ISEレプリケーションの理解および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)でのレプリケーション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。

Cisco ISEでのレプリケーション

ISEのレプリケーションは、導入環境内の複数のノード間で構成データと運用データを同期し、整合性を維持するプロセスです。

プライマリ管理ノードは、導入環境内で行われた変更を、導入環境内の他のすべての（セカンダリ）ノードにレプリケートします。

Cisco ISEは、信頼性の高いグループ通信フレームワークであるJGroupsをレプリケーションアーキテクチャの一部として使用します。JGroupsを使用すると、ISE導入環境のノード間での相互通信やレプリケーションデータの交換が可能になります。このソリューションは、ノード間で構成とデータベースの更新を配信すると同時に、導入環境全体で同期を維持するメッセージングフレームワークを提供します。

- JGroupsは、Cisco ISEがレプリケーションに使用する通信フレームワークで、複製されたデータ自体は保存しません。
- Cisco ISE内のすべてのデータがJGroupsを通じて複製されるわけではありません。サービスが異なれば、転送されるデータのタイプに基づいて異なる通信メカニズムが使用されます。
- レプリケーションが一時的に中断された場合、一部のCisco ISEサービスは、同期が復元されるまで、ローカルで使用可能なデータを使用して動作を継続できます。

データ転送方式の例

データ	通信方式

設定および複製メッセージ	グループ
バンドルコレクションのサポート	HTTPS API（TCPポート443）
デバッグ設定	HTTPS API（TCPポート443）
ライブログおよびレポート	RabbitMQまたはUDP（導入設定による）

Cisco ISEレプリケーションの主な前提条件と検証チェック

- DNS解決：導入に参加するすべてのCisco ISEノードで、DNS前方参照と逆引き参照が正常に解決される必要があります。ノードの通信およびレプリケーション操作には、適切なDNS解決が必要です。
- NTPの同期：導入環境全体でシステム時間が一貫して維持されるように、すべてのCisco ISEノードを信頼できるNTPソースに同期させる必要があります。レプリケーションと証明書の検証には、時刻の同期が不可欠です。
- 証明書：各Cisco ISEノードにインストールされる管理証明書は、有効で信頼できる証明書である必要があります。複製プロセスは、ノード間のセキュア通信で管理証明書に依存します。
- ポート要件：ネットワーク接続は、レプリケーションおよびノード間サービスに必要なポートを介した通信を許可する必要があります。

サービス	プロトコル/ポート
HTTPS(SOAP)	TCP/443
データの同期とレプリケーション(JGroups)	TCP/12001
管理アクセス	TCP/8443
ISEメッセージングサービス(SSL)	TCP/8671

プロファイラエンドポイント所有権の同期 TCP/6379

- ネットワークの到達可能性：Cisco ISEノード間のネットワーク接続は安定している必要があり、遅延は300 msを超えることはできません。ノード間の遅延とパケット損失を確認することで、信頼性の高いレプリケーションを実現できます。
- キューリンクステータス：Cisco ISEメッセージング証明書は、TCPポート8671を介したノード間通信を保護するために使用されます。無効または破損したメッセージング証明書は、キューリンクエラーおよび複製エラーの原因となる可能性があります。このようなシナリオでは、ISEルートCA証明書またはISEメッセージング証明書を適宜再生成する必要があります。
- ISE Stunnel Service:Cisco ISE Stunnel Serviceは、分散導入で動作し、ノード間のセキュアな通信を促進します。レプリケーションをサポートするには、該当するすべてのノードでサービスが実行されている必要があります。サービスステータスは、次のコマンドを使用してCisco ISE CLIから確認できます。
  show tech-support | include stunnel（登録ユーザ専用）
- ISEパッチとバージョン：プライマリ管理ノード(PMP)と参加ノード（スタンドアロンノード）は、ノード登録と同期がシームレスに動作するように、同じバージョンとパッチレベルを持つ必要があります。

Cisco ISEのレプリケーションフェーズ

Cisco ISEのレプリケーションは、3つの異なるフェーズで構成されており、これらのフェーズが連携して、導入環境内のすべてのノード間で同期を確立し、維持します。各フェーズは、ノードのオンボーディングから始まり、最初のデータベースの同期、そして最後にすべてのノードの同期を維持するための差分更新の継続的な交換という特定の目的を果たします。

- ノード登録
- 完全な同期
- 差分同期

Cisco ISEでのノード登録について

ノード登録は、Cisco ISEノードが既存の展開に参加し、プライマリ管理ノード(PAN)との通信を確立するプロセスです。

ノード登録時：

ステップ1：参加ノード（スタンドアロンノード）がプライマリ管理ノードとの通信を開始します。

ステップ2：相互証明書の検証は、Cisco ISE管理証明書を使用して実行されます。

ステップ3：通信プロセスの一環として、DNS解決、NTP同期、ネットワーク到達可能性、および必要なポートアクセシビリティが検証されます。

ステップ4：プライマリ管理ノードは、スタンドアロンノード/参加ノードが互換性のあるCisco ISEバージョンおよびパッチレベルを実行していることを確認します。

ステップ5：導入情報、ノードロール、および信頼関係が交換されます。

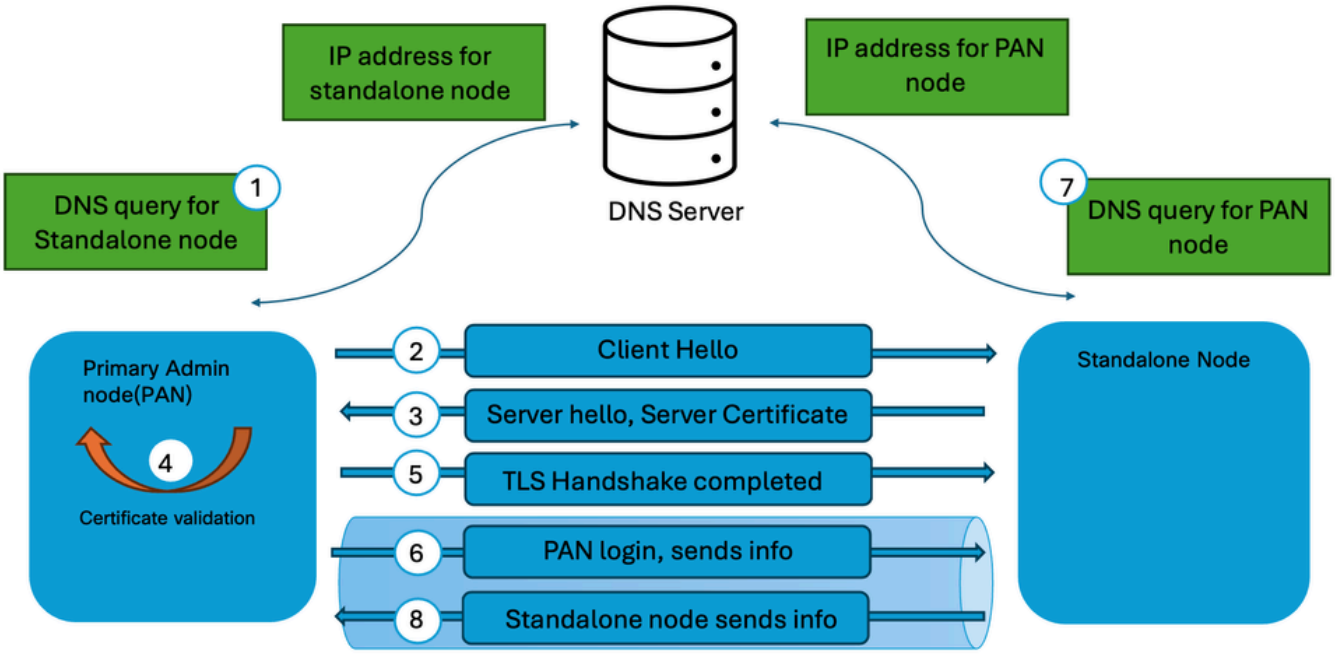
ステップ6：データベースレプリケーションサービスが初期化され、同期用に準備されます。

ノード登録が正常に完了すると、ノードが導入の信頼できるメンバーとして確立され、複製プロセスを開始できるようになります。

主な特徴

- 新しいノードが展開に追加されるときに発生します。
- 信頼および通信チャネルを確立します。
- 設定データベース全体を即座に転送しません。
- 後続の同期操作の前提条件として機能します。

ノード登録プロセスの詳細については、『Cisco ISEのノード登録プロセスについて』を参照してください。



ノード登録プロセス

注：導入に追加するノードは、スタンドアロンノードである必要があります。さらに、Primary Administration Node(PAN)では、Cisco ISEでのノード登録を可能にするために、導入でPrimary Administrationロールを有効にする必要があります。

Cisco ISEでの完全同期について

完全同期は、構成データベース全体がプライマリPANから別のノードに転送される完全なデータベースレプリケーションプロセスです。完全同期では、変更されたレコードのみが転送されます。代わりに、受信ノードで構成データセット全体が再構築されます。

完全同期は、次のようなシナリオで発生する可能性があります。

- ノード登録後の初期同期。
- レプリケーション障害からのリカバリ
- データベースの重大な不整合。
- ノードを展開に再参加しています。
- Cisco TACのトラブルシューティング手順によって開始された手動同期。
- 増分同期でデータベースの整合性を復元できなくなったことを確認する内部レプリケーションメカニズム。

完全同期中：

ステップ1：プライマリ管理ノードは、完全なデータベーススナップショットを準備します。

ステップ2：構成データは.dmpファイルにパッケージ化され、受信ノードに送信されます。

ステップ3：受信ノード上の既存の複製データが検証され、更新されます。

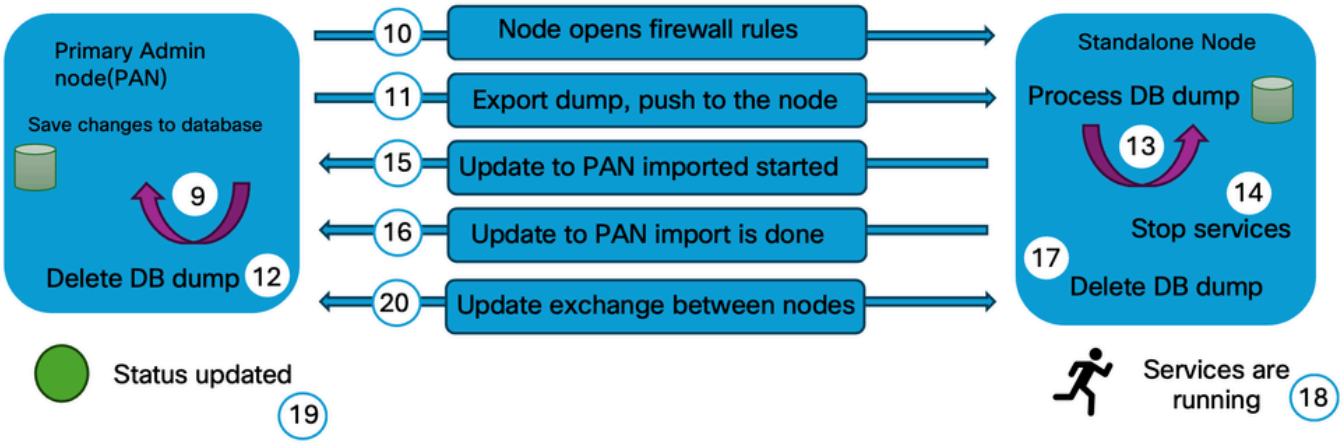
ステップ4：プライマリ管理者ノードと一致するように、設定データベース全体が再構築されます。

ステップ5：レプリケーションのステータスは、完了時に確認されます。

完全同期では、差分同期よりもはるかに多くのデータが含まれるため、処理時間とネットワークリソースが増加します。

完全同期の特性

- 完全な設定データベースを転送します。
- より多くの帯域幅とシステムリソースを消費します。
- 差分同期よりも時間がかかります。
- 不一致が検出された場合にデータベースの整合性をリストアします。
- 通常は、差分同期よりも発生頻度が低くなります。



完全同期プロセス

Cisco ISEでの差分同期について

差分同期は、ノードが展開に正常に参加した後に構成の変更を分散するためにCisco ISEで使用される継続的なレプリケーションメカニズムです。管理者がPANで設定を変更しても、Cisco ISEはデータベース全体を転送しません。代わりに、変更されたレコードだけがサブスクライバノード

に複製されます。

差分同期によってレプリケートされる変更の例は次のとおりです。

- ポリシーの変更
- ネットワークデバイスの追加または更新
- エンドポイントグループの変更
- 許可プロファイルの更新
- 証明書関連の設定変更
- アイデンティティソース設定の更新

差分同期プロセスは継続的に実行され、帯域幅使用率とレプリケーションのオーバーヘッドを最小限に抑えながら、すべてのノードにわたって整合性を維持するように設計されています。

差分同期のメリット

- レプリケーショントラフィックを削減
- 同期時間を短縮します。
- 設定変更の迅速な伝播が可能
- 導入環境全体でほぼリアルタイムの一貫性を維持します。

複製ワークフロー

ステップ1：プライマリ管理ノードで設定が変更されます。

ステップ2：変更がプライマリ管理ノードのデータベースに書き込まれます。

手順3：レプリケーションサービスは、変更されたレコードを識別します。

ステップ4：プライマリ管理ノードが新しいイベントや変更をトランザクションテーブルに書き込みます。

ステップ5:PANからスレッドを切り離して、展開のセカンダリノードに情報または変更を発行します。

ステップ6：配置のセカンダリノードが、プライマリ管理ノードから変更を受信します。

ステップ7：導入のセカンダリノードが、プライマリ管理ノードから受信した変更を適用します。

ステップ8：レプリケーションのステータスは、正常に完了すると更新されます。

通常の稼働状況では、Cisco ISEのほとんどのレプリケーションアクティビティは、差分同期によって行われます。

注意：セカンダリ・ノードは、欠落しているレプリケーション・メッセージを識別した場合、欠落しているメッセージを取得して同期を維持するための要求をプライマリ管理ノード(PAN)に対して開始します

レプリケーション・シーケンスの概要と同期ステータス

Cisco ISE導入における全体的なレプリケーションワークフローは、次のとおりです。

1. ノード登録：信頼を確立し、展開にノードを追加します。

2. 初期フル同期：完全な構成データベースを新しく登録されたノードに転送します。

3. 差分同期：通常の操作全体を通じて設定変更を継続的に伝播します。

4. 完全同期（必要な場合）：レプリケーションの問題またはデータベースの不一致が検出された場合に、データベースの整合性を再構築します。

この段階的なアプローチにより、Cisco ISEは、ネットワーク使用率とレプリケーションパフォーマンスを最適化しながら、すべてのノードで一貫した設定データベースを維持できます。

同期ステータス

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：ノードは導入と同期されており、レプリケーションは正常に機能しています。
- 黄：ノードが同期されていないか、ノード登録が失敗したか、またはクラスタ接続が失われました（過去5分間、ノードにはクラスタから到達できません）。

- 赤：ノードは物理的に到達不能であり、ネットワーク接続チェック（ICMP pingやHTTPSなど）を通じて接続できません。

注：レプリケーションが正しく行われない場合は、プライマリ管理ノードにログインし、管理>システム>導入に移動してノードを選択し、同期をクリックすることによって、プライマリ管理ノードでセカンダリノードに手動で同期を実行できます。

エンドポイントの複製

エンドポイントレプリケーションは、ISEがすべてのポリシーサービスノード(PSN)とプライマリ管理ノード(PAN)のエンドポイントデータベース情報を同期して、導入全体でエンドポイントIDの一貫したビューを維持するためのプロセスです。

- Cisco　ISEは、ネットワークに接続するデバイスに関する情報を保存する一元化されたエンドポイントデータベースを維持します。この情報には、静的に設定されたエンドポイントと、認証、プロファイリング、ポスチャアセスメント、または外部アイデンティティソースとの統合によって動的に学習されたエンドポイントの両方が含まれます。
- エンドポイント情報が作成または変更されると、Cisco　ISEは変更を展開内の他のノードに複製します。この同期により、すべてのポリシーサービスノード(PSN)は、どのPSNが要求を処理しているかにかかわらず、同じエンドポイント情報を使用して認証および許可要求を評価できます。
- エンドポイントレプリケーションはCisco　ISEによって自動的に処理され、データベースレプリケーションメカニズム全体の一部を構成します。管理者は、通常の操作中に手動でエンドポイントの同期を開始する必要はありません。

エンドポイントレプリケーションの仕組み

- エンドポイントの更新：エンドポイントは、認証、プロファイリング、ポスチャ、または手動設定によって作成または更新されます。
- 変更の検出：Cisco　ISEがエンドポイントの変更を検出し、レプリケーションの準備を行います。
- レプリケーション：更新されたエンドポイント情報は、ISEレプリケーションフレームワークを使用して、展開内の他のノードにレプリケートされます。
- データベースの同期：セカンダリノードは、レプリケートされた情報を使用してローカルエンドポイントデータベースを更新します。
- 一貫したポリシーの適用：同期が完了すると、すべてのポリシーサービスノードが同じエンドポイント情報を使用して認証と認可の決定を行います。

Cisco　ISEリリース3.3以降では、動的に検出されたエンドポイントは、すべてのノードに自動的に複製されません。この機能は、「エンドポイントレプリケーション」ウィンドウで有効または無効にできます。必要に応じて、Administration > System > Settings > Endpoint Replicationの順に移動し、有効または無効にします。

注：エンドポイントのレプリケーションとセッションのレプリケーションを区別することが重要です。エンドポイントレプリケーションでは、永続的なエンドポイントデータベースレコード（MACアドレス、エンドポイントグループ、プロファイリング情報など）を同期しますが、セッションレプリケーションでは、ランタイムセッション情報を同期して、ポリシーの適用と運用継続性をサポートします。これらのメカニズムは独立して動作し、Cisco ISEアーキテクチャ内のさまざまな機能を提供します。

一般的なノード複製の問題

シナリオ1:DNS解決の失敗によるノード登録の失敗

「hostname cannot be resolved.Please check your DNS configuration」というエラー理由でノードの登録に失敗しました。

確認手順

- プライマリ管理ノードとスタンドアロンノードで有効なDNSサーバが設定されていることを確認します。show running-config | include name-serverコマンドを使用して、DNSサーバの設定を確認します。
- nslookup FQDN of the node コマンドを使用して前方参照と逆引きDNS検索を、nslookup ip address of the nodeコマンドを使用して、プライマリ管理ノードとスタンドアロンノードで前方参照と逆引きDNS解決を検証します。
- ISEノードのCLIからコマンドping DNS server IPを使用して、プライマリ管理ノードとスタンドアロンノードからのDNSサーバの到達可能性を検証します。

シナリオ2:管理証明書の期限切れが原因でノード登録が失敗する

ノードの登録が失敗し、エラー理由は「Error loading certificates.現在、ノードに到達できません。Try again later」というメッセージが表示されます。

確認手順

- プライマリ管理ノードとスタンドアロンノードの管理証明書を検証し、有効性と証明書のステータスを確認します。Administration > System > Certificatesの順に移動し、ノードを選択して、管理証明書の有効性とステータスを確認します。
- 管理証明書の有効期限が切れている場合は、証明書を交換または更新し、管理用途が割り当てられていることを確認します。

シナリオ3：バージョンの不一致によりノード登録が失敗する

ノードの登録に失敗しました。エラーの理由は「バージョン/パッチの詳細が一致しません」です。

確認手順

- show versionコマンドを使用してバージョンの詳細が一致していることを確認し、プライマリ管理ノードとスタンドアロンノードのパッチとともにソフトウェアバージョンを検証します。

デバッグログのコンポーネント

Cisco ISEでのレプリケーションの切り分けとトラブルシューティングを行うために、デバッグ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)
- caサービス(caservice.log)
- admin-ca(ise-psc.log)

参考

- ISEでのデバッグのトラブルシューティングと有効化
- ISE：キューリンクエラー
- Cisco Identity Services Engine 管理ガイド リリース 3.4
- Cisco Identity Services Engine 管理ガイド リリース 3.5

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。