Stormshield Data Security

Kit de démonstration

|  |  |
| --- | --- |
| **Version** | 1.0 |
| **Référence** | STORMSHIELD/SDS/Documentation/DemoKit |
| **Date** | 07/10/2015 |
| **Mots-clés** |  |
| **Résumé** |  |

Historique des modifications

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Auteurs** | **Relecteurs** | **Description et justification de la modification** |
|  |  |  |  |  |
| 1.0 | 07/10/2015 | JPC |  | Version initiale. |
| 1.1 | 30/01/2019 | APO |  | Ajout de récupération des ACL |

Auteurs / Relecteurs

JPC : Jean-Philippe Ciman

SOMMAIRE

[1 Généralités 4](#_Toc431983034)

[1.1 Introduction 4](#_Toc431983035)

[1.2 Scénario 4](#_Toc431983036)

[2 Implémentation 4](#_Toc431983037)

[2.1 PowerShell 4](#_Toc431983038)

[2.2 .NET 5](#_Toc431983039)

[2.3 Rapport 5](#_Toc431983040)

# Généralités

## Introduction

Ce document décrit comment utiliser le kit de démonstration du module Stormshield Data Connector.

## Scénario

Pour ce kit, on imagine un parc de machines où l’administrateur souhaite qu’un dossier bien particulier soit en permanence chiffré pour les utilisateurs, comme une sorte de coffre-fort.

Une fois un utilisateur connecté à sa session Windows, on souhaite :

1. Connecter l’utilisateur à son compte Stormshield Data Security (en mode interactif);
2. S’assurer qu’un dossier particulier est sécurisé avec le module Team (et le créer si besoin) ;
3. Informer l’utilisateur sur ce qu’il s’est passé.

Le dossier doit être systématiquement sécurisé par une règle Team et les fichiers chiffrés.

# Implémentation

Le scénario décrit plus haut est implémenté à l’identique pour les deux modes d’utilisation du module Connector, à savoir PowerShell et .NET.

Dans les deux implémentations, le dossier configuré est un dossier nommé « Secured » sur le bureau de l’utilisateur.

## Dépendance

Pour utiliser le script SecuredFolderWithAcl vous aurez besoin des modules Powershell suivant :

* [Microsoft.PowerShell.Security](https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.security/?view=powershell-6)
* [Microsoft.PowerShell.LocalAccounts](https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.localaccounts/?view=powershell-5.1)
* [addsadministration](https://docs.microsoft.com/en-us/powershell/module/addsadministration/?view=win10-ps)

## PowerShell

Le script est à exécuter au démarrage de la session Windows de l’utilisateur. Pour ce faire, une possibilité est de créer un raccourci vers l’exécutable PowerShell dans le dossier « Startup » de l’utilisateur.

Dossier « Startup »:

C:\Users\<User>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

Exécutable PowerShell :

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Arguments à passer à l’exécutable PowerShell :

-WindowStyle Hidden "<chemin du script PS1>"

Pour modifier le dossier à sécuriser, éditer le script PS1 et modifier la variable $securedFolder sur la première ligne du script.

## .NET

L’exécutable est à exécuter au démarrage de la session Windows de l’utilisateur. Pour ce faire, une possibilité est de créer un raccourci vers l’exécutable dans le dossier « Startup » de l’utilisateur.

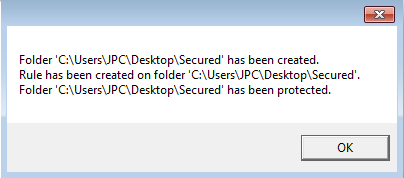
Dossier « Startup » :

C:\Users\<User>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

Pour modifier le dossier à sécuriser, éditer le fichier d’extension .config à côté de l’exécutable et modifier la valeur de la clé « SecuredFolder » (laisser vide pour retrouver le comportement par défaut).

## Rapport

Les deux implémentations informent l’utilisateur sur ce qu’il s’est passé par une boite de dialogue.



Chaque message s’affiche si l’action a été réalisée.

En cas d’erreur, une boite de dialogue similaire est affichée, contenant la description de l’erreur.