ACIアップグレードのベストプラクティスとトラブルシューティング

内容

概要

このドキュメントでは、アプリケーションセントリックインフラストラクチャ(ACI)のアップグレード問題をトラブルシューティングする手順と、アップグレードプロセスの前後および実行中に従うべきベストプラクティスについて説明します。

ACIのアップグレードには、Application Policy Infrastructure Controller(APIC)ソフトウェアとスイッチ（リーフ/スパイン）のアップデートが含まれます。スイッチのアップグレードは通常は非常に簡単ですが、APICのアップグレードではクラスタの問題が発生する場合があります。アップグレードを開始する前に準備しておくことを推奨するプレチェックをいくつか次に示します。

アップグレード前

ACIのアップグレードを開始する前に、予期しない動作を避けるために、いくつかのプレチェックを必ず実行してください。

APICアップグレード前の作業

1. **すべての障害をクリア**

   ACIファブリック状態の多くの障害で、無効または競合ポリシーが存在すること、またはインターフェイスが切断されることなどが挙げられます。アップグレードを開始する前に、トリガーを理解してクリアします。次のような障害に注意してください。 **encap already been used** または **Routed port is in L2 mode** 予期しない停止が発生する可能性があります。スイッチをアップグレードすると、APICからすべてのポリシーが最初からダウンロードされます。その結果、予期しないポリシーが予想されるポリシーを引き継ぎ、停止を引き起こす可能性があります。

2. **VLANプールオーバーラップのクリア**

   VLANプールのオーバーラップは、同じVLAN IDが2つ以上のVLANプールの一部であることを意味します。異なるVLANプールの一部である複数のリーフスイッチに同じVLAN IDが展

開されている場合、これらのスイッチでは異なるVXLAN IDが設定されます。ACIは転送にVXLAN IDを使用するため、特定のVLANを宛先とするトラフィックが異なるVLANで終わるか、ドロップされる可能性があります。アップグレード後にリーフがAPICから設定をダウンロードするため、VLANの導入順序は大きな役割を果たします。そのため、一部のVLANのエンドポイントへの接続が停止したり、断続的に切断される可能性があります。

アップグレードを開始する前に、VLAN IDの重複を確認して修正することが重要です。1つのVLAN IDを1つのVLANプールのみに含め、必要に応じてVLANプールを再利用することを推奨します。

3. **サポートされるアップグレードパスの確認**

APICのアップグレードには、内部で行われるバージョン間のデータ変換が含まれます。データ変換を成功させるには、バージョンの互換性に関する問題を解決する必要があります。現在のACIバージョンから、アップグレード先の新しいターゲットバージョンへの直接アップグレードがシスコでサポートされているかどうかを必ず確認してください。ターゲットバージョンに到達するには、複数のホップを経由する必要がある場合があります。サポートされていないバージョンにアップグレードすると、クラスタの問題と設定の問題が発生する可能性があります。

サポートされているアップグレードパスは、常に『Cisco ACIアップグレードガイド』に記載されています。

4. **バックアップAPICの設定**

アップグレードを開始する前に、設定バックアップを必ずリモートサーバにエクスポートしてください。このエクスポートされたバックアップファイルは、すべての設定が失われた場合、またはアップグレード後にデータが破損した場合に、APICの設定を取り戻すために使用できます。
注：バックアップの暗号化を有効にする場合は、暗号化キーを必ず保存してください。それ以外の場合は、管理者パスワードを含むすべてのユーザーアカウントパスワードが正しくインポートされません。

5. **APIC CIMCアクセスの確認**

Cisco Integrated Management Controller(CIMC)は、APICへのリモートコンソールアクセスを取得する最適な方法です。リブート後にAPICがアップ状態に戻らない場合、またはプロセスがスタックしている場合、APICのアウトオブバンドまたはインバンド管理を通じてAPICに接続できない可能性があります。この段階で、CIMCにログインし、APICのKVMコンソールに接続して、いくつかのチェックを実行し、問題をトラブルシューティングできます。

6. **CIMCバージョンの互換性の確認と確認**

ACIのアップグレードを開始する前に、必ずシスコが推奨するCIMCバージョンとターゲットのACIバージョンとの互換性があることを確認してください。推奨されるAPICおよびCIMCバージョンを参照してください。

7. **APICプロセスがロックされていないことを確認します。**

APICで実行されるアプライアンス要素(AE)と呼ばれるプロセスは、APICでアップグレードをトリガーする役割を担います。CentOS Intelligent Platform Management Interface(IPMI)には、APICのAEプロセスをロックする可能性のある既知のバグがあります。AEプロセスがロックされている場合、APICファームウェアアップグレードは開始されません。このプロセスは、シャーシのIPMIを10秒ごとに照会します。AEプロセスが過去10秒間にシャーシのIPMIを照会しなかった場合は、AEプロセスがロックされていることを意味します。

AEプロセスのステータスをチェックして、最後のIPMIクエリを確認できます。APIC CLIから、次のコマンドを入力します **date** 現在のシステム時刻を確認します。次に、コマンドを入力します **grep "ipmi" /var/log/dme/log/svc_ifc_ae.bin.log | tail -5** AEプロセスがIPMIを最後に照会した時刻を確認します。時刻をシステム時刻と比較して、最後のクエリがシステム時刻の10秒のウィンドウ内にあるかどうかを確認します。

AEプロセスがシステム時間の最後の10秒間にIPMIのクエリに失敗した場合、APICをリブートしてアップグレードを開始する前にAEプロセスを回復できます。
注：クラスタの問題を回避するために、複数のAPICを同時にリブートしないでください。

8. **NTPの可用性の確認と確認**

   各APICからNTPサーバへの到達可能性をpingおよび確認し、APICの時刻の不一致による既知の問題を回避します。詳細については、この記事の「トラブルシューティング」の項を参照してください。

9. **APICヘルス状態の確認**

   アップグレードを開始する前に、クラスタ内のAPICのヘルスステータスを確認して確認します。ヘルススコア255は、APICが正常であることを意味します。次のコマンドを入力します。 **acidiag avread | grep id= | cut -d ' ' -f 9,10,20,26,46** APICのヘルスステータスを確認するために、任意のAPIC CLIからアクセスできます。APICのヘルススコアが255でない場合は、アップグレードを開始しないでください。

10. **新しいバージョンの影響の評価**

    アップグレードを開始する前に、対象のACIバージョンのリリースノートを確認し、アップグレード後の予期しない結果を回避するために、ファブリック設定に適用される動作変更を理解してください。

11. **ラボでのアップグレードのステージング**

    実際の実稼働ファブリックの前にラボまたはテストファブリックでアップグレードを試し、新しいバージョンのアップグレードと動作に習熟することを推奨します。これは、アップグレード後に発生する可能性のある問題の評価にも役立ちます。

スイッチをアップグレードする前に行うこと

1. **仮想ポートチャネル(vPC)と冗長リーフペアを異なるメンテナンスグループに配置する**

ACI APICには、特定のバージョン以降からのvPCペアリーフノードのアップグレードを確認して延期するメカニズムがあります。ただし、vPCペアスイッチを異なるメンテナンスグループに配置して、両方のvPCスイッチが同時にリブートするのを回避することがベストプラクティスです。

ボーダーリーフなどの冗長なvPC以外のスイッチの場合は、停止を避けるために必ず異なるポートグループに配置してください。

アップグレードの問題のトラブルシューティング

アップグレードがスタックまたは失敗した場合は、必ずAPIC1のトラブルシューティングを開始してください。APIC1のアップグレードがまだ完了していない場合は、APIC2とAPIC3で何も行わないでください。APICのアップグレードプロセスは増分されるため、APIC1がアップグレードを完了し、APIC2に通知した後にのみAPIC2がアップグレードされます。このため、この違反により、破損したデータベースを持つクラスタが障害状態になる可能性があり、クラスタの再構築が必要になる場合があります。

シナリオ：APIC ID 2以降が75 %のままになる

このシナリオでは、APIC1は正常にアップグレードされましたが、APIC2はまだ75 %のままになっています。この問題は、APIC1のアップグレードバージョン情報がAPIC2以降に伝搬されない場合に発生します。次の点に注意してください。 svc_ifc_appliance_director プロセスは、APIC間のバージョン同期を担当します。

トラブルシューティング方法

ステップ 1：APIC1がトンネルエンドポイント(TEP)IPアドレスを使用して残りのAPICにpingできることを確認します。これにより、リーフスイッチからのトラブルシューティングが必要か、APIC自体から続行する必要かが決まります。APIC1からAPIC2にpingできない場合は、Technical Assistance Center(TAC)に電話して、スイッチのトラブルシューティングを依頼してください。APIC1がAPIC2にpingできる場合は、次の手順に進みます。

ステップ 2：APICは相互にpingを実行できるため、APIC1バージョン情報はピアに複製される必要がありますが、何らかの理由でピアによって受け入れられませんでした。バージョン情報は、バージョンタイムスタンプによって識別されます。APIC1のバージョンタイムスタンプは、CLIおよび75 %で待機しているAPIC2 CLIから確認できます。

APIC1

```
apic1# acidiag avread | grep id=1 | cut -d ' ' -f20-21
version=2.0(2f) lm(t):1(2018-07-25T18:01:04.907+11:00)
```

APIC2

```
apic2# acidiag avread | grep id=1 | cut -d ' ' -f20-21
version=2.0(1m) lm(t):1(2018-07-25T18:20:04.907+11:00)
```

ご覧のように、この例でバージョン2.0(1m)を実行するAPIC2(18:20:04)のバージョンタイムスタンプは、バージョン2.0(2f)を実行するAPIC1(18:01:04)のバージョンタイムスタンプよりも高くなっています。 したがって、APIC2インストーラプロセスでは、APIC1のアップグレードがまだ完

了していないと見なされ、75 %で待機します。APIC1のバージョンタイムスタンプがAPIC2のバージョンタイムスタンプを超えると、APIC2のアップグレードが開始されます。ただし、これは時間差に基づいて多くの待ち時間になる可能性があります。この状態からファブリックを回復するには、TACケースをオープンして、APIC1からのトラブルシューティングと問題の修正に関するサポートを受けることができます。