Échec de connexion, mot de passe incorrect • Utilisateur – Échec de connexion, nom d'utilisateur inconnu • Utilisateur – Échec du compte, expiration de la connexion • Utilisateur – Déconnexion • Utilisateur – Verrouillage • Utilisateur - Activé • Utilisateur – Changement de mot de passe • Utilisateur – Réinitialisation du mot de passe • Utilisateur – Modification de paramètres/du profil de sécurité • Utilisateur – Créé • Utilisateur – Supprimé/modifié • Groupe/rôle – Suppression/modifié • Groupe/rôle – Modification des autorisations	Oui	Oui
Journaux d'accès	Enregistre l'historique du client de proxy Web.	Oui	Oui
Journaux relatifs à l'environnement d'authentification	Enregistre l'historique et les messages d'authentification.	Non	Oui

Type de fichier journal	Description	Prend en charge Syslog Push?	Activé par défaut?
Journaux relatifs à l'environnement 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 de l'interface de ligne de commande	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
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 chargement évaluées par les filtres de sécurité des données de Cisco.	Oui	Oui
Journaux du module de sécurité des données	Enregistre les messages liés aux filtres de sécurité des données Cisco.	Non	Non
Journaux relatifs à l'environnement du moteur DCA (Dynamic Content Analysis)	Enregistre les messages relatifs à la communication entre le proxy Web et le moteur Cisco Web Usage Controls Dynamic Content Analysis.	Non	Non
Journaux du moteur DCA (Dynamic Content Analysis)	Enregistre les messages liés au moteur Cisco Web Usage Controls Dynamic Content Analysis.	Oui	Oui
Journaux de proxy par défaut	Enregistre les erreurs liées au proxy Web. Il s'agit du plus simple 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 applicable.	Oui	Oui
Journaux du gestionnaire de disque	Enregistre les messages du proxy Web liés 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 extérieure	Enregistre les messages liés à l'utilisation de la fonction d'authentification extérieure tels que la réussite ou l'échec de la communication avec le serveur d'authentification extérieure Même si l'authentification extérieure est désactivée, ce journal contient des messages concernant les utilisateurs locaux qui ont réussi ou non à se connecter.	Non	Oui
Journaux de commentaires	Enregistre les utilisateurs Web ayant signalé des pages mal classées.	Oui	Oui
Journaux de proxy FTP	Enregistre les messages d'erreur et d'avertissement liés au proxy FTP.	Non	Non
Journaux du serveur FTP	Enregistre tous les fichiers chargés sur et téléchargés à partir de Secure Web Appliance au moyen de FTP.	Oui	Oui
Journaux de l'interface graphique utilisateur (GUI)	Enregistre l'historique des actualisations de page dans l'interface Web. Les journaux de l'interface graphique utilisateur comprennent également des informations sur les transactions SMTP, par exemple des informations sur les rapports planifiés envoyés par courriel par l'appliance.	Oui	Oui
Journaux Haystack	Les journaux Haystack enregistrent le traitement des données de suivi des transactions Web.	Oui	Oui
HTTPS Logs (Journaux HTTPS)	Enregistre les messages de proxy Web propres au proxy HTTPS (lorsque le proxy HTTPS est activé).	Non	Non
Journaux de serveur ISE	Enregistre les informations opérationnelles et relatives aux connexions du serveur ISE.	Oui	Oui
Journaux du module de licence	Enregistre les messages relatifs à la licence du proxy Web et au système de gestion des clés de fonctionnalité.	Non	Non
Journaux relatifs à l'environnement de journalisation	Enregistre les messages relatifs au système de journalisation du proxy Web.	Non	Non
Journaux de journalisation	Enregistre les erreurs liées à la gestion des journaux.	Oui	Oui

Type de fichier journal	Description	Prend en charge Syslog Push?	Activé par défaut?
Journaux relatifs à l'environnement d'intégration de McAfee	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 de protection contre les programmes malveillants du moteur d'analyse McAfee.	Oui	Oui
Journaux du gestionnaire de mémoire	Enregistre les messages du proxy Web liés à la gestion de toute la mémoire, y compris le cache en mémoire du processus du proxy Web.	Non	Non
Journaux de divers modules de proxy	Enregistre les messages de proxy Web qui sont principalement utilisés par les développeurs ou l'assistance client.	Non	Non
Journaux du démon d'AnyConnect Secure Mobility	Enregistre l'interaction entre Secure Web Appliance et le client AnyConnect, y compris la vérification de l'état.	Oui	Oui
Journaux NTP (Network Time Protocol)	Enregistre les modifications de l'horloge système effectuées par le protocole Network Time Protocol.	Oui	Oui
Journaux du démon d'hébergement de fichiers PAC	Enregistre l'utilisation du fichier de configuration automatique de proxy (PAC) par les clients.	Oui	Oui
Journaux de contournement de proxy	Enregistre les transactions qui contournent le proxy Web.	Non	Oui
Journaux de rapports	Enregistre un historique de la création de rapports.	Oui	Oui
Journaux des requêtes de rapports	Enregistre les erreurs liées à la génération de rapports.	Oui	Oui
Journaux de débogage des demandes	Enregistre des informations de débogage très détaillées sur une transaction HTTP spécifique à partir de tous les types de journaux de module de proxy Web. Vous souhaiterez peut-être créer cet abonnement au journal pour résoudre un problème de proxy avec une transaction particulière sans créer tous les autres abonnements aux journaux de proxy. **Remarque :** Vous pouvez créer cet abonnement à ce journal uniquement à l'aide de l'interface de ligne de commande.	Non	Non

Type de fichier journal	Description	Prend en charge Syslog Push?	Activé par défaut?
Journaux d'authentification	Enregistre les messages relatifs à la fonction de contrôle d'accès.	Oui	Oui
Journaux SHD (System Health Daemon)	Enregistre un historique de l'état des services du système et un historique des redémarrages inattendus de démon.	Oui	Oui
Journaux SNMP	Enregistre les messages de débogage liés au moteur de gestion réseau SNMP.	Oui	Oui
Journaux du module SNMP	Enregistre les messages de proxy Web liés à l'interaction avec le système de supervision SNMP.	Non	Non
Journaux relatifs à l'environnement d'intégration Sophos	Enregistre les messages liés à la communication entre le proxy Web et le moteur d'analyse Sophos.	Non	Non
Journaux Sophos	Enregistre l'état de l'activité de contrôle des programmes malveillants par le moteur d'analyse Sophos.	Oui	Oui
Journaux d'état	Enregistre les informations relatives au système, telles que les téléchargements de clés de fonctionnalité.	Oui	Oui
Journaux du système	Enregistre le DNS, les erreurs et les activités de validation.	Oui	Oui
Journaux d'erreurs de la supervision du trafic	Enregistre les erreurs de capture et de l'interface de supervision du trafic de la couche 4.	Oui	Oui
Journaux de supervision du trafic	Enregistre les sites ajoutés aux listes de blocage et d'autorisation de la supervision du trafic de la couche 4.	Non	Oui
Journaux UDS (User Discovery Service)	Enregistre les données sur la façon dont le proxy Web détecte le nom d'utilisateur sans effectuer d'authentification réelle. Il contient des informations sur l'interaction avec Cisco Adaptive Security Appliance pour Secure Mobility, ainsi que sur l'intégration au serveur Novell eDirectory pour l'identification transparente des utilisateurs.	Oui	Oui
Journaux du programme de mise à jour	Enregistre un historique de WBRS et d'autres mises à jour.	Oui	Oui

Type de fichier journal	Description	Prend en charge Syslog Push?	Activé par défaut?
Journaux W3C	Enregistre l'historique du client de proxy Web dans un format compatible avec W3C. Pour en savoir plus, consultez Fichiers journaux des accès conformes aux normes W3C, on page 39.	Oui	Non
Journaux WBNP (participation au réseau SensorBase)	Enregistre un historique des chargements de participation au réseau Cisco SensorBase dans le réseau SensorBase.	Non	Oui
Journaux relatifs à l'environnement WBRS (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 du proxy Web liés à la mise en œuvre de WCCP.	Non	Non
Journaux relatifs à l'environnement d'intégration Webcat	Enregistre les messages liés à la communication entre le proxy Web et le moteur de filtrage d'URL associé à Cisco Web Usage Controls.	Non	Non
Journaux relatifs à l'environnement d'intégration Webroot	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 de protection contre les programmes malveillants du moteur d'analyse Webroot.	Oui	Oui
Journaux d'accusé de réception de la page de bienvenue	Enregistre un historique des clients Web qui ont cliqué sur le bouton Accept (Accepter) dans la page d'accusé de réception de l'utilisateur final.	Oui	Oui

Ajout et modification d'abonnements aux journaux

Vous pouvez créer plusieurs abonnements à des journaux pour chaque type de fichier journal. Les abonnements comprennent des détails de configuration pour l'archivage et le stockage, notamment les suivants :

- Les paramètres de renouvellement, qui déterminent quand les fichiers journaux sont archivés.
- Paramètres de compression des journaux archivés
- Les paramètres de récupération des journaux archivés, qui spécifient si les journaux sont archivés sur un serveur distant ou stockés sur l'appliance.

Étape 1 Choisissez **System Administration > Log Subscriptions** (Administration système > Abonnements aux journaux).

Étape 2 Pour ajouter un abonnement à la journalisation, cliquez sur **Add Log Subscription** (Ajouter un abonnement au journal). Ou, pour modifier un abonnement à un journal, cliquez sur le nom du fichier journal dans le champ Log Name (Nom du journal).

Étape 3 Configurez l'abonnement :

Option	Description
Log Type (Type de journal)	Une liste des types de fichiers journaux disponibles auxquels vous pouvez vous abonner. Les autres options de la page peuvent changer en fonction du type de fichier journal que vous choisissez. **Note** Le type de journal Request Debug Logs (Demande de journaux de débogage) ne peut être souscrit que par l'intermédiaire de l'interface de ligne de commande et n'apparaît pas dans cette liste.
Log Name (Nom du journal)	Nom utilisé pour désigner l'abonnement sur Secure Web Appliance. Ce nom est également utilisé pour le répertoire des journaux qui stockera les fichiers journaux de l'abonnement. Saisissez uniquement des caractères ASCII ([0-9], [AZ], [az] et _).
Rollover by File Size (Renouvellement par taille de fichier)	La taille maximale de fichier que le fichier journal actuel peut atteindre avant d'être archivé et qu'un nouveau fichier journal ne démarre. Entrez une valeur comprise entre 100 Ko et 10 Go.
Rollover by Time (Renouvellement par heure)	Intervalle de temps maximal avant l'archivage du fichier journal actuel et le démarrage d'un nouveau fichier journal. Les types d'intervalles suivants sont disponibles : • **Aucun.** AsyncOS n'effectue un remplacement que lorsque le fichier journal atteint la taille maximale de fichier. • **Custom Time Interval.** (Intervalle personnalisé) AsyncOS effectue un renouvellement après un laps de temps spécifié depuis le renouvellement précédent. Indiquez le nombre de jours, d'heures, de minutes et de secondes entre les renouvellements en utilisant d , h , m et s comme suffixes. • **Renouvellement quotidien.** AsyncOS effectue un renouvellement tous les jours à une heure spécifiée. Séparez les heures multiples pendant une journée par une virgule. Utilisez un astérisque (*) dans l'heure pour que le renouvellement se produise toutes les heures de la journée. Vous pouvez également utiliser un astérisque pour remplacer chaque minute d'une heure. • **Weekly Rollover** (Renouvellement hebdomadaire). AsyncOS effectue un renouvellement un ou plusieurs jours de la semaine à une heure spécifiée.
Log Style (Style de journal) (Journaux d'accès)	Indique le format du journal à utiliser, Squid, Apache ou Squid Details.

Option	Description

Custom Fields (Champs personnalisés)
 	
(Journaux d'accès)
	Vous permet d'inclure des informations personnalisées dans chaque entrée du journal des accès.
	
	La syntaxe de saisie des spécificateurs de format dans le champ personnalisé est la suivante :
	
	`<format_specifier_1> <format_specifier_2> ...`
	
	Par exemple : `%a %b %E`
	
	Vous pouvez ajouter des jetons avant les spécificateurs de format pour afficher un texte de description dans le fichier journal des accès. Par exemple :
	
	`client_IP %a body_bytes %b error_type %E`
	
	où `IP_client` est le jeton de description du spécificateur de format de journal `%a`, etc.

File Name (Nom de fichier)	Nom des fichiers journaux. Les fichiers journaux actuels sont dotés d'une extension `.c`, et les fichiers journaux renouvelés sont accompagnés de l'horodatage de création du fichier et d'une extension `.s`.
Log Fields (Champs de journal) (Journaux d'accès W3C)	Vous permet de choisir les champs que vous souhaitez inclure dans le journal des accès W3C. Sélectionnez un champ dans la liste des champs disponibles ou saisissez un champ dans la zone Custom Field (Champ personnalisé), puis cliquez sur Add (Ajouter). L'ordre dans lequel les champs apparaissent dans la liste Selected Log Fields (Champs de journal sélectionnés) détermine l'ordre des champs dans le fichier du journal d'accès W3C. Vous pouvez modifier l'ordre des champs à l'aide des boutons **Déplacement vers le haut** et **Déplacement vers le bas**. Vous pouvez supprimer un champ en le sélectionnant dans la liste Selected Log Fields (Champs de journal sélectionnés) et en cliquant sur **Remove** (Supprimer). Vous pouvez saisir plusieurs champs définis par l'utilisateur dans la zone Custom Fields (Champs personnalisés) et les ajouter simultanément à condition que chaque entrée soit séparée par une nouvelle ligne [cliquez sur Enter (Entrée)] avant de cliquer sur **Add** (Ajouter). Lorsque vous modifiez les champs de journal inclus dans un abonnement à un journal W3C, l'abonnement au journal est automatiquement renouvelé. Cela permet à la dernière version du fichier journal d'inclure les nouveaux en-têtes de champ corrects Vous pouvez anonymiser les champs de journalisation *c-ip*, *cs-username*ou *cs-auth-group* des journaux W3C, au besoin. Cochez la case **Anonymization** (Anonymisation) pour anonymiser les champs *c-ip*, *cs-username* et *cs-auth-group*. Une fois que vous avez sélectionné la case, les noms de champ sont remplacés par *ca-ip*, *cs-a-username* et *cs-a-auth-group*, respectivement. **Note** Vous devez activer l'anonymisation uniquement si le serveur externe vers lequel les fichiers journaux sont envoyés est compatible pour gérer la fonction d'anonymisation. Après la création du journal, vous pouvez désanonymiser les champs anonymisés, si nécessaire. Voir la section Désanonymisation des champs de journalisation W3C, on page 14.

Option	Description
Passphrase for Anonymization (Phrase secrète pour l'anonymisation) (Journaux d'accès W3C)	Vous permet de créer une phrase secrète pour chiffrer les valeurs des champs. Cette zone sera activée uniquement lorsque vous choisirez d'anonymiser les champs de journalisation *c-ip*, *cs-username* ou *cs-auth-group*. **Note** Le système applique les règles de phrase secrète lors de sa configuration pour l'anonymisation. Pour générer automatiquement une phrase secrète, cochez la case à côté de **Auto Generate Passphrase** (Générer automatiquement la phrase secrète) et cliquez sur **Generate** (Générer). **Note** Si vous avez plusieurs périphériques, ils doivent tous définir la même phrase secrète.
Log Compression (Compression journal)	Indique si les fichiers remplacés sont compressés. AsyncOS compresse les fichiers de journalisation au format gzip.
Log Exclusions (Exclusions de journaux) (facultatif) (Journaux d'accès)	Vous permet de préciser les codes d'état HTTP (4xx ou 5xx uniquement) pour exclure les transactions associées d'un journal des accès ou du journal des accès W3C. Par exemple, la saisie de 401 filtrera les demandes d'échec d'authentification qui ont ce numéro de transaction.
Log Level (Niveau du journal)	Spécifie le niveau de détail des entrées de journal. Choisissez parmi : • **Critical** (Critique). Inclut uniquement les erreurs. Il s'agit du paramètre le moins détaillé; il équivaut au niveau d'alerte du journal système. • **Warning** (Avertissement). Inclut erreurs et avertissements. Ce niveau de journalisation est équivalent au niveau d'avertissement du journal système. • **Information**. Inclut les erreurs, les avertissements et les opérations supplémentaires du système. Il s'agit du niveau de détail par défaut et il équivaut au niveau « Info » du journal système. • **Debug** (Débogage). Comprend des données utiles pour le débogage des problèmes du système. Utilisez le niveau de journalisation de débogage lorsque vous essayez de découvrir la cause d'une erreur. Utilisez ce paramètre temporairement, puis revenez au niveau par défaut. Ce niveau de journalisation est équivalent au niveau de débogage du journal système. • **Trace** (Suivi). Il s'agit du paramètre le plus détaillé. Ce niveau comprend un enregistrement complet des opérations et des activités du système. Le niveau de journalisation Trace (Suivi) est recommandé uniquement pour les développeurs. L'utilisation de ce niveau entraîne une grave dégradation des performances du système et n'est pas recommandée. Ce niveau de journalisation est équivalent au niveau de débogage du journal système. **Note** Des paramètres plus détaillés créent des fichiers journaux plus volumineux et ont un impact plus important sur les performances du système.
Retrieval Method (Méthode de récupération)	Spécifie où les fichiers journaux reportés sont stockés et comment ils sont récupérés pour la lecture. Vous trouverez ci-dessous une description des méthodes disponibles.

Option	Description
Retrieval Method (Méthode de récupération) : FTP sur l'appliance	La méthode FTP sur l'appliance (équivalente à interrogation FTP) nécessite un client FTP distant accédant à l'appliance pour récupérer les fichiers journaux à l'aide du nom d'utilisateur et de la phrase secrète d'un administrateur ou opérateur. Lorsque vous choisissez cette méthode, vous devez saisir le nombre maximal de fichiers journaux à stocker sur l'appliance. Lorsque le nombre maximal est atteint, le système supprime le fichier le plus ancien. Il s'agit de la méthode de récupération par défaut.
Retrieval Method (Méthode de récupération) : FTP sur serveur distant	La méthode FTP sur serveur distant (équivalente au transfert FTP) envoie régulièrement les fichiers journaux sur un serveur FTP sur un ordinateur distant. Lorsque vous choisissez cette méthode, vous devez saisir les informations suivantes : • Nom d'hôte du serveur FTP • Répertoire sur le serveur FTP où stocker le fichier journal • Nom d'utilisateur et phrase secrète d'un utilisateur qui est autorisé à se connecter au serveur FTP **Note** AsyncOS pour le Web prend uniquement en charge le mode passif pour les serveurs FTP distants. Les fichiers journaux ne peuvent pas être transférés vers un serveur FTP en mode actif.
Retrieval Method (Méthode de récupération) : SCP sur serveur distant	La méthode SCP sur serveur distant (équivalente à la méthode SCP Push) envoie régulièrement les fichiers journaux à l'aide du protocole de copie sécurisée vers un serveur SCP distant. Cette méthode nécessite un serveur SSH SCP sur un ordinateur distant utilisant le protocole SSH2. L'abonnement nécessite un nom d'utilisateur, une clé SSH et un répertoire de destination sur l'ordinateur distant. Les fichiers journaux sont transférés selon un calendrier de renouvellement que vous définissez. Lorsque vous choisissez cette méthode, vous devez saisir les informations suivantes : • Nom d'hôte du serveur SCP • Répertoire sur le serveur SCP pour stocker le fichier journal • Nom d'utilisateur d'un utilisateur qui est autorisé à se connecter au serveur SCP **Note** Actuellement, nous prenons uniquement en charge SSH-RSA et SSH-DSS en mode non FIPS, ainsi que SSH-RSA en mode FIPS.

Option	Description
Retrieval Method (Méthode de récupération) : Syslog Push	Vous ne pouvez choisir syslog que pour les journaux texte. La méthode Syslog Push envoie des messages de journal à un serveur syslog distant sur le port 514. Cette méthode est conforme à la RFC 3164. Lorsque vous choisissez cette méthode, vous devez saisir les informations suivantes : • Nom d'hôte du serveur Syslog • Protocole à utiliser pour la transmission, UDP ou TCP • Taille maximale des messages Les valeurs correctes pour UDP sont comprises entre 1024 et 9216. Les valeurs correctes pour TCP sont comprises entre 1024 et 65 535. La taille maximale des messages dépend de la configuration du serveur syslog. • Facilité à utiliser avec le journal

Étape 4 Envoyez et validez vos modifications.

What to do next

Si vous avez choisi SCP comme méthode de récupération, remarquez que l'appliance affiche une clé SSH, que vous ajouterez à l'hôte du serveur SCP. Consultez Transmission des fichiers journaux à un autre serveur, on page 15.

Thèmes connexes

- Types de fichiers journaux, on page 3
- Noms des fichiers journaux et structure des répertoires de l'appliance, on page 16

Désanonymisation des champs de journalisation W3C

Si vous avez activé la fonction d'anonymisation pour les valeurs de champ (*c-ip, cs-username* et *cs-auth-group*) lors de l'abonnement au journal, le serveur de journaux de destination recevra les valeurs anonymisées (*c-a-ip*, *cs-a-username* et *cs-a-auth-group*) de ces champs de journal et non des valeurs réelles. Si vous souhaitez afficher les valeurs réelles, vous devez désanonymiser les champs du journal.

Vous pouvez désanonymiser les valeurs des champs de journalisation *ca-ip*, *cs-a-username* et *cs-a-auth-group* qui sont anonymisées lors de l'ajout de l'abonnement au journal W3C.

Étape 1 Choisissez **System Administration** > **Log Subscriptions** (Administration système > Abonnements aux journaux).

Étape 2 Cliquez sur **Deanonymization** (Désanonymisation) dans la colonne Delonymization (Désanonymisation) correspondant au journal pour lequel vous souhaitez désanonymiser les champs anonymisés.

Étape 3 Dans la zone **Method** (Méthode), choisissez l'une des méthodes suivantes pour saisir le texte chiffré à désanonymiser.

- Paste encrypted text (Coller le texte chiffré) : collez uniquement le texte chiffré dans le champ de texte anonymisé. Vous pouvez saisir un maximum de 500 entrées dans ce champ. Vous devez séparer les entrées multiples par une virgule.
- Upload File (Charger un fichier) : choisissez un fichier qui contient le texte chiffré. Le fichier peut contenir un maximum de 1 000 entrées. Le fichier doit être au format CSV. Le système prend en charge les espaces, les retours à la ligne, les tabulations et les points-virgules comme séparateurs de champ.

Remarque Si vous avez modifié la phrase secrète, vous devez l'entrer dans l'ancienne pour anonymiser les anciennes données.

Étape 4 Cliquez sur **Deanonymize** (Désanonymiser) et le tableau des résultats de la désanonymisation affiche les valeurs des champs de journal désanonymisées.

Transmission des fichiers journaux à un autre serveur

Before you begin

Créez ou modifiez l'abonnement au journal souhaité en choisissant SCP comme méthode de récupération. Ajout et modification d'abonnements aux journaux, on page 9

Étape 1 Ajouter des clés au système distant :

a) Accédez à l'interface de ligne de commande.
b) Utilisez la commande `logconfig -> hostkeyconfig`.
c) Utilisez les commandes ci-dessous pour afficher les clés :

Commande	Description
Host (Hôte)	Affichez les clés d'hôte du système. Il s'agit de la valeur à placer dans le fichier « known_hosts » du système distant.
User (Utilisateur)	Affiche la clé publique du compte système qui pousse les journaux vers l'ordinateur distant. Il s'agit de la même clé qui est affichée lors de la configuration d'un abonnement de transmission SCP. Il s'agit de la valeur à placer dans le fichier « autorized_keys » du système distant.

d) Ajoutez ces clés au système distant.

Étape 2 Toujours dans l'interface de ligne de commande, ajoutez la clé d'hôte publique SSH du serveur distant à l'appliance :

Commande	Description
New (Nouvelle)	Ajoutez une nouvelle clé.
Fingerprint (Empreinte)	Affichez les empreintes de la clé d'hôte du système.

Étape 3 Validez vos modifications.

Archivage des fichiers journaux

AsyncOS archive (renouvelle) les abonnements aux journaux lorsqu'un fichier journal actuel atteint la limite spécifiée par l'utilisateur de taille de fichier maximale ou le temps maximal depuis le dernier renouvellement.

Ces paramètres d'archivage sont inclus dans les abonnements aux journaux :

- Rollover by File Size (Renouvellement par taille de fichier)
- Rollover by Time (Renouvellement par heure)
- Log Compression (Compression journal)
- Retrieval Method (Méthode de récupération)

Vous pouvez également archiver manuellement (renouveler) les fichiers journaux.

Étape 1 Choisissez **System Administration > Log Subscriptions** (Administration système > Abonnements aux journaux).

Étape 2 Cochez la case dans la colonne Rollover (Renouvellement) des abonnements aux journaux que vous souhaitez archiver ou cochez la case **All** (Tous) pour sélectionner tous les abonnements.

Étape 3 Cliquez sur **Rollover Now** (Renouveler maintenant) pour archiver les journaux sélectionnés.

What to do next

Thèmes connexes

- Ajout et modification d'abonnements aux journaux, on page 9
- Noms des fichiers journaux et structure des répertoires de l'appliance, on page 16

Noms des fichiers journaux et structure des répertoires de l'appliance

L'appliance crée un répertoire pour chaque abonnement à un journal en fonction du nom d'abonnement au journal. Le nom du fichier journal dans le répertoire est composé des informations suivantes :

- Nom du fichier journal spécifié dans l'abonnement au journal
- Horodatage du démarrage du fichier journal
- Un code d'état à un caractère, soit .c (signifiant actuel) ou .s (signifiant enregistré)

Le nom de fichier des journaux est créé en utilisant la formule suivante :

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

Note Vous ne devez transférer que les fichiers journaux avec l'état enregistré.

Lecture et interprétation des fichiers journaux

Vous pouvez consulter l'activité du fichier journal actuel pour surveiller et dépanner Secure Web Appliance. Cela s'effectue à l'aide de l'interface de l'appliance.

Vous pouvez également lire des fichiers archivés pour un enregistrement de l'activité passée. Cela peut se faire à l'aide de l'interface de l'appliance si les fichiers archivés sont stockés sur l'appliance; sinon, elles doivent être lues à partir de leur emplacement de stockage externe à l'aide d'une méthode appropriée.

Chaque élément d'information d'un fichier journal est représenté par une variable de champ. En identifiant quels champs représentent quels éléments d'information, vous pouvez rechercher la fonction du champ et interpréter le contenu du fichier journal. Pour les journaux d'accès conformes W3C, l'en-tête du fichier indique les noms des champs dans l'ordre dans lequel ils apparaissent dans les entrées du journal. Pour les journaux d'accès standard, cependant, vous devez consulter la documentation concernant ce type de journal pour obtenir des renseignements sur l'ordre des champs.

Thèmes connexes

- Affichage des fichiers journaux, on page 17.
- Informations sur le proxy Web dans les fichiers journaux d'accès, on page 18.
- Interprétation des journaux d'accès W3C, on page 39.
- Interprétation des journaux de supervision du trafic, on page 46.
- Champs et balises des fichiers journaux, on page 46.

Affichage des fichiers journaux

Before you begin

Sachez que cette méthode d'affichage est destinée aux fichiers journaux stockés sur l'appliance. Le processus d'affichage des fichiers stockés à l'externe dépasse le cadre de cette documentation.

Étape 1 Choisissez **System Administration > Log Subscriptions** (Administration système > Abonnements aux journaux).

Étape 2 Cliquez sur le nom de l'abonnement au journal dans la colonne Log Files (Fichiers journaux) de la liste des abonnements aux journaux.

Étape 3 Lorsque vous y êtes invité, saisissez le nom d'utilisateur et la phrase secrète de l'administrateur pour accéder à l'appliance.

Étape 4 Une fois connecté, cliquez sur l'un des fichiers journaux pour l'afficher dans votre navigateur ou l'enregistrer sur le disque.

Étape 5 Actualisez le navigateur pour des résultats à jour.

Note Si un abonnement à un journal est compressé, téléchargez-le, décompressez-le, puis ouvrez-le.

What to do next

Thèmes connexes

Informations sur le proxy Web dans les fichiers journaux d'accès

Les fichiers journaux d'accès fournissent un enregistrement descriptif de toutes les activités de filtrage et d'analyse des proxys Web. Les entrées du fichier journal d'accès affichent un enregistrement de la façon dont l'appliance a traité chaque transaction.

Les journaux d'accès sont disponibles en deux formats : le format standard et celui conforme au W3C. Les fichiers journaux conformes au W3C sont plus personnalisables en ce qui concerne leur contenu et leur disposition que les journaux d'accès standard.

Le texte suivant est un exemple d'entrée de fichier journal des accès pour une transaction unique :

```
1278096903.150 97 172.xx.xx.xx TCP_MISS/200 8187 GET http://my.site.com/ -
DIRECT/my.site.com text/plain DEFAULT_CASE_11-PolicyGroupName-Identity-
OutboundMalwareScanningPolicy-DataSecurityPolicy-ExternalDLPPolicy-RoutingPolicy-NONE
<IW_comp,6.9,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-",""-",-,-,IW_comp,-,"-","-",
"Unknown","Unknown","-","-",198.34,0,-,[Local],"-",37,"W32.CiscoTestVector",33,0,
"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e”>
 -
```

Spécificateur de format	Valeur de champ	Description du champ
%t	`1278096903.150`	Horodatage depuis UNIX.
%e	`97`	Temps écoulé (latence) en millisecondes.
%a	`172.xx.xx.xx`	Adresse IP du client. **Remarque :** Vous pouvez choisir de masquer l'adresse IP dans les journaux d'accès à l'aide de la commande sur l'interface de ligne de commande advancedproxyconfig > authentication.
%w	`TCP_MISS`	Code de résultat de transaction. Pour en savoir plus, consultez Fichiers journaux des accès conformes aux normes W3C, on page 39.
%h	`200`	Code de réponse HTTP.
%s	`8187`	Taille de la réponse (en-têtes + corps)

Spécificateur de format	Valeur de champ	Description du champ
%1r %2r	`GET http://my.site.com/`	Première ligne de la demande. Remarque : Lorsque la première ligne de la demande concerne une transaction FTP native, certains caractères spéciaux du nom de fichier sont codés sous forme d'URL dans les journaux d'accès. Par exemple, le symbole « @ » est inscrit « %40 » dans les journaux d'accès. Les caractères suivants sont codés en mode URL : & # % + , : ; = @ ^ { } [ ]
%A	–	Nom d'utilisateur authentifié **Remarque :** Vous pouvez choisir de masquer le nom d'utilisateur dans les journaux d'accès à l'aide de la commande sur l'interface de ligne de commande `advancedproxyconfig > authentication`.
%H	`DIRECT`	Code qui décrit quel serveur a été contacté pour récupérer le contenu de la demande. Les valeurs les plus courantes comprennent : • **NONE.** Le proxy Web avait le contenu, donc il n'a contacté aucun autre serveur pour récupérer le contenu. • **DIRECT.** Le proxy Web est allé au serveur nommé dans la demande pour obtenir le contenu. • **DEFAULT_PARENT.** Le proxy Web s'est rendu chez son proxy parent principal ou sur un serveur DLP externe pour obtenir le contenu.
%d	`my.site.com`	Adresse IP de la source de données ou du serveur.
%c	`text/plain`	Type de corps de réponse MIME.

Spécificateur de format	Valeur de champ	Description du champ
%D	`DEFAULT_CASE_11`	Balise de décision ACL. **Remarque :** La fin de la balise de décision ACL comprend un numéro généré dynamiquement que le proxy Web utilise en interne. Vous pouvez ignorer ce numéro. Pour en savoir plus, consultez Balises de décision ACL, on page 23.
S.O. (faisant partie de la balise de décision ACL)	`PolicyGroupName`	Nom du groupe de politiques responsable de la décision finale concernant cette transaction (politique d'accès, politique de déchiffrement ou politique de sécurité des données). Lorsque la transaction correspond à une politique globale, cette valeur est « DefaultGroup ». Toute espace dans le nom du groupe de politiques est remplacée par un trait de soulignement (_).
S.O. (faisant partie de la balise de décision ACL)	`Identité`	Nom du groupe de politiques d'identité Toute espace dans le nom du groupe de politiques est remplacée par un trait de soulignement (_).
S.O. (faisant partie de la balise de décision ACL)	`OutboundMalwareScanningPolicy`	Nom du groupe de politiques d'analyse des programmes malveillants sortants. Toute espace dans le nom du groupe de politiques est remplacée par un trait de soulignement (_).

Spécificateur de format	Valeur de champ	Description du champ
S.O. (faisant partie de la balise de décision ACL)	`DataSecurityPolicy`	Nom du groupe de politiques de sécurité des données de Cisco. Lorsque la transaction correspond à la politique de sécurité des données globale de Cisco, cette valeur est « DefaultGroup ». Ce nom de groupe de politiques ne s'affiche que lorsque les filtres de sécurité des données Cisco sont activés. « NONE » s'affiche lorsqu'aucune politique de sécurité des données n'a été appliquée. Toute espace dans le nom du groupe de politiques est remplacée par un trait de soulignement (_).
S.O. (faisant partie de la balise de décision ACL)	`ExternalDLPPolicy`	Nom du groupe de politiques DLP externe. Lorsque la transaction correspond à la politique de DLP externe globale, cette valeur est « DefaultGroup ». « NONE » s'affiche lorsqu'aucune politique DLP externe n'a été appliquée. Toute espace dans le nom du groupe de politiques est remplacée par un trait de soulignement (_).
S.O. (faisant partie de la balise de décision ACL)	`RoutingPolicy`	Le nom du groupe de politiques de routage est *ProxyGroupName/ProxyServerName*. Lorsque la transaction correspond à la politique de routage globale, cette valeur est « DefaultRouting ». Lorsqu'aucun serveur proxy en amont n'est utilisé, cette valeur est « DIRECT ». Toute espace dans le nom du groupe de politiques est remplacée par un trait de soulignement (_).

Spécificateur de format	Valeur de champ	Description du champ
%Xr	<IW_comp,6.9,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,""-","-",-,-,IW_comp,-,"-","-","Unknown","Unknown","-","-",198.34,0,-,[Local],"-",37,"W32.CiscoTestVector",33,0,"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e">	Informations sur le verdict de l'analyse. À l'intérieur des crochets en angle, les journaux d'accès comprennent des renseignements sur les verdicts provenant de divers moteurs d'analyse. **Note** Dans AsyncOS version 11.8 et ultérieure, l'identifiant de catégorie d'URL apparaît entre guillemets doubles. Par exemple, « IW_comp ». Pour en savoir plus sur les valeurs incluses entre les crochets, consultez Interprétation des entrées de verdict d'analyse des journaux d'accès, on page 31 et Valeurs de verdict de la recherche de programmes malveillants, on page 61.
%?BLOCK_SUSPECT_USER_AGENT, MONITOR_SUSPECT_USER_AGENT?% < User-Agent:%!%-%	–	Agent utilisateur suspect.

Codes de résultats de transactions

Les codes de résultats de transaction dans le fichier journal des accès décrivent comment l'appliance résout les demandes des clients. Par exemple, si une demande pour un objet peut être résolue à partir du cache, le code de résultat est `TCP_HIT`. Toutefois, si l'objet ne se trouve pas dans le cache et que l'appliance extrait l'objet d'un serveur d'origine, le code de résultat est `TCP_MISS`. Le tableau suivant décrit les codes de résultats de transactions.

Code de résultat	Description
`TCP_HIT`	L'objet demandé a été récupéré à partir du cache disque.
`TCP_IMS_HIT`	Le client a envoyé une demande IMS (IF-Modified-Since) pour un objet et l'objet a été trouvé dans le cache. Le proxy répond par une réponse 304.
`TCP_MEM_HIT`	L'objet demandé a été récupéré de la mémoire cache.
`TCP_MISS`	L'objet n'a pas été trouvé dans le cache, il a donc été récupéré du serveur d'origine.

Code de résultat	Description
TCP_REFRESH_HIT	L'objet se trouve dans le cache, mais il a expiré. Le proxy a envoyé une demande IMS (IF-Modified-Since) au serveur d'origine et le serveur a confirmé que l'objet n'a pas été modifié. Par conséquent, l'appliance a récupéré l'objet à partir du cache disque ou de la mémoire cache.
TCP_CLIENT_REFRESH_MISS	Le client a envoyé une demande « ne pas récupérer la réponse du cache » en émettant l'en-tête « Pragma: no-cache ». En raison de cet en-tête du client, l'appliance a récupéré l'objet du serveur d'origine.
TCP_DENIED	La demande du client a été refusée en raison des politiques d'accès.
UDP_MISS	L'objet a été récupéré du serveur d'origine.
NONE	Une erreur s'est produite dans la transaction. Par exemple, une défaillance DNS ou un délai d'attente de passerelle.

Balises de décision ACL

Une balise de décision ACL est un champ d'une entrée du journal d'accès qui indique comment le proxy Web a traité la transaction. Elle contient des informations provenant des filtres de réputation Web, des catégories d'URL et des moteurs d'analyse.

Note La fin de la balise de décision ACL comprend un numéro généré dynamiquement que le proxy Web utilise en interne pour augmenter les performances. Vous pouvez ignorer ce numéro.

Le tableau suivant décrit les valeurs des balises de décision d'une liste de contrôle d'accès (ACL).

Balise de décision ACL	Description
ALLOW_ADMIN_ERROR_PAGE	Le proxy Web a autorisé la transaction vers une page de notification et vers tout logo utilisé sur cette page.
ALLOW_CUSTOMCAT	Le proxy Web a autorisé la transaction en fonction des paramètres du filtrage de catégories d'URL personnalisées pour le groupe de politiques d'accès.
ALLOW_REFERER	Le proxy Web a autorisé la transaction en fonction d'une dispense de contenu intégré ou référé.
ALLOW_WBRS	Le proxy Web a autorisé la transaction en fonction des paramètres de filtre de réputation Web pour le groupe de politiques d'accès.

Balise de décision ACL	Description
AMP_FILE_VERDICT	Valeur représentant un verdict à partir du serveur de réputation Cisco Secure Endpoint pour le fichier : • 1 – Inconnu • 2 – Sain • 3 – Malveillant • 4 – Impossible à analyser

Balise de décision ACL	Description
ARCHIVESCAN_ALLCLEAR ARCHIVESCAN_BLOCKEDFILETYPE ARCHIVESCAN_NESTEDTOODEEP ARCHIVESCAN_UNKNOWNFMT ARCHIVESCAN_UNSCANABLE ARCHIVESCAN_FILETOOBIG	**Verdict de l'analyse des archives** ARCHIVESCAN_ALLCLEAR : aucun type de fichier n'est bloqué dans l'archive inspectée. ARCHIVESCAN_BLOCKEDFILETYPE : un type de fichier est bloqué dans l'archive inspectée. Le champ suivant de l'entrée de journal [Verdict Detail (Détails du verdict)] fournit des détails, notamment le type de fichier bloqué et le nom du fichier bloqué. ARCHIVESCAN_NESTEDTOODEEP : l'archive est bloquée, car elle contient plus d'archives « encapsulées » ou imbriquées que le maximum configuré. Le champ Verdict Detail (Détails du verdict) contient la mention « UnScanable Archive-Blocked » (Archive impossible à analyser-Bloquée). ARCHIVESCAN_UNKNOWNFMT : l'archive est bloquée, car elle contient un type de fichier de format inconnu. Le détail du verdict est « UnScanable Archive-Blocked » (Archive impossible à analyser-Bloquée). ARCHIVESCAN_UNSCANABLE : l'archive est bloquée, car elle contient un fichier qui ne peut pas être analysé. Le détail du verdict est « UnScanable Archive-Blocked » (Archive impossible à analyser-Bloquée). ARCHIVESCAN_FILETOOBIG : l'archive est bloquée, car sa taille dépasse la limite maximale configurée. Le détail du verdict est « UnScanable Archive-Blocked » (Archive impossible à analyser-Bloquée). **Détails du verdict de l'analyse des archives** Le champ suivant le champ Verdict dans l'entrée du journal fournit des renseignements supplémentaires sur le verdict, tels que le type de fichier bloqué et le nom du fichier bloqué, « UnScanable Archive-Blocked » (Archive impossible à analyser-Bloquée) ou « - » pour indiquer que l'archive ne contient aucun type de fichier bloqué. Par exemple, si un fichier d'archive pouvant être inspectée est bloqué (ARCHIVESCAN_BLOCKEDFILETYPE) en fonction des paramètres Access Policy: Custom Objects Blocking (Politique d'accès : Blocage d'objets personnalisés), l'entrée Verdict Detail (Détails du verdict) comprend le type de fichier bloqué et le nom du fichier bloqué. Reportez-vous aux sections Politiques d'accès : blocage d'objets et Paramètres d'inspection des archives pour en savoir plus sur l'inspection des archives.
BLOCK_ADC	Transaction bloquée en fonction des paramètres d'application configurés pour le groupe de politiques d'accès.
BLOCK_ADMIN	Transaction bloquée en fonction de certains paramètres par défaut pour le groupe de politiques d'accès.

Balise de décision ACL	Description
BLOCK_ADMIN_CONNECT	Transaction bloquée en fonction du port TCP de la destination, comme défini dans le paramètre HTTP CONNECT Ports (Ports HTTP CONNECT) pour le groupe de politiques d'accès.
BLOCK_ADMIN_CUSTOM_USER_AGENT	Transaction bloquée en fonction de l'agent utilisateur, comme défini dans le paramètre Block Custom User Agents (Bloquer les agents utilisateur personnalisés) pour le groupe de politiques d'accès.
BLOCK_ADMIN_TUNNELING	Le proxy Web a bloqué la transaction en fonction de la tunnellisation du trafic non HTTP sur les ports HTTP pour le groupe de politiques d'accès.
BLOCK_ADMIN_HTTPS_ NonLocalDestination	Transaction bloquée; le client a essayé de contourner l'authentification en utilisant le port SSL comme proxy explicite. Pour éviter cela, si une connexion SSL est établie avec le Secure Web Appliance même, seules les demandes adressées au nom d'hôte de redirection Secure Web Appliance réel sont autorisées.
BLOCK_ADMIN_IDS	Transaction bloquée en fonction du type MIME du corps de la demande, comme défini dans le groupe de politique de sécurité des données.
BLOCK_ADMIN_FILE_TYPE	Transaction bloquée en fonction du type de fichier, comme défini dans le groupe de politiques d'accès.
BLOCK_ADMIN_PROTOCOL	Transaction bloquée sur la base du protocole défini dans le paramètre Block Protocols (Bloquer les protocoles) pour le groupe de politiques d'accès.
BLOCK_ADMIN_SIZE	Transaction bloquée en fonction de la taille de la réponse, comme défini dans les paramètres Object Size (Taille d'objet) pour le groupe de politiques d'accès.
BLOCK_ADMIN_SIZE_IDS	Transaction bloquée en fonction de la taille du contenu du corps de la demande, comme défini dans le groupe de politique de sécurité des données.
BLOCK_AMP_RESP	Le proxy Web a bloqué la réponse en fonction des paramètres Cisco Secure Endpoint du groupe de politiques d'accès.
BLOCK_AMW_REQ	Le proxy Web a bloqué la demande en fonction des paramètres de la protection contre les programmes malveillants pour le groupe de politiques d'analyse des programmes malveillants sortants. Le corps de la demande a produit un verdict positif quant à la présence de programmes malveillants.
BLOCK_AMW_RESP	Le proxy Web a bloqué la réponse en fonction des paramètres de la solution contre les programmes malveillants pour le groupe des politiques d'accès.

Balise de décision ACL	Description
BLOCK_AMW_REQ_URL	Le proxy Web soupçonne que l'URL contenue dans la requête HTTP n'est pas sécurisée. Il a donc bloqué la transaction au moment de la demande en fonction des paramètres contre les programmes malveillants du groupe des politiques d'accès.
BLOCK_AVC	Transaction bloquée en fonction des paramètres d'application configurés pour le groupe de politiques d'accès.
BLOCK_CONTENT_UNSAFE	Transaction bloquée en fonction des paramètres d'évaluation du contenu du site pour le groupe de politiques d'accès. La demande du client visait un contenu pour adultes et la politique est configurée pour bloquer le contenu pour adultes.
BLOCK_CONTINUE_CONTENT_ UNSAFE	Transaction bloquée et affichage de la page Warn and Continue (Avertir et continuer) en fonction des paramètres d'évaluation du contenu du site dans le groupe de politiques d'accès. La demande du client visait du contenu pour adultes et la politique est configurée pour envoyer un avertissement aux utilisateurs qui accèdent à un contenu pour adultes.
BLOCK_CONTINUE_CUSTOMCAT	Transaction bloquée et affichage de la page Warn and Continue (Avertir et continuer) en fonction d'une catégorie d'URL personnalisée dans le groupe de politiques d'accès configurée sur « Warn » (Avertir).
BLOCK_CONTINUE_WEBCAT	Transaction bloquée et affichage de la page Warn and Continue (Avertir et continuer) en fonction d'une catégorie d'URL prédéfinie dans le groupe de politiques d'accès configurée sur « Warn » (Avertir).
BLOCK_CUSTOMCAT	Transaction bloquée en fonction des paramètres de filtrage de catégorie d'URL personnalisée pour le groupe de politiques d'accès.
BLOCK_ICAP	Le proxy Web a bloqué la demande en fonction du verdict du système DLP externe comme défini dans le groupe de politiques DLP externe.
BLOCK_SEARCH_UNSAFE	La demande du client incluait une requête de recherche non sécurisée et la politique d'accès est configurée pour appliquer des recherches sécurisées, de sorte que la demande initiale du client a été bloquée.
BLOCK_SUSPECT_USER_AGENT	Transaction bloquée en fonction du paramètre Suspect User Agent (Agent utilisateur suspect) pour le groupe de politiques d'accès.
BLOCK_UNSUPPORTED_SEARCH_APP	Transaction bloquée en fonction des paramètres de recherche sécurisée pour le groupe de politiques d'accès. La transaction visait un moteur de recherche non pris en charge, et la politique est configurée pour bloquer les moteurs de recherche non pris en charge.
BLOCK_WBRS	Transaction bloquée en fonction des paramètres de filtre de réputation Web pour le groupe de politiques d'accès.
BLOCK_WBRS_IDS	Le proxy Web a bloqué la demande de chargement en fonction des paramètres de filtre de réputation Web pour le groupe de politiques de sécurité des données.

Balise de décision ACL	Description
BLOCK_WEBCAT	Transaction bloquée en fonction des paramètres de filtrage de catégorie d'URL pour le groupe de politiques d'accès.
BLOCK_WEBCAT_IDS	Le proxy Web a bloqué la demande de chargement en fonction des paramètres de filtrage de catégorie d'URL pour le groupe de politiques de sécurité des données.
BLOCK_YTCAT	Le proxy Web a bloqué la transaction en fonction des paramètres de filtrage de catégories YouTube prédéfinis pour le groupe de politiques d'accès.
BLOCK_CONTINUE_YTCAT	Le proxy Web a bloqué la transaction et affiché la page Warn and Continue (Avertir et continuer) en fonction d'une catégorie YouTube prédéfinie dans le groupe de politiques d'accès configurée sur « Warn » (Avertir).
DECRYPT_ADMIN	Le proxy Web a déchiffré la transaction en fonction de certains paramètres par défaut pour le groupe de politiques de déchiffrement.
DECRYPT_ADMIN_EXPIRED_CERT	Le proxy Web a déchiffré la transaction bien que le certificat du serveur ait expiré.
DECRYPT_EUN_ADMIN_DEFAULT_ACTION	Le proxy Web a déchiffré la transaction en fonction des paramètres par défaut comme l'abandon de connexion pour le groupe de politiques de déchiffrement quand EUN est activé.
DECRYPT_EUN_ADMIN_EXPIRED_CERT	Le proxy Web a déchiffré la transaction lorsque les paramètres de proxy HTTPS ont abandonné un certificat expiré avec EUN activé.
DECRYPT_EUN_ADMIN_INVALID_LEAF_CERT	Le proxy Web a déchiffré la transaction lorsque les paramètres de proxy HTTPS ont abandonné un certificat feuille non valide avec EUN activé.
DECRYPT_EUN_ADMIN_MISMATCHED_HOSTNAME	Le proxy Web a déchiffré la transaction lorsque les paramètres de proxy HTTPS suppriment le nom d'hôte non concordant avec EUN activé.
DECRYPT_EUN_ADMIN_OCSP_OTHER_ERROR	Le proxy Web a déchiffré la transaction lorsque les paramètres de proxy HTTPS abandonnent un OCSP avec d'autres erreurs avec EUN activé.
DECRYPT_EUN_ADMIN_OCSP_REVOKED_CERT	Le proxy Web a déchiffré la transaction lorsque les paramètres de proxy HTTPS ont abandonné un certificat OCSP révoqué avec EUN activé.
DECRYPT_EUN_ADMIN_UNRECOGNIZED_ROOT_CERT	Le proxy Web a déchiffré la transaction lorsque les paramètres de proxy HTTPS abandonnent un certificat d'autorité racine ou d'émetteur non reconnu avec EUN activé.
DECRYPT_EUN_CUSTOMCAT	Le proxy Web a déchiffré la transaction en fonction des paramètres de filtrage de catégories d'URL personnalisées pour le groupe de politiques de déchiffrement. Si EUN est activé, le trafic est abandonné.

Balise de décision ACL	Description
DECRYPT_EUN_WBRS	Le proxy Web a déchiffré la transaction en fonction des paramètres de filtre de réputation Web pour le groupe de politiques de déchiffrement. Si EUN est activé, le trafic est abandonné.
DECRYPT_EUN_WBRS_NO_SCORE	Le proxy Web a déchiffré la transaction en fonction des paramètres de filtre de réputation Web pour les URL sans score de réputation dans le groupe de politiques de déchiffrement. Si EUN est activé, le trafic est abandonné.
DECRYPT_EUN_WEBCAT	Le proxy Web a déchiffré la transaction en fonction des paramètres de filtrage de catégories d'URL pour le groupe de politiques de déchiffrement. Si EUN est activé, le trafic est abandonné.
DECRYPT_WEBCAT	Le proxy Web a déchiffré la transaction en fonction des paramètres de filtrage de catégorie d'URL pour le groupe de politiques de déchiffrement.
DECRYPT_WBRS	Le proxy Web a déchiffré la transaction en fonction des paramètres de filtre de réputation Web pour le groupe de politiques de déchiffrement.
DEFAULT_CASE	Le proxy Web a permis au client d'accéder au serveur, car aucun des services AsyncOS, tels que la réputation de sites Web ou l'analyse de protection contre les programmes malveillants , n'a pris de mesures sur la transaction.
DENY_ADMIN	Le proxy Web a refusé la transaction. Cela se produit pour les demandes HTTPS lorsque l'authentification est requise et que l'option « Decrypt for Authentication » (Déchiffrer pour authentification) est désactivée dans les paramètres de proxy HTTPS.
DROP_ADMIN	Le proxy Web a abandonné la transaction en fonction de certains paramètres par défaut pour le groupe de politiques de déchiffrement.
DROP_ADMIN_EXPIRED_CERT	Le proxy Web a abandonné la transaction, car le certificat du serveur a expiré.
DROP_WEBCAT	Le proxy Web a abandonné la transaction en fonction des paramètres de filtrage de catégories d'URL pour le groupe de politiques de déchiffrement.
DROP_WBRS	Le proxy Web a abandonné la transaction en fonction des paramètres de filtre de réputation Web pour le groupe de politiques de déchiffrement.
MONITOR_ADC	Le proxy Web a surveillé la transaction en fonction des paramètres d'application pour le groupe de politiques d'accès.
MONITOR_ADMIN_EXPIRED_CERT	Le proxy Web a surveillé la réponse du serveur, car le certificat du serveur a expiré.

Balise de décision ACL	Description
MONITOR_AMP_RESP	Le proxy Web a surveillé la réponse du serveur en fonction des paramètres Cisco Secure Endpoint du groupe de politiques d'accès.
MONITOR_AMW_RESP	Le proxy Web a surveillé la réponse du serveur en fonction des paramètres contre les programmes malveillants pour le groupe des politiques d'accès.
MONITOR_AMW_RESP_URL	Le proxy Web soupçonne que l'URL contenue dans la demande HTTP n'est pas sûre, mais il a surveillé la transaction en fonction des paramètres contre les programmes malveillants pour le groupe des politiques d'accès.
MONITOR_AVC	Le proxy Web a surveillé la transaction en fonction des paramètres d'application pour le groupe de politiques d'accès.
MONITOR_CONTINUE_CONTENT_ UNSAFE	À l'origine, le proxy Web a bloqué la transaction et affiché la page Warn and Continue (Avertir et continuer) en fonction des paramètres d'évaluation du contenu du site dans le groupe de politiques d'accès. La demande du client visait du contenu pour adultes et la politique est configurée pour envoyer un avertissement aux utilisateurs qui accèdent à un contenu pour adultes. L'utilisateur a accepté l'avertissement et a continué vers le site demandé à l'origine. Aucun autre moteur d'analyse n'a ensuite bloqué la demande.
MONITOR_CONTINUE_CUSTOMCAT	À l'origine, le proxy Web a bloqué la transaction et affiché la page Warn and Continue (Avertir et continuer) en fonction d'une catégorie d'URL personnalisée dans le groupe de politiques d'accès configuré sur « Warn » (Avertir). L'utilisateur a accepté l'avertissement et a continué vers le site demandé à l'origine. Aucun autre moteur d'analyse n'a ensuite bloqué la demande.
MONITOR_CONTINUE_WEBCAT	À l'origine, le proxy Web a bloqué la transaction et affiché la page Warn and Continue (Avertir et continuer) en fonction d'une catégorie d'URL prédéfinie dans le groupe de politiques d'accès configurée sur « Warn » (Avertir). L'utilisateur a accepté l'avertissement et a continué vers le site demandé à l'origine. Aucun autre moteur d'analyse n'a ensuite bloqué la demande.
MONITOR_CONTINUE_YTCAT	À l'origine, le proxy Web a bloqué la transaction et affiché la page Warn and Continue (Avertir et continuer) en fonction d'une catégorie YouTube prédéfinie dans le groupe de politiques d'accès configurée sur « Warn » (Avertir). L'utilisateur a accepté l'avertissement et a continué vers le site demandé à l'origine. Aucun autre moteur d'analyse n'a ensuite bloqué la demande.
MONITOR_IDS	Le proxy Web a analysé la demande de chargement à l'aide d'une politique de sécurité des données ou d'une politique DLP externe, mais n'a pas bloqué la demande. Il a évalué la demande par rapport aux politiques d'accès.

Balise de décision ACL	Description
MONITOR_SUSPECT_USER_AGENT	Le proxy Web a surveillé la transaction en fonction du paramètre Suspect User Agent (Agent utilisateur suspect) pour le groupe de politiques d'accès.
MONITOR_WBRS	Le proxy Web a surveillé la transaction en fonction des paramètres de filtre de réputation Web pour le groupe de politiques d'accès.
NO_AUTHORIZATION	Le proxy Web n'a pas autorisé l'utilisateur à accéder à l'application, car l'utilisateur était déjà authentifié par rapport à un domaine d'authentification, mais pas par rapport à un domaine d'authentification configuré dans la politique d'authentification de l'application.
NO_PASSWORD	L'authentification de l'utilisateur a échoué.
PASSTHRU_ADMIN	Le proxy Web a transmis la transaction en fonction de certains paramètres par défaut pour le groupe de politiques de déchiffrement.
PASSTHRU_ADMIN_EXPIRED_CERT	Le proxy Web a effectué la transaction bien que le certificat du serveur ait expiré.
PASSTHRU_WEBCAT	Le proxy Web a transmis la transaction en fonction des paramètres de filtrage de catégories d'URL pour le groupe de politiques de déchiffrement.
PASSTHRU_WBRS	Le proxy Web a transmis la transaction en fonction des paramètres de filtre de réputation Web pour le groupe de politiques de déchiffrement.
REDIRECT_CUSTOMCAT	Le proxy Web a redirigé la transaction vers une URL différente en fonction d'une catégorie d'URL personnalisée dans le groupe de politiques d'accès configuré sur « Redirect » (Rediriger).
SAAS_AUTH	Le proxy Web a autorisé l'utilisateur à accéder à l'application, car l'utilisateur a été authentifié de manière transparente par rapport au domaine d'authentification configuré dans la politique d'authentification de l'application.
OTHER	Le proxy Web n'a pas traité la demande en raison d'une erreur, comme un échec d'autorisation, la déconnexion du serveur ou une abandon par le client.

Interprétation des entrées de verdict d'analyse des journaux d'accès

Les entrées du fichier journal des accès regroupent et affichent les résultats des différents moteurs d'analyse, tels que le filtrage d'URL, le filtrage de réputation Web et l'analyse contre les programmes malveillants. L'appliance affiche ces informations entre crochets en angle à la fin de chaque entrée du journal d'accès.

Le texte qui suit constitue le verdict d'analyse provenant d'une entrée de fichier journal des accès. Dans cet exemple, le moteur d'analyse Webroot a détecté le programme malveillant :

```
<IW_infr,ns,24,"Trojan-Phisher-Gamec",0,354385,12559,-,"-",-,-,-,"-",-,-,"-","-",
-,-,
IW_infr,-,"Trojan Phisher","-","-","Unknown","Unknown","-","-",489.73,0,

[Local],"-","-",37,"W32.CiscoTestVector",33,0,"WSA-INFECTED-FILE.pdf",

"fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e",

ARCHIVESCAN_BLOCKEDFILETYPE,

EXT_ARCHIVESCAN_VERDICT,

EXT_ARCHIVESCAN_THREATDETAIL,

EXT_WTT_BEHAVIOR,
EXT_YTCAT,
"BlockedFileType: application/x-rpm,
BlockedFile: allfiles/linuxpackage.rp">
```

Note Pour obtenir un exemple d'entrée complète de fichier journal des accès, consultez Informations sur le proxy Web dans les fichiers journaux d'accès, on page 18.

Chaque élément dans cet exemple correspond à un spécificateur de format de fichier journal, comme le montre le tableau suivant :

Position	Valeur de champ	Spécificateur de format	Description
1	`IW_infr`	%XC	La catégorie d'URL personnalisée attribuée à la transaction, en abrégé. Ce champ affiche « nc » lorsqu'aucune catégorie n'est attribuée.
2	`ns`	%XW	Score des filtres de réputation Web Ce champ affiche le score, sous forme de nombre, « ns » pour aucun score ou « dns » en cas d'erreur de recherche DNS.
3	`24`	%Xv	Le verdict d'analyse des programmes malveillants Webroot est transmis au moteur DVS. S'applique aux réponses détectées par Webroot uniquement. Pour en savoir plus, consultez Valeurs de verdict de la recherche de programmes malveillants, on page 61.
4	`"Trojan-Phisher-Gamec"`	"%Xn"	Nom du logiciel espion associé à l'objet. S'applique aux réponses détectées par Webroot uniquement.
5	`0`	%Xt	Valeur spécifique à Webroot associée à la valeur du rapport menaces/risques (TRR) qui détermine la probabilité qu'un programme malveillant existe. S'applique aux réponses détectées par Webroot uniquement.

Position	Valeur de champ	Spécificateur de format	Description
6	354385	%Xs	Valeur que Webroot utilise comme identifiant de menace. L'assistance client de Cisco peut utiliser cette valeur lors du dépannage d'un problème. S'applique aux réponses détectées par Webroot uniquement.
7	12559	%Xi	Valeur que Webroot utilise comme ID Trace. L'assistance client de Cisco peut utiliser cette valeur lors du dépannage d'un problème. S'applique aux réponses détectées par Webroot uniquement.
8	-	%Xd	Le verdict d'analyse contre les programmes malveillants que McAfee a transmis au moteur DVS. S'applique aux réponses détectées par McAfee uniquement. Pour en savoir plus, consultez Valeurs de verdict de la recherche de programmes malveillants, on page 61.
9	"-"	"%Xe"	Nom du fichier analysé par McAfee. S'applique aux réponses détectées par McAfee uniquement.
10	-	%Xf	Valeur que McAfee utilise comme erreur d'analyse. L'assistance client de Cisco peut utiliser cette valeur lors du dépannage d'un problème. S'applique aux réponses détectées par McAfee uniquement.
11	-	%Xg	Valeur que McAfee utilise comme type de détection. L'assistance client de Cisco peut utiliser cette valeur lors du dépannage d'un problème. S'applique aux réponses détectées par McAfee uniquement.
12	-	%Xh	Valeur que McAfee utilise comme type de virus. L'assistance client de Cisco peut utiliser cette valeur lors du dépannage d'un problème. S'applique aux réponses détectées par McAfee uniquement.
13	"-"	"%Xj"	Le nom du virus que McAfee a analysé. S'applique aux réponses détectées par McAfee uniquement.

Position	Valeur de champ	Spécificateur de format	Description
14	-	%XY	Le verdict de l'analyse contre les programmes malveillants Sophos a transmis au moteur DVS. S'applique uniquement aux réponses détectées par Sophos. Pour en savoir plus, consultez Valeurs de verdict de la recherche de programmes malveillants, on page 61.
15	-	%Xx	Une valeur que Sophos utilise comme code de retour d'analyse. L'assistance client de Cisco peut utiliser cette valeur lors du dépannage d'un problème. S'applique uniquement aux réponses détectées par Sophos.
16	"-"	"%Xy"	Nom du fichier dans lequel Sophos a trouvé le contenu répréhensible. S'applique uniquement aux réponses détectées par Sophos.
17	"-"	"%Xz"	Une valeur que Sophos utilise comme nom de menace. L'assistance client de Cisco peut utiliser cette valeur lors du dépannage d'un problème. S'applique uniquement aux réponses détectées par Sophos.
18	-	%Xl	Le verdict de l'analyse sur la sécurité des données de Cisco en fonction de l'action dans la colonne Contenu de la politique de sécurité des données de Cisco. La liste suivante décrit les valeurs possibles pour ce champ : • **0.** Allow (Autoriser) • **1.** Block (Bloquer) • **- (trait d'union).** Aucune analyse n'a été lancée par les filtres de sécurité des données Cisco. Cette valeur s'affiche lorsque les filtres de sécurité des données Cisco sont désactivés ou lorsque l'action de catégorie d'URL est définie sur Allow (autoriser).

Position	Valeur de champ	Spécificateur de format	Description
19	-	%Xp	Verdict de l'analyse DLP externe en fonction du résultat donné dans la réponse ICAP . La liste suivante décrit les valeurs possibles pour ce champ : • **0.** Allow (Autoriser) • **1.** Block (Bloquer) • **- (trait d'union).** Aucune analyse n'a été lancée par le serveur DLP externe. Cette valeur s'affiche lorsque l'analyse DLP externe est désactivée ou lorsque le contenu n'a pas été analysé en raison d'une catégorie d'URL dispensée dans la page External DLP Policies > Destinations (Politiques DLP externes > Destinations).
20	`IW_infr`	%XQ	Verdict de catégorie d'URL prédéfinie déterminé lors de l'analyse côté demande, en abrégé. Ce champ répertorie un tiret (-) lorsque le filtrage d'URL est désactivé. **Note** Dans AsyncOS version 11.8 et ultérieure, l'identifiant de catégorie d'URL apparaît entre guillemets doubles. Par exemple, « IW_infr ». Pour obtenir la liste des abréviations de catégories d'URL, consultez Descriptions des catégories d'URL.
21	-	%XA	Verdict de la catégorie d'URL déterminé par le moteur d'analyse de contenu dynamique lors de l'analyse du côté des réponses, en abrégé. S'applique uniquement au moteur de filtrage d'URL Cisco Web Usage Controls. S'applique uniquement lorsque le moteur d'analyse de contenu dynamique est activé et lorsqu'aucune catégorie n'est attribuée au moment de la demande (une valeur « nc » est indiquée dans le verdict de l'analyse du côté de la demande). Pour obtenir la liste des abréviations de catégories d'URL, consultez Descriptions des catégories d'URL.

Position	Valeur de champ	Spécificateur de format	Description
22	"Trojan Phisher"	"%XZ"	Verdict unifié de l'analyse contre les programmes malveillants côté réponse qui fournit la catégorie de programmes malveillants indépendamment des moteurs d'analyse sont activés. S'applique aux transactions bloquées ou surveillées en raison de l'analyse de la réponse du serveur.
23	"-"	"%Xk"	Le nom de la catégorie ou le type de menace est renvoyé par les filtres de réputation Web. Le nom de la catégorie est renvoyé lorsque la réputation Web est élevée et le type de menace est renvoyé lorsque la réputation est faible.
24	"-"	%X#10#	URL qui est encapsulée dans le moteur de traduction Google. S'il n'y a pas d'URL encapsulée, la valeur du champ sera « - ».
25	"Unknown"	"%XO"	Le nom de l'application tel qu'il a été renvoyé par le moteur AVC, le cas échéant. Ne s'applique que lorsque le moteur AVC est activé.
26	"Unknown"	"%Xu"	Le type d'application tel qu'il est renvoyé par le moteur AVC, le cas échéant. Ne s'applique que lorsque le moteur AVC est activé.
27	"-"	"%Xb"	Le comportement de l'application tel qu'il est renvoyé par le moteur AVC, le cas échéant. Ne s'applique que lorsque le moteur AVC est activé.
28	"-"	"%XS"	Verdict de l'analyse pour une navigation sécurisée Cette valeur indique si la fonction de recherche sécurisée ou d'évaluation du contenu du site a été appliquée à la transaction. Pour obtenir la liste des valeurs possibles, consultez Journalisation de l'accès au contenu pour adultes.
29	489.73	%XB	La bande passante moyenne utilisée pour servir la demande, en Ko/s.
30	0	%XT	Valeur qui indique si la demande a été limitée en raison des paramètres de contrôle de limite de bande passante, où « 1 » indique que la demande a été limitée et « 0 » le contraire.

Position	Valeur de champ	Spécificateur de format	Description
31	`[Local]`	%l	Le type d'utilisateur effectuant la demande, « [Local] » ou « [Remote] ». Ne s'applique que lorsqu'AnyConnect Secure Mobility est activé. Lorsqu'elle n'est pas activée, la valeur est un tiret (-).
32	`"-"`	"%X3"	Verdict unifié de l'analyse contre les programmes malveillants du côté de la demande, quel que soit le moteur d'analyse activé. S'applique aux transactions bloquées ou surveillées en raison de l'analyse des demandes des clients lorsqu'une politique d'analyse des programmes malveillants sortants s'applique.
33	`"-"`	"%X4"	Le nom de menace attribué à la demande du client qui a été bloquée ou surveillée en raison d'une politique d'analyse de programmes malveillants sortants applicable. Ce nom de menace est indépendant des moteurs d'analyse activés de protection contre les programmes malveillants.
34	`37`	%X#1#	Verdict de l'analyse des fichiers Cisco Secure Endpoint : • 0 : le fichier n'est pas malveillant • 1 : Le fichier n'a pas été analysé en raison de son type de fichier • 2 : L'analyse des fichiers a expiré • 3 : Erreur d'analyse • Supérieur à 3 : Le fichier est malveillant
35	`"W32.CiscoTestVector"`	%X#2#	Le nom de la menace, comme déterminé par l'analyse de fichiers Cisco Secure Endpoint; « - » indique l'absence de menace.

Position	Valeur de champ	Spécificateur de format	Description
36	`33`	%X#3#	Score de réputation résultant de l'analyse des fichiers Cisco Secure Endpoint. Ce score est utilisé uniquement si le service de réputation en nuage n'est pas en mesure de déterminer un verdict clair pour le fichier. Pour en savoir plus, consultez les informations sur le score de menaces et le seuil de réputation dans Filtrage de réputation de fichiers et analyse de fichiers. .
37	`0`	%X#4#	Indicateur de chargement et de demande d'analyse : « 0 » indique que Cisco Secure Endpoint n'a pas demandé le chargement du fichier pour analyse. « 1 » indique que Cisco Secure Endpoint a demandé le chargement du fichier pour analyse.
38	`"WSA-INFECTED-FILE.pdf"`	%X#5#	Nom du fichier en cours de téléchargement et d'analyse.
39	`"fd5ef49d4213e05f448 f11ed9c98253d85829614fba 368a421d14e64c426da5e"`	%X#6#	Identifiant SHA-256 de ce fichier.
40	`ARCHIVESCAN_BLOCKEDFILETYPE`	%X#8#	Verdict de l'analyse des archives
41	`EXT_ARCHIVESCAN_VERDICT`	%Xo	Détails du verdict d'analyse d'archives. Si un fichier d'archive pouvant être inspectée est bloqué (`ARCHIVESCAN_BLOCKEDFILETYPE`) en fonction des paramètres de la politique d'accès : blocage des objets personnalisés, cette entrée de détail du verdict inclut le type de fichier bloqué et le nom du fichier bloqué.
42	`EXT_ARCHIVESCAN_THREATDETAIL`	%Xm	Fichier verdict par l'analyseur d'archives
43	`EXT_WTT_BEHAVIOR`	%XU	Comportement de dérivation Web.
44	`EXT_YTCAT`	%X#29#	La catégorie d'URL YouTube attribuée à la transaction, en abrégé. Ce champ affiche « nc » lorsqu'aucune catégorie n'est attribuée.

Reportez-vous à la section Champs et balises des fichiers journaux, on page 46 pour obtenir une description de la fonction de chaque spécificateur de format.

Thèmes connexes

- Informations sur le proxy Web dans les fichiers journaux d'accès, on page 18
- Personnalisation des journaux d'accès, on page 41
- Fichiers journaux des accès conformes aux normes W3C, on page 39
- Affichage des fichiers journaux, on page 17
- Champs et balises des fichiers journaux, on page 46

Fichiers journaux des accès conformes aux normes W3C

Secure Web Appliance fournit deux types de journaux différents pour l'enregistrement des informations sur les transactions par proxy Web : les journaux d'accès et les journaux d'accès au format W3C. Les journaux d'accès W3C sont conformes à la norme World Wide Web Consortium (W3C) et enregistrent l'historique des transactions dans le format ELF (Extended Log File) du W3C.

- Types de champs W3C, on page 39
- Interprétation des journaux d'accès W3C, on page 39

Types de champs W3C

Lors de la définition d'un abonnement au journal des accès W3C, vous devez choisir les champs de journalisation à inclure, comme la balise de décision ACL ou l'adresse IP du client. Vous pouvez inclure l'un des types de champs de journal suivants :

- **Prédéfini.** L'interface Web comprend une liste de champs parmi lesquels vous pouvez choisir.
- **Défini par l'utilisateur.** Vous pouvez saisir un champ de journal qui ne figure pas dans la liste prédéfinie.

Interprétation des journaux d'accès W3C

Tenez compte des règles et des directives suivantes lors de l'interprétation des journaux d'accès W3C :

- Les administrateurs décident quelles données sont enregistrées dans chaque abonnement au journal des accès W3C; par conséquent, les journaux d'accès W3C n'ont pas de format de champ défini.
- Les journaux W3C sont autodescriptifs. Le format de fichier (liste des champs) est défini dans un en-tête au début de chaque fichier journal.
- Les champs des journaux d'accès W3C sont séparés par un espace.
- Si un champ ne contient aucune donnée pour une entrée en particulier, un tiret (-) est inclus dans le fichier journal.
- Chaque ligne du fichier journal des accès W3C est liée à une transaction et chaque ligne se termine par une séquence LF.

- En-têtes des fichiers journaux W3C, on page 40
- Préfixes des champs W3C, on page 40

En-têtes des fichiers journaux W3C

Chaque fichier journal W3C contient un texte d'en-tête au début du fichier. Chaque ligne commence par le caractère # et fournit des renseignements sur Secure Web Appliance qui a créé le fichier journal. Les en-têtes du fichier journal W3C comprennent également le format de fichier (liste des champs), ce qui rend le fichier journal autodescriptif.

Le tableau suivant décrit les champs d'en-tête répertoriés au début de chaque fichier journal W3C.

Champ d'en-tête	Description
Version	Version du format ELF W3C utilisée.
Date	Date et heure auxquelles l'en-tête (et le fichier journal) a été créé.
System (Système)	Secure Web Appliance qui a généré le fichier journal au format « Management_IP - Management_hostname ».
Software (Logiciel)	Logiciel qui a généré ces journaux
Fields (Champs)	Champs enregistrés dans le journal

Exemple de fichier journal W3C :

```
#Version: 1.0
#Date: 2009-06-15 13:55:20
#System: 10.1.1.1 - wsa.qa
#Software: AsyncOS for Web 6.3.0
#Fields: timestamp x-elapsed-time c-ip
x-resultcode-httpstatus sc-bytes cs-method cs-url cs-username
x-hierarchy-origin cs-mime-type x-acltag x-result-code x-suspect-user-agent
```

Préfixes des champs W3C

La plupart des noms de champs des journaux W3C comprennent un préfixe qui identifie l'en-tête dont provient une valeur, comme le client ou le serveur. Les champs de journalisation sans préfixe référencent des valeurs indépendantes des ordinateurs impliqués dans la transaction. Le tableau suivant décrit les préfixes des champs des journaux W3C.

En-tête de préfixe	Description
c	Client
s	Serveur
cs	Client vers serveur
sc	Serveur vers client
x	Identifiant spécifique à l'application.

Par exemple, le champ de journal W3C « cs-method » fait référence à la méthode dans la demande envoyée par le client au serveur et « c-ip » fait référence à l'adresse IP du client.

Thèmes connexes

- Informations sur le proxy Web dans les fichiers journaux d'accès, on page 18.
- Personnalisation des journaux d'accès, on page 41.
- Fichiers journaux de supervision du trafic, on page 46.
- Champs et balises des fichiers journaux, on page 46.
- Affichage des fichiers journaux, on page 17.

Personnalisation des journaux d'accès

Vous pouvez personnaliser les journaux d'accès standard et W3C pour inclure de nombreux champs différents afin de saisir des informations complètes sur le trafic Web au sein du réseau à l'aide de champs prédéfinis ou définis par l'utilisateur.

Thèmes connexes

- Pour obtenir la liste des champs prédéfinis, consultez Champs et balises des fichiers journaux, on page 46.
- Pour en savoir plus sur les champs définis par l'utilisateur, consultez Champs définis par l'utilisateur des journaux d'accès, on page 41.

Champs définis par l'utilisateur des journaux d'accès

Si la liste des champs prédéfinis de journal d'accès et de journal W3C n'inclut pas toutes les informations d'en-tête que vous souhaitez enregistrer à partir des transactions HTTP/HTTPS, vous pouvez taper un champ de journal défini par l'utilisateur dans la zone de texte Champs personnalisés lorsque vous configurez l'accès et le journal W3C.

Les champs de journal personnalisés peuvent comprendre n'importe quelle donnée de n'importe quel en-tête envoyé par le client ou le serveur. Si une demande ou une réponse ne comprend pas l'en-tête ajouté à l'abonnement au journal, le fichier journal comprend un tiret comme valeur de champ de journal.

Le tableau suivant définit la syntaxe à utiliser pour l'accès et les journaux W3C :

Type d'en-tête	Syntaxe du spécificateur de format du journal d'accès	Syntaxe du champ personnalisé du journal W3C
En-tête de l'application cliente	%<*ClientHeaderName* :	cs(*ClientHeaderName*)
En-tête du serveur	%<*ServerHeaderName* :	sc(*ServerHeaderName*)

Par exemple, si vous souhaitez consigner la valeur d'en-tête If-Modified-Since dans les demandes des clients, entrez le texte suivant dans la zone Custom Fields (Champs personnalisés) pour un abonnement de journal W3C :

```
cs(If-Modified-Since)
```

Thèmes connexes

- Personnalisation des journaux d'accès standard, on page 42.
- Personnalisation des journaux d'accès W3C, on page 42.

Personnalisation des journaux d'accès standard

Étape 1 Choisissez **System Administration > Log Subscriptions** (Administration système > Abonnements aux journaux).

Étape 2 Cliquez sur le nom du fichier journal des accès pour modifier l'abonnement au journal des accès.

Étape 3 Entrez les spécificateurs de format requis dans le champ personnalisé.

La syntaxe de saisie des spécificateurs de format dans le champ personnalisé est la suivante :

```
<format_specifier_1> <format_specifier_2> ...
```

Par exemple : `%a %b %E`

Vous pouvez ajouter des jetons avant les spécificateurs de format pour afficher un texte de description dans le fichier journal des accès. Par exemple :

```
client_IP %a body_bytes %b error_type %E
```

où `IP_client` est le jeton de description du spécificateur de format de journal `%a`, etc.

Note Vous pouvez créer un champ personnalisé pour tout en-tête dans une demande de client ou une réponse de serveur.

Étape 4 Envoyez et validez vos modifications.

What to do next

Thèmes connexes

- Informations sur le proxy Web dans les fichiers journaux d'accès, on page 18.
- Champs et balises des fichiers journaux, on page 46.
- Champs définis par l'utilisateur des journaux d'accès, on page 41.

Personnalisation des journaux d'accès W3C

Étape 1 Choisissez **System Administration > Log Subscriptions** (Administration système > Abonnements aux journaux).

Étape 2 Cliquez sur le nom du fichier journal W3C pour modifier l'abonnement au journal W3C.

Étape 3 Saisissez un champ dans la zone Custom Field (Champ personnalisé), puis cliquez sur **Add** (Ajouter).

L'ordre dans lequel les champs apparaissent dans la liste Selected Log Fields (Champs de journal sélectionnés) détermine l'ordre des champs dans le fichier du journal d'accès W3C. Vous pouvez modifier l'ordre des champs à l'aide des boutons **Déplacement vers le haut** et **Déplacement vers le bas**. Vous pouvez supprimer un champ en le sélectionnant dans la liste Selected Log Fields (Champs de journal sélectionnés) et en cliquant sur **Remove** (Supprimer).

Vous pouvez saisir plusieurs champs définis par l'utilisateur dans la zone Custom Fields (Champs personnalisés) et les ajouter simultanément à condition que chaque entrée soit séparée par une nouvelle ligne [cliquez sur Enter (Entrée)] avant de cliquer sur **Add** (Ajouter).

Lorsque vous modifiez les champs de journal inclus dans un abonnement à un journal W3C, l'abonnement au journal est automatiquement renouvelé. Cela permet à la dernière version du fichier journal d'inclure les nouveaux en-têtes de champ corrects

Note Vous pouvez créer un champ personnalisé pour tout en-tête dans une demande de client ou une réponse de serveur.

Étape 4 Envoyez et validez vos modifications.

What to do next

Thèmes connexes

- Fichiers journaux des accès conformes aux normes W3C, on page 39.
- Champs et balises des fichiers journaux, on page 46.
- Champs définis par l'utilisateur des journaux d'accès, on page 41.
- Configuration des journaux W3C personnalisés propres à Cisco CTA, on page 43
- Configuration des journaux W3C personnalisés propres à Cisco Cloudlock, on page 44

Configuration des journaux W3C personnalisés propres à Cisco CTA

Vous pouvez configurer votre appliance pour transmettre les journaux d'accès W3C propres à Cognitive Threat Analytics (CTA) au service Cisco Cloud Web Security à des fins d'analyse et de création de rapports. Cisco ScanCenter est le portail d'administration de Cloud Web Security (CWS). Voir la section https://www.cisco.com/c/en/us/support/security/cloud-web-security/products-installation-and-configuration-guides-list.html.

Avant de commencer

Créez un compte de périphérique dans Cisco ScanCenter pour votre appliance en sélectionnant SCP (Secure Copy Protocol) comme protocole de téléchargement automatique. Voir la section des téléchargements de périphériques de proxy dans le logiciel Cisco ScanCenter Administrator (https://www.cisco.com/c/en/us/td/docs/security/web_security/scancenter/administrator/guide/b_ScanCenter_Administrator_Guide.html).

Notez le nom d'hôte SCP et le nom d'utilisateur généré pour votre appliance. Le nom d'utilisateur est sensible à la casse et unique pour chaque périphérique.

Étape 1 Choisissez **Security Services** > **Cisco Cognitive Threat Analytics** (Services de sécurité > Cisco Cognitive Threat Analytics).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Dans la zone **Log Fields** (Champs de journal), ajoutez des champs de journal supplémentaires, au besoin. Consultez Ajout et modification d'abonnements aux journaux, à la page 9.

Étape 4 Dans **Selected Log Fields** (Champs de journal sélectionnés), cochez les cases en regard de *c-ip*, *cs-username* ou *cs-auth-group* si vous souhaitez anonymiser ces champs individuellement.

Vous pouvez également cocher la case **Anonymization** (Anonymisation) pour anonymiser ces champs simultanément. Consultez Ajout et modification d'abonnements aux journaux, à la page 9.

Étape 5 Dans la zone **Rerieval Method** (Méthode de récupération), saisissez le nom d'utilisateur généré pour votre périphérique dans Cisco ScanCenter. Le nom d'utilisateur du périphérique est sensible à la casse et unique pour chaque périphérique proxy.

Étape 6 Modifiez les valeurs dans **Advanced Options** (Options avancées), si nécessaire.

Étape 7 Cliquez sur **Submit** (Soumettre).

L'appliance génère des clés SSH publiques et les affiche sur la page Cisco Cognitive Threat Analytics.

Étape 8 Copiez une des clés SSH publiques dans le presse-papiers.

Étape 9 Cliquez sur le lien du portail **Cisco Cognitive Threat Analytics** pour basculer vers le portail Cisco ScanCenter, sélectionnez le compte de périphérique approprié, puis collez la clé SSH publique dans la page de provisionnement de l'appareil CTA. (Reportez-vous à la section sur les *chargements de périphériques proxy* du Guide de l'administrateur de Cisco ScanCenter.)

Les fichiers journaux de votre périphérique proxy seront chargés sur le système CTA pour une analyse de l'authentification réussie entre votre périphérique proxy et le système CTA.

Étape 10 Revenez à l'appliance et validez vos modifications.

Vous pouvez également ajouter des journaux CTA W3C en utilisant **System Administration** > **Log Subscription** (Administration système > Abonnement aux journaux). Suivez les instructions à la section Personnalisation des journaux d'accès W3C, à la page 42 pour ajouter un nouvel abonnement au journal des accès W3C avec les options suivantes :

- **Journaux W3C** comme type de journal
- **Cisco Cognitive Threat Analytics Subscription** en tant qu'abonnement
- **SCP** comme type de transfert de fichier

Consultez Ajout et modification d'abonnements aux journaux, à la page 9 pour en savoir plus sur les champs personnalisés.

Remarque Si vous avez déjà configuré un abonnement à la journalisation CTA, vous devez remplacer le nom du journal par *cta_log* pour l'afficher sur la page Cisco Cognitive Threat Analytics de l'appliance.

Après la création du journal, si vous souhaitez supprimer le journal CTA, cliquez sur **Disable** (Désactiver) dans la page Cisco Cognitive Threat Analytics. Vous pouvez également supprimer le journal CTA de la page des abonnements aux journaux [**System Administration** > **Log subscriptions** (Administration système > Abonnements aux journées)].

Cliquez sur **Deanonymize** (Désanonymiser) dans la page Cisco Cognitive Threat Analytics de Cisco Cognitive Threat Analytics pour désanonymiser les champs du journal W3C spécifiques au CTA. Voir la section Désanonymisation des champs de journalisation W3C, à la page 14.

Vous pouvez également désanonymiser les champs de journalisation anonymisés propres au CTA du W3C en utilisant **System Administration** > **Log Subscription** (Administration système > Abonnement aux journaux). Voir la section Désanonymisation des champs de journalisation W3C, à la page 14.

Configuration des journaux W3C personnalisés propres à Cisco Cloudlock

Cisco Cloudlock est une plateforme infonuagique du CASB et de cybersécurité en nuage qui protège les utilisateurs, les données et les applications sur les logiciels-services, les plateformes en tant que service et les infrastructures en tant que service. Vous pouvez configurer votre appliance pour pousser les journaux d'accès W3C vers le portail Cisco Cloudlock à des fins d'analyse et de création de rapports. Ces journaux W3C personnalisés offrent une meilleure visibilité sur l'utilisation des logiciels-services par les clients.

Avant de commencer

Créez un compte de périphérique dans le portail Cloudlock pour votre appliance en sélectionnant SCP comme protocole de téléchargement automatique.

Connectez-vous au portail Cloudlock, accédez à l'aide en ligne et suivez les instructions pour créer un compte de périphérique sur le portail Cloudlock.

Étape 1 Choisissez **Security Services** > **Cisco Cloudlock** (Services de sécurité > Cisco Cloudlock).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Remarque Les champs de journalisation sont sélectionnés par défaut dans la zone **Log Fields** (Champs de journal). Vous ne pouvez pas ajouter d'autres champs de journalisation que les champs de journalisation sélectionnés par défaut. Vous ne devez pas modifier l'ordre des champs du journal affichés dans la zone **Log Fields** (Champs de journal).

Vous ne pouvez pas anonymiser les champs (*c-ip, cs-username* ou *cs-auth-group*) des fichiers journaux Cloudlock.

Étape 3 Dans la zone **Retrieval Method** (Méthode de récupération), entrez les informations suivantes :

- Nom d'hôte et numéro de port du serveur Cloudlock
- Répertoire sur le serveur Cloudlock pour stocker le fichier journal
- Nom de l'utilisateur autorisé à se connecter au serveur Cloudlock

Étape 4 Modifiez les valeurs dans **Advanced Options** (Options avancées), si nécessaire.

Étape 5 Cliquez sur **Submit** (Soumettre).

L'appliance génère des clés SSH publiques et les affiche sur la page Cisco Cloudlock.

Étape 6 Copiez une des clés SSH publiques dans le presse-papiers.

Étape 7 Cliquez sur le lien **View Cloudlock Portal** (Afficher le portail Cisco Cloudlock) pour passer au portail Cisco Cloudlock. Sélectionnez le compte de périphérique approprié, puis collez la clé SSH publique dans la page des paramètres Cloudlock.

Les fichiers journaux de votre périphérique proxy seront téléchargés sur le système Cloudlock pour une analyse de l'authentification réussie entre votre périphérique proxy et le système Cloudlock.

Étape 8 Revenez à l'appliance et validez vos modifications.

Vous pouvez également ajouter des journaux Cloudlock W3C en sélectionnant **System Administration** > **Log Subscription** (Administration système > Abonnement aux journaux). Suivez les instructions à la section Personnalisation des journaux d'accès W3C, à la page 42 pour ajouter un nouvel abonnement au journal des accès W3C avec les options suivantes :

- **Journaux W3C** comme type de journal
- **Cisco Cloudlock** en tant qu'abonnement
- **SCP** comme type de transfert de fichier

Consultez Ajout et modification d'abonnements aux journaux, à la page 9 pour en savoir plus sur les champs personnalisés.

Remarque Si vous avez déjà configuré un abonnement à la journalisation Cloudlock, vous devez remplacer le nom du journal par **cloudlock_log** pour l'afficher sur la page Cisco Cloudlock de l'appliance.

Après la création du journal, si vous souhaitez supprimer le journal Cloudlock, cliquez sur **Disable** (Désactiver) dans la page Cisco Cloudlock. Vous pouvez également supprimer le journal Cloudlock à partir de la page des abonnements aux journaux [**System Administration** > **Log subscriptions** (Administration système > Abonnements aux journaux)].

Fichiers journaux de supervision du trafic

Les fichiers journaux de la supervision du trafic de la couche 4 fournissent un enregistrement détaillé de l'activité de supervision sur la couche 4. Vous pouvez afficher les entrées de fichier journal de la supervision du trafic de la couche 4 pour suivre les mises à jour des listes de blocage et des listes d'autorisation de pare-feu.

Interprétation des journaux de supervision du trafic

Utilisez les exemples ci-dessous pour interpréter les différents types d'entrées contenues dans les journaux de supervision du trafic.

Exemple 1

```
172.xx.xx.xx discovered for blocksite.net (blocksite.net) ajouté à la liste de blocage du
pare-feu.
```

Dans cet exemple, où une correspondance devient une entrée de pare-feu de liste de blocage. La supervision du trafic de la couche 4 a mis en correspondance une adresse IP et un nom de domaine dans la liste de blocage en fonction d'une demande DNS qui est passée par l'appliance. L'adresse IP est ensuite entrée dans la liste de blocage du pare-feu.

Exemple 2

```
172.xx.xx.xx découvert pour www.allowsite.com (www.allowsite.com) ajouté à la liste des
autorisations du pare-feu.
```

Dans cet exemple, une correspondance devient une entrée de pare-feu de liste d'autorisation. La supervision du trafic de la couche 4 a trouvé une entrée de nom de domaine et l'a ajoutée à la liste des autorisations de l'appliance. L'adresse IP est ensuite entrée dans la liste d'autorisation du pare-feu.

Exemple 3

```
Le pare-feu a noté les données de 172.xx.xx.xx to 209.xx.xx.xx (allowsite.net):80.
```

Dans cet exemple, la supervision du trafic de la couche 4 consigne un enregistrement des données transmises entre une adresse IP interne et une adresse IP externe qui se trouve sur la liste de blocage. De plus, la supervision du trafic de la couche 4 est configurée pour surveiller, pas pour bloquer.

Thèmes connexes

- Affichage des fichiers journaux, on page 17

Champs et balises des fichiers journaux

- Spécificateurs de format des journaux d'accès et champs des fichiers journaux W3C, on page 47

- Codes de résultats de transactions, on page 22
- Balises de décision ACL, on page 23
- Valeurs de verdict de la recherche de programmes malveillants, on page 61

Spécificateurs de format des journaux d'accès et champs des fichiers journaux W3C

Les fichiers journaux utilisent des variables pour représenter les éléments d'information qui composent chaque entrée de fichier journal. Ces variables sont appelées spécificateurs de format dans les journaux d'accès et champs de journalisation dans les journaux W3C. Chaque spécificateur de format est associé à un champ de journal.

Pour configurer les journaux d'accès afin d'afficher ces valeurs, consultez Personnalisation des journaux d'accès, on page 41 et les informations sur les champs personnalisés dans Ajout et modification d'abonnements aux journaux, on page 9.

Le tableau suivant décrit ces variables :

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
%:<A	AclTime	Pour imprimer le temps total nécessaire à la transaction de liste de contrôle d'accès.
%{	x-id-shared	Pour imprimer l'état du partage d'ID avec Cisco Umbrella. Si l'ID est partagé pour une transaction, la valeur correspondante du formateur est « ID_SHARED », sinon « - » est affiché dans le journal des accès.
%[	x-spoofed-ip	Adresse IP source utilisée pour l'usurpation d'adresses IP par le proxy.
%)	x-proxy-instance-id	ID d'instance du proxy si le mode haute performance est activé, sinon un tiret est consigné.
%(	cs-domain-map	Nom de domaine résolu à l'aide de la carte de domaine.
%X#11#	ext_auth_sgt	Paramètre de champ personnalisé pour les étiquettes Groupe sécurisé utilisées dans les intégrations ISE.
%$	informations de déchiffrement	Informations de chiffrement des deux étapes de la transaction. (Client-proxy cipher info##proxy-server cipher info). Les informations dans la séquence ci-dessous - <ciphername>, <protocol version>, Kx=<key exchange>, Au=<authentication>, Enc=<symmetric encryption method>, Mac=<message authentication code>

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
%:<1	x-p2s-first-byte-time	Le temps entre le moment où le proxy Web commence à se connecter au serveur et le moment où il est en mesure d'écrire pour la première fois sur le serveur. Si le proxy Web doit se connecter à plusieurs serveurs pour terminer la transaction, il fait la somme de ces temps.
%:<a	x-p2p-auth-wait-time	Temps d'attente pour recevoir la réponse du processus d'authentification du proxy Web, après l'envoi de la demande par le proxy Web.
%:<b	x-p2s-body-time	Temps d'attente pour écrire le corps de la demande sur le serveur après l'en-tête.
%:<d	x-p2p-dns-wait-time	Temps nécessaire au proxy Web pour envoyer la demande DNS au processus DNS du proxy Web.
%:<h	x-p2s-header-time	Temps d'attente pour écrire l'en-tête de demande au serveur après le premier octet
%:<r	x-p2p-reputation- wait-time	Temps d'attente pour recevoir la réponse des filtres de réputation Web, après l'envoi de la demande par le proxy Web.
%:<s	x-p2p-asw-req- wait-time	Temps d'attente pour recevoir le verdict du processus de protection contre les logiciels espions du proxy Web, après l'envoi de la demande par le proxy.
%:>1	x-s2p-first-byte-time	Temps d'attente du premier octet de réponse du serveur
%:>a	x-p2p-auth-svc-time	Temps d'attente pour recevoir la réponse du processus d'authentification du proxy Web, y compris le temps nécessaire au proxy Web pour envoyer la demande.
%:>b	x-s2p-body-time	Temps d'attente du corps de la réponse complet après la réception de l'en-tête
%:>c	x-p2p-fetch-time	Temps requis par le proxy Web pour lire une réponse à partir du cache du disque.
%:>d	x-p2p-dns-svc-time	Temps que le processus DNS du proxy Web met à renvoyer un résultat DNS au proxy Web.
%:>h	x-s2p-header-time	Temps d'attente de l'en-tête du serveur après le premier octet de réponse
%:>g		Informations sur la latence d'établissement de la liaison du serveur SSL
%o	-	Quota de temps consommé.

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
% O	-	Quota de volume consommé.
%X#41#	x-bw-info	Niveau de contrôle de quota de bande passante appliqué, numéro de canal de bande passante mappé sur une requête, limite de quota de bande passante configurée et profil de quota de bande passante utilisé (level-pipe_no-quota_limit-quota_profile).
%:>r	x-p2p-reputation-svc- time	Le temps d'attente pour recevoir le verdict des filtres de réputation Web, y compris le temps nécessaire au proxy Web pour envoyer la demande.
%:>s	x-p2p-asw-req-svc- time	Temps d'attente pour recevoir le verdict du processus de protection contre les logiciels espions du proxy Web, y compris le temps nécessaire au proxy Web pour envoyer la demande.
%:1<	x-c2p-first-byte-time	Temps d'attente du premier octet de demande de la nouvelle connexion client
%:1>	x-p2c-first-byte-time	Temps d'attente pour le premier octet écrit sur le client.
%:A<	x-p2p-avc-svc-time	Temps d'attente pour recevoir la réponse du processus l'AVC, y compris le temps nécessaire au proxy Web pour envoyer la demande.
%:A>	x-p2p-avc-wait-time	Temps d'attente pour recevoir la réponse du processus AVC, après l'envoi de la demande par le proxy Web.
%:b<	x-c2p-body-time	Temps d'attente pour le corps complet du client.
%:b>	x-p2c-body-time	Temps d'attente pour le corps complet du document écrit au client
%:C<	x-p2p-dca-resp- svc-time	Temps d'attente pour recevoir le verdict du moteur d'analyse de contenu dynamique, y compris le temps nécessaire au proxy Web pour envoyer la demande.
%:C>	x-p2p-dca-resp- wait-time	Temps d'attente pour recevoir la réponse du moteur d'analyse de contenu dynamique, après l'envoi de la demande par le proxy Web.
%:h<	x-c2p-header-time	Temps d'attente pour l'en-tête client complet après le premier octet
%:h>	x-p2c-header-time	Temps d'attente pour l'en-tête complet écrit sur le client

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
%:m<	x-p2p-mcafee-resp- svc-time	Temps d'attente pour recevoir le verdict du moteur d'analyse McAfee, y compris le temps nécessaire au proxy Web pour envoyer la demande.
%:m>	x-p2p-mcafee-resp- wait-time	Temps d'attente pour recevoir la réponse du moteur d'analyse McAfee, après l'envoi de la demande par le proxy Web.
%:p<	x-p2p-sophos-resp- svc-time	Temps d'attente avant de recevoir le verdict du moteur d'analyse Sophos, notamment le temps nécessaire au proxy Web pour envoyer la demande.
%:p>	x-p2p-sophos-resp- wait-time	Temps d'attente pour recevoir la réponse du moteur d'analyse Sophos, après l'envoi de la demande par le proxy Web
%:w<	x-p2p-webroot-resp -svc-time	Temps d'attente pour recevoir le verdict du moteur d'analyse depuis Webroot, y compris le temps nécessaire au proxy Web pour envoyer la demande.
%:w>	x-p2p-webroot-resp-wait- time	Temps d'attente pour recevoir la réponse du moteur d'analyse Webroot, après l'envoi de la demande par le proxy Web.
%aBLOCK_SUSPECT_USER_AGENT, MONITOR_SUSPECT_USER_AGENT?%<User-Agent:%!%-%	x-suspect-user-agent	Agent utilisateur suspect, le cas échéant. Si le proxy Web détermine que l'agent utilisateur est suspect, il le consignera dans ce champ. Sinon, il consigne un trait d'union. Ce champ est écrit entre guillemets dans les journaux d'accès.
%<Referer:	cs(Referer)	Référent
%>Server:	sc(Server)	En-tête du serveur dans la réponse.
%a	c-ip	Adresse IP du client.
%A	cs-username	Nom d'utilisateur authentifié. Ce champ est écrit entre guillemets dans les journaux d'accès.
%b	sc-body-size	Octets envoyés au client par le proxy Web pour le corps du message.
%B	octets	Total des octets utilisés (taille de la requête + taille de la réponse, soit %q + %s).
%c	cs-mime-type	Type de corps de réponse MIME. Ce champ est écrit entre guillemets dans les journaux d'accès.

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
%C	cs(Cookie)	En-tête de témoin. Ce champ est écrit entre guillemets dans les journaux d'accès.
%d	s-hostname	Adresse IP de la source de données ou du serveur.
%]	Header_profile	Nom du profil de réécriture de l'en-tête HTTP.
%D	x-acltag	Balise de décision ACL.
%e	x-elapsed-time	Temps écoulé en millisecondes. Pour le trafic TCP, il s'agit du temps écoulé entre l'ouverture et la fermeture de la connexion HTTP. Pour le trafic UDP, il s'agit du temps écoulé entre l'envoi du premier datagramme et le moment où le dernier datagramme peut être accepté. Une valeur de temps écoulé élevée pour le trafic UDP peut indiquer qu'une valeur de délai d'expiration élevée et une association UDP de longue durée ont permis d'accepter des datagrammes plus longtemps que nécessaire.
%E	x-error-code	Numéro de code d'erreur qui peut aider l'assistance client à résoudre la raison de l'échec d'une transaction.(
%f	cs(X-Forwarded-For)	En-tête X-Forwarded-For.
%F	c-port	Port source du client
%g	cs-auth-group	Noms de groupes autorisés. Ce champ est écrit entre guillemets dans les journaux d'accès. Ce champ est utilisé pour résoudre les problèmes de politique ou d'authentification afin de déterminer si un utilisateur correspond au bon groupe ou à la bonne politique.
%G		Horodatage lisible par l'homme.
%h	sc-http-status	Code de réponse HTTP.
%H	s-hierarchy	Récupération de la hiérarchie.
%i	x-icap-server	Adresse IP du dernier serveur ICAP contacté lors du traitement de la demande.
%I	x-transaction-id	ID de transaction.

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
%j	DCF	

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
		Ne pas mettre en cache le code de réponse; indicateurs DCF. Descriptions des codes de réponse : • Code de réponse en fonction de la demande du client : • 1 = la demande comportait un en-tête « no-cache ». • 2 = La mise en cache n'est pas autorisée pour la demande. • 4 = Il manque l'en-tête « Variant » dans la requête. • 8 = Nom d'utilisateur ou phrase secrète requis pour la demande de l'utilisateur. • 20 = Réponse pour la méthode HTTP indiquée. • Code de réponse basé sur la réponse reçue par l'appliance : • id="li_7443F05D141F4D9FB788FD416697DB65"> 40 = La réponse contient l'en-tête « Cache-Control: private ». • 80 = La réponse contient l'en-tête « Cache-Control: no-store ». • 100 = La réponse indique que la demande était une interrogation. • 200 = La réponse a une faible valeur « Expires ». • 400 = La réponse n'a pas d'en-tête « Last Modified ». • 1000 = La réponse expire immédiatement. • 2000 = Le fichier de réponse est trop volumineux pour être mis en cache. • 20000 = Une nouvelle copie du fichier existe. • 40000 = La réponse comporte des valeurs incorrectes ou non valides dans l'en-tête « Vary ». • 80000 = La réponse nécessite l'utilisation de témoins.

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
		• 100000 = Code d'ÉTAT HTTP non mis en cache • 200000 = L'objet reçu par l'appliance est incomplet (en fonction de la taille). • 800000 = Les bandes de fin de réponse indiquent qu'il n'y a pas de mise en cache. • 1000000 = La réponse doit être réécrite.
%k	s-ip	Adresse IP de la source de données (adresse IP du serveur) Cette valeur est utilisée pour déterminer un demandeur lorsque l'adresse IP est signalée par un périphérique de détection d'intrusion sur votre réseau. Vous permet de localiser un client qui a visité une adresse IP qui a été ainsi marquée.
%l	user-type	Type d'utilisateur, local ou distant.
%L	x-local_time	Demandez l'heure locale dans un format lisible par l'homme : JJ/MMM/AAAA : hh:mm:ss +nnnn. Ce champ est écrit entre guillemets dans les journaux d'accès. L'activation de ce champ vous permet de corréler les journaux aux problèmes sans avoir à calculer l'heure locale à partir de l'heure ancienne pour chaque entrée de journal.

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
%m	cs-auth-mechanism	Utilisé pour résoudre les problèmes d'authentification. Mécanisme d'authentification utilisé pour la transaction Les valeurs possibles sont les suivantes : • **BASIC.** Le nom d'utilisateur a été authentifié à l'aide du schéma d'authentification de base. • **NTLMSSP.** Le nom d'utilisateur a été authentifié à l'aide du schéma d'authentification NTLMSSP. • **NEGOTIATE.** Le nom d'utilisateur a été authentifié à l'aide du schéma d'authentification Kerberos. • **SSO_TUI.** Le nom d'utilisateur a été obtenu en faisant correspondre l'adresse IP du client à un nom d'utilisateur authentifié à l'aide d'une identification d'utilisateur transparente. • **SSO_ISE.** L'utilisateur a été authentifié par un serveur ISE. (Le journal indique GUEST (INVITÉ) s'il est choisi comme mécanisme de secours pour l'authentification ISE.) • **SSO_ASA.** L'utilisateur est un utilisateur distant et le nom d'utilisateur a été obtenu auprès d'un Cisco ASA à l'aide de Secure Mobility. • **FORM_AUTH.** L'utilisateur saisit les justificatifs d'authentification dans un formulaire dans le navigateur Web lorsqu'il accède à une application. • **GUEST.** L'utilisateur a échoué à l'authentification et a obtenu l'accès en tant qu'invité.
%M	CMF	Indicateurs d'échec du cache : indicateurs CMF.
%N	s-computerName	Nom du serveur ou nom de l'hôte de destination. Ce champ est écrit entre guillemets dans les journaux d'accès.
%p	s-port	Numéro du port de destination.
%P	cs-version	Protocole.
%q	cs-bytes	Taille de la demande (en-têtes + corps)
%r	x-req-first-line	Première ligne de la demande : méthode de demande, URI.
%s	sc-bytes	Taille de la réponse (en-tête + corps)

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
%t	Horodatage	Horodatage sous UNIX. **Remarque :** si vous souhaitez utiliser un analyseur de journaux tiers pour lire et analyser les journaux d'accès W3C, vous devrez peut-être inclure le champ « timestamp ». La plupart des analyseurs de journaux ne comprennent l'heure que dans le format fourni par ce champ.
%u	cs(User-Agent)	Agent utilisateur. Ce champ est écrit entre guillemets dans les journaux d'accès. Ce champ permet de déterminer si une application échoue à l'authentification et/ou nécessite des autorisations d'accès différentes.
%U	cs-uri	URI de la demande.
%v	date	Date au format AAAA-MM-JJ.
%V	de temps	Heure au format HH:MM:SS.
%w	sc-result-code	Code de résultat. Par exemple : TCP_MISS, TCP_HIT.
%W	sc-result-code-denial	Code de résultat refusé.
%x	x-latency	Latence.
%X0	x-resp-dvs-scanverdict	Verdict unifié de l'analyse de protection contre les programmes malveillants côté réponse qui fournit le *numéro de catégorie de programmes malveillants*, quel que soit le moteur d'analyse activé. S'applique aux transactions bloquées ou surveillées en raison de l'analyse de la réponse du serveur. Ce champ est écrit entre guillemets dans les journaux d'accès.
%X1	x-resp-dvs-threat-name	Verdict unifié de l'analyse de protection contre les programmes malveillants côté réponse qui fournit le *nom du programme malveillant*, quel que soit le moteur d'analyse activé. S'applique aux transactions bloquées ou surveillées en raison de l'analyse de la réponse du serveur. Ce champ est écrit entre guillemets dans les journaux d'accès.
%X2	x-req-dvs-scanverdict	Verdict de l'analyse DVS côté demande
%X3	x-req-dvs-verdictname	Nom du verdict DVS côté demande

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
%X4	x-req-dvs-threat-name	Nom de la menace DVS côté demande
%X6	x-as-malware-threat-name	Indique si l'analyse adaptative a bloqué la transaction sans faire appel au moteur d'analyse de protection contre les programmes malveillants. Les valeurs possibles sont les suivantes : • **1.** La transaction a été bloquée. • **0.** La transaction n'a pas été bloquée. Cette variable est incluse dans les informations sur le verdict de l'analyse (entre les crochets à la fin de chaque entrée du journal des accès).
%XA	x-webcat-resp-code- abbr	Verdict de catégorie d'URL déterminé lors de l'analyse côté réponse, en abrégé. S'applique uniquement au moteur de filtrage d'URL Cisco Web Usage Controls.
%Xb	x-avc-behavior	Comportement de l'application Web identifié par le moteur AVC.
%XB	x-avg-bw	Bande passante moyenne de l'utilisateur si les limites de bande passante sont définies par le moteur AVC.
%XC	x-webcat-code-abbr	Abréviation de catégorie d'URL de la catégorie d'URL personnalisée attribuée à la transaction.
%Xd	x-mcafee-scanverdict	Identifiant spécifique à McAfee : (verdict d'analyse)
%Xe	x-mcafee-filename	Identifiant spécifique à McAfee : (Nom du fichier produisant le verdict) ce champ est écrit avec des guillemets dans les journaux d'accès.
%Xf	x-mcafee-av-scanerror	Identifiant propre à McAfee : (erreur d'analyse).
%XF	x-webcat-code-full	Nom complet de la catégorie d'URL attribuée à la transaction. Ce champ est écrit entre guillemets dans les journaux d'accès.
%Xg	x-mcafee-av-detecttype	Identifiant spécifique à McAfee : (type de détection).
%XG	x-avc-reqhead-scanverdict	Verdict de l'en-tête de la demande AVC
%Xh	x-mcafee-av-virustype	Identifiant spécifique à McAfee : (type de virus)
%XH	x-avc-reqbody- scanverdict	Verdict du corps de la demande AVC.
%Xi	x-webroot-trace-id	Identifiant d'analyse spécifique à Webroot : (ID Trace)

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
%Xj	x-mcafee-virus-name	Identifiant spécifique à McAfee : (nom du virus) Ce champ est écrit entre guillemets dans les journaux d'accès.
%Xk	x-wbrs-threat-type	Type de menace pour la réputation Web.
%XK	x-wbrs-threat-reason	Motif de la menace pour la réputation Web.
%Xl	x-ids-verdict	Verdict d'analyse de la politique de sécurité des données de Cisco. Si ce champ est inclus, il affichera le verdict IDS, ou « 0 » si l'IDS était actif mais le document analysé à jour, ou « - » si aucune politique IDS n'était active pour la demande.
%XL	x-webcat-resp-code- full	Verdict de catégorie d'URL déterminé lors de l'analyse côté réponse, nom complet. S'applique uniquement au moteur de filtrage d'URL Cisco Web Usage Controls.
%XM	x-avc-resphead- scanverdict	Verdict de l'en-tête de réponse AVC
%Xn	x-webroot-threat-name	Identifiant spécifique à Webroot : (Nom de la menace) Ce champ est écrit entre guillemets dans les journaux d'accès.
%XN	x-avc-reqbody-scanverdict	Verdict du corps de la réponse AVC.
%XO	x-avc-app	Application Web identifiée par le moteur AVC.
%Xp	x-icap-verdict	Verdict de l'analyse du serveur DLP externe
%XP	x-acl-added-headers	En-tête non reconnu. Utilisez ce champ pour consigner des en-têtes supplémentaires dans les demandes des clients. Cela prend en charge le dépannage de systèmes spécialisés qui ajoutent des en-têtes aux demandes des clients pour les authentifier et les rediriger, par exemple YouTube for Schools.
%XQ	x-webcat-req-code- abbr	Verdict de catégorie d'URL prédéfinie déterminé lors de l'analyse côté demande, en abrégé.
%Xr	x-result-code	Informations sur le verdict de l'analyse.
%XR	x-webcat-req-code-full	Verdict de catégorie d'URL déterminé lors de l'analyse côté demande, nom complet.
%Xs	x-webroot-spyid	Identifiant spécifique à Webroot : (ID espion).

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
%XS	x-request-rewrite	Verdict de l'analyse pour une navigation sécurisée Indique si la recherche sécurisée ou la fonction d'évaluation du contenu du site a été appliquée à la transaction.
%Xt	x-webroot-trr	Identifiant propre à Webroot : [Rapport menaces/risques (TRR)].
%XT	x-bw-throttled	Indicateur qui indique si des limites de bande passante ont été appliquées à la transaction.
%Xu	x-avc-type	Type d'application Web identifié par le moteur AVC.
%Xv	x-webroot-scanverdict	Verdict de l'analyse des programmes malveillants depuis Webroot.
%XV	x-request-source-ip	L'adresse IP en aval lorsque la case « Enable Identification of Client IP Addresses using X-Forwarded-For » (Activer l'identification des adresses IP clientes à l'aide de X-Forwarded-For) est cochée pour les paramètres du proxy Web.
%XW	x-wbrs-score	Score WBRS décodé <-10.0-10.0>.
%Xx	x-sophos-scanerror	Identifiant spécifique à Sophos : (code de retour de l'analyse).
%Xy	x-sophos-file-name	Nom du fichier dans lequel Sophos a trouvé le contenu répréhensible. S'applique uniquement aux réponses détectées par Sophos.
%XY	x-sophos-scanverdict	Identifiant spécifique à Sophos : (verdict de l'analyse).
%Xz	x-sophos-virus-name	Identifiant spécifique à Sophos : (nom de la menace).
%XZ	x-resp-dvs-verdictname	Verdict unifié de l'analyse de protection contre les programmes malveillants côté réponse qui fournit la *catégorie de programmes malveillants* indépendamment des moteurs d'analyse activés. S'applique aux transactions bloquées ou surveillées en raison de l'analyse de la réponse du serveur. Ce champ est écrit entre guillemets dans les journaux d'accès.

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
%X#1#	x-amp-verdict	Verdict de l'analyse des fichiers Cisco Secure Endpoint : • 0 : Le fichier n'est pas malveillant. • 1 : Le fichier n'a pas été analysé en raison de son type de fichier. • 2 : L'analyse des fichiers a expiré. • 3 : Erreur de l'analyse. • Supérieur à 3 : Le fichier est malveillant.
%X#2#	x-amp-malware-name	Nom de la menace, comme déterminé par l'analyse des fichiers Cisco Secure Endpoint. « - » indique l'absence de menace.
%X#3#	x-amp-score	Score de réputation résultant de l'analyse des fichiers Cisco Secure Endpoint. Ce score est utilisé uniquement si le service de réputation en nuage n'est pas en mesure de déterminer un verdict clair pour le fichier. Pour en savoir plus, consultez les informations sur le score de menace et le seuil de réputation dans Filtrage de réputation de fichiers et analyse de fichiers
%X#4#	x-amp-upload	Indicateur de chargement et de demande d'analyse : « 0 » indique que Cisco Secure Endpoint n'a pas demandé le chargement du fichier pour analyse. « 1 » indique que Cisco Secure Endpoint a demandé le chargement du fichier pour analyse.
%X#5#	x-amp-filename	Nom du fichier en cours de téléchargement et d'analyse.
%X#6#	x-amp-sha	Identifiant SHA-256 de ce fichier.
%y	cs-method	Méthode.
%Y	cs-url	URL complète.
%:e<	x-p2p-amp-svc-time	Temps d'attente pour recevoir le verdict du moteur d'analyse Cisco Secure Endpoint , y compris le temps nécessaire au proxy Web pour envoyer la demande.
%:e>	x-p2p-amp-wait-time	Temps d'attente pour recevoir la réponse du moteur d'analyse Cisco Secure Endpoint , après l'envoi de la demande par le proxy Web.

Spécificateur de format dans les journaux d'accès	Champ de journal dans les journaux W3C	Description
S. O.	x-hierarchy-origin	Code qui décrit le serveur contacté pour récupérer le contenu de la demande (par exemple, DIRECT/www.exemple.com).
S. O.	x-resultcode-httpstatus	Code de résultat et le code de réponse HTTP, séparés par une barre oblique (/).
S. O.	x-archivescan-verdict	Affiche le verdict de l'inspection des archives.
S. O.	x-archivescan-verdict- reason	Détails du fichier bloqué par l'analyse des archives
%XU	S. O.	Pour utilisation future.

Thèmes connexes

- Informations sur le proxy Web dans les fichiers journaux d'accès, on page 18.
- Interprétation des journaux d'accès W3C, on page 39.

Valeurs de verdict de la recherche de programmes malveillants

Un verdict d'analyse contre les programmes malveillants est une valeur affectée à une requête d'URL ou à une réponse d'un serveur qui détermine la probabilité qu'elle convienne à des programmes malveillants. Les moteurs d'analyse Webroot, McAfee et Sophos renvoient un verdict de recherche de programmes malveillants au moteur DVS pour que ce dernier puisse déterminer s'il faut surveiller ou bloquer l'objet analysé. Chaque verdict d'analyse contre les programmes malveillants correspond à une catégorie de programmes malveillants répertoriée sur la page Access Policies > Reputation and Anti-Malware Settings (Politiques d'accès > Paramètres de protection contre les programmes malveillants et de réputation) lorsque vous modifiez les paramètres de protection contre les programmes malveillants pour une politique d'accès particulière.

La liste suivante présente les différentes valeurs de verdict d'analyse contre les programmes malveillants et chaque catégorie de programmes malveillants correspondante :

Valeur du verdict de l'analyse des programmes malveillants	Catégorie de programmes malveillants
-	Non défini
0	Inconnu
1	Non analysé
2	Délai d'expiration
3	Erreur
4	Impossible à analyser
10	Logiciel espion générique

Valeur du verdict de l'analyse des programmes malveillants	Catégorie de programmes malveillants
12	Objet de l'assistant du navigateur
13	Logiciels publicitaires
14	Moniteur système
18	Supervision de système commercial
19	Composeur automatique
20	Détournement d'identité
21	URL d'hameçonnage
22	Outil de téléchargement de chevaux de Troie
23	Cheval de Troie
24	Cheval de Troie pour hameçonnage
25	Vers
26	Fichier chiffré
27	Virus
33	Autres programmes malveillants
34	API (applications potentiellement indésirables)
35	Abandonné
36	Heuristique des épidémies
37	Fichiers malveillants ou à risque élevé connus

Thèmes connexes

- Informations sur le proxy Web dans les fichiers journaux d'accès, on page 18.
- Interprétation des journaux d'accès W3C, on page 39.

Résolution des problèmes de journalisation

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.