

Cisco Crosswork Change Automation NSO 機能パック

インストールガイド

バージョン 5.0.0

目次

はじめに.....	3
インストールと設定	4
機能パックのインストール	4
Cisco NSO での特別アクセスユーザーの作成.....	4
Cisco NSO authgroup への usermap (umap) の追加	6
Cisco Crosswork での DLM の設定	8
ca_device_auth_nso ログイン情報プロファイルの作成	8
DLM プロバイダープロパティの追加.....	9
トラブルシューティング	10

はじめに

このドキュメントでは、Cisco Network Services Orchestrator (NSO) で Cisco Crosswork Change Automation (CA) 機能パックをダウンロード、インストール、および設定する方法について説明します。さらに、このドキュメントでは、Cisco Crosswork での Crosswork Change Automation に必要な設定についても説明します。

目的

このガイドでは、以下について説明します。

- **cw-na-fp-ca-5.0.0-nso-6.1.tar.gz** 機能パックの Cisco NSO 6.1 へのインストールと、機能パックに関連した設定の Cisco NSO へのインストール。
- Change Automation 用の一意のユーザーマップ (**umap**) を作成するための **authgroup** 設定。
- DLM の設定と、Cisco Crosswork 5.0.0 で必要な Change Automation アプリケーションの設定。

前提条件

以下のリストは、Crosswork Change Automation 機能パック v5.0 と互換性のある Cisco NSO および Cisco Crosswork の最小バージョンを示しています。

- Cisco NSO : v6.1 システムインストール
- Cisco Crosswork : v5.0.0

インストールと設定

以下のセクションでは、システムインストール Cisco NSO 6.1 以降に **cw-device-auth** 機能パックをインストールする方法を示します。

機能パックのインストール

1. リポジトリから Cisco NSO に **cw-device-auth** v5.0.0 をダウンロードします。
2. ダウンロードした機能パックの tar.gz アーカイブをパッケージリポジトリにコピーします。

注： パッケージディレクトリは、インストール時に選択した設定に基づいて決定されるので、異なる場合があります。システムにインストールされたほとんどの Cisco NSO の場合、パッケージディレクトリはデフォルトでは「/var/opt/ncs/packages」にあります。インストールの ncs.conf を確認して、パッケージディレクトリを見つけます。

3. NCS CLI を起動し、次のコマンドを実行します。

```
admin@nsol:~$ ncs_cli -C -u admin
admin connected from 2003:10:11::50 using ssh on nsol
admin@ncs# packages reload
```

4. リロードが完了したら、パッケージが正常にインストールされたことを確認します。

```
admin@ncs# show packages package cw-device-auth
packages package cw-device-auth
package-version 5.0.0
description      "Crosswork device authorization actions pack"
ncs-min-version [ 6.0]
python-package  vm-name cw-device-auth
directory        /var/opt/ncs/state/packages-in-use/1/cw-device-auth
component action
application python-class-name cw_device_auth.action.App
application start-phase phase2
oper-status up
```

Cisco NSO での特別アクセスユーザーの作成

Cisco Crosswork Change Automation は、すべての設定変更に関して、特別アクセスユーザーを使用して Cisco NSO に接続します。つまり、DLM サービスや収集サービスと同じユーザーを使用して Cisco NSO にアクセスすることはできません。このセクションでは、ユーザーの作成に必要な前提条件について説明します。

注： 以下の手順は、Cisco NSO が Ubuntu VM で実行されていることを前提としています。Cisco NSO のインストールが別のオペレーティングシステムで実行されている場合は、それに応じて手順を変更してください。

1. Ubuntu VM で新しい sudo ユーザーを作成します。例が[こちら](#)に示されています。以下の手順は、Ubuntu VM でユーザー「**cwuser**」を作成する方法を示しています。この新しいユーザー名には、任意の名前を使用できます。

```
root@nso:/home/admin# adduser cwuser
Adding user `cwuser' ...
Adding new group `cwuser' (1004) ...
Adding new user `cwuser' (1002) with group `cwuser' ...
Creating home directory `/home/cwuser' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for cwuser
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] y
root@nso:/home/admin# usermod -aG sudo cwuser
root@nso:/home/admin# usermod -a -G ncsadmin cwuser
```

2. 作成した新しいユーザーが Cisco NSO サーバーに HTTP アクセスおよび HTTPS アクセスできることを確認します。確認は、以下に示すシンプルな RESTCONF API を使用して実行できます。

```
curl -u <USERNAME>:<PASSWORD> --location --request
GET 'https://<IP>:8888/restconf/data/taillf-ncs:packages/package=cw-device-auth' \
--header 'Accept: application/yang-data+json' \
--header 'Content-Type: application/yang-data+json' \
--data-raw ''
```

上記の curl コマンドを呼び出すと、以下のような応答が返されます。それ以外の応答は、これより前のもう 1 つの設定が機能しなかったことを示唆します。

```
{
  "taillf-ncs:package": [
    {
      "name": "cw-device-auth",
      "package-version": "1.0.0",
      "description": "Crosswork device authorization actions pack",
      "ncs-min-version": ["6.0"],
      "python-package": {
        "vm-name": "cw-device-auth"
      },
      "directory": "/var/opt/ncs/state/packages-in-use/1/cw-device-auth",
      "component": [
        {
```

```

    "name": "action",
    "application": {
      "python-class-name": "cw_device_auth.action.App",
      "start-phase": "phase2"
    }
  },
],
"oper-status": {
  "up": [null]
}
}
]
}

```

Cisco NSO authgroup への usermap (umap) の追加

Cisco NSO では、サウスバウンド デバイス アクセス用のログイン情報を指定するための authgroup を定義できます。authgroup には、default-map または usermap (umap) を含めることができます。さらに、umap を authgroup で定義して、default-map またはその他の umaps からのデフォルトのログイン情報をオーバーライドすることもできます。

Crosswork Change Automation の「override credentials passthrough」機能は、この umap を使用します。Crosswork Change Automation を使用するには、デバイスの authgroup に umap 構成を作成する必要があります。

たとえば、デバイス「**xrv9k-1**」が Cisco NSO に登録されているとします。このデバイスは、authgroup「**crosswork**」を使用します。

```

cwuser@ncs# show running-config devices device xrv9k-1 authgroup
devices device xrv9k-1
  authgroup crosswork
!

```

authgroup「**crosswork**」の構成は次のとおりです。

```

cwuser@ncs# show running-config devices authgroups group crosswork
devices authgroups group crosswork
  umap admin
  remote-name      cisco
  remote-password  $9$LzskzrvZd7LeWwVNGZTdUBDdKN7IgvV/UkJebwM1eKg=
!
!

```

作成した新しいユーザー（この例では **cwuser**）に **umap** を追加します。この操作は、次のように実行できます。

```

cwuser@ncs# config
cwuser@ncs(config)# devices authgroups group crosswork umap cwuser callback-node /cw-creds-get action-name get
cwuser@ncs(config-umap-cwuser)# commit dry-run

```

```
cli {
  local-node {
    data devices {
      authgroups {
        group crosswork {
+         umap cwuser {
+           callback-node /cw-creds-get;
+           action-name get;
+         }
        }
      }
    }
  }
}
cwuser@ncs(config-umap-cwuser)# commit
Commit complete.
```

構成後、authgroup は次のように表示されます。

```
cwuser@ncs# show running-config devices authgroups group crosswork
devices authgroups group crosswork
  umap admin
    remote-name      cisco
    remote-password  $9$LzskzrvZd7LeWwVNGZTdUBDdKN7IgvV/UkJebwM1eKg=
  !
  umap cwuser
    callback-node   /cw-creds-get
    action-name     get
  !
  !
```

次の内容を確認してください。

- umap が対象デバイスの既存の authgroup に追加されている。
 - umap で正しいユーザー名を使用している。
- 上記のいずれかが正しくない場合、実行時に問題が発生します。

Cisco Crosswork での DLM の設定

Cisco NSO で機能パックをインストールして設定した後、Cisco Crosswork の DLM で構成を設定する必要があります。これらの構成設定により、Change Automation が、新しく作成されたユーザーを介して Cisco NSO にアクセスし、必要に応じてオーバーライドされたログイン情報を使用して設定できるようになります。

ca_device_auth_nso ログイン情報プロファイルの作成

このガイドの「Cisco NSO での特別アクセスユーザーの作成」セクションで作成した特別アクセスユーザーの新しいログイン情報プロファイルを Cisco NSO で作成します。このログイン情報プロファイルに、ユーザーの HTTP ログイン情報と HTTPS ログイン情報を追加します。下のイメージは、ユーザー「cwuser」のユーザー名とパスワードを指定する画面です。

Profile Name * ca_device_auth_nso

Add Credential Protocols

Connectivity Type	User Name *	Password *	Confirm Password *	
HTTPS	cwuser	*****	*****	🗑️
Connectivity Type	User Name *	Password *	Confirm Password *	
HTTP	cwuser	*****	*****	🗑️

+ Add Another

Save Cancel

重要

ca_device_auth_nso ログイン情報プロファイルと共に、DLM に別のログイン情報プロファイルがあり、そのプロファイルにより、Cisco Crosswork の他の全コンポーネントに関して、Cisco NSO へのユーザー名/パスワード情報が指定されます。以下の例では、このログイン情報プロファイルが「nso-creds」と呼ばれています。

重要：通常の DLM ログイン情報プロファイルのユーザー名が、**ca_device_auth_nso** プロファイルのユーザー名と異なることを確認してください。

Profile Name * nso-creds

Add Credential Protocols

This username should be different from the username of the ca_device_auth_nso cred profile

Connectivity Type SSH User Name * admin Password * Confirm Password *

Enable Password

Connectivity Type TELNET User Name * admin Password * Confirm Password *

Enable Password

Connectivity Type NETCONF User Name * admin Password * Confirm Password *

Connectivity Type HTTP User Name * admin Password * Confirm Password *

+ Add Another

DLM プロバイダープロパティの追加

DLM でログイン情報プロファイルを作成した後、Crosswork CA で使用される DLM のすべての Cisco NSO プロバイダーにプロパティを追加する必要があります。下のイメージは、プロパティを指定する画面です。

Properties for nso

×

Property Key	Property Value
ca_device_auth_nso	ca_device_auth_nso

Make sure that property key and property value are both set to "ca_device_auth_nso"

トラブルシューティング

次の表に、発生する可能性のある一般的なエラーのリストを示します。

番号	エラー部分文字列	問題	対処法
1.	nso umap user must also be a nso credential profile user	ca_device_auth_nso ユーザー名がどの umap ユーザーにも一致しない。	1. umap を追加/修正します。 2. ca_device_auth_nso ログイン情報プロファイルを編集します。
2.	empty auth group umap from nso	Cisco NSO authgroup で umap が見つからない。	umap を追加します。
3.	failed to retrieve RESTCONF resource root. please verify NSO <IP> is reachable via RESTCONF	Crosswork CA が RESTCONF 経由で Cisco NSO に接続できなかった。	cw_device_auth_nso ログイン情報プロファイルで指定されたユーザー名/パスワードを使用して RESTCONF 経由で Cisco NSO に接続できることを確認します。
4.	Failed to set device override credentials in NSO, access denied (3): access denied	nso config 欠落している。tm-tc fp は、cli NED デバイスと Crosswork で動作する。	nso non-cisco モードで次の 2 つの設定を適用します。 <pre>set cisco-tm-tc-fp:cfp-configurations dynamic-device-mapping cisco-iosxr-cli-7.33:cisco-iosxr-cli-7.33 python-impl- class-name tm_tc_multi_vendors.IosXR</pre> <pre>set cisco-tm-tc-fp:cfp-configurations stacked-service-enabled</pre>

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。

リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。

あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)