

Copyright 2021 Trend Micro Incorporated. All rights reserved.

# agent\_migration\_ds2c1ws

---

オンプレミス版Deep Security Manager (DSM)で管理するDeep Security AgentをTrend Micro Cloud One – Workload Security (C1WS)へ移行するサンプルプログラム

## 本プログラムで実行できること

- DSMのポリシーをC1WSに移行する
- 管理対象のコンピュータ全台または一部をDSMからC1WSに移行する

## 動作確認環境

- OS
  - Windows10
- Python
  - Version: 3.7
  - requirements
    - [requests](#)

## インストール

**Python3, pip3の環境があることが前提**

依存ライブラリをインストールします

```
%pip3 install -r .\requirements.txt
```

## 利用方法

1. ./config\_files/config.iniの中身を自身の環境に合わせて書き換えます
2. 複数テナントある場合は、config\_filesフォルダ配下に同様のiniファイルを作成します
3. ./src/agent\_migration\_ds2c1ws.pyのCONFIG\_FILE\_DIRにconfig\_filesフォルダの絶対パスを記入します
4. ./src/agent\_migration\_ds2c1ws.pyを実行します

```
%python3 ./src/agent_migration_ds2c1ws.py
```

5. C1WSコンソールにて移行対象が管理対象であることを確認します。
6. ./src/clear\_workload\_security\_links.pyのCONFIG\_FILE\_DIRにconfig\_filesフォルダの絶対パスを記入します
7. ./src/clear\_workload\_security\_links.pyを実行します

```
%python3 ./src/clear_workload_security_links.py
```

## 資料

### config.iniについて

- ファイル形式
  - Pythonのconfigparserライブラリで解析できるINIファイルの構成に準拠してください。
  - 詳細については [こちら](#) を参照ください。
- パラメータ
  - DS\_api\_key
    - DSMのAPIキーを指定してください。
    - APIキーの作成手順は [こちら](#) を参照ください。
  - C1WS\_api\_key
    - C1WSのAPIキーを指定してください。APIキー作成時の[役割]は、「Deep Security Migration」を指定することを推奨します。詳細は [こちら](#) を参照ください。
    - APIキー作成の手順は [こちら](#) を参照ください。
  - DSM\_url
    - REST APIを呼び出すエンドポイントを指定してください。
    - https://xxx.xxx.xxx.xxx:4119/ あるいは https://hosturl:4119/ となります。
  - workloadSecurityUrl
    - Workload Security Linkの作成で使用するworkloadSecurityUrlを指定してください。
    - 2021年8月4日以前に作成したCloud Oneアカウントの場合「cloudone.trendmicro.com」となります。
    - 2021年8月4日以降に作成したCloud Oneアカウントの場合「workload.{region}.cloudone.trendmicro.com」となります。regionは、Cloud Oneコンソールの[User Management] - [Account Settings]を参照ください。
  - workloadSecurityCA
    - Workload Security Linksの作成で使用するworkloadSecurityCAを指定してください。
    - 最新のworkloadSecurityCAは [こちら](#) を参照ください。
  - policy\_migration
    - DSMのポリシーをC1WSに移行する場合は「YES」を、移行しない場合は「NO」を指定してください。
  - target\_computers\_file\_path
    - DSMの管理対象コンピュータを全てC1WSに移行する場合は「ALL」を指定してください。
    - DSMの管理対象コンピュータの内、一部を移行する場合は下記手順でエクスポートしたファイルの絶対パスを指定してください。  
<移行対象コンピュータリストのエクスポート手順>
      1. DSM管理コンソールにログインします。
      2. DSM管理コンソール上部のユーザ名を選択し、[ユーザプロパティ]をクリックします。
      3. [一般]タブから[言語]を「English (US)」に設定し、[保存]をクリックします。
      4. [Administration]を選択し、左ペイン[System Settings]をクリックします。

5. [Advanced]タブから[Exported file Character Encoding]を「UTF-8」に設定し、[Save]をクリックします。
  6. [Computers]を選択し[Columns]ボタンより、「Host GUID」の列を追加します。
  7. 移行対象コンピュータを選択し、「Export Selected to CSV...」をクリックします。
    - ※エクスポートしたファイルの文字コードはUTF-8から変更しないでください。
    - ※「Export to CSV...」より、エクスポートしたリストから移行対象でないコンピュータの行を削除する手順でも問題ございません。
- proxy\_manager\_hostname
    - 移行対象コンピュータからC1WSのManagerへの接続に利用されるプロキシのホスト名を指定してください。
    - プロキシを使用しない場合は空白にしてください。
  - proxy\_manager\_port
    - 移行対象コンピュータからC1WSのManagerへの接続に利用されるプロキシのポートを指定してください。
    - プロキシを使用しない場合は空白にしてください。
  - proxy\_manager\_user
    - 移行対象コンピュータからC1WSのManagerへの接続に利用されるプロキシのユーザ名を指定してください。
    - プロキシを使用しない場合や、プロキシの認証が必要ない場合は空白にしてください。
  - proxy\_manager\_password
    - 移行対象コンピュータからC1WSのManagerへの接続に利用されるプロキシのパスワードを指定してください。
    - プロキシを使用しない場合や、プロキシの認証が必要ない場合は空白にしてください。
  - proxy\_relay\_hostname
    - 移行対象コンピュータからC1WSのRelayへの接続に利用されるプロキシのホスト名を指定してください。
    - プロキシを使用しない場合は空白にしてください。
  - proxy\_relay\_port
    - 移行対象コンピュータからC1WSのRelayへの接続に利用されるプロキシのポートを指定してください。
    - プロキシを使用しない場合は空白にしてください。
  - proxy\_relay\_user
    - 移行対象コンピュータからC1WSのRelayへの接続に利用されるプロキシのユーザ名を指定してください。
    - プロキシを使用しない場合や、プロキシの認証が必要ない場合は空白にしてください。
  - proxy\_relay\_password
    - 移行対象コンピュータからC1WSのRelayへの接続に利用されるプロキシのパスワードを指定してください。
    - プロキシを使用しない場合や、プロキシの認証が必要ない場合は空白にしてください。

## プログラムの説明

- ./src/agent\_migration\_ds2c1ws.py
  - main : メイン処理
    - ds\_utilsクラスインスタンスを初期化する
  - clear\_workload\_security\_links : 既存のWorkload Security Linksを削除する
  - create\_workload\_security\_links : Workload Security Linkを作成する

- create\_policy\_migration\_task : Policy Migration Taskを作成する
  - config.iniの policy\_migration 項目が「YES」の場合タスクが作成され、「NO」の場合タスクは作成されない
- describe\_policy\_migration\_task : Policy Migration Taskの情報を取得する
- get\_target\_computers: 移行対象コンピュータのリストを取得する
  - config.iniの target\_computers\_file\_path 項目が「ALL」の場合、空のリストが作成される
  - config.iniの target\_computers\_file\_path 項目にコンピュータリストのファイルのパスが指定された場合、HOST GUIDのリストが作成される
- list\_computer\_policy\_id: 移行対象コンピュータの情報を取得する
- create\_computer\_move\_task: Computer Move Taskを作成する
- ./src/clear\_workload\_security\_links.py
  - main : メイン処理
    - ds\_utilsクラスインスタンスを初期化する
  - clear\_workload\_security\_links : 既存のWorkload Security Linksを削除する
- ./src/ds\_utils/ds\_utils.py
  - APIUtils class : コンピューター一覧取得処理を保持するクラス
    - \_\_init\_\_ : クラスの初期化時に呼び出される
      - config\_file\_path(引数) で受け取ったINIファイルを読み出す
    - clear\_workload\_security\_links : 既存のWorkload Security Linksを削除する
      - GET /workloadsecuritylinksを実行する
      - DELETE /workloadsecuritylinks/{workloadSecurityLinkID}を実行する
    - create\_workload\_security\_links : Workload Security Linkを作成する
      - POST /workloadsecuritylinksを実行する
    - create\_policy\_migration\_task : Policy Migration Taskを作成する
      - POST /policymigrationtasksを実行する
    - describe\_policy\_migration\_task: Policy Migration Taskの情報を取得する
      - statusがcompleteでない場合、ポリシー移行中と判断し 1分間待機した後リトライする
      - 5回のリトライ実行後、statusがcompleteにならない場合は終了する
      - statusがcompleteの場合、policyMappings情報を取得する
    - get\_target\_computers : 移行対象コンピュータのリストを取得する
      - target\_computers\_file\_path 項目に指定されたファイルを読み込み、ファイルヘッダ「Host GUID」列の値のリストを作成する
    - list\_computer\_policy\_id: 移行対象コンピュータの情報を取得する
      - target\_computers(引数)に値が含まれる場合、POST /computers/searchを実行し、移行対象の内agentStatusがactiveであるコンピュータのhostIDとpolicyIDを取得する
      - target\_computers(引数)が空の場合、GET /computersを実行し、agentStatusがactiveであるコンピュータのhostIDとpolicyIDを取得する
    - create\_computer\_move\_task : Computer Move Taskを作成する
      - ポリシーのID、コンピュータのID、プロキシ情報を用いて POST /computermovetasksを実行する

## 注意事項

- Deep Security Manager、Deep Security Agent共に、最新のビルドを利用することを推奨いたします。APIをサポートするバージョンの詳細は[こちら](#)を参照ください。

- FIPSモードが無効であること、DSMの管理対象にAgent-lessまたはコンバインモードで保護された仮想マシンが含まれないことをご確認ください。詳細は[こちらの](#)「Feature limitations」を参照ください。
- ソフトウェアパッケージの公開停止により、オンプレミス版Deep Securityにて使用していたソフトウェアがC1WSにインポートされていない場合がございますため、C1WSにてDSA有効化の自動アップグレード機能を設定いただくことを推奨いたします。設定手順の詳細は[こちら](#)を参照ください。
- config.iniのpolicy\_migration項目に「NO」を指定した場合、移行後のコンピュータに適用されるポリシーは「なし」となります。
- config.iniのtarget\_computers\_file\_path項目に指定するファイルは、ヘッダに「Host GUID」が含まれており、文字エンコードがUTF-8であることをご確認ください。
- 移行完了前に./src/clear\_workload\_security\_links.pyを実行しないようご注意ください。

## 免責事項

---

本ドキュメントのご利用に際しては、以下の点にご留意いただきますようお願いいたします。

### 1. 本ドキュメントの内容・情報について

本ドキュメントは当社製品をご利用頂く際に必要となる各種設定をご提供させて頂くことを目的としております。本ドキュメントの内容や情報は、明示または黙示を問わず何らかの保証を伴うことなく現存するままの状態を提供されるものです。当社は、本ドキュメントに掲載する情報について、充分注意・確認をした上で掲載することに努めますが、情報が古くなったり、閲覧された時点で間違っていたりする場合もございます。また、本ドキュメントを通じてアクセスできるデータやプログラム、資料の正確性の確認に際し、当社は責任を負いません。したがって、提供される情報の正確性、適時性若しくは完全性、また特定のいかなる目的に対する妥当性・適性について保証するものではありません。本ドキュメントのご利用につきましては、当社は一切責任を負いかねますので、本ドキュメントの情報は利用者ご自身の責任においてご利用下さい。本ドキュメントの内容や情報は予告なく変更・改訂される場合があります。本ドキュメントのご利用に関しては日本の法令に準拠し、解釈されるものとします。

### 2. 製品情報および技術情報について

本ドキュメントの情報は、将来における技術上の可能性を含む場合があります。また、技術上不正確な記載や誤植を含む場合があります。これらの情報については、通知なしに変更または更新される場合があります。当社は、これらの情報に記載された製品またはサービス、技術を予告なしにいつでも変更することがあります。

## 著作権について

---

ドキュメントの内容を、複製、配布、賃貸、貸与、販売、許諾ならびに譲渡等行うことはできません。ドキュメントの内容を、複製ならびに翻訳、翻案等を行い二次的著作物を創作することはできません。

TRENDMICRO はトレンドマイクロ株式会社の登録商標です。Copyright(C) 1995-2021 Trend Micro Incorporated. All rights reserved.

その他、製品名等の固有名詞は各社の商標または登録商標です。なお、本文中では™、®マークは明記しておりません。