



# Cisco SD-WAN Cloud onRamp for Colocation ソリューションのトラブルシューティング

- [コロケーションマルチテナント機能の問題のトラブルシューティング \(1 ページ\)](#)
- [Catalyst 9500 の問題のトラブルシューティング \(2 ページ\)](#)
- [Cisco Cloud サービスプラットフォームの問題のトラブルシューティング \(8 ページ\)](#)
- [DHCP IP アドレス割り当て \(16 ページ\)](#)
- [Cisco Colo Manager の問題のトラブルシューティング \(17 ページ\)](#)
- [サービスチェーンの問題のトラブルシューティング \(19 ページ\)](#)
- [物理ネットワーク機能管理の問題のトラブルシューティング \(21 ページ\)](#)
- [CSP からのログ収集 \(22 ページ\)](#)
- [Cisco vManage の問題のトラブルシューティング \(22 ページ\)](#)

## コロケーションマルチテナント機能の問題のトラブル シューティング

次のコマンドを使用して、出力を表示し、問題を特定できます。

- 存在するブリッジなど、各 VNF の VNIC と VLAN の概要を表示するには、`support ovs vsctl show` コマンドを使用します。

```
nfvis# support ovs vsctl show
```

- ブリッジ、ネットワーク、または VLAN を使用したサービスチェーンの展開の詳細を確認するには、`show service-chains` コマンドを使用します。
- コロケーションクラスタ内の CSP デバイスとピア CSP デバイスのデータと HA VTEP IP アドレスを表示するには、`show cluster-compute-details` コマンドを使用します。
- 各 HA ブリッジの送信元および宛先のシリアル番号と、対応する VLAN および VNID の関連付けを表示するには、`show vxlan tunnels` コマンドを使用します。
- VLAN のユーザー ID、VNID マッピングによって識別できるテナントごとのデータフローを表示するには、`show vxlan flows` コマンドを使用します。

- VXLAN フロー統計を表示するには、`support ovs ofctl dump-flows vxlan-br` コマンドを使用します。
- VM ライフサイクルの全体的な展開ステータスを表示するには、`show vm_lifecycle deployments` コマンドを使用します。

### エンドツーエンドの Ping が失敗する

1. `show vm_lifecycle deployments all` コマンドを使用して、VM が展開されているかどうかを確認します。
2. `show service-chains` コマンドを使用して、サービスチェーンに接続されているチェーン名が表示されることを確認します。
3. `show notification stream viptela` を使用して、Cisco SD-WAN デバイスで発生したイベントに関する通知を確認します。
4. `show cluster-compute-details` コマンドを使用して、CSP ピアデバイスの `data-vtep-ip` と `ha-vtep-ip` に ping を実行します。
5. ブリッジ、ネットワーク、または VLAN ごとの VLAN の関連付けが、各 VNF の VNIC および VLAN と一致していることを確認します。`show service-chain chain-name` コマンドの出力が `support ovs vsctl show` コマンドの出力と一致することを確認します。
6. 接続に失敗し、ピア CSP デバイスに ping できない場合は、テクニカルサポートにお問い合わせください。

## Catalyst 9500 の問題のトラブルシューティング

ここでは、一般的な Catalyst 9500 の問題とそのトラブルシューティング方法について説明します。

### 一般的な Catalyst 9500 の問題

#### スイッチデバイスが PNP または Cisco Colo Manager にコールホームしていない

Cisco Colo Manager の PNP リストを確認して、スイッチデバイスがコールホームしていないかどうかを判断します。次に、`show pnp list` コマンドを使用した場合の良いシナリオと悪いシナリオをそれぞれ示します。

#### デバイスがコールホームした

```
admin@ncs# show pnp list
SERIAL IP ADDRESS CONFIGURED ADDED SYNCED LAST CONTACT
-----
FCW2223A3VN 192.168.10.40 true true true 2018-12-18 22:53:26
FCW2223A4B3 192.168.30.42 true true true 2018-12-11 00:41:19
```

#### デバイスがコールホームしていない

```
admin@ncs# show pnp list
```

```
SERIAL IP ADDRESS CONFIGURED ADDED SYNCED LAST CONTACT
```

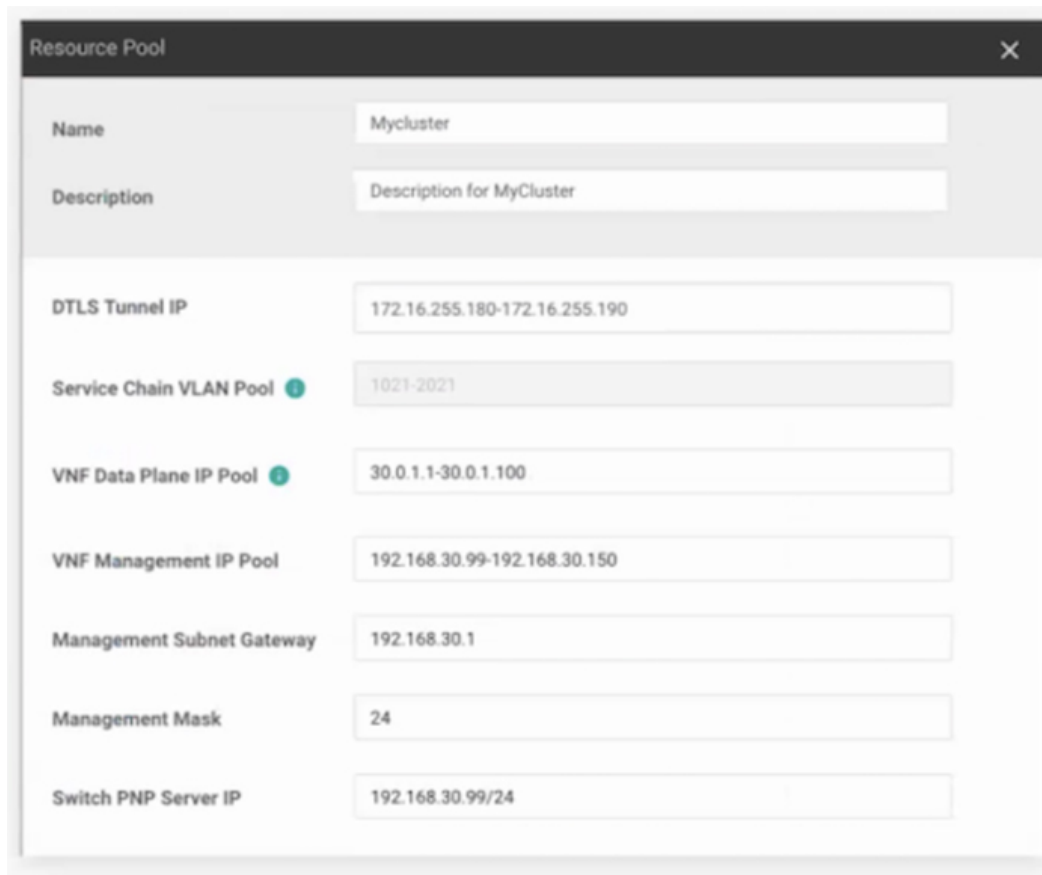
<- 空のリスト

Action:

1. 両方のスイッチの管理インターフェイスがシャットダウンされておらず、IPアドレスがあることを確認します。
2. スイッチで **write erase** コマンドを実行してから、リロードしてみます。IPアドレスが管理インターフェイスに表示されることを確認します。
3. DHCP オプション43の構成が有効であることを確認します。PNP IP アドレスが 192.168.30.99 であるサンプル DHCP 構成を次に示します。

```
ip dhcp pool 192_NET network 192.168.30.0 255.255.255.0 dns-server 192.168.30.1
default-router 192.168.30.1 option 43 ascii "5A;B2;K4;I192.168.30.99;J9191" lease
infinite
```

4. 次のように、リソースプールの Cisco vManage で提供される PNP IP アドレスが DHCP 構成の IP アドレスと一致することを確認します。



Field	Value
Name	Mycluster
Description	Description for MyCluster
DTLS Tunnel IP	172.16.255.180-172.16.255.190
Service Chain VLAN Pool	1021-2021
VNF Data Plane IP Pool	30.0.1.1-30.0.1.100
VNF Management IP Pool	192.168.30.99-192.168.30.150
Management Subnet Gateway	192.168.30.1
Management Mask	24
Switch PNP Server IP	192.168.30.99/24

5. ping を実行して、両方のスイッチに到達可能かどうかを確認します。

### Catalyst 9500 は DHCP オプション 43 を使用して到達できなかった

ここで、Cisco Colo Manager はホスト側で正常な状態にあり、Cisco Colo Manager の内部状態は進行中です。クラスタがすでにアクティブ化されている場合は、クラスタがアクティブ化保留状態にあることを示します。クラスタがアクティブ化されていない場合は、クラスタがアクティブ化されていない状態であることを示します。

Action:

1. 管理ユーザーとしてNFVISにSSHで接続します。`ccm-console` コマンドを使用して、Cisco Colo Manager にログインします。`show pnp list` コマンドを実行します。
2. PNP リストが空の場合は、OOB スイッチで Cisco Colo Manager の IP アドレスが正しく設定されているかどうかを OOB ステータスで確認します。

### Day-0 構成のプッシュが両方の Catalyst 9500 スイッチで失敗した

ここで、Cisco Colo Manager はホスト側で正常な状態にあり、Cisco Colo Manager の内部状態は進行中です。PnP 構成のプッシュはエラーで失敗し、Cisco Colo Manager は進行中の状態です。

Action:

1. `renumber` コマンドと `write erase` コマンドを使用して、Catalyst 9500 スイッチをクリーニングします。
2. Cisco vManage からクラスタを非アクティブ化してから再度アクティブ化して、Day-0 構成を再プッシュします。

### セカンダリ Catalyst 9K スイッチで Day-0 構成のプッシュが失敗する

ここで、Cisco Colo Manager はホスト側で正常な状態にあり、Cisco Colo Manager の内部状態は「Failure」を示しています。Cisco Colo Manager は、1つのスイッチのみが正常に起動し、セカンダリスイッチの障害を検出できないことを示しています。

Action:

1. `renumber` コマンドと `write erase` コマンドを使用して、セカンダリ Catalyst 9500 スイッチをクリーニングします。
2. vManage からクラスタを非アクティブ化してから再度アクティブ化して、Day-0 構成を再プッシュします。

### Catalyst9500 スイッチの1つが稼働している。セカンダリスイッチがSVL構成になっておらず、SVL リンクケーブルが接続されていない

ここで、Cisco Colo Manager はホスト側で正常な状態にあり、Cisco Colo Manager の内部状態は「Failure」を示しています。どちらのスイッチも IP アドレスを使用してオンボードされています。スイッチの SVL リンクが見つからないため、Cisco Colo Manager は両方のスイッチが接続されているときにエラーを検出します。Cisco vManage で両方のスイッチが「緑」として表示されます。

Action:

1. SVL リンクケーブルを確認します。
2. 両方の Catalyst 9500 スイッチのライセンスを確認します。

### Day-0 構成のプッシュが失敗し、スイッチへの接続がダウンしている

ここで、Cisco Colo Manager はホスト側で正常な状態にあり、Cisco Colo Manager の内部状態は、次の Day-0 構成プッシュまで「Failure」と表示されます。NSO は、構成をプッシュできないという通知を送信します。Cisco vManage でスイッチが「赤」として表示されます。これは、接続がダウンしていることを意味します。

Action:

1. Catalyst 9500 スイッチの正常性を確認します。
2. スイッチをオンラインに戻します。
3. Day-0 構成のプッシュを再開します。

### Cisco vManage から PNP 後に Catalyst 9500 にログインできない

PNP の後、Cisco vManage が Catalyst 9500 にさらに構成をプッシュできない場合は、スイッチからロックアウトされている可能性があります。

Action:

1. ログイン名として **admin** を使用し、デフォルトのパスワードとして **Admin123 #** を使用して、NFVIS にログインします。



---

(注) 初めてログイン試行すると、デフォルトのパスワードを変更するように求められます。画面の指示に従って強力なパスワードを設定してください。

---

2. Cisco NFVIS で **ccm console** コマンドを使用して、Cisco Colo Manager にログインします。Cisco Colo Manager で次のコマンドを実行して、ユーザーを Catalyst 9500 スイッチに追加します。

```
• config t
  cluster <cluster-name>
  system rbac users user admin password
  $9$yYkZqj7lQcrRL3$sZ23jqv5buK4lYCkt0dCbO6xYefxRHQJiQnr1FdYHBg
```



---

(注) パスワードは必ずスクリプト文字列として設定してください。

---

これで、対応するユーザーが Catalyst 9500 スイッチに追加され、ユーザーとパスワードを使用してスイッチに SSH で接続できます。

クラスタのアクティブ化の問題、管理者およびパスワードを **Catalyst 9500** にプッシュできない

Action:

1. クラスタのアクティブ化がまだ保留状態の場合は、colo-config-status が進行中状態であるかどうかを確認します。状態が進行中の場合、同期は行われておらず、新しい構成をプッシュできません。このプロセスには最大 20 分かかります。
  1. CloudOnRamp for Colocation の構成ステータスが長時間進行中の状態になっている場合は、管理者ユーザーとして NFVIS に SSH で接続します。 **ccm-console** コマンドを使用して、Cisco Colo Manager にログインします。 **show pnp list** コマンドを実行します。2 つのスイッチが追加されているかどうかを確認します。
  2. スイッチが 1 つしか表示されない場合は、 **write erase** コマンドを使用して他のスイッチ構成が消去され、リロードされていることを確認してください。セカンダリスイッチのスタートアップ構成を消去して、初期状態に戻す必要があります。
  3. Cisco Colo Manager の PNP サーバーとのスイッチ接続を確認します。
2. クラスタが正常にアクティブ化されている場合は、colo-config-status が「SUCCESS」状態であるかどうかを確認します。ステータスが Success と表示されている場合は、管理者パスワードがスイッチにプッシュされている必要があります。そうでない場合は、Cisco vManage で新しいログイン情報をスイッチに追加してから、新しい構成をプッシュします。
3. クラスタのアクティブ化が失敗し、colo-config-status が「FAILED」状態の場合は、RBAC を使用して ccm コンソールから新しい認証をプッシュします。次の例では、パスワードは「Cisco-123」の暗号化です。

```
cluster cluster system rbac users user Alpha password
$9$Z9Sr2VOuwjwC74$qEYAmxgoaW4m07.UjPGR9gL2ksFkcCIcIcEYOUWxDfo role
administrators
```



(注) クラスタがアクティブ状態の場合、RBAC 構成をプッシュすることはできません。Cisco vManage は、Cisco Colo Manager への境界外の変更を許可しません。

スイッチの構成を消去し、スイッチを工場出荷時のデフォルトにリセットする

クラスタの作成、クラスタのクリア、クラスタの削除中に、両方のスイッチの設定を消去する必要があります。クラスタ構成を消去するには、次の手順を実行します。

Action:

1. **show switch** コマンドを使用して、スイッチ番号とスイッチスタックにプロビジョニングされたスイッチが存在するかどうかを特定します。スイッチ番号が 2 の場合は、 **switch 2 renumber 1** コマンドを使用します。



(注) スイッチの再番号付けは、SVL スタックモードに不可欠です。

2. スイッチのスタートアップ構成を消去して初期状態に戻すには、**write erase** コマンドを使用します。
3. 新しい構成でスイッチをリロードするには、特権 EXEC モードで次のコマンドを使用し、変更した構成を保存しない場合は **n** を入力します。

```
switch(config)#reload
```

4. 最初のスイッチでスイッチスタックのリロードが完了したら、2 番目のスイッチデバイスで手順 2 と 3 を実行します。

Cisco Colo Manager からのスイッチデバイスの追加を確認するには、次の手順を実行します。

1. Cisco Colo Manager にログインし、**show pnp list** コマンドを使用します。

2 つのスイッチデバイスが表示されます。PNP は、Day-0 構成をプッシュし、スイッチデバイスを Cisco Colo Manager デバイスツリーに追加し、デバイス構成を Cisco Colo Manager と同期します。いずれかのスイッチデバイスを表示できない場合は、見つからないスイッチデバイスの PNP が正しく構成されていないか、ネットワークがダウンしている可能性があります。

スイッチにプッシュされた SVL 構成は、リポート後にスイッチにリポートコマンドを発行します。両方のスイッチデバイスが起動し、1 つのスタックになります。

2. Cisco Colo Manager で、約 14 分のタイマーをトリガーして、プライマリデバイスで別の同期を実行します。
3. デバイス構成と現在のステータスを表示するには、**show cluster cluster-name** コマンドを使用します。

ステータスが「GREY」と表示されている場合、スイッチデバイスはまだ Cisco Colo Manager のデバイスリストに追加されていません。ステータスが「RED」と表示されている場合、スイッチデバイスに到達できません。ステータスが「GREEN」と表示されている場合、デバイスは現在接続されています。また、プライマリスイッチデバイスを表示することもできます。

4. コロケーション内のデバイスステータスを表示するには、**show colo-config-status** コマンドを使用します。ステータスが「In-progress」の場合、スイッチデバイスはまだ同期されておらず、Cisco vManage はそれ以上の構成を送信できません。Cisco Colo Manager の状態遷移の詳細については、[Cisco SD-WAN Cloud onRamp for Colocation ソリューションデバイスのモニタリング](#)の章を参照してください。

タイマーがその時間（たとえば、14 分）に達すると、Cisco Colo Manager は、プライマリ Catalyst 9500 デバイスとの再同期を試みます。

2 回目の同期が完了すると、Cisco Colo Manager の状態が「SUCCESS」と表示されます。

### QoS ポリシー適用後のスイッチの構成

QoS ポリシーが適用されている場合、サービスチェーンの帯域幅を設定して展開すると、次の構成がスイッチデバイスに表示されます。

```
class ASAvOnly_chain1_VLAN_210police 2000000000class ASAvOnly_chain1_VLAN_310police
2000000000policy-map
service-chain-qosclass ASAvOnly_chain1_VLAN_210police 2000000000class
ASAvOnly_chain1_VLAN_310police 2000000000
```

## Cisco Cloud サービスプラットフォームの問題のトラブルシューティング

ここでは、一般的なクラウドサービスプラットフォーム（CSP）の問題とそのトラブルシューティング方法について説明します。

### Cisco CSP デバイスの RMA

Cisco vManage から CSP デバイスの **admin tech** コマンドを使用し、**[Tools] > [Operational Commands]**画面でデバイスのログ情報を収集します。次のログファイルを確認します。

- `nfvis_config.log` : デバイス構成関連のログを表示します
- `escmanager.log` : VM 展開関連のログを表示します。
- `Tech-support-output` : CSP デバイスから利用できる次の `show` コマンドを使用します。
  - `cat/proc/mounts` : マウント情報を表示します
  - `show hostaction backup status` : CSP デバイスで実行された最新の 5 つのバックアップのステータスを表示します
  - `show hostaction restore-status` : 全体的な復元プロセスと、デバイス、イメージとフレージャー、VM などの各コンポーネントのステータスを表示します
  - `show vm_lifecycle deployments` : 展開名と VM グループ名を表示します。

次に、NFS サーバーでのマウント操作の例を示します。

```
nfvis# show running-config mount
mount nfs-mount storage sujathast/
storagetype nfs
storage_space_total_gb 5000.0
server_ip 192.168.0.1
server_path /NFS/colobackup
```

次に、最新の 5 つのバックアップ操作の操作ステータス出力と、最新のバックアップに関する Cisco vManage の通知の例を示します。

```
eventTime 2021-02-02T04:02:25.577705+00:00
viptela
severity-level minor
host-name nfvis
```



```
system-ip 10.0.0.1
user_id admin
config_change false
transaction_id 0
status SUCCESS
status_code 0
status_message Backup configuration-only to nfs:test_storage/test_config_only.bkup
completed successfully with operational status: BACKUP-COMPLETED-PARTIALLY
details NA
event_type BACKUP_SUCCESS
severity INFO
host_name nfvis
!
```

次の例は、`show hostaction restore-status` コマンドを使用した後のデバイスのステータスを示しています。

```
nfvis# show hostaction restore-status
hostaction restore-status 2021-03-19T20:53:15-00:00
source nfs:sujathast/WZP22160NC7_2021_03_19T19_10_04.bkup
status RESTORE-ERROR
components NFVIS
status RESTORE-ERROR
last update 2021-03-19T21:02:11-00:00
details "Unable to load configuration Editing of storage definitions is not allowed"
components nfs:sujathast/WZP22160NC7_2021_03_19T19_10_04.bkup
status VERIFICATION-SUCCESS
```

## VNIC および PNIC のステータスのクリア

1. PNIC 統計を表示するには、`show pnice stats` コマンドを使用します。
2. VNIC 統計を表示するには、次のいずれかのコマンドを使用します。
  - すべての VM に対して `show vm_lifecycle vnic_stats`
  - 単一の VM に対して `show vm_lifecycle vnic_stats vm-name`

3. 1 つ以上の VM の統計をクリアするには、次のコマンドを実行します。

```
clear counters vm all
clear counters vm vm-name vnic vnic-id
clear counters vm vm-name vnic all
```

4. すべての PNIC および VNIC の統計をクリアするには、`clear counters all` コマンドを使用します。

CSP をリブートすると、すべての PNIC および VNIC のカウンタが消去され、カウンタがクリアされます。VNIC と PNIC の統計が表示されない場合は、次のコマンドを使用して統計を表示できます。

```
show pnice-clear-counter
show vm_lifecycle tx_rx_clear_counters
```

## Cisco CSP デバイスのオンボーディングの問題

1. デバイスが SD-WAN コントローラとのセキュアな制御接続を確立したことを確認するには、`show control connections` コマンドを使用します。

2. デバイスの認証に使用されるデバイスプロパティを確認するには、**show control local-properties** コマンドを使用します。

表示された出力から、次のことを確認します。

- システムパラメータは、**organization-name** と **site-id** を含むように設定されている
- **certificate-status** および **root-ca-chain-status** がインストールされている
- **certificate-validity** が [Valid] になっている
- **dns-name** が vBond IP アドレスまたは DNS を指している
- **system-ip** が構成され、**chassis-num/unique-id** および **serial-num/token** がデバイスで使用可能

3. デバイスが Cisco SD-WAN コントローラとの接続を確立できない場合、失敗の理由を表示するには、**show control connections-history** コマンドを使用します。[LOCAL ERROR] および [REMOTE ERROR] 列を表示して、エラーの詳細を収集します。

Cisco CSP デバイスが Cisco SD-WAN コントローラとの制御接続を確立できない理由は次のとおりです。

- **CRTVERFL** : エラー状態は、デバイスと Cisco SD-WAN コントローラ間のルート CA 証明書の不一致が原因で、デバイスの認証が失敗したことを示します。Cisco CSP デバイスで **show certificate root-ca-cert** を使用して、デバイスと Cisco SD-WAN コントローラに同じ証明書がインストールされていることを確認します。
- **CTORGNMMIS** : エラー状態は、Cisco SD-WAN コントローラで設定された組織名と比較して、組織名が一致しないためにデバイスの認証が失敗したことを示します。CSP デバイスで **show sdwan control local-properties** を使用して、すべての SD-WAN コンポーネントが同じ組織名で構成されていることを確認します。
- **NOVMCFG** : エラーステータスは、デバイスが Cisco vManage のデバイステンプレートにアタッチされていないことを示します。このステータスは、自動展開オプション (PnP) を使用してデバイスをオンボーディングするときに表示されます。
- **VB\_TMO**、**VM\_TMO**、**VP\_TMO**、**VS\_TMO** : このエラーは、デバイスが Cisco SD-WAN コントローラに到達できないことを示します。

### クラスタのアクティブ化の失敗

CCM で、CCM 通知ステータスを表示して、スイッチの SVL 形成が完了し、デバイスがオンボードされているかどうかを確認します。

1. すべての SR-IOV および OVS ポートが Catalyst 9500 スイッチに正しくケーブル接続されていて、インターフェイスがリンクアップ状態になっていることを確認します。
2. CSP デバイスで **show lldp neighbors** コマンドを使用し、CSP デバイスと Catalyst 9500 スイッチ間の配線を確認して、SR-IOV および OVS ポートを特定します。

**show lldp neighbors** コマンドで 8 つのポートすべてに電源が入っていることが表示され、ネイバーについて報告されることを確認します。

- Catalyst 9500 スイッチが SVL モードであり、インターフェイスに「SVL Complete」という説明があることを確認します。

#### 証明書のインストールの失敗

**show control connections-history** コマンドを使用して、証明書のインストールの失敗を判別します。

図 1: 証明書のインストールの失敗

PEER TYPE	PEER PROTOCOL	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER PRIVATE IP	PEER PUBLIC IP	PEER LOCAL	PEER PUBLIC	LOCAL COLOR	STATE	LOCAL ERROR	REMOTE ERROR	REPEAT COUNT	DOWN TIME
vBond	dtls	0.0.0.0	0	0	172.23.191.87	13344	172.23.191.87	13344	default	tear_down	DISCVBO	NOERR	0	2018-12-20T03:13:20+0000
vBond	dtls	0.0.0.0	0	0	172.23.191.87	13344	172.23.191.87	13344	default	up	RXTXDN	VCRTREV	0	2018-12-20T03:12:04+0000
vManage	dtls	172.16.255.200	100	0	172.23.191.86	13444	172.23.191.86	13444	default	up	RXTXDN	VCRTREV	0	2018-12-20T03:12:04+0000
vManage	dtls	172.16.255.200	100	0	172.23.191.86	13444	172.23.191.86	13444	default	tear_down	SVSIPCHG	NOERR	0	2018-12-20T03:12:30+0000
vBond	dtls	0.0.0.0	0	0	172.23.191.87	13344	172.23.191.87	13344	default	tear_down	SVSIPCHG	NOERR	0	2018-12-20T03:12:30+0000

Action:

発生する可能性のあるエラーに基づいて実行できる検証は次のとおりです。

- vBond with error SERNTPRES : このエラーは、デバイスのシリアルまたはトークンが vBond のシリアルまたはトークンと一致しない場合に発生します。vManage をチェックして、デバイスが「有効」な状態であり、適切にデコミッションされたことを確認します。
- Cisco vManage with error NOVMCFG : このエラーは、テンプレートがデバイスに接続されていない場合に発生します。クラスタをアクティブ化すると、この問題が解決します。
- vBond で、**show orchestrator valid-vedges** コマンドがデバイスを正しく表示することを確認します。これは、使用したトークンと同じトークンでデバイスが有効であることを意味します。
- Cisco vManage および CSP デバイスのクロックが同期していることを確認します。

#### 制御接続の失敗

**show control connections-history** で DCONFAIL が表示されます。ファイアウォールを開いて、開く必要があるポートを表示します。

図 2: 制御接続の失敗、**DCONFAIL**

INSTANCE	PEER TYPE	PEER PROTOCOL	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER PRIVATE IP	PEER PRIVATE PORT	PEER PUBLIC IP	PEER PUBLIC PORT	REMOTE COLOR	STATE	ORGANIZATION NAME	UPTIME
0	vmanage	dtls	209.165.202.129	4294958113	0	209.165.201.1	12346	209.165.201.1	12346	default	up	JamesLo_honeywell - 3853220:00:00:03	
0	vmanage	dtls	209.165.202.129	4294958113	0	209.165.201.1	12446	209.165.201.1	12446	default	up	JamesLo_honeywell - 3853220:00:00:03	
0	vmanage	dtls	209.165.202.129	4294958113	0	209.165.201.1	12546	209.165.201.1	12546	default	up	JamesLo_honeywell - 3853220:00:00:02	
0	vmanage	dtls	209.165.202.129	4294958113	0	209.165.201.1	12646	209.165.201.1	12646	default	up	JamesLo_honeywell - 3853220:00:00:02	
0	vmanage	dtls	209.165.202.129	4294958113	0	209.165.201.1	12746	209.165.201.1	12746	default	up	JamesLo_honeywell - 3853220:00:00:03	

Action:

次のポートが開いている必要があります。

表 1: 開く **UDS** および **TCP** ポート

コア番号	DTLS (UDP) のポート	TLS (TCP) のポート
Core0	12346	23456
Core1	12446	23556
Core2	12546	23656
Core3	12646	23756
Core4	12746	23856
Core5	12846	23956
Core6	12946	24056
Core7	13046	24156

### CSP に DHCP IP アドレスがない

CSP デバイスは、接続されたデバイスとして Cisco vManage に表示されません。

Action:

1. CIMC インターフェイスを使用して CSP に接続します。
2. Cloud OnRamp for Colocation 管理ポートで **show system:system settings** コマンドを実行して、CSP に IP アドレスがあるかどうかを確認します。
3. DHCP サーバーに IP アドレスがあるかどうかを確認します。静的 IP アドレスを割り当てて DHCP スティック IP を設定するには、[DHCP IP アドレス割り当て \(16 ページ\)](#) を参照してください。
4. ping を使用して、PNP サーバーに到達可能であることを確認します。
5. PNP サーバーから、CSP デバイスに接続して要求できるかどうか、またはリダイレクトが成功するかどうかを確認します。PNP ポータルで、デバイスの保留中のリダイレクトが表示されている場合は、シリアル番号が CSP デバイスと同じかどうかを確認します。
6. CSP で **show platform-details** コマンドを使用して、シリアル番号を確認します。
7. PNP ポータルで、接続済みと表示されているかどうかを確認します。

## CSP が Cisco vManage との接続を確立していない

CSP デバイスは、接続されたデバイスとして Cisco vManage に表示されません。

Action:

1. **show certificate installed** および **show certificate root-ca-cert** を使用して、CSP デバイスに PNP からインストールされたルート CA があるかどうかを確認します。
2. CSP が vBond IP アドレスに ping できるかどうかを確認します。次に、**show running-config viptela-system:system** を使用して vBond IP を取得します
3. vBond への ping が失敗した場合は、管理インターフェイスでネットワーク接続を確認します。
4. vBond への ping が通る場合は、**running-config vpn 0** を使用して、制御接続の構成を表示します。
5. 制御接続構成が存在する場合は、Cisco vManage 設定を確認します。
6. Cisco vManage で、**show control connections** および **show control local-properties** コマンドを使用して、クラスタがアクティブ化され、デバイスの OTP 情報が含まれているかどうかを確認します。
7. **request vedge-cloud activate chassi-number token-number** コマンドを使用して、CSP トークン番号が手動で入力されているかどうかを確認します。正しい OTP を使用してコマンドを再実行します。

## CSP デバイスの工場出荷時設定へのリセット

CSP デバイスを工場出荷時のデフォルトにリセットするには、次のコマンドを使用します。

### CSPxx# factory-default-reset all

このコマンドは、VM とボリューム、ログ、通知、イメージ、証明書などのファイルを削除します。すべての設定を削除します。接続が切断され、管理者パスワードが工場出荷時のデフォルトパスワードに変更されます。リセット後、システムは自動的にリブートします。出荷時設定へのリセットが進行中の 15～20 分間は、何も操作を実行しないでください。工場出荷時設定へのリセットプロセスを続行するように求められたら、続行できます。

## ストレージディスクが不良な CSP

制御接続が確立され、クラスタがアクティブ化されます。Cisco vManage モニタリング画面には、使用可能な 8 つの CSP ディスクすべてと、障害のあるディスクの 1 つが表示されます。

Action:

不良ディスクを交換します。

### CSP デバイスのメモリまたは CPU が少ない

制御接続が確立され、クラスタがアクティブ化されます。Cisco vManage モニタリング画面に、メモリのしきい値に達したことが表示されます。

Action:

最小要件に一致する特定の CSP デバイスをアップグレードします。

### CSP デバイスの I/O カードが間違っただスロットにある

Action:

CIMC インベントリからスロットの詳細を確認します。

### Colo Manager が CSP デバイスで正常でない

Action:

1. Cisco Colo Manager の状態を確認するには、次の手順を実行します。
  1. **show container ColoMgr** コマンドを使用して、コンテナの正常性を確認します。  
『[Cisco Colo Manager の問題のトラブルシューティング \(17 ページ\)](#)』を参照してください。
  2. **show notification stream viptela** コマンドを使用して、Viptela デバイスからのイベントに関する通知を表示します
2. Cisco Colo Manager にアクセスするには、Cisco Colo Manager が有効になっている CSP デバイスで **ccm console** コマンドを実行します。  
このアクションにより、Cisco Colo Manager CLI に移動します。**show running-config cluster cluster name** コマンドを実行します。
3. **admin-tech** コマンドを使用して、Cisco vManage からログを取得します。または、デバイスから直接ログを取得することもできます。『[CSP からのログ収集 \(22 ページ\)](#)』を参照してください。

### CSP への Day-0 構成プッシュが失敗する

この障害は、CSP に適切なハードウェアがないか、VNF の Day-0 構成に間違っただ入力があることが原因である可能性があります。

Action:

1. CSP のハードウェア構成を確認し、サポートされている構成であることを確認します。
2. サービスチェーンの Day-0 構成を確認してから、構成プッシュを再度トリガーします。

### CSP がクラスタに追加されない

[vManage] > [Configuration] > [Cloud OnRamp for Colocation] のインターフェイスのクラスタ状態は、「FAILED」を示します。追加された CSP は、Cloud OnRamp for Colocation のグラフィック表示で「RED」として示されます。

Action:

1. CSP のハードウェア構成を確認し、サポートされていることを確認します。
2. クラスタのアクティブ化を再試行します

### CSP との IP 接続を維持できない

CSP デバイスが DHCP IP を更新すると、CSP への IP 接続を維持できません。

Action:

DHCP IP アドレスの割り当てについては、DHCP サーバーが常に CSP デバイスと同じサブネット上にあることを確認してください。

### CSP デバイスが Cisco vManage に到達できない

Action:

次の操作を行ってください。

1. KVM コンソールを使用して、CSP デバイスに Cisco NFVIS をインストールします。NFVIS のインストールについては、『[Cisco Enterprise NFV Infrastructure Software Configuration Guide](#)』を参照してください。
2. NFVIS システムにログインし、ゲートウェイに ping を送信します

ping を送信していないまたは到達可能でない場合は、スイッチに接続されている OOB スイッチポートのポートチャネル構成が完了していることを確認します。

1. スイッチのポートチャネル構成がない場合は、`nfvis# support ovs appctl bond-show mgmt-bond` コマンドを実行します。出力は次のとおりです。

```
--- mgmt-bond ----
bond_mode: balance-slb
bond may use recirculation: no, Recirc-ID : -1
bond-hash-basis: 0
updelay: 0 ms
downdelay: 0 ms
next rebalance: 3479 ms
lACP_status: configured
active slave mac: 00:00:00:00:00:00 (none)
slave eth0-1: disabled
    may_enable: false
slave eth0-2: disabled
    may_enable: false
```

2. スイッチのポートチャネルは構成されているが、`eth0-2` がスイッチに接続されていない場合は、`nfvis# support ovs appctl bond-show mgmt-bond` コマンドを実行します。次の出力は、`eth0-2` がスイッチに接続されていないことを示しています。

```

---- mgmt-bond ----
bond_mode: balance-slb
bond may use recirculation: no, Recirc-ID : -1
bond-hash-basis: 0
updelay: 0 ms
downdelay: 0 ms
next rebalance: 4938 ms
lacp_status: off
active slave mac: 50:2f:a8:c7:64:c2(eth0-1)

slave eth0-1: enabled
active slave
may_enable: true
hash 195: 2 kB load

slave eth0-2: disabled
may_enable: false

```



(注) Cisco vManage は CSP デバイスを管理するため、NETCONF または REST API または CLI を介した OOB 構成により、デバイスが Cisco vManage と同期しなくなります。Cisco vManage は、次の構成がそこからプッシュされるときに、この構成を削除します。トラブルシューティングの場合、Cisco CSP または NFVIS を構成するには、共有モードまたは NETCONF ターゲット候補でのみ構成を使用してからコミットします。この構成は、Confd データベースのように必要であり、CDB は Cisco SD-WAN Cloud onRamp for Colocation ソリューションの Cisco NFVIS で候補モードになっています。**config t** CLI モードまたは NETCONF ターゲットの実行が使用されている場合、CDB データベースが同期されていない可能性があり、CSP デバイスで異常な動作が発生し、クラスタが使用できなくなります。

## DHCP IP アドレス割り当て

静的 IP アドレスを構成するには、次の手順を実行します。

1. DHCP サーバーのクリーンインストール後、**confd cli** を実行します。
2. **nfvis# show running-config vm\_lifecycle** コマンドを使用して、既存の構成を確認します。

次に例を示します。

```
nfvis# show running-config vm_lifecycle networks
```

```
vm_lifecycle networks network int-mgmt-net
!
```

3. **nfvis# config shared** コマンドを使用して、静的 IPv4 アドレスを設定します。

次に例を示します。

```
nfvis# config shared
```



```
Entering configuration mode terminal
nfvis(config)# vm_lifecycle networks network int-mgmt-net subnet int-mgmt-net-subnet
address <host-ip> gateway <host-ip-gateway> netmask <your-host-ip-netmask> dhcp
false
nfvis(config-ip-receive-acl-0.0.0.0/0)# commit
Commit complete.
nfvis(config-ip-receive-acl-0.0.0.0/0)# end
nfvis#
```

## DHCP スティック IP の構成

スティック DHCP IP の場合は、DHCP サーバーを構成します。デバイスのシリアル番号をすぐに利用できることを確認してください。

1. CentOS 7.4 を DHCP サーバーとして使用する場合は、`/etc/dhcp/dhcpd.conf` に次の同様の構成があることを確認します。

```
host abcxxxx175 {
option dhcp-client-identifier <serial number>;
}
```

2. IOS を DHCP サーバーとして使用する場合は、IOS DHCP サーバーまたはプールに次の同様の構成があることを確認してください。

```
ip dhcp pool P_112
host 209.165.201.12 255.255.255.0
client-identifier 4643.4832.3xxx.3256.3xxx.48
```

この例では、IP アドレス 209.165.201.12 は、識別子が 4643.4832.3xxx.3256.3xxx.48 のクライアントの DHCP スティック IP です。次に、クライアント識別子を見つけることができます。

3. クライアント識別子を見つけるには、IOS DHCP サーバーで `debug ip dhcp server packet` をオンにします。

デバッグコンソールの出力から、SD-WAN Cloud OnRamp for Colocation デバイスの DHCP クライアント識別子を表示できます。

# Cisco Colo Manager の問題のトラブルシューティング

ここでは、一般的な Cisco Colo Manager の問題とそのトラブルシューティング方法について説明します。

一般的な Cisco Colo Manager の問題

## SVL の形成に失敗した場合のポート接続の確認

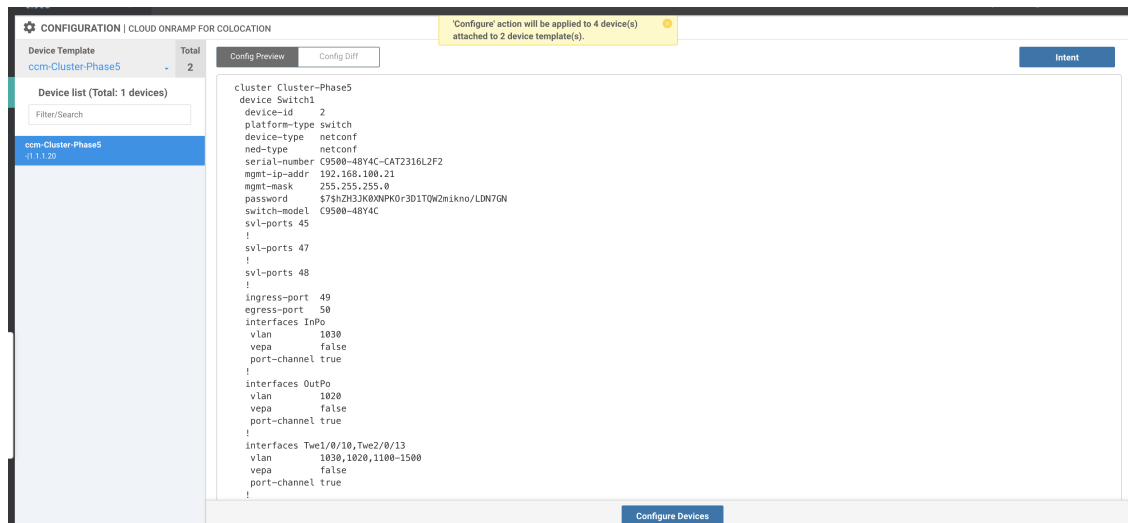
クラスタをアクティブ化した後、CCM からの SVL およびアップリンクポートを確認するには、次の手順を実行します。

1. Cisco vManage で、**[Configuration]** > **[Cloud OnRamp for Colocation]** をクリックします。

2. クラスタのポート接続を確認するには、テーブルからクラスタを選択し、行の右側にある [More Actions] アイコンをクリックしてから、[Sync] を選択します。
3. [Device Template] で、コロケーションクラスタをクリックし、ドロップダウンリストから CCM クラスタを選択します。
4. CCM 構成を表示するには、CCM クラスタをクリックします。

クラスタ内の両方のスイッチデバイスのポート接続の詳細を表示し、接続の問題を特定できるようにしました。

図 3: SVL およびアップリンクポートの検証



### Cisco Catalyst 9500 SVL 形成の失敗

1. 管理者ユーザーとして Cisco NFVIS との SSH セッションを確立します。 **ccm-console** コマンドを使用して Cisco Colo Manager にログインし、 **show colo-config-status** コマンドを実行します。

```
admin@ncs# show colo-config-status
```

推奨されるアクションを表示します。

```
colo-config-status status failure
colo-config-status description "Step 4 of 7:
Device c9500-2 : 192.168.6.252 (CAT2324L42L)
SVL ports specified by vmanage does not match with
actual cabled svl ports. Recommended action: Correct
the configured svl ports specified in cluster
configuration by vmanage in accordance with switch
SVL port cabling" colo-config-status severity critical
```

2. Cisco vManage の SVL 用に選択したポートが物理的にケーブル接続されたポートと一致していること、およびそれらが Cisco Catalyst 9500 スイッチによって検出されることを確認してください。

**Day-0**のクラスタをアクティブにしているときに **Cisco Colo Manager**が異常であるか、**Cisco Colo Manager**の実行中に **Cisco CSP**が削除されます。また、新しく追加された **Cisco CSP** デバイスの新しい **Cisco Colo Manager** がインスタンス化に失敗するか、異常になります

ここで、Cisco Colo Manager はホスト側で異常な状態にあり、Cisco Colo Manager の内部状態は「FAILURE」を示しています。Cisco vManage モニタリングでも、Cisco Colo Manager が「UNHEALTHY」状態で表示されます。

Action:

1. **show container ColoMgr** コマンドを実行して、新しく追加された Cisco CSP デバイスの Cisco Colo Manager の状態を確認します。

```
CSP1# show container ColoMgr
container ColoMgr
  uuid      57b9b8646ff1066ba24707415b5449111d915664629f56221e141c1171ee283d
  ip-address 172.31.232.182
  netmask    24
  default-gw 172.31.232.2
  bridge     int-mgmt-net-br
  state      healthy
  error
CSP1#
```

2. 前の手順で示したエラーフィールドを調べて、Cisco Colo Manager が異常な状態になっている理由を確認します。
3. ゲートウェイへの ping に関連する障害の場合は、IP アドレス、マスク、ゲートウェイ IP アドレスなどの Cisco Colo Manager パラメータが有効であることを確認します。また、ゲートウェイへの物理接続の到達可能性を確認します。
4. いずれかのパラメータが正しくない場合は、Cisco vManage からそれらを修正してから、クラスタのアクティブ化または同期を再試行します。
5. Cisco Colo Manager が正常でない理由がパッケージエラーである場合は、テクニカルサポートに連絡してください。

## サービスチェーンの問題のトラブルシューティング

ここでは、一般的なサービスチェーンの問題とそのトラブルシューティング方法について説明します。

一般的なサービスチェーンの問題

サービスグループへのサービスチェーンの追加または削除が失敗する

• Action:

- Cisco Colo Manager はホスト側で正常な状態にあり、Cisco Colo Manager の内部状態は、構成プッシュに対して「FAILURE」を示しています。構成プッシュが失敗し、Cisco Colo Manager が「FAILURE」状態になり、クラスタが「FAILURE」状態になります。

Action:

1. Cisco Colo Manager にアクセスするには、Cisco Colo Manager が有効になっている CSP デバイスで **ccm console** コマンドを実行します。

このアクションにより、Cisco Colo Manager の CLI に移動します。次のコマンドを実行します。

1. **show colo-config-status**

このアクションにより、説明に失敗の理由を表示できます。

2. 障害をデバッグするためにさらに情報が必要な場合は、Cisco Colo Manager をホストしている CSP で **admin-tech** コマンドを使用してログを収集します。または、デバイスから直接ログを取得することもできます。『[CSP からのログ収集 \(22 ページ\)](#)』を参照してください。

2. VNF サービスチェーンの Day-0 構成を確認します。

3. VNF サービスチェーンを再度プロビジョニングします。



---

(注) サービスチェーンの追加または削除によって Cisco Colo Manager で障害が発生した場合は、同期するオプションがあります。

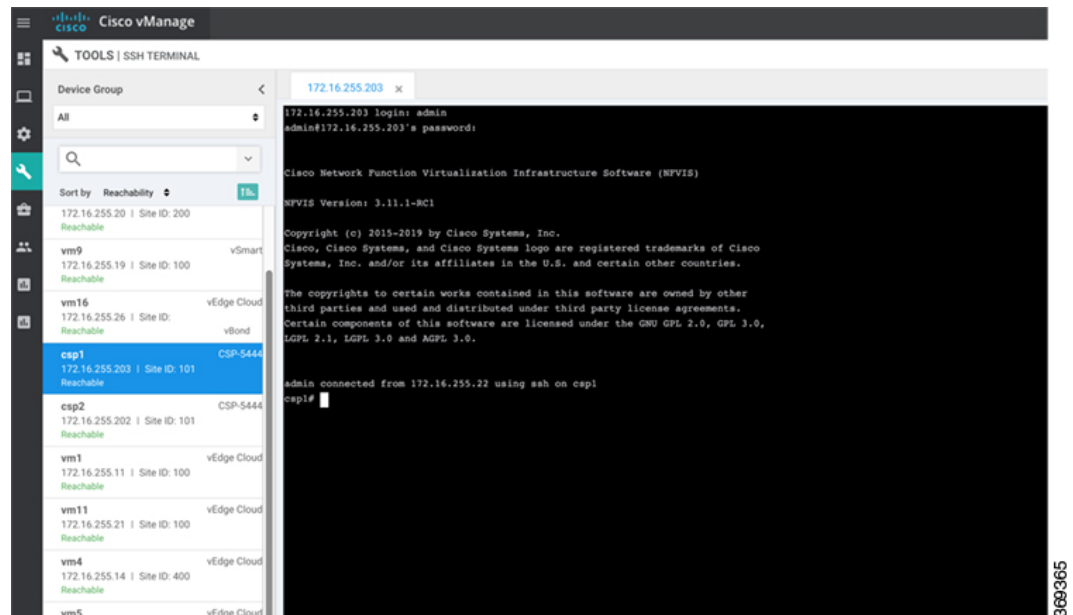
---

#### サービスチェーンの追加中に、VNF がエラー状態になる

VNF が Cisco vManage でダウンとして表示されます。

Action:

1. VNF の Day-0 構成を確認します。
2. Cisco vManage から SSH を使用して、VNF をホストしている CSP に移動します。



3. 次のコマンドを実行します。

```
nfvis# show system:system deployments
```

```
nfvis# get the VNF ID
```

次に例を示します。

```
NAME ID STATE
```

```
-----
```

```
Firewall2_SG-3 40 running
```

```
nfvis# support show config-drive content 40
```

すべての変数がキーと値のペアで適切に置き換えられていることを確認してください。

## 物理ネットワーク機能管理の問題のトラブルシューティング

PNF デバイスの共有の問題を解決するには、次の点を考慮してください。

1. Catalyst 9500 への PNF デバイスのケーブル接続が正しく、VLAN 構成は Catalyst 9500 の正しいポートにあること。
2. LLDP の有効化を確認すること。デフォルトでは、LLDP は Catalyst 9500 で有効になっています。PNF で LLDP が有効になっていることを確認し、LLDP ネイバーとネイバーインターフェイスをチェックして接続を確認します。
3. PNF で欠落している構成を確認すること。

## CSP からのログ収集

Cisco vManage から CSP に到達できず、デバッグのためにログを収集する必要がある場合は、CSP から **tech-support** コマンドを使用します。

次に、tech-support コマンドの使用例を示します。

```
nfvis# tech-support
nfvis# show system:system file-list
system:system file-list disk local 1
  name          nfvis_scp.log
  path          /data/intdatastore/logs
  size          2.1K
  typ
```

Cisco NFVIS から外部システムへ、または外部システムから Cisco NFVIS へのログファイルのコピーを保護するには、管理ユーザーは特権 EXEC モードで **scp** コマンドを使用できます。次の例は、**scp techsupport** コマンドを示しています。

```
nfvis# scp techsupport:NFVIS_nfvis_2019-04-11T15-33-09.tar.gz
cisco@172.31.232.182:/home/cisco/.
```

## Cisco vManage の問題のトラブルシューティング

次の場所を使用して、Cisco vManage の問題をトラブルシューティングします。

[SD-WAN Techzone ナレッジベース](#)

## 翻訳について

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。