Verständnis und Fehlerbehebung bei ISE-Replikationen

Inhalt

Einleitung

In diesem Dokument werden die Replikation und die Fehlerbehebung in der Cisco Identity Services Engine® (ISE) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse der Cisco Identity Services Engine® (ISE) verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Hardware- und Software-Versionen.

- Cisco Identity Services Engine 3.4 und höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Replikation in der Cisco ISE

Bei der Replikation in der ISE werden Konfigurations- und Betriebsdaten über mehrere Knoten in einer Bereitstellung synchronisiert, um sie konsistent zu halten.

Der primäre Administrationsknoten repliziert die Änderungen, die in der Bereitstellung vorgenommen wurden, auf alle anderen (sekundären) Knoten in der Bereitstellung.

Die Cisco ISE verwendet JGroups, ein zuverlässiges Gruppenkommunikations-Framework, als Teil ihrer Replikationsarchitektur. Mithilfe von JGroups können die Knoten in einer ISE-Bereitstellung miteinander kommunizieren und Replikationsdaten austauschen. Es stellt das Messaging-Framework bereit, das die Bereitstellung von Konfigurations- und Datenbankaktualisierungen zwischen Knoten erleichtert und die Synchronisierung der gesamten Bereitstellung aufrechterhält.

- JGroups ist ein Kommunikations-Framework, das von der Cisco ISE für die Replikation verwendet wird. Die replizierten Daten werden nicht gespeichert.
- Nicht alle Daten innerhalb der Cisco ISE werden über JGroups repliziert. Je nach Art der zu übertragenden Daten nutzen verschiedene Dienste unterschiedliche Kommunikationsmechanismen.
- Wenn die Replikation vorübergehend unterbrochen wird, können einige Cisco ISE-Services unter Verwendung lokal verfügbarer Daten weiter ausgeführt werden, bis die Synchronisierung wiederhergestellt ist.

Beispiele für Datenübertragungsmethoden

Daten	Kommunikationsmethode
Konfigurations- und Replikationsmeldungen	JGruppen
Sammlung von Supportpaketen	HTTPS-API (TCP-Port 443)
Debugkonfiguration	HTTPS-API (TCP-Port 443)
Live-Protokolle und -Berichte	RabbitMQ oder UDP, je nach Bereitstellungskonfiguration

Wichtige Voraussetzungen und Validierungsprüfungen für die Cisco ISE-Replikation

- DNS Resolution (DNS-Auflösung): Vorwärts- und Rückwärts-DNS-Lookups müssen für alle an der Bereitstellung beteiligten Cisco ISE-Knoten erfolgreich aufgelöst werden. Für die Knotenkommunikation und Replikationsvorgänge ist eine ordnungsgemäße DNS-Auflösung erforderlich.
- NTP-Synchronisierung: Alle Cisco ISE-Knoten müssen mit einer zuverlässigen NTP-Quelle synchronisiert werden, um eine konsistente Systemzeit in der gesamten Bereitstellung zu gewährleisten. Die Zeitsynchronisierung ist für die Replikation und die Zertifikatsvalidierung unverzichtbar.
- Zertifikate: Das auf jedem Cisco ISE-Knoten installierte Administratorzertifikat muss gültig und vertrauenswürdig sein. Replikationsprozesse sind für die sichere Kommunikation zwischen Knoten auf das Admin-Zertifikat angewiesen.
- Port-Anforderungen: Die Netzwerkkonnektivität muss die Kommunikation über die für Replikations- und Inter-Node-Services erforderlichen Ports ermöglichen:

Service	Protokoll/Port
HTTPS (SOAP)	TCP/443
Datensynchronisierung und -replikation (JGroups)	TCP/12001

Administratorzugriff	TCP/8443
ISE Messaging Service (SSL)	TCP/8671
Synchronisierung der Besitzrechte von Profilern für Endgeräte	TCP/6379

- Netzwerkerreichbarkeit: Netzwerkverbindungen zwischen Cisco ISE-Knoten müssen stabil sein, und die Latenz darf 300 ms nicht überschreiten. Die Überprüfung der Latenz und des Paketverlusts zwischen Knoten trägt zur zuverlässigen Replikation bei.
- Warteschlangen-Verbindungsstatus: Cisco ISE Messaging-Zertifikate werden verwendet, um die Kommunikation zwischen Knoten über den TCP-Port 8671 zu sichern. Ungültige oder beschädigte Messaging-Zertifikate können zu Warteschlangenverbindungsfehlern und Replikationsfehlern führen. In solchen Szenarien muss das ISE-Stammzertifikat der Zertifizierungsstelle oder das ISE-Messaging-Zertifikat ggf. neu generiert werden.
- ISE-Stunnel-Service: Der Cisco ISE-Stunnel-Service wird in verteilten Bereitstellungen ausgeführt und vereinfacht die sichere Kommunikation zwischen Knoten. Der Dienst muss auf allen geeigneten Knoten ausgeführt werden, um die Replikation zu unterstützen. Der Servicestatus kann über die Cisco ISE CLI mit dem folgenden Befehl überprüft werden:
  show tech-support | Stunnel einschließen
- ISE-Patch und -Version: Der primäre Administrationsknoten und der Beitrittsknoten (Standalone-Knoten) müssen die gleiche Version und die gleiche Patch-Ebene aufweisen, damit die Knotenregistrierung und -synchronisierung reibungslos funktionieren.

Phasen der Replikation in der Cisco ISE

Die Replikation in der Cisco ISE besteht aus drei unterschiedlichen Phasen, die zusammenarbeiten, um die Synchronisierung über alle Knoten in der Bereitstellung hinweg herzustellen und aufrechtzuerhalten. Jede Phase dient einem bestimmten Zweck, angefangen bei der Knotenintegration über die anfängliche Datenbanksynchronisierung bis hin zum kontinuierlichen Austausch inkrementeller Updates, um alle Knoten synchronisiert zu halten.

- Knotenregistrierung
- Vollständige Synchronisierung
- Inkrementelle Synchronisierung aktiv

Knotenregistrierung in der Cisco ISE verstehen

Die Knotenregistrierung ist der Prozess, über den ein Cisco ISE-Knoten einer vorhandenen Bereitstellung beitritt und die Kommunikation mit dem primären Administrationsknoten (PAN) herstellt.

Während der Knotenregistrierung:

Schritt 1: Der Beitrittsknoten (eigenständiger Knoten) initiiert die Kommunikation mit dem primären Administrationsknoten.

Phase 2: Die gegenseitige Zertifikatsvalidierung wird mithilfe des Cisco ISE-Admin-Zertifikats durchgeführt.

Schritt 3: DNS-Auflösung, NTP-Synchronisierung, Netzwerkerreichbarkeit und erforderliche Portzugriffsmöglichkeiten werden im Rahmen des Kommunikationsprozesses validiert.

Schritt 4: Der primäre Admin-Knoten überprüft, ob auf dem eigenständigen bzw. verbundenen Knoten eine kompatible Cisco ISE-Version und ein kompatibles Patch-Level ausgeführt wird.

Schritt 5: Bereitstellungsinformationen, Knotenrollen und Vertrauensstellungen werden ausgetauscht.

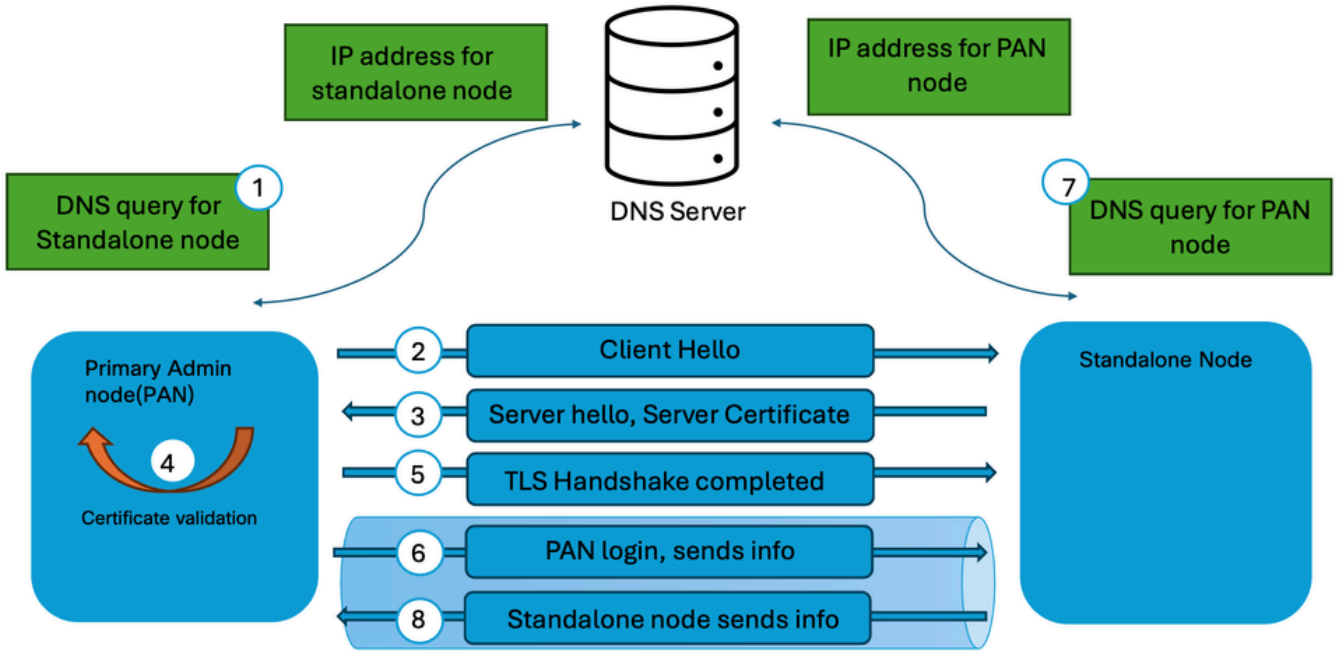
Schritt 6: Datenbankreplikationsdienste werden initialisiert und für die Synchronisierung vorbereitet.

Nach erfolgreichem Abschluss der Knotenregistrierung wird der Knoten als vertrauenswürdiges Mitglied der Bereitstellung eingerichtet, und die Replikationsprozesse können beginnen.

Wichtigste Merkmale

- Tritt auf, wenn der Bereitstellung ein neuer Knoten hinzugefügt wird.
- Schafft Vertrauen und Kommunikationskanäle.
- Es wird nicht sofort die gesamte Konfigurationsdatenbank übertragen.
- Dient als Voraussetzung für nachfolgende Synchronisierungsvorgänge.

Eine detaillierte Erläuterung des Knotenregistrierungsprozesses finden Sie unter Der Knotenregistrierungsprozess in der Cisco ISE.



Knotenregistrierungsprozess

Anmerkung: Bei dem Knoten, der der Bereitstellung hinzugefügt wird, muss es sich um einen eigenständigen Knoten handeln. Darüber hinaus muss die primäre Administrationsfunktion des primären Administrationsknotens (PAN) in der Bereitstellung aktiviert sein, damit eine Knotenregistrierung in der Cisco ISE möglich ist.

Vollständige Synchronisierung auf der Cisco ISE

Die vollständige Synchronisierung ist ein vollständiger Datenbankreplikationsprozess, bei dem die gesamte Konfigurationsdatenbank vom primären PAN auf einen anderen Knoten übertragen wird. Bei der vollständigen Synchronisierung werden nicht nur geänderte Datensätze übertragen. Stattdessen wird der gesamte Konfigurationssatz auf dem empfangenden Knoten neu erstellt.

Eine vollständige Synchronisierung kann in folgenden Szenarien auftreten:

- Erste Synchronisierung nach Knotenregistrierung.
- Recovery nach Replikationsfehlern.
- Erhebliche Datenbankinkonsistenzen
- Erneutes Verbinden eines Knotens mit der Bereitstellung
- Manuelle Synchronisierung, initiiert durch Cisco TAC-Fehlerbehebungsverfahren.
- Interne Replikationsmechanismen stellen fest, dass die inkrementelle Synchronisierung die Datenbankkonsistenz nicht mehr wiederherstellen kann.

Während der vollständigen Synchronisierung:

Schritt 1: Der primäre Administrationsknoten bereitet einen vollständigen Datenbank-Snapshot vor.

Phase 2: Konfigurationsdaten werden in der DMP-Datei gepackt und an den empfangenden Knoten übertragen.

Schritt 3: Vorhandene replizierte Daten auf dem empfangenden Knoten werden validiert und aktualisiert.

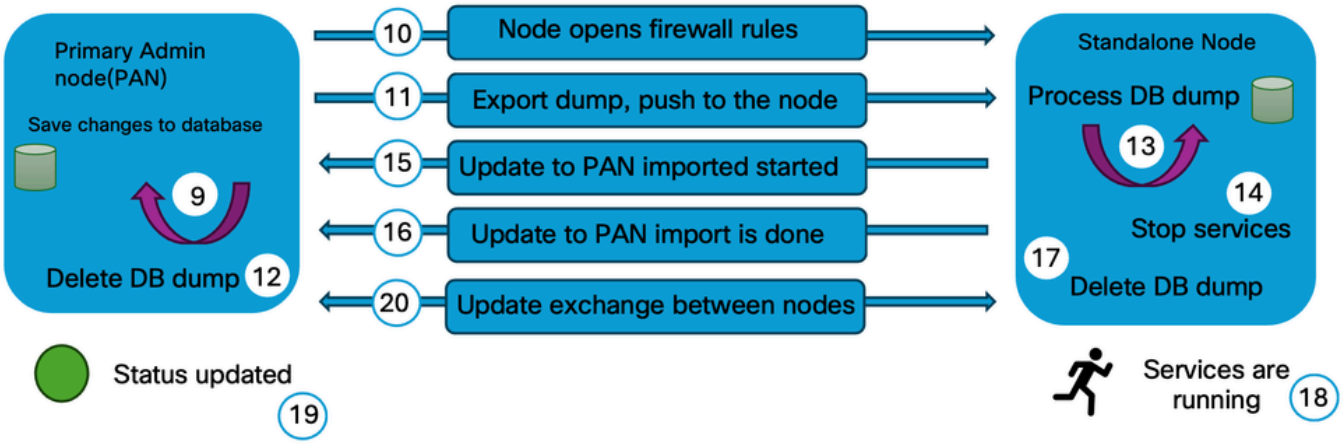
Schritt 4: Die gesamte Konfigurationsdatenbank wird neu erstellt, sodass sie mit dem primären Admin-Knoten übereinstimmt.

Schritt 5: Der Replikationsstatus wird nach Abschluss überprüft.

Da eine vollständige Synchronisierung wesentlich mehr Daten als eine inkrementelle Synchronisierung erfordert, sind zusätzliche Verarbeitungszeit und Netzwerkressourcen erforderlich.

Merkmale der vollständigen Synchronisierung

- Überträgt die gesamte Konfigurationsdatenbank.
- mehr Bandbreite und Systemressourcen verbraucht.
- Dauert länger als die inkrementelle Synchronisierung.
- Stellt Datenbankkonsistenz wieder her, wenn Diskrepanzen erkannt werden.
- tritt in der Regel seltener auf als inkrementelle Synchronisierungen.



Vollständiger Synchronisierungsprozess

Inkrementelle Synchronisierung in der Cisco ISE

Die inkrementelle Synchronisierung ist der fortlaufende Replikationsmechanismus, der von der Cisco ISE verwendet wird, um Konfigurationsänderungen zu verteilen, nachdem Knoten der Bereitstellung erfolgreich beigetreten sind. Wenn ein Administrator am PAN eine Konfigurationsänderung vornimmt, überträgt die Cisco ISE nicht die gesamte Datenbank. Stattdessen werden nur die modifizierten Datensätze auf die Subscriber-Knoten repliziert.

Beispiele für Änderungen, die durch inkrementelle Synchronisierung repliziert werden:

- Richtlinienänderungen
- Ergänzungen oder Updates von Netzwerkgeräten
- Änderungen an Endpunktgruppen
- Autorisierungsprofil-Updates
- Zertifikatbezogene Konfigurationsänderungen
- Konfigurationsaktualisierungen für die Identitätsquelle

Der inkrementelle Synchronisierungsprozess wird kontinuierlich ausgeführt und ist so konzipiert, dass die Konsistenz über alle Knoten hinweg erhalten bleibt, während gleichzeitig die Bandbreitennutzung und der Replikationsaufwand minimiert werden.

Vorteile der inkrementellen Synchronisierung

- Reduzierung des Replikationsdatenverkehrs
- Minimiert die Synchronisierungszeit.
- Ermöglicht die schnelle Übertragung von Konfigurationsänderungen.
- Erhält nahezu in Echtzeit Konsistenz über die gesamte Bereitstellung hinweg.

Replikations-Workflow

Schritt 1: Die Konfiguration wird im primären Administrationsknoten geändert.

Phase 2: Die Änderung wird in die Datenbank des primären Administrationsknotens geschrieben.

Schritt 3: Replikationsdienste identifizieren die geänderten Datensätze.

Schritt 4: Der primäre Administrationsknoten schreibt die neuen Ereignisse/Änderungen in eine Transaktionstabelle.

Schritt 5: Separate Threads von PAN veröffentlichen die Informationen/Änderungen an den sekundären Knoten in der Bereitstellung.

Schritt 6: Sekundäre Knoten in der Bereitstellung erhalten die Änderungen vom primären Administrationsknoten.

Schritt 7: Sekundäre Knoten in der Bereitstellung wenden die vom primären Administrationsknoten empfangenen Änderungen an.

Schritt 8: Der Replikationsstatus wird nach erfolgreichem Abschluss aktualisiert.

Unter normalen Betriebsbedingungen erfolgen die meisten Replikationsaktivitäten in der Cisco ISE durch inkrementelle Synchronisierung.

Anmerkung: Wenn ein sekundärer Knoten fehlende Replikationsmeldungen identifiziert, initiiert er eine Anforderung an den primären Administrationsknoten (PAN), um die fehlenden Meldungen abzurufen und die Synchronisierung aufrechtzuerhalten.

Übersicht über die Replikationssequenz und Synchronisierungsstatus

Der gesamte Replikations-Workflow in einer Cisco ISE-Bereitstellung kann wie folgt zusammengefasst werden:

1. Knotenregistrierung: Erstellt Vertrauenswürdigkeit und fügt den Knoten zur Bereitstellung hinzu.

2. Anfängliche vollständige Synchronisierung: Überträgt die gesamte Konfigurationsdatenbank an den neu registrierten Knoten.

3. Inkrementelle Synchronisierung: Kontinuierliche Weitergabe von Konfigurationsänderungen im gesamten normalen Betrieb

4. Vollständige Synchronisierung (falls erforderlich): Stellt Datenbankkonsistenz wieder her, wenn

Replikationsprobleme oder Datenbankkonflikte erkannt werden.

Dieser Ansatz in mehreren Phasen ermöglicht es der Cisco ISE, eine konsistente Konfigurationsdatenbank für alle Knoten zu verwalten und gleichzeitig die Netzwerkauslastung und die Replikations-Performance zu optimieren.

Synchronisierungsstatus

Der für jeden Knoten angezeigte Synchronisierungsstatus gibt den aktuellen Replikations- und Verbindungsstatus an:

- Grün - Der Knoten ist mit der Bereitstellung synchronisiert, und die Replikation funktioniert normal.
- Gelb - Der Knoten ist nicht synchronisiert, die Knotenregistrierung ist fehlgeschlagen, oder die Clusterverbindung wurde unterbrochen (der Knoten war vom Cluster in den letzten fünf Minuten nicht erreichbar).
- Rot - Der Knoten ist physisch nicht erreichbar und kann nicht durch Netzwerkverbindungsprüfungen (z. B. ICMP-Ping und HTTPS) kontaktiert werden.

Anmerkung: Wenn die Replikation nicht ordnungsgemäß ausgeführt wird, können Sie die manuelle Synchronisierung mit den sekundären Knoten mit dem Knoten für die primäre Administration durchführen, indem Sie sich beim Knoten für die primäre Administration anmelden. Navigieren Sie zu Administration > System > Deployment > wählen Sie den Knoten aus, und klicken Sie auf Sync up (Synchronisieren).

Endgeräte-Replikation

Die Endpunktreplikation ist der Prozess, bei dem die ISE Endpunktdatenbankinformationen über alle Policy Service Nodes (PSNs) und den Primary Administration Node (PAN) synchronisiert, um eine konsistente Ansicht der Endpunktidentität während der gesamten Bereitstellung zu erhalten.

- Die Cisco ISE unterhält eine zentralisierte Endgerätedatenbank, in der Informationen zu den mit dem Netzwerk verbundenen Geräten gespeichert werden. Diese Informationen umfassen sowohl statisch konfigurierte Endpunkte als auch dynamisch erfasste Endpunkte durch Authentifizierung, Profilerstellung, Statusüberprüfung oder Integration mit externen Identitätsquellen.
- Wenn Endgeräteinformationen erstellt oder geändert werden, repliziert die Cisco ISE die Änderungen an anderen Knoten in der Bereitstellung. Diese Synchronisierung ermöglicht es jedem Policy Service Node, Authentifizierungs- und Autorisierungsanforderungen unter Verwendung derselben Endpunktinformationen auszuwerten, unabhängig davon, welches

PSN die Anforderung verarbeitet.

- Die Endpunktreplikation wird automatisch von der Cisco ISE verarbeitet und ist Teil des allgemeinen Datenbankreplikationsmechanismus. Administratoren müssen die Endpunktsynchronisierung während des normalen Betriebs nicht manuell initiieren.

Funktionsweise der Endpunktreplikation

- Endpunkt-Update: Ein Endpunkt wird durch Authentifizierung, Profilerstellung, Status oder manuelle Konfiguration erstellt oder aktualisiert.
- Änderungserkennung: Die Cisco ISE erkennt die Änderung an den Endgeräten und bereitet sie auf die Replikation vor.
- Replikation: Die aktualisierten Endpunktinformationen werden mithilfe des ISE-Replikations-Frameworks auf die anderen Knoten in der Bereitstellung repliziert.
- Datenbanksynchronisierung: Die sekundären Knoten aktualisieren ihre lokale Endpunktdatenbank mit den replizierten Informationen.
- Konsistente Richtliniendurchsetzung: Nach Abschluss der Synchronisierung verwenden alle Policy Service Nodes dieselben Endpunktinformationen für Authentifizierungs- und Autorisierungsentscheidungen.

Ab Cisco ISE Version 3.3 werden dynamisch erkannte Endgeräte nicht automatisch auf alle Knoten repliziert. Diese Funktion kann im Fenster für die Endpunktreplikation aktiviert oder deaktiviert werden. Navigieren Sie zu Administration > System > Settings > Endpoint Replication, aktivieren oder deaktivieren Sie diese Option je nach Anforderung.

Anmerkung: Es ist wichtig, zwischen Endpunktreplikation und Sitzungsreplikation zu unterscheiden. Bei der Endpunktreplikation werden persistente Datensätze der Endpunktdatenbank (z. B. MAC-Adressen, Endpunktgruppen und Profilierungsinformationen) synchronisiert, während bei der Sitzungsreplikation Laufzeitsitzungsinformationen synchronisiert werden, um die Durchsetzung von Richtlinien und die Betriebskontinuität zu unterstützen. Diese Mechanismen arbeiten unabhängig voneinander und erfüllen unterschiedliche Funktionen innerhalb der Cisco ISE-Architektur.

Häufige Probleme bei der Knotenreplikation

Szenario 1: Knotenregistrierung aufgrund eines DNS-Auflösungsfehlers fehlgeschlagen

Fehler bei der Knotenregistrierung. Fehlerursache: "Hostname kann nicht aufgelöst werden.Bitte überprüfen Sie Ihre DNS-Konfiguration."

Schritte zur Verifizierung

- Stellen Sie sicher, dass der gültige DNS-Server im primären Administrationsknoten und im eigenständigen Knoten konfiguriert ist. Überprüfen Sie die Konfiguration des DNS-Servers mit dem Befehl show running-config. | Name-Server einschließen
- Validieren Sie die Auflösung von Forward- und Reverse-DNS im primären Administrationsknoten und im Standalone-Knoten. Verwenden Sie dazu den Befehl nslookup FQDN des Knotens für Forward-DNS-Lookup und die nslookup IP-Adresse des Knotens für Reverse-DNS-Lookup.
- Überprüfen Sie die Erreichbarkeit des DNS-Servers über den primären Administrationsknoten und den eigenständigen Knoten, indem Sie den Befehl ping DNS server IP von der CLI der ISE-Knoten verwenden.

Szenario 2: Fehler bei der Knotenregistrierung aufgrund des Ablaufs des Administratorzertifikats.

Fehler bei der Knotenregistrierung. Fehlerursache: "Fehler beim Laden der Zertifikate. Knoten derzeit nicht erreichbar. Versuchen Sie es später erneut".

Schritte zur Verifizierung

- Validieren Sie die Admin-Zertifikate des primären Administrationsknotens und des Standalone-Knotens, um die Gültigkeit und den Zertifikatsstatus sicherzustellen. Navigieren Sie zu Administration > System > Certificates, wählen Sie den Knoten aus, und überprüfen Sie die Gültigkeit und den Status des Admin-Zertifikats.
- Wenn das Administratorzertifikat abgelaufen ist, ersetzen oder erneuern Sie das Zertifikat, und stellen Sie sicher, dass die Administratorbenutzung zugewiesen ist.

Szenario 3: Knotenregistrierung aufgrund von Versionskonflikt fehlgeschlagen

Fehler bei der Knotenregistrierung. Fehlerursache: "Version/Patch-Details stimmen nicht überein".

Schritte zur Verifizierung

- Validieren Sie die Softwareversion zusammen mit dem Patch für den primären Admin-Knoten und den eigenständigen Knoten, indem Sie den Befehl show version verwenden, um sicherzustellen, dass die Versionsdetails übereinstimmen.

Komponenten für Debug-Protokolle

Dies sind die allgemeinen Komponenten, die im Debug-Modus eingerichtet werden müssen, um die Replikation in der Cisco ISE zu isolieren und Fehler zu beheben.

- Replication-Deployment (Replication.log und ise-psc.log)
- Replication-JGroup (Replication.log und ise-psc.log)
- Replication Tracker (tracking.log)
- hibernate (hibernate.log)
- JMS (replikation.log)
- ca-service (caservice.log)
- admin-ca (ise-psc.log)

Referenz

- Fehlerbehebung und Aktivieren von Debuggen auf der ISE
- ISE - Warteschlangenverbindungsfehler
- Administratorleitfaden für die Cisco Identity Services Engine, Version 3.4
- Administratoranleitung für die Cisco Identity Services Engine, Version 3.5

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.