Comprendre les journaux d'accès sécurisés des appliances Web

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Structure Accesslog
  - Heure d'époque
  - Temps Écoulé
  - Adresse IP source
  - Code résultat du mouvement
  - Code de réponse HTTP
  - Taille totale transférée
  - Méthode HTTP
  - Destination
  - Nom d'utilisateur et domaine d'authentification
  - Type d'accès
  - Adresse du serveur
  - Type/sous-type de contenu MIME
  - Étiquette de décision ACL
  - Nom de stratégie
  - Politique d'identité
  - Groupe de stratégie de sécurité des données
  - Groupe de stratégies DLP externe
  - Routing Policy Group
  - Robinet Trafic Web
  - Abréviation de catégorie URL
  - Score de réputation Web
  - Analyse Webroot
  - Analyse McAfee
  - Analyse Sophos
  - Verdict d'analyse de sécurité des données Cisco
  - Verdict d'analyse DLP externe
  - Verdict de catégorie d'URL prédéfinie
  - Verdict de catégorie URL
  - Verdict DVS entrant unifié
  - Type de menace de filtre de réputation Web
  - URL encapsulée Google Translate

- Contrôle des applications (AVC/ADC)
- Verdict de navigation sécurisée
- Bande passante moyenne
- Contrôle de bande passante limite
- Type d'utilisateur
- Analyse des programmes malveillants sortants
- Protection avancée contre les malwares
- Analyse des archives
- Effleurez Web
- Catégorie URL YouTube

Code de réponse HTTP

Étiquette de décision ACL

Valeurs de verdict d'analyse de programme malveillant

Autres informations utiles

Introduction

Ce document décrit la structure du journal d'accès SWA (Secure Web Appliance).

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- Accès à l'interface de ligne de commande (CLI) de SWA.

- Accès administratif au SWA.
- Compréhension de base du processus SWA.

Composants utilisés

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

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

Structure Accesslog

Dans cet article, la structure Accesslog est expliquée par cet exemple :

```
1726597763.348 68855 192.168.1.10 TCP_MISS/200 97645 TCP_CONNECT 10.37.145.84:443 "AMOJARRA\amirhossein
```

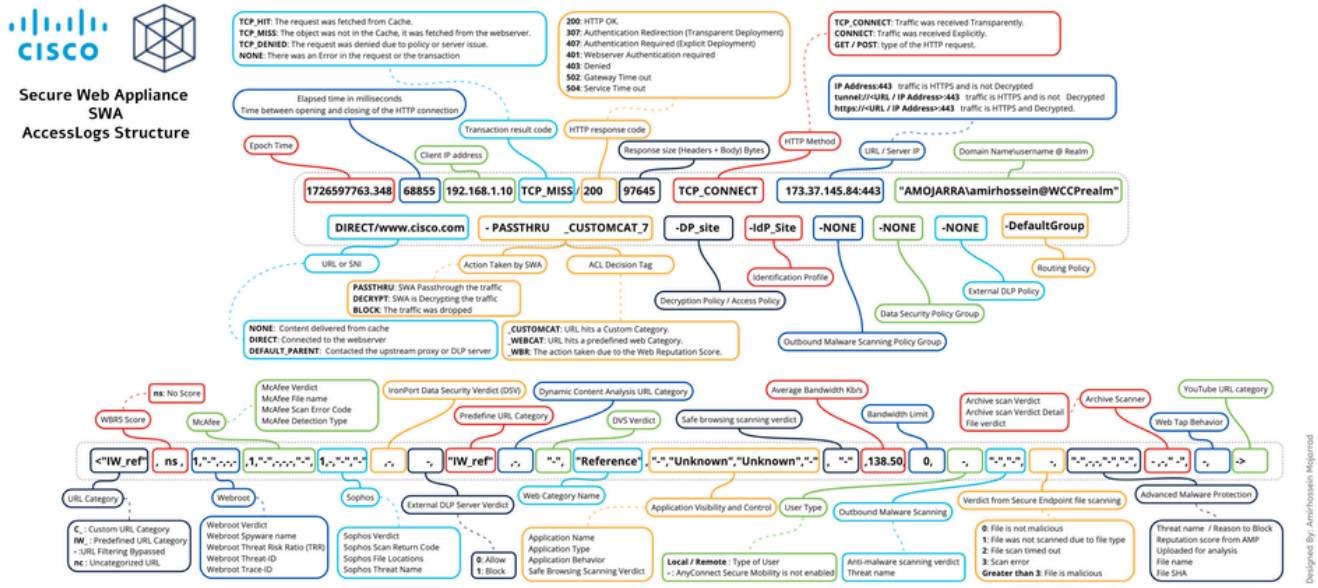


Image - Structure du journal d'accès

Remarque : La structure des journaux d'accès dépend de la version de SWA. Au début de chaque fichier Accesslog, une ligne indique sa structure et l'ordre du spécificateur de format.

Profilé	Exemple dans Accesslog	Spécificateur de format	Détails
Heure d'époque	1726597763.348	%t	L'heure d'époque (souvent ap un système de suivi du temps (ou millisecondes/microsecon 1970, à 00:00:00 UTC Heure d'époque à laquelle la t Vous pouvez convertir cette va

			en ligne ou tout système d'exp
Temps Écoulé	68855	%e	Durée en millisecondes de la c terminée/abandonnée et que l
Adresse IP source	192.168.1.10	%a	Adresse IP client/source.
Code résultat du mouvement	TCP_MANQUANT	%w	Le code de résultat de la trans les requêtes du client. Voici la liste des codes de rés

TCP_HIT
TCP_IMS_HIT
TCP_MEM_HIT
TCP_MANQUANT
TCP_REFRESH_HIT

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td></tr>
<tr><td>TCP_CLIENT_REFRESH_MI</td></tr>
<tr><td>TCP_REFUSÉ</td></tr>
<tr><td>HTTPS TCP_REFUSÉ_SSL</td></tr>
<tr><td>TCP_CLIENT_REFRESH_MI</td></tr>
<tr><td>HTTPS TCP_MISS_SSL</td></tr>
</table>
</td></tr>
<tr><td>Code de réponse HTTP</td><td>/200</td><td>%h</td><td>Le code de réponse HTTP rep
serveur Web en réponse à la

Voici la liste des codes de rép
plus d'informations, veuillez co
HTTP dans cet article)
<table>
<tr><td>Code de statut</td><td>Signification</td></tr>
<tr><td>000</td><td>000 est un code</td></tr>
</table>
</td></tr>
</table>

	interruption de la ou plus tard pend
2xx a réussi	
200	OK
204	Aucun contenu
206	Contenu partiel (e
Redirection 3xx	
301	Redirection perm
302	Redirection temp
304	Non modifié
307	Redirection temp (Généralement vi pendant que SWA
Erreur client 4xx	
400	Requête incorrec
401	Authentification d visible dans le dé SWA authentifie l
403	Interdit
404	Non trouvé
407	Authentification p
Erreur de serveur 5xx	
500	Erreur interne du
502	Passerelle incorre
503	Service non dispo
504	Délai de passerel

<table>
<tr><td>Taille totale transférée</td><td>97645</td><td>%s</td><td>Nombre total d'octets transfér</td></tr>
<tr><td>Méthode HTTP</td><td>TCP_CONNECT</td><td>%1r</td><td>Un procédé HTTP est un moy
spécifier l'action souhaitée à e
serveur Web, telle que la récu
l'envoi de données avec POS
<table><tr><td>GET</td><td>La
der
cor
info
de
sig</td></tr><tr><td>POST</td><td>La
env
gér
req
l'en
fich
l'éta</td></tr><tr><td>CONNEXION</td><td>La
pou
per
cor
des
traf
cor

Ind
exp
que
dire</td></tr><tr><td>TCP_CONNECT</td><td>Ind
tra
WC</td></tr></table></td></tr>
<tr><td>Destination</td><td>10.37.145.84:443</td><td>%2r</td><td>Cette section indique l'URL du
port TCP.</td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td>Dans la redirection transparen
SWA affiche l'adresse IP de d

Si l'URL commence par tunne
encore déchiffré le trafic.

Si l'URL commence par https:/
trafic.</td></tr>
<tr><td>Nom d'utilisateur et domaine d'authentification</td><td>AMOJARRA\amirhossein@WCCPrealm</td><td>%A</td><td>Identifiants utilisés pour cette

Si la demande est authentifiée
les domaines d'authentificatio

<Nom de domaine> \ <Nom d'
d'authentification>

Si la demande n'est pas encor
l'authentification, le trait d'unio</td></tr>
<tr><td>Type d'accès</td><td>DIRECT/</td><td>%H</td><td>Code qui décrit le serveur con
la demande.

Les valeurs les plus courantes
<table><tr><td>NONE</td><td>Le p
pas
le co</td></tr><tr><td>DIRECT</td><td>Le p
dans</td></tr><tr><td>PARENT_PAR_DÉFAUT</td><td>Le p
princ
Prev</td></tr></table></td></tr>
<tr><td>Adresse du serveur</td><td>www.cisco.com</td><td>%d</td><td>Adresse IP de la source de do</td></tr>
<tr><td>Type/sous-type de contenu</td><td>-</td><td>%c</td><td>Multipurpose Internet Mail Ex
format d'un document, d'un fic
types MIME sont définis et no</td></tr>
</table>

<table>
<tr>
<td>MIME</td>
<td></td>
<td></td>
<td>Deux types MIME principaux s
par défaut :
text/plain est la valeur pa
texte doit être lisible par
données binaires.
application/octet-stream
autres cas. Un type de fi
navigateurs font particuli
manipulation de ces fich
contre les vulnérabilités
potentiellement dangere
Pour obtenir la liste complète
(iana)</td>
</tr>
<tr>
<td>Étiquette de décision ACL</td>
<td>PASSTHRU_CUSTOMCAT_7-</td>
<td>%D</td>
<td>Une balise de décision de liste
d'une entrée du journal d'accè
géré la transaction. Il inclut de
réputation de sites Web, des c
d'analyse.

Remarque : la fin de la ba
d'accès inclut un numéro
Web utilise en interne pou
pouvez ignorer ce nombr

Voici une liste des balises de c
plus d'informations, consultez
cet article)
<table><tr><td>Étiquette de décision ACL</td></tr><tr><td>AUTORISER_CATÉGORIE_F</td></tr><tr><td>AUTORISER_WBRS</td></tr></table></td>
</tr>
</table>

			VERDICT_FICHIER_AMP
			ADMIN_BLOC
			BLOCK_ADMIN_CONNECT
			BLOCK_ADMIN_CUSTOM_U
			TUNNELING_ADMIN_BLOC
			TYPE_FICHIER_ADMIN_BLC

			PROTOCOLE_ADMIN_BLOC
			RESP_AMP_BLOC
			AVC_BLOC
			BLOCK_CONTENT_UNSAFE
			BLOC_PERSONNALISER

			BLOC_ICAP
			BLOC_WBRS
			BLOCK_WEBCAT
			BLOC_YTCAT
			ADMIN_DÉCHIFFREMENT
			DECRYPT_EUN_CUSTOMCA

			DECRYPT_EUN_WBRS
			DECRYPT_EUN_WEBCAT
			DÉCHIFFRER_CHAT_WEB
			DÉCHIFFRER_WBRS
			DROP_ADMIN

			DROP_WEBCAT
			DROP_WBRS
			ADMIN_PASSTHRU
			PASSTHRU_WEBCAT
			PASSTHRU_WBRS

			OTHER (AUTRE)
Nom de stratégie	Site_DP-	S/O	En fonction du type de trafic, v • Nom de la stratégie de d n'est pas encore déchiffr • Nom de la stratégie d'ac déchiffré.
Politique d'identité	IdP_Site-	S/O	Affiche le nom du profil d'ident
Groupe de stratégies d'analyse des programmes malveillants sortants	NONE-	S/O	Nom du groupe Stratégie d'an sortants. Tout espace dans le nom du g trait de soulignement (_)
groupe de stratégie de sécurité des données	NONE-	S/O	Nom du groupe Stratégie de s transaction correspond à la str Cisco, cette valeur est Default apparaît uniquement lorsque l sont activés. NONE apparaît l données n'est appliquée. Tout espace dans le nom du g trait de soulignement (_)
Groupe de stratégies DLP externe	NONE-	S/O	Lorsque la transaction corresp cette valeur est DefaultGroup. DLP externe n'a été appliquée Tout espace dans le nom du g trait de soulignement (_).

<table>
<tr><td>Routing Policy Group</td><td>GroupeParDéfaut-</td><td>S/O</td><td>Nom du groupe de stratégie d
ProxyGroupName/ProxyServe

Lorsque la transaction corresp
cette valeur est DefaultRoutin
n'est utilisé, cette valeur est D

Tout espace dans le nom du g
trait de soulignement (_).</td></tr>
<tr><td>Robinet Trafic Web</td><td>NONE</td><td>S/O</td><td>Trafic Web Effleurez Nom de</td></tr>
<tr><td>Abréviation de catégorie URL</td><td><"C_Cisco",</td><td>%XC</td><td>Catégorie d'URL à laquelle la
<table><tr><td>-</td><td>Filtrage des URL</td></tr><tr><td>nc</td><td>URL non classée</td></tr><tr><td>se tromper</td><td>Filtrage des URL</td></tr><tr><td>lutin</td><td>Impossible</td></tr><tr><td>IW_</td><td>Si le nom de la ca
commence par IW
que la demande a
catégorie d'URL p</td></tr><tr><td>C_</td><td>Si le nom de la ca
commence par IC
que la demande a
catégorie d'URL p</td></tr></table></td></tr>
<tr><td>Score de réputation Web</td><td>-,</td><td>%XW</td><td>Ce champ affiche le score de

ns signifie que l'URL n'a pas d</td></tr>
<tr><td>Analyse Webroot</td><td>-,"-",-,-,-,-</td><td></td><td>Ces 5 champs sont liés à l'ana</td></tr>
</table>

			Verdict Webroot,	%Xv
			Nom d'espion Webroot	« %Xn »
			Webroot TRR,	%Xt
			Webroot ThreatID,	%Xs
			Webroot TraceID,	%Xi

<table>
<tr>
<td>Analyse McAfee</td>
<td>-,"-",-,-,-,"-",</td>
<td></td>
<td>Ces 6 champs sont liés à l'ana
<table>
<tr><td>Verdict McAfee,</td><td>%Xd</td></tr>
<tr><td>Nom de fichier McAfee,</td><td>« %Xe »</td></tr>
<tr><td>Code d'erreur d'analyse McAfee,</td><td>%Xf</td></tr>
<tr><td>Type de détection McAfee,</td><td>%Xg</td></tr>
<tr><td>Type de virus McAfee,</td><td>%Xh</td></tr>
</table>
</td>
</tr>
</table>

			Nom du virus McAfee,	« %Xj »
Analyse Sophos	-,-,"-","-",		Ces 4 champs sont liés à l'ana	
			Verdict Sophos,	%XY
			Sophos Scan Return Code,	%Xx
			Emplacements des fichiers Sophos,	« %Xy »
			Nom de la menace Sophos,	« %Xz »
Verdict d'analyse	-,	%Xl	Le verdict d'analyse de la sécu	

de sécurité des données Cisco			l'action de la colonne Contenu Cisco. Cette liste décrit les valeurs po 0. Autoriser 1. Bloquer - (trait d'union). Aucune analys sécurité des données Cisco. C de sécurité des données Cisco catégorie d'URL est définie su
Verdict d'analyse DLP externe	-,	%Xp	Verdict d'analyse DLP externe réponse ICAP (Internet Conter Cette liste décrit les valeurs po 0. Autoriser 1. Bloquer - (trait d'union). Aucune analys externe. Cette valeur apparaît désactivée ou lorsque le conte catégorie d'URL d'exemption s Destinations.
Verdict de catégorie d'URL prédéfinie	"-",	%XQ	Verdict de catégorie d'URL pre l'analyse côté requête. Ce champ contient un trait d'u désactivé. Si la demande atteint une caté pouvez toujours voir le nom de votre Accesslog, mais la décis personnalisée. Pour obtenir la liste des abrév Description des catégories d'U
Verdict de catégorie URL	-,	%XA	Verdict de catégorie d'URL dé contenu dynamique (DCA) lors S'applique uniquement au mo

			Usage Controls. nc : Cette valeur apparaît dans lorsque le moteur d'analyse dy qu'aucune catégorie d'URL n'e indiquant que l'URL n'est pas demande initiale avant que l'a
Verdict DVS entrant unifié	"-",	%XZ	Verdict d'analyse anti-program fournit la catégorie de program moteurs d'analyse activés. S'a surveillées en raison de l'analy
Type de menace de filtre de réputation Web	"-",	%Xk	Le nom de catégorie ou le type de réputation Web. Le nom de réputation Web est élevée et l est faible. En général, ce champ est rens est inférieure ou égale à -4.
URL encapsulée Google Translate	"-",	%X#10#	URL encapsulée dans le mote d'URL encapsulée, la valeur d
Contrôle des applications (AVC/ADC)	"-","-","-",		Dans ces 3 champs, les statis applications (AVC) et de Déco (ADC) sont consignées.

Nom de l'application AVC/ADC	"%XO"	N p e l
Type d'application AVC/ADC	« %Xu »	T A u A
Comportement des	« %Xb »	C n

			applications AVC/ADC
Verdict de navigation sécurisée	"-",	%XS	Cette valeur indique si la fonct d'évaluation du contenu du sit ensorceler : La demande initia fonction de reche encart : La demande initia fonctionnalité d'év appliquée. désappuyer : La demande initia de recherche non se tromper : La demande initia ni la fonction de r d'évaluation du co en raison d'une er - : Ni la fonction de r classification du c demande du clien exemple, la transa catégorie d'URL p effectuée à partir
Bande passante moyenne	11.35,	%XB	Bande passante moyenne cor Ko/s.
Contrôle de bande passante limite	0,	%XT	Valeur indiquant si la demand de contrôle de la limite de ban «1» indique que la demande a «0» indique que la demande n

<table>
<tr><td>Type d'utilisateur</td><td>-,</td><td>%l</td><td>Type d'utilisateur effectuant la

S'applique uniquement lorsqu
Mobility est activée.

Lorsqu'elle n'est pas activée, l</td></tr>
<tr><td>Analyse des programmes malveillants sortants</td><td>"-","-",</td><td></td><td>Ces 2 champs s'appliquent au
en raison de l'analyse des req
d'analyse des programmes ma
<table><tr><td>Verdict DVS sortant unifié</td><td>« %X3</td></tr><tr><td>Nom de la menace sortante</td><td>« %X4</td></tr></table></td></tr>
<tr><td>Protection avancée contre les malwares</td><td>-,"-",-,-,"-","-",</td><td></td><td>Ces 6 champs sont liés à Secu
Advanced Malware Protection
<table><tr><td>Verdict de fichier</td><td>%X#</td></tr></table></td></tr>
</table>

			Nom de la menace	%X#
			Score de réputation	%X#
			Télécharger l'action pour analyse	%X#
			Nom de fichier	%X#
			Fichier SHA	%X#

Analyse des archives	-,-,"-",		Ces 3 champs indiquent l'état			
			Verdict d'analyse des archives	%X#8#	Verdict d'ana	
					ARCHIVES	
					ARCHIVES	
					ARCHIVES	

					ARCHIVES
					ARCHIVES
					ARCHIVES

			Détail du verdict d'analyse des archives	%Xo	Détail du ver fichier d'arch (ARCHIVES de la stratég Paramètres verdict inclu fichier bloqu «Unscanabl que l'archive bloqué.
			Verdict de fichier	%Xm	Verdict de fi
Effleurez Web	-,	%XU	Comportement des effleureme		
Catégorie URL YouTube	->	%X#29#	Catégorie d'URL YouTube attr champ affiche nc lorsqu'aucun		

Code de réponse HTTP

Voici la liste complète des codes de réponse HTTP

Code de statut	Signification
Informations 1xx	
100	Continuer
101	Protocoles de commutation
102	Traitement

103	Indices préliminaires
2xx a réussi	
200	OK
201	Créé
202	Accepté
203	Informations ne faisant pas autorité
204	Aucun contenu
205	Réinitialiser le contenu
206	Contenu partiel
207	Multi-état
208	Déjà signalé
226	IM utilisé
Redirection 3xx	
300	Choix multiples
301	Déplacé définitivement
302	Trouvé (Précédemment "Déplacé Temporairement")
303	Voir Autre
304	Non modifié
305	Utiliser le proxy
306	Proxy de commutateur
307	Redirection temporaire pour authentification (Généralement visible dans le déploiement transparent pendant que SWA authentifie l'utilisateur)
308	Redirection permanente
Erreur client 4xx	
400	Requête incorrecte

401	Authentification du serveur Web requise (généralement visible dans le déploiement transparent pendant que SWA authentifie l'utilisateur)
402	Paiement requis
403	Interdit
404	Non trouvé
405	Méthode non autorisée
406	Non acceptable
407	Authentification par proxy explicite requise
408	Délai de demande
409	Conflit
410	Disparu
411	Longueur requise
412	Échec de la précondition
413	Charge Utile Trop Importante
414	URI trop long
415	Type de support non pris en charge
416	Intervalle non satisfaisant
417	Echec de la prévision
418	Je suis une théière
421	Requête mal redirigée
422	Entité Imtraitable
423	Verrouillé
424	Dépendance défaillante
425	Trop Tôt
426	Mise à niveau requise
428	Précondition requise
429	Trop de demandes
431	Champs d'en-tête de demande trop volumineux
451	Non Disponible Pour Des Raisons Juridiques
Erreur de serveur 5xx	

500	Erreur interne du serveur
501	Non implémenté
502	Passerelle incorrecte
503	Service non disponible
504	Délai de passerelle
505	Version HTTP non prise en charge
506	La variante négocie également
507	Stockage insuffisant
508	Boucle détectée
510	Non étendu
511	Authentification réseau requise

Étiquette de décision ACL

Voici la liste complète des balises de décision ACL :

Étiquette de décision ACL	Description
PAGE_ERREUR_ADMIN_AUTORISATION	Le proxy Web a autorisé la transaction à accéder à une page de notification et à tout logo utilisé sur cette page.
AUTORISER_CATÉGORIE_PERSONNALISÉE	Le proxy Web a autorisé la transaction en fonction des paramètres de filtrage de catégorie d'URL personnalisés pour le groupe de stratégie d'accès.
RÉFÉRENTIEL_AUTORISÉ	Le proxy Web a autorisé la transaction sur la base d'une exemption de contenu intégré/référencé.
AUTORISER_WBRS	Le proxy Web a autorisé la transaction en fonction des paramètres de filtre de réputation Web pour le groupe de stratégie d'accès.
VERDICT_FICHIER_AMP	Valeur représentant un verdict du

	serveur de réputation AMP pour le fichier :
	1 - Inconnu
	2 - Nettoyer
	3 - Malveillant
	4 - Non analysable
ARCHIVESCAN_ALLCLEAR	Verdict d'analyse des archives
ARCHIVESCAN_BLOCKEDFILETYPE	ARCHIVESCAN_ALLCLEAR - L'archive inspectée ne contient aucun type de fichier bloqué.
ARCHIVESCAN_NESTEDTOODEEP	ARCHIVESCAN_BLOCKEDFILETYPE - L'archive inspectée contient un type de fichier bloqué. Le champ suivant de l'entrée de journal (Verdict Detail) fournit des détails, en particulier le type de fichier bloqué et le nom du fichier bloqué.
ARCHIVESCAN_UNKNOWNFMT	ARCHIVESCAN_NESTEDTOODEEP - L'archive est bloquée car elle contient plus d'archives « encapsulées » ou imbriquées que le maximum configuré. Le champ Verdict Detail contient « Unscanable Archive-Blocked ».
ARCHIVESCAN_UNSCANABLE	ARCHIVESCAN_UNKNOWNFMT - L'archive est bloquée car elle contient un type de fichier de format inconnu. Le détail du verdict est « Non-Scannable Archive-Blocked ».
ARCHIVESCAN_FILETOOBIG	ARCHIVESCAN_UNSCANABLE -

	L'archive est bloquée car elle contient un fichier qui ne peut pas être analysé. Le détail du verdict est « Non-Scannable Archive-Blocked ».
	ARCHIVESCAN_FILETOOBIG - L'archive est bloquée car sa taille est supérieure au maximum configuré. Le détail du verdict est « NonScannable Archive-Blocked ».
	Détail du verdict d'analyse des archives.
	Le champ et le champ Verdict de l'entrée de journal fournissent des informations supplémentaires sur le verdict, telles que le type de fichier bloqué et le nom du fichier bloqué, « Archive non analysable-bloquée » ou « - » pour indiquer que l'archive ne contient aucun type de fichier bloqué.
	Par exemple, si un fichier d'archive inspectable est bloqué (ARCHIVESCAN_BLOCKEDFILETYPE) en fonction de la stratégie d'accès : Objets personnalisés Paramètres de blocage, l'entrée Détails du verdict inclut le type de fichier bloqué et le nom du fichier bloqué.
	Reportez-vous à Politiques d'accès : Blocage d'objets et paramètres de contrôle d'archivage pour plus d'informations sur le contrôle d'archivage.
ADMIN_BLOC	Transaction bloquée en fonction de certains paramètres par défaut du groupe de stratégie d'accès.

BLOCK_ADMIN_CONNECT	Transaction bloquée en fonction du port TCP de la destination, comme défini dans le paramètre HTTP CONNECT Ports pour le groupe de stratégie d'accès.
BLOCK_ADMIN_CUSTOM_USER_AGENT	Transaction bloquée en fonction de l'agent utilisateur tel que défini dans le paramètre Bloquer les agents utilisateur personnalisés pour le groupe Stratégie d'accès.
TUNNELING_ADMIN_BLOC	Le proxy Web a bloqué la transaction en fonction de la transmission tunnel du trafic non HTTP sur les ports HTTP pour le groupe de stratégie d'accès.
BLOCK_ADMIN_HTTPS_NonLocalDestination	Transaction bloquée ; Le client a tenté de contourner l'authentification en utilisant le port SSL comme proxy explicite. Pour éviter cela, si une connexion SSL est établie avec le SWA lui-même, seules les requêtes au nom d'hôte de redirection SWA réel sont autorisées.
ID_ADMIN_BLOC	Transaction bloquée en fonction du type MIME du contenu du corps de la demande tel que défini dans le groupe Stratégie de sécurité des données.
TYPE_FICHIER_ADMIN_BLOC	Transaction bloquée en fonction du type de fichier défini dans le groupe Stratégie d'accès.
PROTOCOLE_ADMIN_BLOC	Transaction bloquée en fonction du protocole défini dans le paramètre Protocoles de blocage pour le groupe Stratégie d'accès.
TAILLE_ADMIN_BLOC	Transaction bloquée en fonction de la

	taille de la réponse, telle que définie dans les paramètres Taille de l'objet pour le groupe Stratégie d'accès.
ID_TAILLE_ADMINISTRATEUR_BLOC	Transaction bloquée en fonction de la taille du contenu du corps de la demande, comme défini dans le groupe Stratégie de sécurité des données.
RESP_AMP_BLOC	Le proxy Web a bloqué la réponse en fonction des paramètres de protection avancée contre les programmes malveillants pour le groupe Stratégie d'accès.
REQUÊTE_AMW_BLOC	Le proxy Web a bloqué la demande en fonction des paramètres de protection contre les programmes malveillants pour le groupe Stratégie d'analyse des programmes malveillants sortants. Le corps de la requête a produit un verdict positif de Malware.
RESP_AMW_BLOC	Le proxy Web a bloqué la réponse en fonction des paramètres de protection contre les programmes malveillants du groupe Stratégie d'accès.
BLOCK_AMW_REQ_URL	Le proxy Web suspecte que l'URL de la demande HTTP ne peut pas être sécurisée. Il a donc bloqué la transaction au moment de la demande en fonction des paramètres de protection contre les programmes malveillants pour le groupe Stratégie d'accès.
AVC_BLOC	Transaction bloquée en fonction des paramètres d'application configurés pour le groupe de stratégie d'accès.

BLOCK_CONTENT_UNSAFE	Transaction bloquée en fonction des paramètres d'évaluation du contenu du site pour le groupe Stratégie d'accès. La demande du client portait sur du contenu pour adultes et la stratégie est configurée pour bloquer le contenu pour adultes.
BLOCK_CONTINUE_CONTENT_UNSAFE	La transaction a été bloquée et a affiché la page Avertir et continuer en fonction des paramètres de classification du contenu du site dans le groupe Stratégie d'accès. La demande du client portait sur du contenu pour adultes et la stratégie est configurée pour avertir les utilisateurs qui accèdent à du contenu pour adultes.
BLOCK_CONTINUE_CUSTOMCAT	La transaction a été bloquée et a affiché la page Avertir et continuer en fonction d'une catégorie d'URL personnalisée dans le groupe de stratégies d'accès configuré sur Avertir.
BLOCK_CONTINUE_WEBCAT	La transaction a été bloquée et a affiché la page Avertir et continuer en fonction d'une catégorie d'URL prédéfinie dans le groupe de stratégies d'accès configuré sur Avertir.
BLOC_PERSONNALISER	Transaction bloquée en fonction des paramètres de filtrage de catégorie d'URL personnalisés pour le groupe de stratégie d'accès.
BLOC_ICAP	Le proxy Web a bloqué la demande en fonction du verdict du système DLP externe tel que défini dans le groupe de stratégies DLP externe.
BLOCK_SEARCH_UNSAFE	La requête du client inclut une requête de recherche non sécurisée et la

	stratégie d'accès est configurée pour appliquer des recherches sécurisées, de sorte que la requête du client d'origine a été bloquée.
AGENT_UTILISATEUR_SUSPECT_BLOC	Transaction bloquée en fonction du paramètre Agent d'utilisateur suspect pour le groupe de stratégies d'accès.
BLOCK_UNSUPPORTED_SEARCH_APP	Transaction bloquée en fonction des paramètres de recherche sécurisée du groupe de stratégie d'accès. La transaction concernait un moteur de recherche non pris en charge et la stratégie est configurée pour bloquer les moteurs de recherche non pris en charge.
BLOC_WBRS	Transaction bloquée en fonction des paramètres de filtre de réputation Web du groupe de stratégies d'accès.
BLOCK_WBRS_IDS	Le proxy Web a bloqué la demande de téléchargement en fonction des paramètres de filtre de réputation Web du groupe Stratégie de sécurité des données.
BLOCK_WEBCAT	Transaction bloquée en fonction des paramètres de filtrage de catégorie d'URL pour le groupe de stratégie d'accès.
BLOCK_WEBCAT_IDS	Le proxy Web a bloqué la demande de téléchargement en fonction des paramètres de filtrage de catégorie d'URL pour le groupe Stratégie de sécurité des données.
BLOC_YTCAT	Le proxy Web a bloqué la transaction en fonction des paramètres de filtrage

	de catégorie YouTube prédéfinis pour le groupe Stratégie d'accès.
BLOCK_CONTINUE_YTCAT	Le proxy Web a bloqué la transaction et affiché la page Avertir et continuer en fonction d'une catégorie YouTube prédéfinie dans le groupe Stratégie d'accès configuré sur Avertir.
ADMIN_DÉCHIFFREMENT	Le proxy Web a décrypté la transaction en fonction de certains paramètres par défaut du groupe Stratégie de décryptage.
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 décrypté la transaction en fonction des paramètres par défaut en tant que connexion d'abandon pour le groupe de stratégies de décryptage lorsque l'EUN est activé.
DECRYPT_EUN_ADMIN_EXPIRED_CERT	Le proxy Web a déchiffré la transaction lorsque les paramètres du proxy HTTPS abandonnent un certificat expiré avec l'activation de l'EUN.
DECRYPT_EUN_ADMIN_INVALID_LEAF_CERT	Le proxy Web a déchiffré la transaction lorsque les paramètres du proxy HTTPS abandonnent un certificat leaf non valide avec l'activation de l'EUN.
DECRYPT_EUN_ADMIN_MISMATCHED_HOSTNAME	Le proxy Web a décrypté la transaction lorsque les paramètres du proxy HTTPS supprimaient le nom d'hôte incompatible avec l'EUN activé.
DECRYPT_EUN_ADMIN_OCSP_OTHER_ERROR	Le proxy Web a déchiffré la transaction lorsque les paramètres du proxy HTTPS

	abandonnent un protocole OCSP (Online Certificate Status Protocol) avec d'autres erreurs avec l'activation de l'EUN.
DECRYPT_EUN_ADMIN_OCSP_REVOKED_CERT	Le proxy Web a déchiffré la transaction lorsque les paramètres du proxy HTTPS abandonnent un certificat OCSP révoqué avec l'activation de l'EUN.
DECRYPT_EUN_ADMIN_UNRECOGNIZED_ROOT_CERT	Le proxy Web a déchiffré la transaction lorsque les paramètres du proxy HTTPS abandonnent une autorité racine ou un certificat émetteur non reconnu avec l'activation de l'EUN.
DECRYPT_EUN_CUSTOMCAT	Le proxy Web a déchiffré la transaction en fonction des paramètres de filtrage de catégorie d'URL personnalisés pour le groupe de stratégies de déchiffrement. Si EUN est activé, le trafic est abandonné.
DECRYPT_EUN_WBRS	Le proxy Web a déchiffré la transaction en fonction des paramètres de filtre de réputation Web du groupe de stratégies 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 l'URL sans score dans le groupe de stratégies 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 catégorie d'URL pour le groupe de stratégies de déchiffrement. Si EUN est activé, le trafic est abandonné.

DÉCHIFFRER_CHAT_WEB	Le proxy Web a déchiffré la transaction en fonction des paramètres de filtrage de catégorie d'URL pour le groupe de stratégie de déchiffrement.
DÉCHIFFRER_WBRS	Le proxy Web a déchiffré la transaction en fonction des paramètres de filtre de réputation Web du groupe Stratégie de déchiffrement.
CAS_PAR_DÉFAUT	Le proxy Web a autorisé le client à accéder au serveur car aucun des services AsyncOS, tels que la réputation Web ou l'analyse anti-programme malveillant, n'a effectué d'action 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 le déchiffrement pour l'authentification est désactivé dans les paramètres de proxy HTTPS.
DROP_ADMIN	Le proxy Web a abandonné la transaction en fonction de certains paramètres par défaut du groupe Stratégie de décodage.
CERT_EXPIRATION_ADMIN_DROP	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 catégorie d'URL pour le groupe Stratégie de décodage.
DROP_WBRS	Le proxy Web a abandonné la transaction en fonction des paramètres de filtre de réputation Web pour le

	groupe de stratégie de décodage.
CERTIFICAT_EXPIRATION_ADMINISTRATEUR_MONITEUR	Le proxy Web a surveillé la réponse du serveur car le certificat du serveur a expiré.
MONITOR_AMP_RESP	Le proxy Web a surveillé la réponse du serveur en fonction des paramètres Advanced Malware Protection pour le groupe Access Policy.
MONITOR_AMW_RESP	Le proxy Web a surveillé la réponse du serveur en fonction des paramètres de protection contre les programmes malveillants pour le groupe de stratégies d'accès.
MONITOR_AMW_RESP_URL	Le proxy Web suspecte que l'URL de la requête HTTP ne peut pas être sécurisée, mais il a surveillé la transaction en fonction des paramètres de protection contre les programmes malveillants pour le groupe Stratégie d'accès.
AVC_SURVEILLANCE	Le proxy Web a surveillé la transaction en fonction des paramètres d'application du groupe de stratégie d'accès.
MONITOR_CONTINUE_CONTENT_UNSAFE	À l'origine, le proxy Web a bloqué la transaction et affiché la page Avertir et continuer en fonction des paramètres de classification du contenu du site dans le groupe Stratégie d'accès. La demande du client portait sur du contenu pour adultes et la stratégie est configurée pour avertir les utilisateurs qui accèdent à du contenu pour adultes. L'utilisateur a accepté l'avertissement et a continué sur le site initialement demandé, et aucun autre moteur

	d'analyse n'a par la suite bloqué la demande.
MONITOR_CONTINUE_CUSTOMCAT	À l'origine, le proxy Web bloquait la transaction et affichait la page Avertir et continuer en fonction d'une catégorie d'URL personnalisée dans le groupe Stratégie d'accès configurée sur Avertir. L'utilisateur a accepté l'avertissement et a continué sur le site initialement demandé, et aucun autre moteur d'analyse n'a par la suite bloqué la demande.
MONITOR_CONTINUE_WEBCAT	À l'origine, le proxy Web a bloqué la transaction et affiché la page Avertir et continuer en fonction d'une catégorie d'URL prédéfinie dans le groupe Stratégie d'accès configuré pour Avertir.L'utilisateur a accepté l'avertissement et a continué sur le site demandé à l'origine, et aucun autre moteur d'analyse n'a bloqué la demande par la suite.
MONITOR_CONTINUE_YTCAT	À l'origine, le proxy Web a bloqué la transaction et affiché la page Avertir et continuer en fonction d'une catégorie YouTube prédéfinie dans le groupe Stratégie d'accès configuré sur Avertir. L'utilisateur a accepté l'avertissement et a continué sur le site initialement demandé, et aucun autre moteur d'analyse n'a par la suite bloqué la demande.
ID_MONITEUR	Le proxy Web a analysé la demande de téléchargement à l'aide d'une stratégie de sécurité des données ou d'une stratégie DLP externe, mais n'a pas bloqué la demande. Il a évalué la demande par rapport aux stratégies d'accès.

AGENT_UTILISATEUR_SUSPECT_MONITOR	Le proxy Web a surveillé la transaction en fonction du paramètre Agent d'utilisateur suspect pour le groupe de stratégies d'accès.
MONITOR_WBRS	Le proxy Web a surveillé la transaction en fonction des paramètres de filtre de réputation Web pour le groupe de stratégies d'accès.
NO_AUTORISATION	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 stratégie d'authentification de l'application.
NO_MOT_DE_PASSE	L'authentification de l'utilisateur a échoué.
ADMIN_PASSTHRU	Le proxy Web a transmis la transaction en fonction de certains paramètres par défaut du groupe Stratégie de décodage.
PASSTHRU_ADMIN_EXPIRED_CERT	Le proxy Web a transité par 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 catégorie d'URL pour le groupe Stratégie de décodage.
PASSTHRU_WBRS	Le proxy Web a transmis la transaction en fonction des paramètres de filtre de réputation Web du groupe Stratégie de décodage.

REDIRECT_CUSTOMCAT	Le proxy Web a redirigé la transaction vers une autre URL en fonction d'une catégorie d'URL personnalisée dans le groupe de stratégies d'accès configuré pour la redirection.
AUTH_SAAS	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 stratégie d'authentification de l'application.
OTHER (AUTRE)	Le proxy Web n'a pas terminé la demande en raison d'une erreur, telle qu'un échec d'autorisation, une déconnexion du serveur ou un abandon du client.

Valeurs de verdict d'analyse de programme malveillant

Un verdict d'analyse de programme malveillant est une valeur attribuée à une requête d'URL ou à une réponse du serveur qui détermine la probabilité qu'il contienne un programme malveillant. Les moteurs d'analyse Webroot, McAfee et Sophos renvoient le verdict d'analyse des programmes malveillants au moteur DVS afin qu'il puisse déterminer s'il faut surveiller ou bloquer l'objet analysé. Chaque verdict d'analyse de programme malveillant correspond à une catégorie de programme malveillant répertoriée sur la page Access Policies > Reputation and Anti-Malware Settings lorsque vous modifiez les paramètres Anti-Malware pour une stratégie d'accès particulière.

Cette liste présente les différentes valeurs de verdict d'analyse des programmes malveillants et chaque catégorie de programme malveillant correspondante :

Valeur du verdict d'analyse des programmes malveillants	Catégorie de programme malveillant
-	Non défini
0	Inconnu

Valeur du verdict d'analyse des programmes malveillants	Catégorie de programme malveillant
1	Non analysé
2	Timeout (Délai d’expiration)
3	Erreur
4	Inanalysable
10	Logiciel espion générique
12	Browser Helper, objet
13	Logiciel publicitaire
14	Moniteur système
18	Moniteur système commercial
19	Numéroteur
20	Pirate
21	URL d'hameçonnage
22	Trojan Downloader
23	Cheval de Troie
24	Phisher Troyen
25	Ver

Valeur du verdict d'analyse des programmes malveillants	Catégorie de programme malveillant
26	Fichier chiffré
27	Virus
33	Autres programmes malveillants
34	PUA
35	Interrompu
36	Heuristique des attaques
37	Fichiers malveillants et à haut risque connus

Autres informations utiles

- Guide de l'utilisateur d'AsyncOS 15.2 pour Cisco Secure Web Appliance
- Utilisation des meilleures pratiques de sécurisation des appliances Web
- Garantir le bon fonctionnement du groupe WSA HA virtuel dans un environnement VMware
- Configurer le paramètre de performance dans les journaux d'accès
- Comprendre le format de journal d'accès HTTPS dans l'appliance Web sécurisée
- Accéder aux journaux de l'appliance Web sécurisée

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.