Comprendere e risolvere i problemi relativi agli allarmi di replica dei certificati ISE

Sommario

Introduzione

Questo documento descrive gli allarmi di replica e la relativa risoluzione dei problemi in Cisco Identity Services Engine® (ISE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di Cisco Identity Services Engine® (ISE).

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni hardware e software.

- Cisco Identity Services Engine® (ISE) 3.4 e versioni successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Allarme di replica

Gli allarmi di replica in Cisco ISE forniscono visibilità sullo stato e sullo stato di sincronizzazione del framework di replica nell'intera implementazione. Questi allarmi consentono di identificare le condizioni che possono influire sulla coerenza dei dati, sulla comunicazione dei nodi o sui processi di replica, consentendo agli amministratori di rilevare e risolvere i problemi prima che abbiano un impatto sulle operazioni del sistema. Comprendere lo scopo e l'importanza degli allarmi di replica è essenziale per mantenere un'implementazione ISE efficiente e garantire che la configurazione e i dati operativi rimangano sincronizzati su tutti i nodi.

Avvisi di replica certificati ISE

Replica certificato non riuscita

L'allarme Replica del certificato non riuscita viene generato quando Cisco ISE non riesce a replicare i dati relativi ai certificati dal PAN (Primary Administration Node) a uno o più nodi nella distribuzione. ISE replica automaticamente i certificati e la configurazione associata ogni volta che i certificati vengono importati, generati, rinnovati o modificati sulla PAN primaria per mantenere la coerenza su tutti i nodi. Questo avviso indica che il processo di replica non è riuscito e ha generato una configurazione del certificato incoerente nei nodi interessati.

Motivo dell'allarme

L'allarme Replica del certificato non riuscita può verificarsi quando Cisco ISE non è in grado di trasferire, convalidare o installare correttamente i dati relativi ai certificati su uno o più nodi. Le cause più comuni includono

- Problemi di comunicazione di rete: Perdita di pacchetti, latenza di rete elevata, restrizioni del firewall che bloccano il traffico di replica, problemi di routing tra i nodi ISE o una mancata corrispondenza MTU che causa la frammentazione dei pacchetti o le perdite possono interrompere la replica dei certificati.

- Problemi relativi al servizio di replica: La replica dei certificati può avere esito negativo se RabbitMQ, JGroups o altri servizi di replica interni non sono disponibili, vengono riavviati o non funzionano correttamente.
- Errori di convalida certificato: La replica può avere esito negativo se la catena di certificati è incompleta, mancano certificati intermedi o CA, il certificato è scaduto o danneggiato oppure contiene un utilizzo di chiavi non supportato o un formato non valido.
- Problemi di comunicazione dei nodi: Se il nodo di destinazione è offline, è in corso il riavvio, è stata annullata la registrazione, è stata disconnessa dalla distribuzione o non è raggiungibile, non sarà possibile completare la replica dei certificati.
- Spazio su disco insufficiente: Il nodo di destinazione non dispone di spazio su disco sufficiente per importare e installare il certificato replicato.
- Problemi relativi al database interno: La replica può avere esito negativo se il database di configurazione ISE non è in grado di archiviare o aggiornare i metadati del certificato.

Impatto dell'allarme

L'impatto di questo avviso dipende dal tipo di certificato replicato e dai servizi che lo utilizzano. La replica non riuscita dei certificati può causare una configurazione incoerente dei certificati nei nodi ISE, mancate corrispondenze dei certificati HTTPS, errori di autenticazione EAP, problemi di definizione dell'attendibilità PxGrid, errori di registrazione SCEP o di provisioning dei certificati, incoerenze nell'archivio certificati attendibile ed errori di convalida TLS con integrazioni esterne.

Replica certificati temporaneamente non riuscita

L'allarme Replica temporanea dei certificati viene generato quando Cisco ISE non è temporaneamente in grado di replicare i dati relativi ai certificati dal nodo di amministrazione primario (PAN) a uno o più nodi nella distribuzione. A differenza dell'allarme Certificate Replication Failed, questo allarme indica che l'errore di replica è considerato transitorio e Cisco ISE riprova automaticamente l'operazione di replica quando la condizione sottostante viene risolta.

Motivo dell'allarme

L'avviso viene in genere generato a causa di condizioni transitorie che impediscono temporaneamente la replica dei certificati. Le cause più comuni sono:

- Problemi temporanei di comunicazione di rete: Brevi interruzioni di rete, perdita di pacchetti, alta latenza, ritardi del firewall o problemi di routing temporanei tra i nodi ISE.
- Inizializzazione o riavvio del servizio di replica: RabbitMQ, JGroups o altri servizi di replica interni sono in fase di riavvio o temporaneamente non disponibili.
- Non disponibilità nodo temporaneo: Il nodo di destinazione sta eseguendo l'avvio, il riavvio dei servizi dell'applicazione, il rientro nella distribuzione o è temporaneamente

irraggiungibile.
- Vincoli risorse di sistema temporanei: L'elevato utilizzo della CPU, la pressione della memoria o la contesa di I/O su disco ritardano temporaneamente l'elaborazione della replica.
- Operazioni amministrative simultanee: La replica dei certificati può essere ritardata mentre è in corso un'altra sincronizzazione di importazione, backup, ripristino, installazione di patch o distribuzione dei certificati.
- Ritardi temporanei nella coda di replica o nel database: Le operazioni interne del database o le code di replica sono temporaneamente occupate nell'elaborazione di altre richieste di sincronizzazione.

Impatto dell'allarme

Nella maggior parte dei casi, questo allarme ha un impatto operativo minimo perché Cisco ISE ripete automaticamente l'operazione di replica. Tuttavia, fino a quando la replica non viene completata correttamente, possono esistere incoerenze temporanee tra i nodi, tra cui:

- Propagazione ritardata dei nuovi certificati importati o rinnovati
- Configurazione del certificato temporaneo non corrispondente nella distribuzione
- Disponibilità ritardata dei servizi basati su certificati nel nodo interessato
- Ritardi temporanei nei servizi HTTPS, EAP, pxGrid o SCEP se dipendono dal certificato replicato

Se l'avviso persiste o si verifica ripetutamente, viene generato l'avviso Replica certificato non riuscita.

Risoluzione dei problemi relativi agli allarmi di replica dei certificati ISE

Questi sono i fattori comuni da verificare durante la risoluzione dei problemi o la verifica degli allarmi di replica dei certificati in ISE.

1. Verificare lo stato della distribuzione per il nodo

Affinché la replica dei certificati abbia esito positivo, il nodo secondario deve essere in stato Connected all'interno dell'implementazione di Cisco ISE. Passare a Amministrazione > Sistema > Distribuzione e verificare lo stato del nodo interessato. Posizionare il puntatore del mouse sull'icona Informazioni (i) accanto allo stato del nodo per esaminare i dettagli della sincronizzazione ed eventuali messaggi di replica in sospeso.

Lo stato di sincronizzazione visualizzato per ogni nodo indica lo stato corrente di replica e

connettività:

- Verde: il nodo è sincronizzato con la distribuzione e la replica funziona normalmente.
- Giallo: il nodo non è sincronizzato, la registrazione del nodo non è riuscita o la connettività del cluster è stata persa. Questo stato indica che il nodo non è stato raggiungibile dal cluster negli ultimi cinque minuti.
- Rosso: il nodo non è raggiungibile e non può essere contattato tramite controlli della connettività di rete, ad esempio ping ICMP o HTTPS.

Se nel nodo viene visualizzato lo stato Giallo o Rosso, significa che si è verificato un problema di replica o di connettività che interessa il nodo. Verificare inoltre il conteggio dei messaggi di replica visualizzato nelle informazioni sul nodo. Il numero di messaggi in sospeso deve essere minore o uguale a 5.000. Una coda contenente più di 5.000 messaggi in sospeso indica che la coda di replica è stata accumulata, con il rischio di ritardare o impedire il completamento della replica.

2. Verificare l'allarme del collegamento alla coda nella distribuzione

Il successo della replica in Cisco ISE dipende dalla disponibilità e dalla comunicazione del servizio di messaggistica RabbitMQ e della struttura di comunicazione del cluster JGroups. Se uno dei componenti incontra problemi di comunicazione, Cisco ISE genera errori di collegamento coda, che possono interrompere la replica tra i nodi di implementazione.

Per verificare lo stato dell'allarme, selezionare Operazioni > Dashboard > Allarmi e controllare la presenza di errori di collegamento coda sui nodi interessati.

Se sono presenti errori di collegamento coda, rinnovare il certificato CA radice Cisco ISE, in quanto errori di comunicazione relativi al certificato in genere causano errori di collegamento coda. Una volta risolto il problema del certificato, la replica viene in genere ripresa automaticamente senza richiedere ulteriori interventi.

Nota: Per informazioni dettagliate sugli errori di collegamento alla coda, consultare la documentazione ISE Queue Link Errors.

---

3. Verifica della latenza e della connettività della rete

La replica di Cisco ISE si basa su una connettività di rete stabile tra i nodi di implementazione. Un'elevata latenza di rete o una connettività intermittente possono ritardare la replica e causare errori di sincronizzazione, in particolare in installazioni distribuite in aree geografiche diverse.

Verificare la latenza di rete tra i nodi interessati utilizzando test di connettività, ad esempio ping. Per una replica affidabile, la latenza di andata e ritorno tra i nodi deve rimanere entro circa 300 ms. Il costante superamento di questa soglia può influire negativamente sulle prestazioni e sulla sincronizzazione della replica. Verificare inoltre che non vi siano interruzioni intermittenti della rete, perdita di pacchetti o limitazioni del firewall che influiscono sulla comunicazione tra i nodi di distribuzione.

4. Verificare che il certificato non sia già presente nel nodo interessato

La replica dei certificati può avere esito negativo se il certificato da replicare esiste già nel nodo secondario.

Passare a Amministrazione > Sistema > Certificati, selezionare il nodo interessato e verificare se il certificato è già installato. Se il certificato è presente, esaminarne le proprietà per verificare che corrisponda al certificato replicato e determinare se esistono certificati duplicati o in conflitto.

5. Verifica dell'utilizzo delle risorse di sistema

Un elevato utilizzo delle risorse di sistema può influire sulle prestazioni di Cisco ISE e ritardare le attività di replica. Un utilizzo eccessivo della CPU, della memoria o del disco può impedire il corretto completamento dei processi di replica.

Verificare che il nodo interessato disponga di risorse di sistema sufficienti e che l'utilizzo delle risorse rimanga entro i limiti operativi consigliati. Se l'utilizzo delle risorse è costantemente elevato, allocare risorse aggiuntive o ridurre il carico di lavoro sul nodo per ripristinare le normali prestazioni di replica.

Nota: Per le linee guida consigliate sul dimensionamento dell'hardware e sull'allocazione delle risorse per le implementazioni di Cisco ISE, consultare la Guida alle prestazioni e alla scalabilità.

---

6. Verificare la disponibilità delle porte nella distribuzione e nella rete

La replica di Cisco ISE richiede porte TCP specifiche che rimangano aperte tra tutti i nodi dell'implementazione per garantire una comunicazione ininterrotta e la riuscita della replica. Se una di queste porte è bloccata da un firewall, da un criterio di controllo dell'accesso o da un dispositivo di rete, possono verificarsi errori di replica o problemi di sincronizzazione.

Verificare che le porte TCP siano aperte e raggiungibili tra tutti i nodi Cisco ISE:

- TCP 443 - Comunicazione HTTPS
- TCP 8443 - Comunicazione amministrativa
- TCP 12001 - Comunicazione e replica cluster JGroups
- TCP 6379 - Servizi di messaggistica interna
- TCP 8671 - Cisco ISE Messaging (RabbitMQ)

Accedere alla CLI di Cisco ISE ed eseguire il comando show ports per verificare le porte consentite nel nodo.

Verificare che le porte richieste siano abilitate sul nodo Cisco ISE e che siano consentite sul percorso di rete. Verificare che nessun firewall intermedio, dispositivo di sicurezza o criterio di rete blocchi la comunicazione tra i nodi di distribuzione su queste porte.

Raccolta log per avvisi di replica

Questi sono i componenti comuni da impostare in modalità debug per isolare e risolvere gli allarmi di replica in Cisco ISE.

- Replication-Deployment (replication.log e ise-psc.log)
- Replication-JGroup (replication.log e ise-psc.log)
- Tracker repliche (tracking.log)
- ibernazione (hibernate.log)
- JMS (replication.log)

Riferimento

- Guida dell'amministratore di Cisco Identity Services Engine, versione 3.5
- Risoluzione dei problemi e abilitazione dei debug su ISE
- Raccogli pacchetto di supporto su Identity Services Engine

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).