ISE-Zertifikatreplikations-Alarme verstehen und Fehlerbehebung dafür durchführen

Inhalt

Einleitung

Dieses Dokument beschreibt die Replikations-Alarme und deren Fehlerbehebung in Cisco Identity Services Engine® (ISE).

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® (ISE) 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.

Replikations-Alarm

Replikationswarnungen in der Cisco ISE bieten Transparenz hinsichtlich des Status und der Synchronisierung des Replikations-Frameworks in der gesamten Bereitstellung. Diese Alarme helfen, Bedingungen zu identifizieren, die die Datenkonsistenz, Knotenkommunikation oder Replikationsprozesse beeinträchtigen können, sodass Administratoren Probleme erkennen und beheben können, bevor sie sich auf den Systembetrieb auswirken. Um eine intakte ISE-Bereitstellung aufrechtzuerhalten und sicherzustellen, dass Konfigurations- und Betriebsdaten über alle Knoten hinweg synchronisiert bleiben, ist es wichtig, den Zweck und die Bedeutung von Replikationswarnungen zu kennen.

ISE-Zertifikatreplikations-Alarme

Fehler bei der Zertifikatreplikation

Der Alarm "Certificate Replication Failed" wird generiert, wenn die Cisco ISE keine zertifikatbezogenen Daten vom primären Administrationsknoten (PAN) auf einen oder mehrere Knoten in der Bereitstellung replizieren kann. Die ISE repliziert Zertifikate und die zugehörige Konfiguration automatisch, wenn Zertifikate auf dem primären PAN importiert, generiert, erneuert oder geändert werden, um die Konsistenz über alle Knoten hinweg aufrechtzuerhalten. Dieser Alarm zeigt an, dass der Replikationsprozess nicht erfolgreich war, was zu einer inkonsistenten Zertifikatkonfiguration auf den betroffenen Knoten geführt hat.

Grund für Alarm

Der Alarm "Certificate Replication Failed" (Replikation von Zertifikaten fehlgeschlagen) kann ausgelöst werden, wenn die Cisco ISE nicht in der Lage ist, zertifikatbezogene Daten auf einem oder mehreren Knoten erfolgreich zu übertragen, zu validieren oder zu installieren. Häufige Ursachen:

- Probleme bei der Netzwerkkommunikation: Paketverlust, hohe Netzwerklatenz, Firewall-

Beschränkungen, die den Replikationsverkehr blockieren, Routing-Probleme zwischen ISE-Knoten oder eine MTU-Diskrepanz, die zu einer Paketfragmentierung oder Paketverlusten führt, können die Zertifikatreplikation unterbrechen.
- Probleme mit dem Replikationsdienst: Die Zertifikatreplikation kann fehlschlagen, wenn RabbitMQ, JGroups oder andere interne Replikationsdienste nicht verfügbar sind, neu starten oder nicht ordnungsgemäß funktionieren.
- Fehler bei der Zertifikatsüberprüfung: Die Replikation kann fehlschlagen, wenn die Zertifikatkette unvollständig ist, CA- oder Zwischenzertifikate fehlen, das Zertifikat abgelaufen oder beschädigt ist oder eine nicht unterstützte Schlüsselverwendung oder ein ungültiges Format enthält.
- Probleme bei der Knotenkommunikation: Wenn der Zielknoten offline, neu gestartet, registriert, von der Bereitstellung getrennt oder nicht erreichbar ist, kann die Zertifikatreplikation nicht abgeschlossen werden.
- Unzureichender Speicherplatz: Der Zielknoten verfügt nicht über genügend Speicherplatz, um das replizierte Zertifikat zu importieren und zu installieren.
- Interne Datenbankprobleme: Die Replikation kann fehlschlagen, wenn die ISE-Konfigurationsdatenbank die Zertifikatmetadaten nicht speichern oder aktualisieren kann.

Auswirkungen des Alarms

Die Auswirkung dieses Alarms hängt vom Typ des replizierten Zertifikats und den Diensten ab, die darauf angewiesen sind. Fehlgeschlagene Zertifikatreplikation kann zu inkonsistenter Zertifikatkonfiguration über ISE-Knoten, HTTPS-Zertifikatfehlübereinstimmungen, EAP-Authentifizierungsfehlern, pxGrid-Vertrauensstellungsproblemen, SCEP-Registrierung oder Zertifikatbereitstellungsfehlern, Inkonsistenzen im vertrauenswürdigen Zertifikatspeicher und TLS-Validierungsfehlern mit externen Integrationen führen.

Zertifikatreplikation vorübergehend fehlgeschlagen

Der Alarm "Zertifikatsreplikation vorübergehend fehlgeschlagen" wird generiert, wenn die Cisco ISE vorübergehend nicht in der Lage ist, zertifikatbezogene Daten vom primären Administrationsknoten (PAN) auf einen oder mehrere Knoten in der Bereitstellung zu replizieren. Im Gegensatz zum Alarm "Certificate Replication Failed" (Replikation mit Zertifikat fehlgeschlagen) weist dieser Alarm darauf hin, dass der Replikationsfehler als vorübergehend gilt, und die Cisco ISE wiederholt den Replikationsvorgang automatisch, wenn die zugrunde liegende Bedingung behoben ist.

Grund für Alarm

Der Alarm wird in der Regel aufgrund vorübergehender Bedingungen generiert, die die Replikation des Zertifikats vorübergehend verhindern. Zu den häufigen Ursachen gehören:

- Temporäre Netzwerkkommunikationsprobleme: Kurze Netzwerkunterbrechungen, Paketverluste, hohe Latenz, Firewall-Verzögerungen oder vorübergehende Routing-Probleme zwischen ISE-Knoten.
- Initialisierung oder Neustart des Replikationsdiensts: RabbitMQ, JGroups oder andere interne Replikationsdienste werden neu gestartet oder sind vorübergehend nicht verfügbar.
- Nichtverfügbarkeit temporärer Knoten: Der Zielknoten wird gestartet, die Anwendungsdienste werden neu gestartet, die Bereitstellung wird wieder aufgenommen, oder er ist vorübergehend nicht erreichbar.
- Temporäre Systemressourceneinschränkungen: Hohe CPU-Auslastung, Arbeitsspeicherdruck oder Festplatten-E/A-Konflikte verzögern die Replikationsverarbeitung vorübergehend.
- Gleichzeitige Verwaltungsvorgänge: Die Zertifikatreplikation kann verzögert werden, während ein anderer Zertifikatimport, eine andere Sicherung, Wiederherstellung, Patch-Installation oder eine andere Bereitstellungssynchronisierung ausgeführt werden.
- Verzögerungen bei temporären Datenbanken oder Replikationswarteschlangen: Interne Datenbankvorgänge oder Replikationswarteschlangen sind vorübergehend mit der Verarbeitung anderer Synchronisierungsanforderungen beschäftigt.

Auswirkungen des Alarms

In den meisten Fällen hat dieser Alarm nur minimale Auswirkungen auf den Betrieb, da die Cisco ISE den Replikationsvorgang automatisch wiederholt. Bis die Replikation erfolgreich abgeschlossen ist, können jedoch temporäre Inkonsistenzen zwischen den Knoten bestehen, darunter:

- Verzögerte Übertragung neu importierter oder verlängerter Zertifikate
- Temporäre Zertifikatkonfigurationskonflikte in der gesamten Bereitstellung
- Verzögerte Verfügbarkeit zertifikatbasierter Services auf dem betroffenen Knoten
- Temporäre Verzögerungen bei HTTPS-, EAP-, pxGrid- oder SCEP-Services, wenn diese vom replizierten Zertifikat abhängen

Wenn der Alarm andauert oder wiederholt auftritt, führt dies zu einem Alarm "Zertifikatreplikation fehlgeschlagen".

Fehlerbehebung bei ISE-Zertifikatreplikations-Alarmen

Dies sind die allgemeinen Faktoren, die bei der Fehlerbehebung oder Überprüfung von Zertifikatsreplikations-Alarmen in der ISE überprüft werden müssen.

1. Überprüfen des Bereitstellungsstatus für den Knoten

Damit die Zertifikatreplikation erfolgreich ist, muss sich der sekundäre Knoten in der Cisco ISE-Bereitstellung im Status Verbunden befinden. Navigieren Sie zu Administration > System > Deployment, und überprüfen Sie den Status des betroffenen Knotens. Bewegen Sie den Mauszeiger über das Informationssymbol (i) neben dem Knotenstatus, um die Synchronisierungsdetails und alle ausstehenden Replikationsmeldungen anzuzeigen.

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 ist unterbrochen. Dieser Status zeigt an, dass der Knoten vom Cluster in den letzten fünf Minuten nicht erreichbar war.
- Rot - Der Knoten ist nicht erreichbar und kann nicht durch Netzwerkverbindungsprüfungen wie ICMP-Ping oder HTTPS kontaktiert werden.

Wenn der Knoten einen gelben oder roten Status anzeigt, weist er auf ein Replikations- oder Verbindungsproblem hin, das diesen Knoten betrifft. Überprüfen Sie außerdem die Anzahl der Replikationsmeldungen, die in den Knoteninformationen angezeigt wird. Die Anzahl ausstehender Nachrichten muss 5.000 oder weniger betragen. Eine Warteschlange mit mehr als 5.000 ausstehenden Nachrichten zeigt an, dass sich die Replikationswarteschlange angesammelt hat, was eine erfolgreiche Replikation verzögern oder verhindern kann.

2. Überprüfen Sie den Warteschlangenverbindungsalarm in der Bereitstellung.

Die erfolgreiche Replikation in der Cisco ISE hängt von der Verfügbarkeit und Kommunikation des RabbitMQ-Messaging-Services und des Cluster-Kommunikations-Frameworks von JGroups ab. Wenn bei einer der Komponenten Kommunikationsprobleme auftreten, generiert die Cisco ISE Warteschlangenverbindungsfehler, die die Replikation zwischen Bereitstellungsknoten unterbrechen können.

Um den Alarmstatus zu überprüfen, navigieren Sie zu Operations > Dashboard > Alarms, und überprüfen Sie die betroffenen Knoten auf Queue Link Errors (Verbindungsfehler in der Warteschlange).

Wenn Verbindungsfehler in der Warteschlange vorhanden sind, erneuern Sie das Cisco ISE Root CA-Zertifikat, da Kommunikationsfehler aufgrund von Zertifikaten in der Regel zu Verbindungsfehlern in der Warteschlange führen. Sobald das Zertifikatproblem behoben ist, wird die Replikation in der Regel automatisch ohne zusätzlichen Eingriff fortgesetzt.

Anmerkung: Ausführliche Informationen zu Warteschlangenverbindungsfehlern finden Sie in der Dokumentation zu ISE-Warteschlangenverbindungsfehlern.

3. Überprüfung der Netzwerklatenz und -anbindung

Die Cisco ISE-Replikation basiert auf einer stabilen Netzwerkverbindung zwischen Bereitstellungsknoten. Hohe Netzwerklatenz oder intermittierende Verbindungen können die Replikation verzögern und zu Synchronisierungsfehlern führen, insbesondere in geografisch verteilten Bereitstellungen.

Überprüfen Sie die Netzwerklatenz zwischen den betroffenen Knoten mithilfe von Verbindungstests wie Ping. Für eine zuverlässige Replikation muss die Round-Trip-Latenz zwischen Knoten innerhalb von ca. 300 ms bleiben. Eine konsistente Latenz, die diesen Schwellenwert überschreitet, kann sich negativ auf die Replikations-Performance und die Synchronisierung auswirken.Stellen Sie außerdem sicher, dass es keine intermittierenden Netzwerkausfälle, Paketverluste oder Firewall-Beschränkungen gibt, die die Kommunikation zwischen den Bereitstellungsknoten beeinträchtigen.

4. Überprüfen Sie, ob das Zertifikat auf dem betroffenen Knoten bereits vorhanden ist.

Die Zertifikatreplikation kann fehlschlagen, wenn das replizierte Zertifikat bereits auf dem sekundären Knoten vorhanden ist.

Navigieren Sie zu Administration > System > Certificates, wählen Sie den betroffenen Knoten aus, und überprüfen Sie, ob das Zertifikat bereits installiert ist. Wenn das Zertifikat vorhanden ist, überprüfen Sie seine Eigenschaften, um sicherzustellen, dass es mit dem replizierten Zertifikat übereinstimmt, und ermitteln Sie, ob doppelte oder in Konflikt stehende Zertifikate vorhanden sind.

5. Überprüfen der Auslastung der Systemressourcen

Eine hohe Auslastung der Systemressourcen kann die Leistung der Cisco ISE beeinträchtigen und Replikationsaufgaben verzögern. Eine übermäßige CPU-, Arbeitsspeicher- oder Festplattennutzung kann den erfolgreichen Abschluss von Replikationsprozessen verhindern.

Überprüfen Sie, ob der betroffene Knoten über ausreichende Systemressourcen verfügt und die Ressourcenauslastung innerhalb der empfohlenen Betriebsgrenzen bleibt. Wenn die Ressourcenauslastung konstant hoch ist, weisen Sie zusätzliche Ressourcen zu oder reduzieren die Arbeitslast auf dem Knoten, um die normale Replikations-Performance wiederherzustellen.

Anmerkung: Im Leitfaden zu Leistung und Skalierbarkeit finden Sie die empfohlenen Richtlinien zur Hardwaredimensionierung und Ressourcenzuweisung für Cisco ISE-Bereitstellungen.

6. Überprüfen der Portverfügbarkeit in der Bereitstellung und im Netzwerk

Für die Cisco ISE-Replikation müssen bestimmte TCP-Ports zwischen allen Knoten in der Bereitstellung offen bleiben, um eine unterbrechungsfreie Kommunikation und eine erfolgreiche Replikation zu gewährleisten. Wenn einer dieser Ports durch eine Firewall, eine Zugriffskontrollrichtlinie oder ein Netzwerkgerät blockiert wird, können Replikationsfehler oder Synchronisierungsprobleme auftreten.

Stellen Sie sicher, dass diese TCP-Ports offen sind und zwischen allen Cisco ISE-Knoten erreichbar sind:

- TCP 443 - HTTPS-Kommunikation
- TCP 8443 - Administrative Kommunikation
- TCP 12001 - Clusterkommunikation und Replikation von Gruppen
- TCP 6379 - Interne Messaging-Services
- TCP 8671 - Cisco ISE Messaging (RabbitMQ)

Melden Sie sich bei der Cisco ISE CLI an, und führen Sie den Befehl show ports aus, um die im Knoten zulässigen Ports zu überprüfen.

Vergewissern Sie sich, dass die erforderlichen Ports auf dem Cisco ISE-Knoten aktiviert sind, und stellen Sie sicher, dass sie über den Netzwerkpfad zugelassen sind. Vergewissern Sie sich, dass keine zwischengeschalteten Firewalls, Sicherheitsgeräte oder Netzwerkrichtlinien die Kommunikation zwischen den Bereitstellungsknoten auf diesen Ports blockieren.

Protokollerfassung für Replikationswarnungen

Dies sind die allgemeinen Komponenten, die im Debug-Modus eingerichtet werden müssen, um Replikationswarnungen in der Cisco ISE zu isolieren und Probleme damit 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)

Referenz

- Administratoranleitung für die Cisco Identity Services Engine, Version 3.5
- Fehlerbehebung und Aktivieren von Debuggen auf der ISE
- Collect Support-Paket auf der Identity Services Engine

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.