ISE証明書複製アラームの説明とトラブルシューティング

内容

はじめに

このドキュメントでは、Cisco Identity Services Engine®(ISE)での複製アラームとそのトラブルシューティングについて説明します。

前提条件

要件

Cisco Identity Services Engine®(ISE)に関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、次のハードウェアとソフトウェアのバージョンに基づくものです。

- Cisco Identity Services Engine®(ISE)3.4以降のバージョン

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

複製アラーム

Cisco ISEのレプリケーションアラームは、導入環境全体のレプリケーションフレームワークの状態と同期ステータスを可視化します。これらのアラームは、データの整合性、ノードの通信、または複製プロセスに影響を与える可能性がある状態を特定するのに役立ち、管理者はシステムの運用に影響が及ぶ前に問題を検出して解決できます。正常なISE導入を維持し、設定データと運用データがすべてのノード間で確実に同期されるようにするためには、レプリケーションアラームの目的と重要性を理解することが不可欠です。

ISE証明書レプリケーションアラーム

証明書の複製に失敗しました

Certificate Replication Failedアラームは、Cisco ISEがプライマリ管理ノード(PAN)から環境内の1つ以上のノードに証明書関連データを複製できない場合に生成されます。プライマリPANで証明書のインポート、生成、更新、または変更が行われるたびに、ISEは証明書とそれに関連する設定を自動的に複製し、すべてのノードの整合性を維持します。このアラームは、複製プロセスが失敗し、影響を受けるノードで証明書の設定に一貫性がないことが原因で発生したことを示します。

アラームの理由

Certificate Replication Failedアラームは、Cisco ISEが1つ以上のノードで証明書関連データを正常に転送、検証、またはインストールできない場合に発生します。一般的な原因としては以下のものがある：

- ネットワーク通信の問題：パケット損失、高いネットワーク遅延、レプリケーショントラフィックをブロックするファイアウォール制限、ISEノード間のルーティングの問題、またはパケットのフラグメンテーションやドロップを引き起こすMTUの不一致により、証明書のレプリケーションが中断される場合があります。
- レプリケーションサービスの問題： RabbitMQ、JGroups、またはその他の内部レプリケー

ションサービスが利用できない、再起動する、または正しく機能していない場合、証明書のレプリケーションが失敗する可能性があります。
- 証明書の検証エラー：証明書チェーンが不完全な場合、CA証明書または中間証明書が見つからない場合、証明書の有効期限が切れている場合、証明書が壊れている場合、証明書チェーンにサポートされていないキーの使用が含まれている場合、証明書チェーンのレプリケーションが失敗する可能性があります。
- ノード通信の問題：宛先ノードがオフラインの場合、再起動、登録解除、展開からの切断、または到達不能の場合は、証明書の複製を完了できません。
- ディスク領域が不足しています：宛先ノードには、レプリケートされた証明書をインポートおよびインストールするのに十分なディスク領域がありません。
- 内部データベースの問題：ISE設定データベースが証明書のメタデータを保存または更新できない場合、レプリケーションが失敗する可能性があります。

アラームの影響

このアラームの影響は、複製される証明書のタイプと、それに依存するサービスによって異なります。証明書の複製に失敗すると、ISEノード間での証明書設定の不整合、HTTPS証明書の不一致、EAP認証の失敗、pxGrid信頼確立の問題、SCEP登録または証明書プロビジョニングの失敗、信頼できる証明書ストアでの不整合、外部統合でのTLS検証の失敗などが発生する可能性があります。

証明書のレプリケーションが一時的に失敗しました

Certificate Replication Temporarily Failedアラームは、Cisco ISEがプライマリ管理ノード(PAN)から展開内の1つ以上のノードに証明書関連データを一時的に複製できない場合に生成されます。Certificate Replication Failedアラームとは異なり、このアラームではレプリケーション障害が一時的なものと見なされ、基盤となる状態が解決されると、Cisco ISEが自動的にレプリケーション操作を再試行します。

アラームの理由

通常、このアラームは、証明書の複製を一時的に妨げる一時的な状態のために生成されます。一般的な原因には次のものがあります。

- 一時的なネットワーク通信の問題：短時間のネットワーク中断、パケット損失、高い遅延、ファイアウォール遅延、またはISEノード間の一時的なルーティングの問題。
- レプリケーションサービスの初期化または再起動： RabbitMQ、JGroups、またはその他の内部レプリケーションサービスが再起動しているか、一時的に使用できません。
- 一時的なノード使用不可：宛先ノードが起動中、アプリケーション・サービスの再起動中、デプロイへの再参加中、または一時的に到達不能です。
- システムリソースの一時的な制約：CPU使用率が高い、メモリ負荷が高い、またはディス

クI/Oコンテンションが発生していると、レプリケーション処理が一時的に遅延します。
- 同時管理操作：別の証明書のインポート、バックアップ、復元、パッチのインストール、または展開の同期が進行中の間、証明書の複製を遅延させることができます。
- データベースまたはレプリケーションキューの一時的な遅延：内部データベース操作またはレプリケーションキューが、他の同期要求の処理で一時的にビジー状態になっています。

アラームの影響

ほとんどの場合、Cisco ISEはレプリケーション操作を自動的に再試行するため、このアラームによる運用上の影響は最小限です。ただし、レプリケーションが正常に完了するまで、ノード間で一時的な不整合が発生する可能性があります。これには、次のものが含まれます。

- 新しくインポートまたは更新された証明書の伝達の遅延
- 一時的な証明書の構成が展開全体で一致していません
- 影響を受けるノードで証明書ベースのサービスの利用開始が遅れる
- HTTPS、EAP、pxGrid、またはSCEPサービスが複製された証明書に依存している場合の一時的な遅延

アラームが持続するか、繰り返し発生する場合は、Certificate Replication Failedアラームが発生します。

ISE証明書レプリケーションアラームのトラブルシューティング

これらは、ISEの証明書複製アラームのトラブルシューティングまたは検証時に確認する必要がある一般的な要因です。

1. ノードの展開ステータスの確認

証明書のレプリケーションを正常に行うには、Cisco ISE導入環境内でセカンダリノードがConnected状態になっている必要があります。Administration > System > Deploymentの順に選択し、該当するノードのステータスを確認します。ノードのステータスの横にある情報(i)アイコンにカーソルを合わせると、同期の詳細と保留中の複製メッセージが表示されます。

各ノードについて表示される同期ステータスは、現在のレプリケーションと接続の状態を示します。

- 緑：ノードが導入と同期され、レプリケーションが正常に動作しています。
- 黄：ノードが同期されていない、ノード登録に失敗した、またはクラスタ接続が失われた。このステータスは、過去5分間にクラスタからノードに到達できなかったことを示します。
- 赤 – ノードは到達不能であり、ICMP pingやHTTPSなどのネットワーク接続チェックを通じ

て接続できません。

ノードのステータスが黄色または赤色の場合は、そのノードに影響を与えているレプリケーションまたは接続の問題を示しています。さらに、ノード情報に表示されるレプリケーションメッセージ数を確認します。保留中のメッセージ数は5,000以下にする必要があります。保留中のメッセージが5,000個を超えるキューは、レプリケーションキューが累積されていることを示します。これにより、レプリケーションの成功が遅れたり、妨げられたりする可能性があります。

2. 展開でのキューリンクアラームの確認

Cisco　ISEで正常に複製を行うには、RabbitMQメッセージングサービスとJGroupsクラスタ通信フレームワークが使用可能で通信している必要があります。どちらかのコンポーネントで通信の問題が発生すると、Cisco ISEによってキューリンクエラーが生成され、導入ノード間のレプリケーションが中断される可能性があります。

アラームのステータスを確認するには、Operations > Dashboard > Alarmsの順に移動し、該当するノードでQueue Link Errorsを確認します。

キューリンクエラーがある場合は、Cisco ISE ルートCA証明書を更新してください。証明書関連の通信エラーは通常、キューリンクエラーの原因となります。証明書の問題が解決されると、通常は追加の介入を必要とせずにレプリケーションが自動的に再開されます。

注：キューリンクエラーの詳細については、『ISEキューリンクエラー』ドキュメントを参照してください。

---

3. ネットワーク遅延と接続の確認

Cisco ISEレプリケーションは、導入ノード間の安定したネットワーク接続に依存します。ネットワークの遅延や断続的な接続が多いと、レプリケーションに遅延が発生し、特に地理的に分散した環境で同期障害が発生する可能性があります。

pingなどの接続テストを使用して、影響を受けるノード間のネットワーク遅延を確認します。信頼性の高いレプリケーションを行うには、ノード間のラウンドトリップ遅延を約300 ms以内に抑える必要があります。このしきい値を一貫して超える遅延は、レプリケーションのパフォーマンスと同期に悪影響を与える可能性があります。また、展開ノード間の通信に影響を与える、断続的なネットワーク停止、パケット損失、またはファイアウォールの制限がないことも確認してください。

4. 影響を受けるノードに証明書が存在していないことを確認します

複製される証明書がセカンダリノードにすでに存在する場合、証明書の複製が失敗する可能性があります。

Administration > System > Certificatesの順に移動し、該当するノードを選択して、証明書がすでにインストールされているかどうかを確認します。証明書が存在する場合は、そのプロパティを確認して、レプリケートされる証明書と一致することを確認し、重複する証明書または競合する証明書が存在するかどうかを確認します。

5. システムリソース使用率の確認

システムリソースの使用率が高いと、Cisco ISEのパフォーマンスに影響を与え、レプリケーションタスクが遅延する可能性があります。CPU、メモリ、またはディスクの過剰な使用率により、レプリケーション・プロセスが正常に完了しない場合があります。

影響を受けるノードに使用可能なシステムリソースが十分にあり、リソースの使用率が推奨動作制限内であることを確認します。リソース使用率が常に高い場合は、ノード上で追加のリソースを割り当てるか、ワークロードを削減して、通常のレプリケーション・パフォーマンスをリストアします。

注:Cisco ISE導入のための推奨されるハードウェアサイジングとリソース割り当てのガイドラインについては、『パフォーマンスとスケーラビリティのガイド』を参照してください。

---

6. 導入およびネットワークでのポートの可用性の確認

Cisco ISEレプリケーションでは、中断のない通信とレプリケーションの成功を保証するために、展開内のすべてのノード間で特定のTCPポートを開いたままにしておく必要があります。これらのポートのいずれかがファイアウォール、アクセスコントロールポリシー、またはネットワークデバイスによってブロックされると、複製の失敗や同期の問題が発生する可能性があります。

すべてのCisco ISEノード間で次のTCPポートが開いていて到達可能であることを確認します。

- TCP 443 - HTTPS通信
- TCP 8443：管理通信
- TCP 12001:JGroupsクラスタの通信および複製
- TCP 6379：内部メッセージングサービス
- TCP 8671:Cisco ISEメッセージング(RabbitMQ)

Cisco ISE CLIにログインし、コマンドshow portsを実行して、ノードで許可されている上記のポ

ートを確認します。

必要なポートがCisco ISEノードで有効になっていることを確認し、ネットワークパスで許可されていることを確認します。中間ファイアウォール、セキュリティデバイス、またはネットワークポリシーが、展開ノード間のこれらのポートで通信をブロックしていないことを確認します。

複製アラームのログ収集

Cisco ISEの複製アラームを切り分けてトラブルシューティングするために、debugモードで設定する必要がある一般的なコンポーネントを次に示します。

- Replication-Deployment（replication.logおよびise-psc.log）
- Replication-JGroup（replication.logおよびise-psc.log）
- レプリケーショントラッカー(tracking.log)
- hibernate (hibernate.log)
- JMS(replication.log)

参考

- Cisco Identity Services Engine 管理ガイド リリース 3.5
- ISEでのデバッグのトラブルシューティングと有効化
- Identity Services Engineのサポートバンドルの収集

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。