

SOLUTION OLFEO V6.4

Notes de release



INFORMATIONS LÉGALES

Copyright

© Copyright 2019 Olfeo. Tous droits réservés. Cette documentation ne peut être utilisée que dans le cadre d'un contrat de licence logiciel avec la société Olfeo.

Aucune partie de cette publication ne doit être reproduite, transmise, transcrite, conservée dans un système d'archivage ou convertie en un quelconque langage machine, sous quelque forme ou quelque moyen que ce soit sans autorisation écrite antérieure d'Olfeo. Olfeo vous accorde des droits limités vous autorisant à imprimer ou à effectuer d'autres reproductions de toute documentation informatique pour votre propre utilisation, dans la mesure où ces reproductions comportent la mention de copyright d'Olfeo. Nul autre droit sous copyright n'est accordé sans autorisation écrite antérieure d'Olfeo.

Les sujets traités dans cette documentation sont sujets au changement sans avertissement préalable.

Marques déposées

Olfeo est une marque déposée internationalement par la société Olfeo.

Ce document contient des noms, des logos, des composants logiciels ou matériels qui sont la propriété d'éditeurs ou de fabricants tiers :

- JavaScript et son logo sont des marques déposées de Oracle Corporation.
- SSH est une marque déposée de Communications Security Corp CORPORATION FINLAND.
- Linux est une marque déposée de Linus Torvalds.
- Windows Media Player, Microsoft, Windows, Active Directory, Hyper-V, Internet Explorer et leurs logos respectifs sont des marques déposées de Microsoft Corporation.
- Check Point, FireWall-1, SmartDashboard, SmartCenter, OPSEC et leurs logos respectifs sont des marques déposées ou des marques commerciales de Check Point Software Technologies Limited.
- eDirectory est une marque commerciale de Novell, Inc.
- OpenLDAP est une marque commerciale de OpenLDAP Foundation.
- ClamAV est une marque déposée de Sourcefire, Inc.
- Websense est une marque déposée de Websense, Inc.
- WISP est le protocole développé par la société Websense, Inc.
- Cisco, Pix, ASA sont des marques commerciales ou des marques déposées de Cisco Technology, Inc.
- Firefox est une marque déposée de la Fondation Mozilla.
- HTML, XML, XHTML et W3C sont des marques commerciales ou des marques déposées de W3C, World Wide Web Consortium, Massachusetts Institute of Technology.
- Squid est le logiciel proxy distribué selon les termes de la licence GPL (GNU General Public License).
- ICAP est le protocole documenté dans la RFC 3507.

Tous les autres noms de marque mentionnés dans ce manuel ou dans toute autre documentation fournie avec les produits Olfeo sont des marques commerciales ou des marques déposées de leurs propriétaires respectifs.

CONTACTS

Siège social

Olfeo
4 rue de Ventadour
75001 Paris
France

Services

Support technique	+33 (0)1 78 09 68 01 support@olfeo.com	<p>Le support technique d'Olfeo est dédié :</p> <ul style="list-style-type: none">Aux clients ayant souscrit le support direct éditeur. <p>Pour voir si vous bénéficiez actuellement du support direct, rendez-vous à la page Paramétrage > Mise à jour > Abonnement, section Support direct Olfeo.</p> <ul style="list-style-type: none">Aux ingénieurs techniques de nos partenaires ayant suivi la certification technique Olfeo et ayant souscrit à l'assistance partenaire Olfeo.
Service relation client	+33 (0)1 78 09 68 07 client@olfeo.com	
Service classification d'URL	classification@olfeo.com	Demandes de reclassement d'URL .
Service documentation	documentation@olfeo.com	Envoyer des commentaires ou des demandes de correction concernant la documentation technique Olfeo.
Service conseil et formation	consulting@olfeo.com formation@olfeo.com	Envoyer des commentaires ou des demandes concernant le service conseil et formation Olfeo.

SOMMAIRE

Historique de la version 6.....	5
6.4 Versions correctives.....	6
6.4.....	7
6.4 Nouvelles fonctionnalités.....	7
6.3 Versions correctives.....	8
6.3.....	10
6.3 Correctifs.....	10
6.3 Nouvelles fonctionnalités.....	12
6.3 Note importante.....	13
6.2.0.....	14
6.2.0 Correctifs.....	14
6.2.0 Nouvelles fonctionnalités.....	15
6.2.0 Problèmes connus.....	18
6.2.0 Note importante.....	18
6.0.8.....	19
6.0.8 Correctifs.....	19
6.0.7.....	21
6.0.7 Correctifs.....	21
6.0.7 Problèmes connus.....	23

HISTORIQUE DE LA VERSION 6

Version	Date de sortie
6.4	14/03/2019
6.3.3 à 6.3.11	Versions correctives
6.3	08/10/2018
6.2.1	13/07/2018
6.2.0	02/05/2018
6.1.1	22/01/2018
6.1.0	30/11/2017
6.0.8	03/07/2017
6.0.7	16/05/2017
6.0.6	10/02/2017
6.0.3 à 6.0.5	Versions non publiées
6.0.2	14/10/2016
6.0.1	Version non publiée
6.0.0	30/09/2016

6.4 VERSIONS CORRECTIVES

6.4.4

Ajout fonctionnel

- OL-233 [Authentification] Montée de version des services d'authentification (winbind et samba)
- OL-235 [G-Suite] L'authentification d'utilisateur se fait grâce à un plugin
- OL-166 [Antivirus] Montée de version et meilleure gestion de clamav / freshclam
- OL-228 Ajout de l'id du domaine dans les remontées

Correctif

- OL-290 [SSL] Problème déchiffrement SSL
- OL-249 [Portail opérateur] Erreur "... : not found TICKET"
- OL-16 [Portail opérateur] Créer / Renouveler un ticket pour un utilisateur existant
- OL-124 [Diffusion] Erreur "StatsFetcherError 400: Bad data received, not an analysis"
- OL-20 [Coaching] Le champ "Adresse mail de test" est limité à 50 caractères
- OL-21 [Coaching] La description des analyses ne s'affiche pas
- OL-232 [Filtering] Vérification syntax regex moteur de règle
- OL-307 [MAJ] Impossible de faire une mise à jour de 6.1 à 6.4

6.4

6.4 Nouvelles fonctionnalités

Proxy

#8086 Désactivation du cache Kerberos

- Possibilité de désactiver le cache pour Kerberos grâce à une clef de configuration
- Désactivé par défaut.

#8052 Gestion des erreurs de révocation de certificat SSL

- Les certificats utilisant les protocoles CRL et OCSP peuvent être reconnus comme étant révoqué
- Désactivé par défaut

#7845 Montée de version du proxy (Squid 4.4)

- Les méthodes SSL v2 et v3 ne sont plus utilisées, seul le TLS est utilisé pour le déchiffrement.
- Modification du protocole de communication des binaires d'aide de Squid.
- On ne parle plus de «Client d'abord / serveur d'abord» pour les actions des règles de déchiffrement, mais plus simplement de «Déchiffrer» ou «Pas déchiffrer».

Sécurité

#8110 Désactivation de SMB v1

Suite aux différentes vulnérabilités du protocole SMB v1, ce protocole n'est plus disponible sur l'Olfeo.

Nomadisme

7815 Fonctionnalité Nomadisme

- Permet aux clients de filtrer leurs utilisateurs nomades (utilisateurs non présents dans les locaux de l'entreprise).
- Un agent est disponible au téléchargement depuis l'Olfeo. Il devra être installé sur le poste de l'utilisateur nomade.

6.3 VERSIONS CORRECTIVES

6.3.11

- OL-50 Liste URL supprimée dans une politique encore existante
- OL-174 Check d'intégrité de la confbase pour les whitelist
- OL-176 Double free or corruption (filtering)
- OL-210 Webauth sur identifiant ip2login
- OL-214 Mauvaise écriture redis-ip2login.conf (crash filtering)
- OL-12 Menu Liste des diffusions vide

6.3.10

- OL-7 Erreur journalière can't connect to clamd server
- OL-155 Comportement des licences
- OL-139 Liens mort dans la webadmin
- OL-41 cliadmin reset ne fonctionne plus
- OL-11 Filtres d'analyses invisibles
- OL-92 redirection de la webadmin vers le port 7081
- OL-124 Erreur "StatsFetcherError 400: Bad data received, not an analysis" dans le mail de diffusion

6.3.9

- OL-148 hits aggregate prend trop de temps à créer ses lots d'agrégation

6.3.8

- OL-56 Bascule intempestive du maître de secours
- OL-121 Perte de l'accès internet lorsque le maître est arrêté
- OL-144 Userbase affiche l'erreur "...Detail: KEY (user_id,netchart_id)=(15799, 145) already exists"
- OL-145 Mise à jour vers 6.3.7.0: "Error : /opt/olfeo/bin/keepalived not found or not executable"
- OL-66 Perte de stats lorsque le maître de secours devient maître
- OL-38 Arrêt de la base redis ip2login
- OL-179 Filtering segfault

6.3.7

- #7488 hostname avec caractère/symbole interdit

6.3.6

- #7544 [Portail public] Recherche d'un utilisateur dans le portail public
- #8068 [Filtrage DNS] Activation des modes restreint sur Youtube et Qwant

6.3.5

- #8066 Cohabitation des services Nginx et WPAD
- #8085 Erreur de synchronisation d'annuaire LDAP avec des groupes conteneurs
- #7988 Erreurs d'orthographe sur le coaching
- #7692 Sysconfig bloqué sur changement de configuration
- #8087 Erreurs d'orthographe dans les descriptions d'analyse sur le coaching
- #8095 Installation du master de secours KO sur les OVA

6.3.4

- #8035 Problème lors de l'ajout d'un esclave
 - Désormais une adresse IP valide est nécessaire à la création d'un esclave
 - Si la jonction au domaine (coté esclave) est faite en renseignant un mauvais ID de maître, la jonction ne se fait pas, et l'esclave est toujours utilisable
- #8054 Mettre une limite de fichier utilisé à PowerDNS
- #7674 [Proxy avancé] Icône d'aide non visible
- #8062 Migration des analyses 6.1 en 6.3
- #7813 Restauration d'une sauvegarde d'un maître
- #8030 Robustification de l'installation d'un maître de secours
- #7919 Erreur de synchronisation de fichier lors de l'installation d'un maître de secours
- #7924 Problème lors de la désinstallation de maître de secours
- #7987 Problème avec les statistiques suite à l'installation d'un maître de secours

6.3.3

- #8042 Augmenter le nombre de connexions icap acceptées par le module de filtrage

6.3

6.3 Correctifs

Portail Public

#7499 "Ticket not found"

Une icône grise apparaissait lorsqu'aucun ticket n'était trouvé.

Migration

#7695 Utilisateurs supprimés suite à la mise à jour en 6.2

Les utilisateurs en erreur n'étaient plus synchronisés.

Statistiques

#7575 Hits importer s'arrête sur un champ invalide

Quand un champ utf-8 de url_importer contenait le caractère 0, cela bloquait l'outil lorsqu'il était lancé avec le logd.

Authentification

#7250 Gestion des certificats révoqués

Bloquer les erreurs SSL via une v6 avec le déchiffrement activé laissait quand même accès aux pages au lieu de les bloquer.

#7430 Userbase affiche l'erreur "...DETAIL: Key (id)=(30) already exists"

L'erreur apparaissait lors de la synchronisation des utilisateurs.

#6210 Impossible de retirer une plage horaire sur une règle

Il n'était pas possible de retirer une plage horaire sur une règle.

Domaine Olfeo

#7702 Userbase

Le service userbase s'arrêtait pour une raison inconnue.

Sauvegarde

#6571 Syntaxe ligne crontab pour sauvegarde FTP/ sauvegarde conf

Lors d'une sauvegarde programmée via FTP, le password défini n'était pas lu correctement.

Divers

#7804 [DNS] Ajout du protocole dans le moteur d'ACL

Ajout du champ protocole dans le moteur d'ACL de la section DNS.

#7807 [ALPHA] Format des URLs pour le filtrage DNS

Optimisation des formats d'URLs pour le filtrage DNS.

#7882 [Mise à jour] Redis-ip2login ne démarre pas après MàJ 6.3 -> 6.3

Correction du problème dans lequel redis-ip2login ne démarrait pas après la mise à jour de la version 6.3.0 vers 6.3.X.

#7901 [Portail Public] Login avec espace ne fonctionne pas dans le portail captif

Correction du problème de la section portail captif qui apparaissait lors de la présence du caractère espace dans le champ login.

#7929 [DNS] La licence DNS nécessite le filtrage d'URL pour fonctionner

Correction du problème dans lequel la licence filtrage d'URL était nécessaire pour utiliser la fonctionnalité de filtrage DNS.

#7960 [DNS] Plus de résolution de nom lors de l'absence de licence DNS

Correction du problème pour lequel il n'y avait plus de résolution de nom lors de l'absence de licence DNS.

#7809 [Statistiques] "elasticsearch is not running ... failed!" au démarrage

Correction du problème "elasticsearch is not running ... failed!" au démarrage du serveur.

#7977 [DNS] Libellé bloquer/autoriser

Changement du label de la liste déroulante "Si le service de filtrage n'est pas disponible" de la section DNS avec les nouvelles valeurs "Bloquer" et "Autoriser".

#7555 [Statistiques] Affichage des analyses et boutons radios

Correction de l'affichage pour le chargement d'une analyse.

#7833 [Migration] Problème import RAW lors d'une migration v5-->v6.3.05 Alpha

Correction du problème "Import RAW" qui apparaissait lors d'une migration de version 5 vers version 6.3.0.5 Alpha.

#7837 [Webadmin] Mise à jour olfeo non possible si "olfeo-dbg" est présent

Correction du problème qui empêchait la mise à jour du logiciel Olfeo si le paquet olfeo-dbg était installé.

#7839 [Active Directory] Hostname, jonction domaine

Correction de l'écriture du fichier /etc/hosts pour faire la jonction au domaine Active Directory.

6.3 Nouvelles fonctionnalités

Le Filtrage DNS

7375 Nouveau mode d'intégration

- Gestion de la configuration depuis l'interface d'administration Web
- Amélioration des performances de filtrage

Authentification G SUITE

7324 Prise en charge du mode d'Authentification Google G Suite

- Gestion de la configuration depuis l'interface d'administration Web
- Prise en charge dans le moteur de règles

Domaine

7120 Optimisation du chargement des listes d'utilisateurs contenant de nombreux objet

Elastic search

7433 Gestion des filtres dans l'interface des statistiques

Mise en place d'un moteur de recherche dans les thèmes et catégories.

Coaching

7598 Liste d'analyses de coaching par défaut

Les analyses par défaut contiennent : un type de graphe, un nom, une description et des séries pré-établies. L'utilisateur est libre de choisir la cible (utilisateur et/ou UO) et la mesure (hits ou bande passante).

7572 Avoir la liste des coaching

Possibilité d'avoir plusieurs coaching.

7737 Permettre de choisir la cible d'une analyse de coaching

Possibilité de choisir la cible : Utilisateur, UO ou Utilisateur vs UO.

7621 Sélection des destinataires

Possibilité de choisir les destinataires par UO, Groupe ou individuellement et d'en exclure.

Diagnostic

7329 Script de diagnostic

Un script de diagnostic est maintenant mis à disposition des administrateurs et exploitants de la solution. Ce script est disponible dans l'environnement Olfeo, une fois connecté en console, sous le nom `olfeo_diag`. Nous vous invitons à l'invoquer et à vous familiariser avec celui-ci.

6.3 Note importante

Dimensionnement des machines

Le moteur de statistiques repose désormais sur Elastic Search, apportant un gain de performances significatif. Il est recommandé d'optimiser le dimensionnement des machines, comme indiqué dans le tableau ci-dessous, mettant en avant le dimensionnement des appliances physiques Olfeo.

Caractéristiques matérielles	Critères	Olfeo BOX 8000 *	Olfeo BOX 12 000	Olfeo BOX 20 000
Stockage	Disques durs	1	2	
	RAID	N/A	RAID1	
	Stockage total	500 Go	2 x 1 To	2 x 2 To
Coeurs CPU	-	2	4	
Mémoire vive	-	8 Go	16 Go	32 Go
Interfaces réseau	Bypass	8 x 1000 Mbit/s (2 bypass)		
Alimentation	-	Unique		Redondante

*Dans un domaine Olfeo, il est recommandé d'utiliser ce modèle dans un rôle de machine esclave uniquement

Migration : changement important dans la gestion des statistiques

Suite au passage de PostGre SQL à Elastic Search, la gestion des statistiques a été revue dans le produit Olfeo. L'outil de génération de rapports repose sur cette nouvelle base de données et prendra en compte uniquement les données traitées après migration. Les logs de navigation enregistrés dans la base de données avant la migration restent exploitables via l'outil d'extraction de hits.

6.2.0

6.2.0 Correctifs

Configuration

7582 Service winbind en état "Failed"

Le message "winbind is not running ... failed!" pouvait être retourné au démarrage de certaines box. Il suffit de le démarrer avec la commande "/etc/init.d/winbind start".

7505 Synchronisation LDAP

Une erreur "no group found" était retournée lors de la synchronisation d'un annuaire LDAP avec Olfeo. Alors que l'on peut effectivement lister ces utilisateurs dans le contexte avec un LDAP search.

7057 Crash du service filtering suite à un import de configuration

Ceci était dû au fait que celui-ci lançait des connecteurs utilisant des interfaces qui n'existaient pas sur la machine.

7251 Heure d'été

Prise en compte de façon totalement transparente la notion d'heure d'été.

7309 Crash du service filtering

Crash du service filtering lors de la modification du range d'IP à exclure des associations IP/identifiants.

7311 Impossible de démarrer le service rsync si son pid existe déjà

Le correctif a consisté à mettre à jour le service rsync.

7341 Problème de jonction au domaine Windows

Lorsqu'on accédait à la page de jonction à un domaine Windows, un timeout était parfois affiché. Le timeout a été augmenté sur la Webadmin à 40 secondes, ce qui permet de retourner l'erreur reçue par le sysconfig via la commande "net ads info".

7378 Suppression des alertes RTSP dans la supervision lorsque le service n'est pas activé.

7380 Le port ne change pas lors du basculement de LDAP vers LDAPS

Le port passe dorénavant au 636 comme attendu.

7404 Envoi en double exemplaire des tâches de diffusion

Les tâches de diffusion étaient répliquées du Master vers le Slave, d'où les doublons.

Migration/Mise à jour

7547 Absence de pid pour le service squid3 suite à une migration de l'Olfeo v5 vers l'Olfeo v6

Sans pid il était impossible de redémarrer ou d'arrêter le service squid3, le status indiquait par contre bien le service squid3 "started".

7450 Durant la phase d'import certaines configurations utilisateur du portail public pouvaient rendre l'import impossible

Cette erreur a été corrigée.

7506 Erreur link lors d'un chargement d'interface après une migration d'Olfeo v5 vers Olfeo v6 sur les OlfeoBox

Dans la Webadmin, lors de la configuration d'une interface apparaissait une erreur "link", il était ensuite impossible de modifier cette interface.

Filtage

7263 Erreur quotidienne "can't connect to clamd server"

Dans dans le contexte de plusieurs Olfeo, l'erreur "can't connect to clamd server (/var/run/clamav/clamd.ctl) (/var/run/clamav/clamd.ctl) No such file or directory" était retournée de manière journalière sur le service clamd produit. Le phénomène avait été observé sur plusieurs Olfeo en v6, les horaires variant un peu selon les clients entre 00h00 et 00h40. Il est maintenant possible de redémarrer le service.

6.2.0 Nouvelles fonctionnalités

Statistiques

6053 Naviguer dans les données via le graphique

Avec la fonctionnalité *drill down*, il est désormais possible de "zoomer" en cliquant sur une information du graphique .

6357 Possibilité de supprimer une analyse dans la liste des analyses

Un nouvel onglet dans la WebUI présente une vue de toute les analyses de l'utilisateur. C'est ici qu'il sera possible de supprimer une analyse. Si l'on désire supprimer une analyse appartenant à une diffusion c'est possible, mais alors un message d'avertissement préviendra l'utilisateur. Dans le cas où l'on voudrait supprimer la dernière analyse d'une diffusion, la diffusion serait désactivée et l'utilisateur ne pourrait pas la réactiver tant qu'il n'aurait pas modifié la diffusion pour lui ajouter au moins une analyse. Comme pour les diffusions, la suppression de l'analyse ne se fait qu'après avoir cliqué sur le bouton "Valider".

6616 Extraction des hits

L'extraction était auparavant limitée à 48h, elle est dorénavant illimitée. L'interface d'extraction a été déplacée vers l'interface des statistiques de la WebUI

Attention, il n'est pas possible de créer des taches d'extraction comme auparavant. Cependant les taches créées avant la version 6.2 fonctionneront toujours avec la limitation historique de 48 h.

6771 Export CSV

Un bouton a été ajouté permettant d'exporter les résultats d'une analyse au format CSV. Ce sont les données de la vue en tableau qui apparaissent dans l'analyse au format CSV.

7075 Possibilité de supprimer une analyse directement dans la page de création de diffusion

L'icône "corbeille" située en bout de ligne sur le tableau listant les analyses d'une diffusion autorise la suppression.

7090 L'objet du mail est différencié de l'objet de la diffusion

Il demeure en tant que champ à remplir par l'administrateur.

7121 Navigation dans l'historique

Il est possible de revenir sur une analyse réalisée précédemment en cliquant sur le bouton **Page précédente** du navigateur. Une nouvelle analyse est générée dès que l'on change ou qu'on ajoute une série, des filtres, une date ou des mesures. Lorsque l'on change de type de graphique on ne crée pas de nouvelle analyse, il n'y a donc pas de nouvel élément dans l'historique.

Domaines

7065 Une base de données Redis sert de stockage des informations du domaine

Un démon de gestion du domaine a été intégré : l'ensemble des changements propres à l'usage de chaque membre d'un domaine est effectué par un nouveau service écoutant sur le port 8002, le "DomainManager".

7070 La désignation d'un Master de secours est désormais possible sur la WebUI

Via l'onglet **Haute disponibilité**, on peut choisir un Master de secours, parmi les Slaves en ligne dans la liste. Cette liste est désormais dynamique et le statut en ligne/hors ligne change en temps réel en fonction de l'état des services de chaque machine. Si l'un des services parmi confbase, userbase, filtering et logd sur le Master tombe, alors le Master de secours devient automatiquement Master, les Slaves envoient leurs données sur le nouveau Master et l'ancien Master devient Slave du domaine. Attention, le fait de se rendre dans l'interface haute-disponibilité vous fait changer de port. Vous passez alors sur la suite de port 8443 à 8445.

7074 Le changement de Master est maintenant possible

Ce changement correspond à une désignation d'un Slave en tant que Master de secours, puis à une bascule manuelle depuis le Master ou le Master de secours, via la WebUI.

7139 Sortir un Slave d'un domaine Olfeo

La sortie d'un Slave d'un domaine Olfeo est possible, mais elle doit d'abord être effectuée depuis le Slave avant de pouvoir le supprimer sur le Master.

7198 Maintenance ou de mise à jour du Master

En cas de maintenance ou de mise à jour du Master, un script est fourni pour empêcher la bascule automatique du Master vers le Master de secours : `olfeo-switch-prevent.sh`, et son annulation `olfeo-switch-allow.sh`.

Appliances physiques

7399 Nouveau Partitionnement

Squid n'est plus sur une partition à part entière, il est passé dans la partition Data.

Pour les OlfeoBox 11000 et 15000 la partition de boot est dupliquée sur les deux disques (RAID logiciel), il en est de même pour la partition data.

Impacts sur le produit

Refonte de la page "Olfeo et vous"

Cette page vous permet d'accéder à la documentation et aux ressources, de contacter le service client et support, de rester à jour sur les événements et actualités, mais également de participer au développement du produit Olfeo.

7066 HAProxy a été intégré

- Afin de pouvoir changer dynamiquement de Master les services des Slaves sans les redémarrer, HAProxy a été installé en 6.2 pour rediriger les connexions sur le Master effectif.
- L'ensemble des ports des services Olfeo a changé pour une meilleure cohérence :
 - Les ports de 7000 à 7999 ont été réaffectés pour les services proxifiés.
 - Les ports de 8000 et 8299 ont été réaffectés pour les services normaux.
 - Les services occupant les ports à partir 8300 ne sont pas réaffectés.

7081 La base de données "PostgreSQL" est maintenant scindée en 2 entités :

- la base de stats écoute sur le port 5433, comme en 6X,
- une nouvelle base contenant confbase et userbase écoute sur le port 5432.

7194 Session de quotas réinitialisées

Les sessions des quotas seront toutes réinitialisées à la mise à jour.

7252 La WebUI comporte désormais deux modules

L'un pour l'interface de statistiques, l'autre pour l'interface des domaines.

7368 Les objets par défaut des consultants ont été pris pour modèles permettant de faciliter la mise en place de la solution Olfeo

Politiques : nouveaux critères pour la politique par défaut

Ports en écoute : désactivation de l'option «Utiliser l'en-tête http "Via"»,

Types de requêtes autorisées par port de destination : 1-65535

Authentification

- **Authentification** : Nombre d'instances = 100
- **Cache** : option activée par défaut
- **Options globales SSL** : par défaut l'option est positionnée sur «Suites cryptographiques par défaut» et le champ personnalisé "!NULL:ALL".
- **Règles de déchiffrement** :
 - outrepassement du déchiffrement *activé* pour la catégorie Banques, Assurances, Caisses et Santé,
 - outrepassement du déchiffrement *désactivé* pour la catégorie Webmail,
 - outrepassement du déchiffrement *activé* pour la liste de domaines "Liste des domaines Microsoft Windows Update"
 - création d'une règle d'outrepassement du déchiffrement pour toutes les listes de domaines créées en objets par défaut.

Accès Administrateurs/Utilisateurs

- création d'une règle activée qui autorise pour tous les flux la destination "Liste des domaines Microsoft Windows Update",
- création d'une règle désactivée qui autorise pour les flux HTTP, HTTPS la destination "Liste des domaines des portails captifs",
- création d'une règle désactivée de *réécriture d'URL* permettant d'activer la fonction Safesearch de Google,
- création d'une règle désactivée de type "Charte Internet".

Listes d'URL/Listes de domaines

- Liste des domaines **Microsoft Windows Update**
- Liste des domaines **Cisco WebEX**
- Liste des domaines **MS Office 365**
- Liste des domaines **Citrix produits GoTo**
- Liste des domaines **TeamViewer**
- Liste des domaines **Dropbox**
- Liste des domaines **WeTransfer**
- Liste des domaines **Adobe Creative Cloud Network Endpoints**
- Liste des domaines **Autodesk**
- Liste des domaines des portails captifs

Messages : suppression du champ %118n.**License.LicensedTo%**, affichant la license Olfeo en pied de page.

Support>Support Technique Olfeo : L'adresse tunnel olfeo.com est renseignée dans le champ Adresse IP du support.

Keys>Clés : Pour assurer la compatibilité avec Microsoft Office 365, la clef `squid_dns_v4_only` est passée à "on".

7432 Augmentation du timeout de la page de gestion des domaines

Trop court il pouvait poser problème, il a donc été porté de 30 minutes à 30 jours.

Migration v5-v6

7224 Amélioration des contextes d'import lors d'une migration v5 vers v6

Certains contextes liés à l'import des fichiers logs raws ont été améliorés. Un panel plus large de considération est pris en charge lors de l'import de ces fichiers d'une version v5 vers une version v6.

7302 Difficultés à monter le partage CIFS avant de la phase d'import dans le contexte d'une migration de l'Olfeo v5 vers l'Olfeo v6

Le message suivant apparaissait : "le partage CIFS est mal configuré mount error (13) Permission denied". Ajout de l'option `section` dans la ligne de montage du partage cifs car avec le passage de samba 4 l'option par défaut est désormais du `ntlmssp`.

7328 Perte de jonction au domaine Windows aléatoire sur un domaine Olfeo

Dans le cas où chaque esclave était connecté à un AD différent et faisait du filtrage pour un client particulier, ces esclaves perdaient aléatoirement la jonction à leur domaine respectif. Ce type d'intégration est désormais fonctionnel.

7356 Le client a la possibilité de ne pas importer les logs (RAW5) lors de l'import en v6

Le cas échéant, l'espace disque disponible n'est pas calculé et la phase à chaud n'est pas exécutée.

7371 Phase d'import

Pour certains formats d'adresses mail, l'activation de l'envoi par mail rendait parfois la phase d'import impossible le problème est maintenant corrigé.

7410 Echec de migration

En cas d'échec de la migration, un script d'init lancé au démarrage de l'Olfeo la relance automatiquement et reprend sur erreur, jusqu'à ce qu'elle soit terminée. Il envoie également un mail à l'administrateur en cas de CIFS immontable ou de succès.

6.2.0 Problèmes connus

Olfeo ne prend actuellement pas en compte les cas de slave isolé

En effet dans un contexte où l'Olfeo ne pourrait ni joindre son maître ni un maître de secours, il s'arrêterait. Nous vous recommandons donc de déployer un maître de secours et de bien répartir les machines ayant ce rôle. Certains cas d'erreurs peuvent arriver lors des migrations V5-V6.

Veuillez consulter les articles suivants de notre Base de Connaissances avant de migrer :

- en cas d'erreur réseau : <https://www.olfeo.com/fr/base-de-connaissances/erreur140-migration-v6>.
- le service Customer Success Olfeo vous incite à réfléchir à la question suivante : *dois-je migrer ma configuration ou dois-je partir sur une nouvelle installation ?* L'article suivant peut vous aider lors de cette prise de décision : <https://www.olfeo.com/fr/base-de-connaissances/v6-migration-ou-nouvelle-installation>.

Le navigateur IE 11 trop restrictif

Etant donné son ancienneté, il est techniquement trop restrictif, il n'est donc plus supporté pour l'affichage de l'interface administrateur.

L'Agent SSO

L'Agent SSO pour Windows n'est pas compatible avec la solution Olfeo actuelle. L'identification des utilisateurs par ce biais ne sera donc pas possible. Nous vous conseillons de vous retourner vers des méthodes d'authentification fortes.

6.2.0 Note importante

Installations du logiciel Olfeo en domaine

Pour les installations du logiciel Olfeo en domaine (un maître et un esclave minimum), il est obligatoire de redémarrer tous les esclaves du domaine avant d'appliquer la mise à jour.

6.0.8

Version publiée le 03/07/2017.

6.0.8 Correctifs

Arrêt des services

#6507 Le service logd s'arrête et renvoie l'erreur suivante : "no matching request packet (race condition?)"

Un caractère spécial dans le user-agent d'une requête reçue par le proxy faisait s'arrêter le service logd. L'Olfeo filtrait toujours, mais les hits n'étaient plus loggués jusqu'au redémarrage du service. Après correction, le caractère en question dans le user-agent ne provoque plus d'erreur.

#6824 Blocage du service de filtrage suite à une mauvaise synchronisation des services

Ce problème provoquait une interruption de service. La synchronisation des services a été améliorée et il n'y a plus d'interruption de service.

Domaines Olfeo

#6904 Erreur dans la supervision : Hook 'baseuser_get_user_by_id' not set

Dans un domaine Olfeo, dès qu'on créait une règle de blocage avec outrepassement, des erreurs de type "Hook 'baseuser_get_user_by_id' not set" pouvaient apparaître à la page **Supervision > Journal**. Si les alertes e-mail étaient activées, l'administrateur pouvait recevoir un certain nombre d'emails. Le message a été reclassé en simple warning et ne donne plus lieu à l'envoi d'e-mails.

Synchronisation des utilisateurs

#6192 Message lors de la synchronisation d'un groupe vide

Lorsqu'on synchronisait un groupe vide, on obtenait l'erreur suivante dans la page de l'annuaire : "Sync program returned an error: 1". Le message a été amélioré : celui-ci indique maintenant que le groupe ne contient aucun utilisateur synchronisable.

#6681 Alerte lors d'un ajout d'un nouvel utilisateur

Lorsqu'on restaurait une configuration v6 (depuis la page **Paramétrage > Sauvegarde > Restaurer**), puis qu'on essayait de synchroniser un annuaire, on obtenait une erreur par utilisateur qu'on essayait de synchroniser :

- DBMS Error: ERROR: duplicate key value violates unique constraint "ub_user_pkey"
- Can't add the user 'user' in the userbase: -1

Le problème a été corrigé.

#6791 DBMS Error: ERROR: invalid byte sequence for encoding "UTF8": 0xc3

Ce message d'erreur apparaissait lorsque les données en provenance de l'annuaire étaient tronquées. La taille du champ **ldapdn** a été augmentée pour résoudre ce problème.

#6891 Désynchronisation des groupes d'un annuaire impossible

Lors de la désynchronisation d'un groupe, une erreur apparaissait et il était impossible de désynchroniser celui-ci. Ce problème a été corrigé et il est désormais possible de désynchroniser des groupes.

Mise à jour (v6 vers v6)

#6910 Crash du service logd suite à une mise à jour

Lors de l'import des hits d'une version 6 ancienne à une version 6 plus récente, s'il existait des trous dans les logs, la migration des hits s'arrêtait, ainsi que le service logd. Le cas des trous dans les logs est maintenant géré correctement et n'entraîne plus d'erreurs.

#6908 Redémarrage suite à une mise à jour de la 6.0.6 vers la 6.0.7

La gestion des services clamav et freshclam a été améliorée : il n'est plus nécessaire de redémarrer le système après une mise à jour.

Migration v5/v6

#6856 Suite à une migration v5/v6, certaines règles de cache ne sont plus présentes

Lors d'une migration, certaines règles de cache pouvaient disparaître. Ce problème a été corrigé.

Authentification

#6564 Authentification Kerberos natif non fonctionnelle

L'authentification "Kerberos natif" ne fonctionnait pas : si Kerberos envoyait "identifiant@royaume" à l'Olfeo, l'Olfeo considérait que la chaîne complète "identifiant@royaume" était l'identifiant de l'utilisateur.

Statistiques

#6877 Gestion du drag and drop dans l'interface de statistiques

Il était possible lors de la sélection d'un objet « draggable » de n'envoyer que la sélection et pas l'objet en entier, ce qui entraînait une erreur. La gestion de la fonction drag and drop a été améliorée afin de résoudre ce problème.

SSL

#6876 Déchiffrement SSL non fonctionnel suite à la mise à jour de Chrome en version 58

Depuis la version 58 de Chrome, le déchiffrement SSL ne fonctionnait plus. En effet, le certificat de substitution généré par l'Olfeo ne contenait pas le champ **SubjectAlternativeName** : la nouvelle version de Chrome rejette les certificats ne contenant pas ce champ. Le champ a donc été ajouté au certificat généré par l'Olfeo.

Divers

#6811 Un type MIME incorrect était bloqué (Application/octet-stream au lieu de Archives)

Dans l'onglet **Contenu** du moteur de règles, si une règle bloquait le type mime Archive, le type MIME Application/octet-stream était également bloqué, même si celui-ci n'était pas coché dans la règle de blocage.

#6748 Erreur lors du clonage d'un objet par un sous-administrateur

Lorsqu'un sous-administrateur ne disposant pas du droit **Administration** tentait de cloner un objet dans l'interface d'administration, il obtenait des messages d'erreur.

#6872 Plage des ports locaux inadaptée

Les ports utilisés par les services internes Olfeo pouvaient entrer en conflit avec des ports clients. La plage de ports a donc été adaptée.

6.0.7

Version publiée le 16/05/2017.

6.0.7 Correctifs

Politiques

#6288 - Suppression d'un utilisateur référencé dans une règle du moteur de règles

Si on supprime un utilisateur sur lequel on a défini une règle du moteur de règles (ACL), celui-ci est retiré de la règle. Si cet utilisateur était le seul utilisateur concerné par la règle, la règle affiche "Utilisateur supprimé". Dans la supervision, un message informe l'administrateur que l'utilisateur a été supprimé alors qu'il était utilisé dans une ACL.

Domaines Olfeo

#6170 - Jonction à un domaine Olfeo : maître et esclave avec deux bases différentes

On peut joindre une machine esclave à un domaine Olfeo même si la base d'URLs de l'esclave est différente de celle du maître. La base d'URLs de l'esclave est remplacée par celle du maître. Un message de type "info" l'indique dans l'écran de supervision du maître (**Paramétrage > Supervision > Journal**).

#6487 - Continuité du filtrage dans le domaine Olfeo quand la machine maître est éteinte

Dans un domaine Olfeo, lorsque la machine maître est inaccessible (par exemple lors d'une mise à jour), les machines esclaves continuent leur activité normalement. Si des modifications ont été apportées à la configuration d'un maître alors que la connexion entre maître et esclave était coupée, la configuration des esclaves se met à jour lorsque la connexion est rétablie. Attention, ne pas tenter de redémarrer les services de la machine esclave pendant que la machine maître est injoignable : la machine esclave ne pourrait plus redémarrer. Les services redémarrant automatiquement à minuit, les machines esclaves deviennent alors indisponibles si la machine maître n'a pas été redémarrée entre-temps.

#6792 - Écrasement de l'IP de l'esclave lors du changement de l'IP du maître

Dans un domaine Olfeo comprenant des box, modifier l'adresse IP d'une box modifiait celle des autres machines présentes dans le domaine.

Filtrage d'URLs

#6071 - Listes de domaines utilisées dans le moteur de règles : matching des domaines/sous-domaines

Les sous-domaines n'étaient plus pris en compte lorsque le FQDN était préfixé par un point.

Antivirus

#6600 - Journal de logs de l'antivirus vide

La page **Antivirus > Journal** n'affichait rien. Le problème est corrigé : la page affiche maintenant la liste des virus détectés par l'Olfeo.

Migration

#6620 - Bouton Précédent grisé lors de l'import de façon à ne pas interrompre ce dernier

Dans l'assistant de migration, Le bouton "Précédent" de la page "import des données en cours" est grisé tant que l'import se déroule sans erreur, afin d'éviter que l'utilisateur clique dessus par erreur et interrompe l'import. Si une erreur stoppe l'import, le bouton se dégrise pour permettre à l'utilisateur de relancer l'import.

#6689 - Réduction de l'espace nécessaire lors de l'import des hits

Pour pouvoir importer les hits v5 en v6, l'espace nécessaire sur votre disque est maintenant 3 fois la taille du dossier d'export et non plus 10 fois. Dans le cas où le dossier d'export contient un fichier RAW nettement plus gros que les autres, l'espace nécessaire sera 10 fois la taille de celui-ci.

#6854 - Suppression des liens "Favoris" dans l'interface des statistiques (suite à un import v5)

Lors d'une migration de la v5 à la v6, la page **Statistiques** > **Temps réel** affichait des liens **Favoris**, invalides. Ces liens correspondaient aux rapports et analyses v5, qui ne sont pas migrés. Ils ont donc été supprimés.

#6857 - Administrateur créé en v5 absent en v6

Certains administrateurs créés en v5 pouvaient ne pas apparaître dans l'interface d'administration après migration en v6.

Supervision

#6465 - Alerte lorsqu'aucun user-agent n'est sélectionné

Une alerte apparaissait lorsqu'aucun user agent n'était sélectionné dans une règle du moteur d'authentification du proxy HTTP. Certaines requêtes ne contiennent pas d'en-tête user-agent. 2 cas sont maintenant gérés :

- "Obligatoire" (case .* cochée) correspond à n'importe quel user-agent, mais il doit y avoir un user-agent
- "Tous" (aucune case cochée) : toutes les requêtes, qu'il y ait ou non un en-tête user-agent, et s'il y en a un, quel que soit le user-agent.

Partage d'objets

#6156 - Rétablissement du partage des objets admin/sous-admin

Un sous-administrateur pouvait voir les objets créés par tous les autres administrateurs, même si le mode **Partage des objets** n'était pas activé.

Portail public

#6380 - Application des politiques sur le ticket par défaut du portail public

Lorsqu'on crée un type de ticket, on lui assigne des politiques par défaut (politique de filtrage d'URLs et de filtrage protocolaire). Une fois un ticket créé (par autoenregistrement ou création manuelle dans le portail opérateur), cette politique apparaissait à l'intérieur du ticket, mais elle n'apparaissait pas dans les colonnes **Filtrage d'URL** et **Filtrage protocolaire** de la liste des utilisateurs et n'était pas appliquée.

Robustesse

#6475 - Vérification de la valeur entrée dans les champs date dans la page d'extraction des hits

À la page **Statistiques** > **Extraction**, un message d'erreur informe maintenant l'utilisateur de la présence de caractères invalides dans les champs **Date de début** et **Date de fin**.

#6508 - Meilleure gestion des services clamav

À la page **Paramétrage** > **Supervision** > **Journal**, une erreur `Service clamav-daemon reports an error` apparaissait plusieurs fois par jour.

#6584 - L'accès à une URL en FTP entraînait un redémarrage du proxy**#6625 - Résolution d'un problème d'affichage des graphiques lors de modifications en série**

Si l'utilisateur modifiait un graphique plusieurs fois de suite très rapidement, un phénomène de flickering pouvait apparaître dans l'interface : plusieurs graphiques s'affichaient avant le graphique final. La gestion des requêtes envoyées au navigateur a été améliorée afin de résoudre ces problèmes.

#6633 - Indexation des tables de hits par jour

Des tables ont été indexées, ce qui donne la possibilité d'informer l'utilisateur que ses statistiques sont en cours de migration.

#6703 - Synchronisation des utilisateurs membres d'un groupe membre de lui-même

Dans le cas où un groupe était membre de lui-même, la synchronisation des utilisateurs était impossible. La correction permet de prendre ce cas particulier en charge.

Interface graphique

#6149 - Nouveaux styles permettant de différencier un bouton actif d'un bouton inactif

Les styles suivants ont été introduits :

- Au survol, le libellé des boutons actifs prend une couleur légèrement différente afin d'indiquer à l'utilisateur que le bouton est cliquable.
- Les boutons inactifs apparaissent grisés, et la couleur de leur libellé ne change pas au survol.

#6163 - Mise en forme de l'assistant de configuration

Un défaut d'alignement a été corrigé et les boutons ont été rendus conformes à la charte graphique.

#6825 - Affichage du nombre de hits par seconde dans l'interface d'administration

Le nombre de hits par seconde reçu par le moteur Olfeo est indiqué en bas à gauche de l'interface d'administration. Cette information était présente en v5.

Mise à jour

Correctifs consistant à s'assurer que les services redémarrent lors d'une mise à jour

- #6509 : Certaines variables d'environnement n'étaient plus définies après une mise à jour en 6.0.6.
- #6734 : Certains services ne démarraient pas.

6.0.7 Problèmes connus

Redémarrage nécessaire après mise à jour

Lors d'une mise à jour depuis la 6.0.6 vers la 6.0.7, il est nécessaire de redémarrer le système d'exploitation.

- Pour les box, utiliser le bouton **Redémarrer la box** à la page **Paramétrage > Système > Services**.
- Pour une machine virtuelle : redémarrer celle-ci.