



JATP環境構築マニュアル 07.MCM編

ジュニパーネットワークス株式会社

2019年1月25日

JUNIPER
NETWORKS | Engineering
Simplicity

はじめに

- ・本資料にある内容は、資料作成時点におけるものであり、事前の予告なしに内容を変更する場合があります。
- ・本資料は内容の正確さを保つために努めて作成しておりますが、本資料を利用することによって生じた損害について、当社は一切責任を負わないものとします。
- ・また、本資料の内容と公式情報との間に差分がある場合、公式情報を正としてお取り扱いください。
- ・本資料は下記のソフトウェア/サービスを用いてJATPのセットアップを行っています。
 - JATP(OVA版/OVF版) v5.0.4
 - ESXi/vCenter Server 6.0

更新履歴

バージョン	更新日	更新内容
1.0	2019/01/25	初版公開
1.1	2019/07/30	マニュアルのフォーマットを変更

アジェンダ

- MCM設定手順
- MCMコマンド一例
- 制限事項



MCM 設定手順

MCMの設定について

- MCM専用のLicenseが必要となります
※通常のCore/CM用LicenseではMCMはご利用いただけません。
- MCMは、Core/CMをMCMへ変換して使用します。
⇒Core/CMの設定方法は”01.JATP環境構築マニュアル(Core／CM)”を参照

MCM設定手順(MCM)

MCM

- ①MCMとして使用するCoreのCLIでcmモードに入る

```
Hostname-MCM:MCM# cm
```

- ②set mcmコマンドを入力(ローカルループバックアドレス、パスフレーズを指定)

```
Hostname-MCM:MCM# (cm) # set mcm ip 127.0.0.1 passphrase PASSPHRASE
```

確認コマンドなど

- ・ MCMの設定確認

```
Hostname-MCM:MCM# cm
```

```
Hostname-MCM:MCM# (cm) # show mcm
```

- ・ MCMの設定を削除する場合(MCMから通常のCoreへ戻す)

```
Hostname-MCM:MCM# cm
```

```
Hostname-MCM:MCM# (cm) # set mcm remove
```

※MCMの設定が完全に削除されます

MCM設定手順(MCM)

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health J-ATP Admin

Incidents Config

All Incidents (4 shown, 4 total)

Status	Risk	Threat	Progression	Collector Type	Threat Source	Threat Target	Target OS	Collector	Date & Time	CM Name	
New	HIGH	EICAR-TEST-SIGNATURE	DL	Web SRX	213.211.198.62	192.168.0.1	unknown	2 Collectors	May 30 15:02:38 GMT+0900	Sub-Core	
New	28	EICAR-TEST-SIGNATURE	DL	Web SRX	www.eicar.org	192.168.0.1	Windows NT 10.0	2 Collectors	May 29 18:21:39 GMT+0900	Sub-Core	
New	27	EICAR-TEST-SIGNATURE	DL	SRX	213.211.198.62	192.168.0.1	unknown	2 Collectors	May 29 11:39:13 GMT+0900	Sub-Core	
New	27	HIGH	EICAR-TEST-SIGNATURE	DL	SRX	213.211.198.62	192.168.0.1	unknown	Core HTTP Collector	May 28 17:39:56 GMT+0900	Sub-Core

MCMの設定後、Web UIの表示項目が変更される

Details for EICAR-TEST-SIGNATURE

SUMMARY DOWNLOADS

Target:

- Incident Id: 30
- Hostname: -
- Username: -
- IP Address: 192.168.0.1
- FQDN: 192.168.0.1
- Source Email ID: -
- Destination Email ID: -

Progression:

DELIVERY > EXPLOITATION & INSTALLATION > COMMAND & CONTROL > ACTION ON TARGETS

Phishing 0	Exploits 0	Downloads 26	Executions 0	Infections 0	Custom Rules 0	Lateral Spread 0
------------	------------	--------------	--------------	--------------	----------------	------------------

Triggers:

Reputation Behavior Network Static

Powered by Juniper Version 5.0.2.14 Content Version 5.0.2.9

Support | Resources | Contact Us

MCM設定手順(MCM)

The screenshot shows the Juniper Advanced Threat Prevention Appliance interface. The top navigation bar includes the logo, 'ADVANCED THREAT PREVENTION APPLIANCE', 'Refresh Data', 'System Health', and 'J-ATP Admin'. The main menu on the left is titled 'System Profiles' and lists various configuration options: Password Reset, Roles, Users, SAML Settings, RADIUS Settings, System Settings, Certificate Management, GSS Settings, Secondary CMs, Licensing, and Backup/Restore. A red box highlights the 'System Profiles' menu item. The central content area displays a configuration form with fields for 'Old Password' and 'New Password', and a 'Submit' button. A green callout box points to the form with the text 'Config画面もMCM用に表示変更される'. A yellow callout box contains the text 'MCMの設定は以上となります。つづいてMCMの管理化に置くCore/CMの設定を行うためCore/CMへアクセスします。' at the bottom of the configuration page.

Config画面もMCM用に表示変更される

MCMの設定は以上となります。
つづいてMCMの管理化に置くCore/CMの設定を行うため
Core/CMへアクセスします。

Powered by Juniper Version 5.0.2.14 Content Version 5.0.2.9

Support | Resources | Contact Us

MCM設定手順(CORE/CM)

The screenshot shows the ATP configuration interface with the following steps highlighted:

- ① Click the "Add New User" button.
- ② Click the "Users" link in the left sidebar.
- ③ Select the user account to be used for MCM communication.

The interface includes a navigation bar with "ADVANCED THREAT PREVENTION APPLIANCE", "Refresh Data", "System Health", and "J-ATP Admin". The left sidebar lists "Notifications", "System Profiles", "Password Reset", "Roles", "Zones", and "Users" (which is selected and highlighted with a red box). The main content area shows a table of users with columns: User Name, Full Name, Role Name, and Email. A green callout box points to the "Add New User" button with the instruction ① クリック (Click). Another green callout box points to the "Users" link in the sidebar with the instruction ② クリック (Click). A large green box at the bottom right contains the instruction ③ MCMとの通信に使用するユーザーを選択 (Select the user to be used for MCM communication).

User Name	Full Name	Role Name	Email
admin	J-ATP Admin	Admin Role	

MCM設定手順(CORE/CM)

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health J-ATP Admin

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

Notifications System Profiles 0+ Password Reset Roles Zones

Users SAML Settings RADIUS Settings System Settings Certificate Management GSS Settings Web Collectors SRX Settings Email Collectors Secondary Cores

User Name: admin Full Name: J-ATP Admin Admin: yes Role Name: Default Admin Role Email:

Add New User

Update User

User Name	Full Name	Role	Email
admin	J-ATP Admin	Default Admin Role	

New Password: Repeat Password: Generate New API Key

Update User Delete User Cancel

① チェックを入れる
② クリック

Powered by Juniper Version 5.0.2.14 Content Version 5.0.2.9

Support | Resources | Contact Us

MCM設定手順(CORE/CM)

MCM管理下に置くCore

- ①管理下に置くCoreのCLIでcmモードに入る

```
Hostname-Core:Core# cm
```

- ②set mcmコマンドを入力 (MCMのIPアドレス、MCMで設定したパスフレーズ、MCMと通信するユーザーの指定)

```
Hostname-Core:Core# (cm) # set mcm ip xxxx.xxxx.xxxx.xxxx passphrase PASSPHRASE username USERNAME
```

確認コマンドなど

- ・ MCMの設定確認

```
Hostname-Core:Core# cm
```

```
Hostname-Core:Core# (cm) # show mcm
```

- ・ MCMの設定を削除

```
Hostname-Core:Core# cm
```

```
Hostname-Core:Core# (cm) # set mcm remove
```

- ・ CoreとMCMを再同期させる

```
Hostname-Core:Core# cm
```

```
Hostname-Core:Core# (cm) # set mcm resync
```

- ・ SIEM logをMCM経由で送る

```
Hostname-Core:Core# cm
```

```
Hostname-Core:Core# (cm) # set mcm SIEM-redirect enable on
```



MCM コマンド一例

MCMコマンド一例

CLI画面で設定の確認・変更を行う際は、各モードに入る必要があります

cm	Central Managerの設定変更・確認 (MCMの設定、JATPソフトウェアのアップグレードなど)
diagnosis	Diagnosisの設定やステータス確認
exit	CLIセッションを終了
help	使用可能なSyntax一覧の表示
history	現在のセッションでのコマンド履歴の表示
server	Serverの設定変更・確認 (UUIDの確認、Pingの送信、サーバー設定の変更、サーバーの再起動など)
wizard	Wizardを起動して再設定

MCMコマンド一例

- ・インターフェース情報の確認

```
Hostname-MCM:MCM# server
Hostname-MCM:MCM#(server)# show interface
Interface: management (eth0) Enabled: Yes Link: Yes
  IP Address: 172.27.112.98 Mask: 255.255.252.0 MTU: 1500
  MAC Address: 00:50:56:b4:f5:5d Speed: 10000Mb/s Duplex: Full
  Auto-negotiation: No Medium: Copper
  RX packets: 10238 Bytes: 1417570 Errors: 0 Overruns: 0
  TX packets: 1760 Bytes: 975221 Errors: 0 Overruns: 0
  Traffic rate for the last 5 seconds/1 minute/5 minutes
    RX bits/sec: 41472/41576/19592
    RX packets/sec: 34/33/15
    TX bits/sec: 35584/39792/18920
    TX packets/sec: 6/7/3
```

- ・ソフトウェアとコンテンツのバージョン確認

```
Hostname-MCM:MCM# server
Hostname-MCM:MCM#(server)# show version
Software: 5.0.4.25
Content: 5.0.4.17
```

MCMコマンド一例

- ・タイムゾーンの設定

```
Hostname-MCM:MCM# server  
Hostname-MCM:MCM#(server)# set timezone Asia/Tokyo
```

- ・NTPサーバーの設定

```
Hostname-MCM:MCM# server  
Hostname-MCM:MCM#(server)# set ntpserver  
Change the ntp server settings? (Yes/No)? yes  
Enter the new ntp server name: xxxx.xxxx.xxxx.xxxx
```

- ・UUIDの確認

```
Hostname-MCM:MCM# server  
Hostname-MCM:MCM#(server)# show uuid  
System UUID: 42341181-EBAA-69C4-807E-961A154536B2
```

- ・Pingの送信

```
Hostname-MCM:MCM# server  
Hostname-MCM:MCM#(server)# ping xxxx.xxxx.xxxx.xxxx
```

- ・サーバーのシャットダウン

```
Hostname-MCM:MCM# server  
Hostname-MCM:MCM#(server)# shutdown
```

MCMコマンド一例

- ・IPアドレスの個別設定

```
Hostname-MCM:MCM# server
Hostname-MCM:MCM#(server)# set ip interface management
Use DHCP to obtain an IP address for management (eth0) interface (Yes/No)? yes / no
Enter IP address for the management (eth0) interface: xxxx.xxxx.xxxx.xxxx
Enter netmask for the management (eth0) interface: xxxx.xxxx.xxxx.xxxx
Enter gateway IP Address for the management (eth0) interface: xxxx.xxxx.xxxx.xxxx
```

- ・CMの指定

```
Hostname-MCM:MCM# server
Hostname-MCM:MCM#(server)# set cm 127.0.0.1
```

- ・CLIログインパスワードの変更

```
Hostname-MCM:MCM# server
Hostname-MCM:MCM#(server)# set password
Enter the current password of CLI admin: 現在のパスワード
Enter the new password of CLI admin: 新しいパスワード
Retype the new password of CLI admin: 新しいパスワードを再入力
```

- ・CLIタイムアウト時間の設定

```
Hostname-MCM:MCM# server
Hostname-MCM:MCM#(server)# set cli timeout 0 (秒単位 : 0=タイムアウトなし)
```

MCMコマンド一例

- ・セットアップチェック

```
Hostname-MCM:MCM# diagnosis  
Hostname-MCM:MCM# (diagnosis) # setupcheck all / report / basic / analysis
```

- ・パケットキャプチャー

```
Hostname-MCM:MCM# diagnosis  
Hostname-MCM:MCM# (diagnosis) # capture-start
```

- ・キャプチーファイルのコピー

```
Hostname-MCM:MCM# diagnosis  
Hostname-MCM:MCM# (diagnosis) # copy capture user@hostname:path
```

- ・接続デバイスのステータス確認

```
Hostname-MCM:MCM# diagnosis  
Hostname-MCM:MCM# (diagnosis) # show device collectorstatus / corestatus / slavecorestatus
```



制限事項

制限事項

- MCMは管理下のCoreへリアルタイムに情報を受け取りに行くため、以下のような場合は情報を受け取ることができずエラー表示がでます。
 - Coreへアクセスできない場合
[Couldn't get incident details: server request failed with HTTP status 503.]
 - Coreが自身のデータベースをクリアした場合
[Couldn't get incident details: no incident id.]



THANK YOU

JUNIPER
NETWORKS | Engineering
Simplicity