Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2019/06

One Identity syslog-ng Store Box
Version 5.0.2

Paris, le 9 juillet 2019

Le directeur général de l'agence nationale
de la sécurité des systèmes d'information

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié. C'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CSPN-2019/06

Nom du produit

One Identity syslog-ng Store Box

Référence/version du produit

Version 5.0.2

Catégorie de produit

Administration et supervision de la sécurité

Critères d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)

Commanditaire

One Identity
Alíz street 2. H-1117 Budapest,
Hungary

Développeur

One Identity
Alíz street 2. H-1117 Budapest,
Hungary

Centre d'évaluation

Oppida
4-6 avenue du vieil étang,
Bâtiment B, 78180 Montigny le Bretonneux,
France

Fonctions de sécurité évaluées

Protection des journaux en confidentialité et intégrité
Sécurisation des communications entre les clients et le serveur
Protection en confidentialité des données stockées
Gestion des rôles
Validation en entrée des journaux
Authentification des acteurs se connectant au serveur

Fonction(s) de sécurité non évaluées

Néant

Restriction(s) d'usage

Non

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification CSPN sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est la solution « One Identity syslog-ng Store Box, version 5.0.2 » développée par *ONE IDENTITY*.

Ce produit est destiné à centraliser au sein d'un SI la collecte des journaux d'évènements des ordinateurs. Il est implémenté en deux parties, un client et le serveur. La partie cliente est installée sur un ordinateur exécutant un système d'exploitation *WINDOWS* ou *LINUX*. Quant à la partie serveur, elle est installée sur une *appliance*, exécutant un système d'exploitation basé sur *UBUNTU*. Le serveur reçoit des journaux émis par les logiciels clients, pour ensuite les traiter et les stocker de façon sécurisé en les signant et chiffrant.

Le produit offre également une interface d'administration accessible depuis un navigateur. La séparation des rôles permet de configurer des utilisateurs standards et des administrateurs de la solution.

La figure ci-dessous explicite l'architecture du produit.

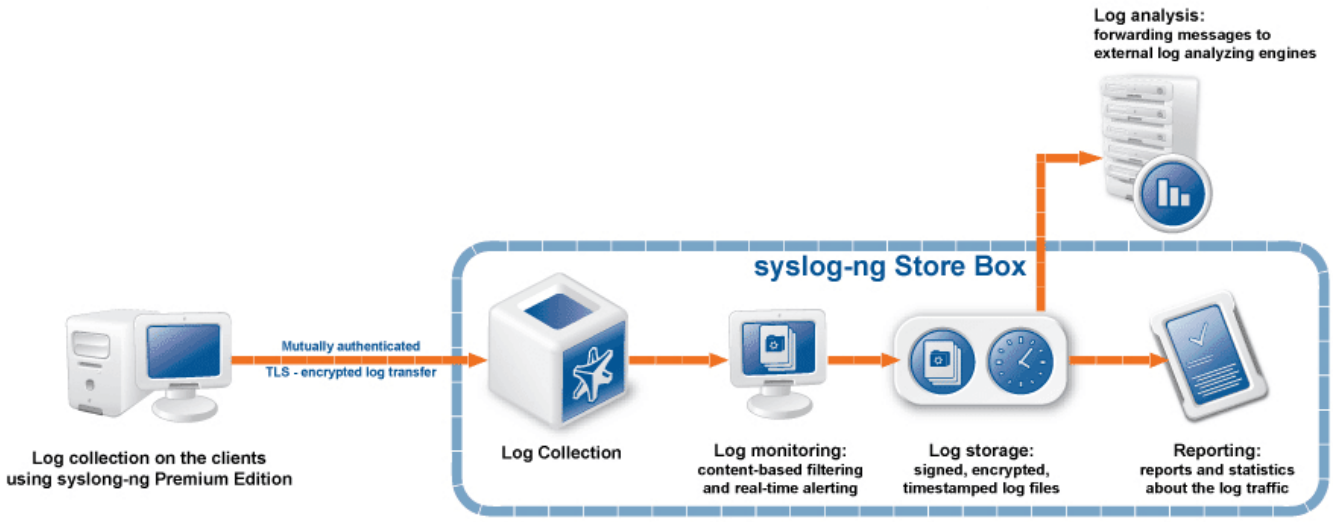

Figure 1 - Architecture Produit.

1.2. Description du produit évalué

La cible de sécurité [CDS] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1. Catégorie du produit

☐ 1 – détection d'intrusions
☐ 2 – anti-virus, protection contre les codes malicieux
☐ 3 – pare-feu
☐ 4 – effacement de données
☒ **5 – administration et supervision de la sécurité**
☐ 6 – identification, authentification et contrôle d'accès
☐ 7 – communication sécurisée
☐ 8 – messagerie sécurisée
☐ 9 – stockage sécurisé
☐ 10 – environnement d'exécution sécurisé
☐ 11 – terminal de réception numérique (*Set top box*, STB)
☐ 12 – matériel et logiciel embarqué
☐ 13 – automate programmable industriel
☐ 99 – autre

1.2.2. Identification du produit

Nom du produit	One Identity syslog-ng Store Box
Numéro de la version évaluée	5.0.2

La version certifiée du produit peut être identifiée de la manière suivante :

- se connecter en http au serveur : le titre (balise *title* en html) de l'interface d'administration détaille la version du produit ;
- en accédant à la racine du disque : le fichier MANIFEST détaille la version du produit sous le mot clé *technical_version* ;
- en se connectant en SSH au serveur : le menu « *Firmware management* » détaille la version du produit sous « *Firmware slots* ».

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- la protection des journaux en confidentialité et intégrité ;
- la sécurisation des communications entre les clients et le serveur en utilisant TLS ;
- la protection en confidentialité des données stockées : les secrets cryptographiques et des données de connexion ;
- la gestion des rôles permettant une séparation des tâches accessibles aux utilisateur et administrateurs ;
- la validation en entrée des journaux ;
- l'authentification des acteurs se connectant au serveur : les administrateurs se connectant au serveur en utilisant un compte et un mot de passe. Les clients se connectent au serveur en utilisant un certificat.

1.2.4. Configuration évaluée

La configuration évaluée correspond à celle décrite dans la cible de sécurité ([CDS]), à savoir la partie serveur du produit. Les deux clients pour les plateformes *WINDOWS* et *LINUX* ne font pas partie du périmètre de l'évaluation. Le produit configuré n'utilise pas les fonctionnalités suivantes :

- l'administration à distance par SSH et *Intelligent Platform Management Interface* (IPMI) ;
- la haute disponibilité ;
- la base de données SQL ;
- le protocole *Reliable Log Transfer Protocol* (RLTP) ;
- la gestion de la sauvegarde ;
- l'accès à distance des bases de données.

La configuration évaluée s'appuie également sur le guide de sécurité de l'éditeur ([GUIDES]), les règles suivantes ont été appliquées :

- la désactivation du serveur SSH, sauf en cas de dépannage ou d'installation du produit ;
- l'utilisation d'un « *logstore* » chiffré ;
- la collecte de journaux en utilisant TLS avec authentification mutuelle et avec le paramétrage « *Cipher suite : Strong* ».

La plateforme de test est constituée d'un PC exécutant le produit.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. Les références des documents se trouvent en Annexe 2.

2.2. Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation est conforme à la charge de travail prévue dans le dossier d'évaluation.

2.3. Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, des menaces, des utilisateurs et des fonctions de sécurité définis dans la cible de sécurité [CDS].

2.3.1. Installation du produit

2.3.1.1. Particularités de paramétrage de l'environnement et options d'installation

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

2.3.1.2. Description de l'installation et des non-conformités éventuelles

L'installation du produit est simple et revient à passer par six étapes où l'on renseigne, si besoin, une précédente configuration, puis une licence d'utilisation, une gestion réseau, les utilisateurs identifiés et enfin le certificat du serveur.

2.3.1.3. Durée de l'installation

L'installation prend moins d'une heure.

2.3.1.4. Notes et remarques diverses

L'installation est simple et s'effectue au travers d'une interface graphique.

2.3.2. Analyse de la documentation

L'évaluateur a eu accès aux documents [GUIDES] dans le cadre de cette évaluation. Ils sont librement accessibles sur le site de développeur.

Les guides du produit permettent d'installer et d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

2.3.3. Revue du code source (facultative)

L'évaluateur a revu le code source le code source PHP de l'interface d'administration Web. L'analyse a été effectuée à l'aide des outils *SONARQUBE* et *DOXYGEN*.

Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

2.3.4. Analyse de la conformité des fonctions de sécurité

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

2.3.5. Analyse de la résistance des mécanismes des fonctions de sécurité

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

2.3.6. Analyse des vulnérabilités (conception, construction, etc.)

2.3.6.1. Liste des vulnérabilités connues

Aucune vulnérabilité connue et exploitable affectant la version évaluée du produit n'a été identifiée.

2.3.6.2. Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Il n'a pas été découvert de vulnérabilité propre au produit, ni dans son implémentation, qui puisse remettre en cause la sécurité du produit.

2.3.7. Accès aux développeurs

Sans objet.

2.3.8. Analyse de la facilité d'emploi

2.3.8.1. Cas où la sécurité est remise en cause

L'évaluateur n'a pas identifié de cas où la sécurité de la TOE est remise en cause.

2.3.8.2. Avis d'expert sur la facilité d'emploi

Le produit est globalement bien documenté, et sa mise en œuvre ne présente pas de difficulté.

2.3.8.3. Notes et remarques diverses

Aucune note, ni remarque n'a été formulée dans le [RTE].

2.4. Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN. Celle-ci n'a pas identifié de non-conformité au RGS ni de vulnérabilité exploitable.

2.5. Analyse du générateur d'aléas

Le produit n'implémente pas de générateur d'aléas.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé.

Ce certificat atteste que le produit « One Identity syslog-ng Store Box, version 5.0.2 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

3.2. Recommandations et restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.
Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [GUIDES] fournis.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Security Target – syslog-ng Store Box For CSPN evaluation* Version : 1.1 ; Date : *20 juin 2018*
[RTE]	*Rapport Technique d'Évaluation CSPN Syslog-ng Store Box* Référence : OPPIDA/CESTI/SSB/RTE/1.1 Version : 1.1 ; Date : *29 avril 2019.*
[GUIDES]	*Syslog-ng Store Box 5.0 User Guide* Version : 5.0 ; Date : *juillet 2018.* *Syslog-ng Store Box 5.0 Administration Guide* Version : 5.0 ; Date : *août 2018.* *Syslog-ng Store Box 5.0 Security checklist for syslog-ng Store Box appliances* Version : 5.0 ; Date : *juillet 2018*

Annexe 2. Références à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	Certification de sécurité de premier niveau des produits des technologies de l'information, version 1.1, référence ANSSI-CSPN-CER-P-01/1.1 du 07 avril 2014. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1.1, référence ANSSI-CSPN-CER-I-02/1.1 du 23 avril 2014. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/2 du 23 avril 2014. Documents disponibles sur www.ssi.gouv.fr.
[RGS]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.