Comprensione e risoluzione dei problemi delle repliche ISE

Sommario

Introduzione

Questo documento descrive la 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 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.

Replica in Cisco ISE

La replica in ISE è il processo di sincronizzazione dei dati di configurazione e operativi su più nodi in un'implementazione per mantenerli coerenti.

Il nodo di amministrazione primario è responsabile della replica delle modifiche apportate nella distribuzione in tutti gli altri nodi (secondari) della distribuzione.

Cisco ISE utilizza JGroups, un framework affidabile per le comunicazioni di gruppo, come parte della sua architettura di replica. JGroups consente ai nodi di un'implementazione ISE di comunicare tra loro e scambiare i dati di replica. Fornisce il framework di messaggistica che consente di distribuire aggiornamenti di configurazione e database tra i nodi mantenendo la sincronizzazione nell'intera distribuzione.

- JGroups è una struttura di comunicazione utilizzata da Cisco ISE per la replica; non memorizza i dati replicati.
- Non tutti i dati in Cisco ISE vengono replicati tramite JGroups. I diversi servizi utilizzano meccanismi di comunicazione diversi in base al tipo di dati trasferiti.
- Se la replica viene temporaneamente interrotta, alcuni servizi Cisco ISE possono continuare a funzionare utilizzando i dati disponibili localmente fino al ripristino della sincronizzazione.

Esempi di metodi di trasferimento dei dati

Dati	Metodo di comunicazione
Messaggi di configurazione e	JGroup

replica	
Raccolta pacchetti di supporto	API HTTPS (porta TCP 443)
Configurazione debug	API HTTPS (porta TCP 443)
Registri e rapporti attivi	RabbitMQ o UDP, a seconda della configurazione di installazione

Prerequisiti principali e controlli di convalida per la replica di Cisco ISE

- Risoluzione DNS: le ricerche DNS dirette e inverse devono essere risolte correttamente per tutti i nodi Cisco ISE che partecipano alla distribuzione. Per le operazioni di comunicazione e replica dei nodi è necessaria una risoluzione DNS appropriata.
- Sincronizzazione NTP: tutti i nodi Cisco ISE devono essere sincronizzati su un'origine NTP affidabile per mantenere un tempo di sistema coerente nell'intera implementazione. La sincronizzazione dell'ora è essenziale per la replica e la convalida dei certificati.
- Certificati: il certificato Admin installato su ciascun nodo Cisco ISE deve essere valido e attendibile. I processi di replica si basano sul certificato di amministrazione per garantire una comunicazione sicura tra i nodi.
- Requisiti delle porte: la connettività di rete deve consentire la comunicazione sulle porte necessarie per la replica e i servizi tra nodi:

Servizio	Protocollo/porta
HTTPS (SOAP)	TCP/443
Sincronizzazione e replica dei dati (JGroups)	TCP/12001
Accesso amministrativo	TCP/8443
SSL (ISE Messaging Service)	TCP/8671

Sincronizzazione proprietà endpoint profiler	TCP/6379

- Raggiungibilità della rete: la connettività di rete tra i nodi Cisco ISE deve essere stabile e la latenza non deve superare i 300 ms. La verifica della latenza e della perdita di pacchetti tra i nodi contribuisce a garantire una replica affidabile.
- Stato collegamento coda: i certificati di messaggistica Cisco ISE vengono utilizzati per proteggere la comunicazione tra nodi sulla porta TCP 8671. Certificati di messaggistica non validi o danneggiati possono causare errori di collegamento alla coda ed errori di replica. In questi scenari, è necessario rigenerare il certificato CA radice ISE o i certificati di messaggistica ISE in base alle esigenze.
- ISE Stunnel Service: il servizio Cisco ISE Stunnel opera in implementazioni distribuite e facilita la comunicazione sicura tra i nodi. Il servizio deve essere in esecuzione su tutti i nodi applicabili per supportare la replica. Lo stato del servizio può essere verificato dalla CLI di Cisco ISE con il comando:
  show tech-support | comprendono lo storno
- ISE Patch and Version: il nodo di amministrazione principale e il nodo di unione (nodo standalone) devono avere la stessa versione e lo stesso livello di patch per consentire la registrazione e la sincronizzazione dei nodi.

Fasi della replica in Cisco ISE

La replica in Cisco ISE è costituita da tre fasi distinte che operano congiuntamente per stabilire e mantenere la sincronizzazione tra tutti i nodi dell'implementazione. Ogni fase ha uno scopo specifico, a partire dall'avvio del nodo, seguito dalla sincronizzazione iniziale del database e, infine, dallo scambio continuo di aggiornamenti incrementali per mantenere sincronizzati tutti i nodi.

- Registrazione nodo
- Sincronizzazione completa
- Sincronizzazione incrementale attiva

Informazioni sulla registrazione dei nodi in Cisco ISE

La registrazione del nodo è il processo attraverso il quale un nodo Cisco ISE si unisce a un'implementazione esistente e stabilisce la comunicazione con il PAN (Primary Administration Node).

Durante la registrazione del nodo:

Passaggio 1: Il nodo di unione (nodo autonomo) avvia la comunicazione con il nodo di amministrazione primario.

Passaggio 2: La convalida reciproca dei certificati viene eseguita utilizzando il certificato Cisco ISE Admin.

Passaggio 3: La risoluzione DNS, la sincronizzazione NTP, la raggiungibilità della rete e l'accessibilità necessaria alle porte sono convalidate nell'ambito del processo di comunicazione.

Passaggio 4: Il nodo di amministrazione primario verifica che il nodo standalone/di unione stia eseguendo una versione compatibile di Cisco ISE e che il livello di patch sia in esecuzione.

Passaggio 5: Le informazioni sulla distribuzione, i ruoli dei nodi e le relazioni di trust vengono scambiate.

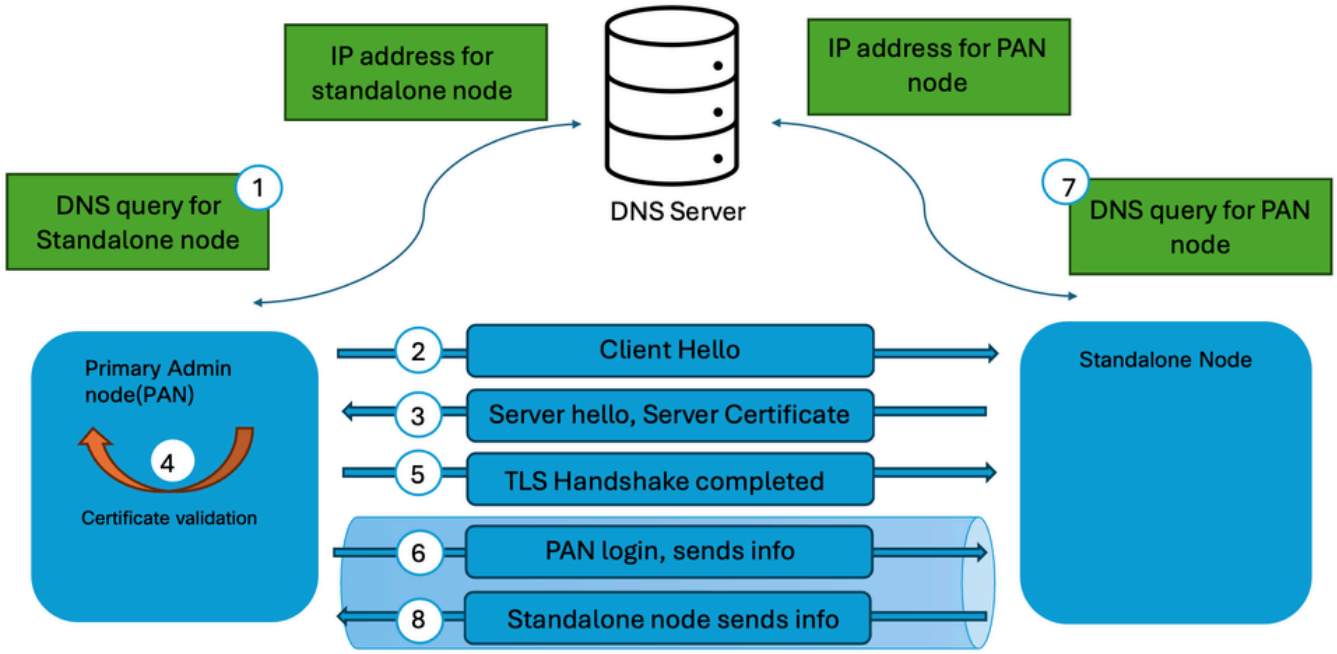
Passaggio 6: I servizi di replica di database vengono inizializzati e preparati per la sincronizzazione.

Il completamento della registrazione del nodo stabilisce che il nodo è un membro attendibile della distribuzione e consente l'avvio dei processi di replica.

Caratteristiche principali

- Viene generato quando viene aggiunto un nuovo nodo alla distribuzione.
- Stabilisce i canali di comunicazione e di trust.
- Non trasferisce immediatamente l'intero database di configurazione.
- Rappresenta un prerequisito per le successive operazioni di sincronizzazione.

Per una spiegazione dettagliata del processo di registrazione dei nodi, consultare il documento sulla procedura di registrazione dei nodi in Cisco ISE.



Processo di registrazione dei nodi

Nota: Il nodo da aggiungere alla distribuzione deve essere un nodo autonomo. Inoltre, per consentire la registrazione del nodo in Cisco ISE, è necessario che il ruolo Amministrazione primaria (PAN, Primary Administration Node) sia abilitato nella distribuzione.

Informazioni su Full Sync Up in Cisco ISE

La sincronizzazione completa è un processo completo di replica del database in cui l'intero database di configurazione viene trasferito dal PAN primario a un altro nodo. La sincronizzazione completa non trasferisce solo i record modificati. Al contrario, l'intero dataset di configurazione viene ricostruito sul nodo ricevente.

Una sincronizzazione completa può verificarsi in scenari quali:

- Sincronizzazione iniziale dopo la registrazione del nodo.
- Ripristino da errori di replica.
- Incoerenze significative nel database.
- Aggiunta di un nodo alla distribuzione.
- Sincronizzazione manuale avviata tramite le procedure di risoluzione dei problemi di Cisco TAC.
- Meccanismi di replica interni che determinano che la sincronizzazione incrementale non è più in grado di ripristinare la coerenza del database.

Durante la sincronizzazione completa:

Passaggio 1: Il nodo Amministrazione primaria prepara uno snapshot di database completo.

Passaggio 2: I dati di configurazione vengono inseriti nel file con estensione dmp e trasmessi al nodo ricevente.

Passaggio 3: I dati replicati esistenti nel nodo ricevente vengono convalidati e aggiornati.

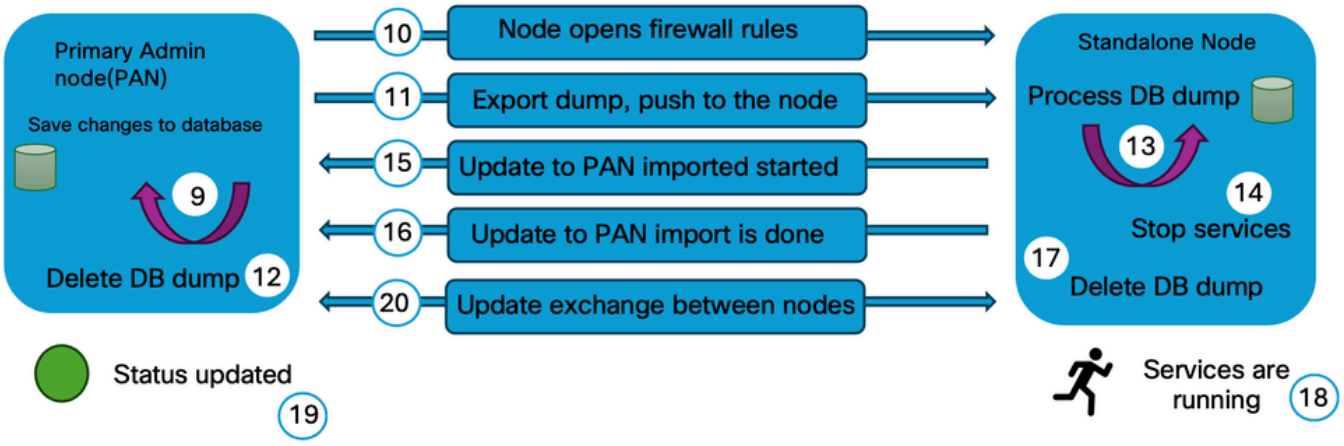
Passaggio 4: L'intero database di configurazione viene ricreato in modo da corrispondere al nodo Amministratore primario.

Passaggio 5: Lo stato della replica viene verificato al completamento.

Poiché una sincronizzazione completa comporta una quantità di dati notevolmente superiore rispetto a una sincronizzazione incrementale, richiede tempi di elaborazione aggiuntivi e risorse di rete.

Caratteristiche della sincronizzazione completa

- Trasferisce l'intero database di configurazione.
- Utilizzo di maggiore larghezza di banda e risorse di sistema.
- Richiede più tempo della sincronizzazione incrementale.
- Ripristina la coerenza del database quando vengono rilevate discrepanze.
- In genere si verifica con minore frequenza rispetto alla sincronizzazione incrementale.



Processo di sincronizzazione completa

Informazioni sulla sincronizzazione incrementale in Cisco ISE

La sincronizzazione incrementale è il meccanismo di replica in corso utilizzato da Cisco ISE per distribuire le modifiche alla configurazione dopo che i nodi sono stati aggiunti correttamente all'implementazione. Quando un amministratore apporta una modifica alla configurazione sulla PAN, Cisco ISE non trasferisce l'intero database. Al contrario, solo i record modificati vengono replicati nei nodi del sottoscrittore.

Di seguito sono riportati alcuni esempi di modifiche replicate tramite la sincronizzazione incrementale:

- Modifiche criteri
- Aggiunta o aggiornamento di dispositivi di rete
- Modifiche gruppo endpoint
- Aggiornamenti del profilo di autorizzazione
- Modifiche alla configurazione relative ai certificati
- Aggiornamenti configurazione origine identità

Il processo di sincronizzazione incrementale funziona in modo continuo ed è progettato per mantenere la coerenza su tutti i nodi, riducendo al minimo l'utilizzo della larghezza di banda e il sovraccarico di replica.

Vantaggi della sincronizzazione incrementale

- Riduzione del traffico di replica.
- Riduce i tempi di sincronizzazione.
- Propagazione rapida delle modifiche alla configurazione.
- Mantiene la coerenza pressoché in tempo reale nell'intera implementazione.

Workflow di replica

Passaggio 1: La configurazione viene modificata nel nodo di amministrazione principale.

Passaggio 2: La modifica viene scritta nel database del nodo di amministrazione primario.

Passaggio 3: I record modificati sono identificati dai servizi di replica.

Passaggio 4: Il nodo di amministrazione principale scrive i nuovi eventi/modifiche in una tabella delle transazioni.

Passaggio 5: I thread separati da PAN pubblicano le informazioni o le modifiche ai nodi secondari nella distribuzione.

Passaggio 6: I nodi secondari della distribuzione ricevono le modifiche dal nodo di amministrazione primario.

Passaggio 7: I nodi secondari nella distribuzione applicano le modifiche ricevute dal nodo di amministrazione primario.

Passaggio 8: Lo stato della replica viene aggiornato al completamento.

In condizioni operative normali, la maggior parte delle attività di replica in Cisco ISE avviene tramite sincronizzazione incrementale.

Nota: Se un nodo secondario identifica messaggi di replica mancanti, avvia una richiesta al nodo di amministrazione principale (PAN, Primary Administration Node) per recuperare i messaggi mancanti e mantenere la sincronizzazione

---

Panoramica della sequenza di replica e stato della sincronizzazione

Il flusso di lavoro complessivo della replica in un'implementazione Cisco ISE può essere riepilogato come segue:

1. Registrazione del nodo: Stabilisce l'attendibilità e aggiunge il nodo alla distribuzione.

2. Sincronizzazione completa iniziale: Trasferisce l'intero database di configurazione al nodo appena registrato.

3. Sincronizzazione incrementale: propaga in modo continuo le modifiche alla configurazione durante il normale funzionamento.

4. Sincronizzazione completa (quando richiesto): Ricrea la coerenza del database se vengono rilevati problemi di replica o mancate corrispondenze del database.

Questo approccio in più fasi consente a Cisco ISE di mantenere un database di configurazione coerente su tutti i nodi, ottimizzando al contempo l'utilizzo della rete e le prestazioni di replica.

Stato sincronizzazione

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 (il nodo non è stato raggiungibile dal cluster negli ultimi cinque minuti).
- Rosso: il nodo è fisicamente irraggiungibile e non può essere contattato tramite controlli della connettività di rete (ad esempio, ping ICMP e HTTPS).

Nota: Se la replica non viene eseguita correttamente, è possibile eseguire la sincronizzazione manuale con i nodi secondari con il nodo Amministrazione primaria accedendo al nodo Amministrazione primaria, selezionando Amministrazione > Sistema > Distribuzione > selezionare il nodo, quindi facendo clic su Sincronizza.

Replica degli endpoint

La replica degli endpoint è il processo con cui ISE sincronizza le informazioni del database degli endpoint tra tutti i PSN (Policy Service Nodes) e il PAN (Primary Administration Node) per mantenere una vista coerente dell'identità degli endpoint durante l'intera distribuzione.

- Cisco ISE gestisce un database centralizzato degli endpoint in cui vengono memorizzate le informazioni sui dispositivi che si connettono alla rete. Queste informazioni includono sia gli endpoint configurati in modo statico che quelli appresi in modo dinamico tramite autenticazione, profiling, valutazione della postura o integrazione con origini di identità esterne.

- Quando si creano o si modificano le informazioni sull'endpoint, Cisco ISE replica le modifiche negli altri nodi dell'implementazione. Questa sincronizzazione consente a ogni nodo del servizio criteri di valutare le richieste di autenticazione e autorizzazione utilizzando le stesse informazioni sull'endpoint, indipendentemente dal PSN che elabora la richiesta.

- La replica degli endpoint viene gestita automaticamente da Cisco ISE e fa parte del meccanismo generale di replica del database. Non è necessario che gli amministratori avviino manualmente la sincronizzazione degli endpoint durante le normali operazioni.

Funzionamento della replica degli endpoint

- Aggiornamento endpoint: Un endpoint viene creato o aggiornato tramite autenticazione, profilatura, postura o configurazione manuale.
- Rilevamento modifiche: Cisco ISE rileva la modifica dell'endpoint e la prepara per la replica.
- Replica: Le informazioni aggiornate sull'endpoint vengono replicate negli altri nodi della distribuzione utilizzando il framework di replica ISE.
- Sincronizzazione database: I nodi secondari aggiornano il proprio database di endpoint locale con le informazioni replicate.
- Applicazione coerente delle regole: Al termine della sincronizzazione, tutti i nodi del servizio criteri utilizzano le stesse informazioni sull'endpoint per le decisioni di autenticazione e autorizzazione.

Da Cisco ISE release 3.3, gli endpoint individuati dinamicamente non vengono replicati automaticamente su tutti i nodi. Questa funzionalità può essere abilitata o disabilitata dalla finestra Replica endpoint. Passare a Amministrazione > Sistema > Impostazioni > Replica endpoint, abilitare o disabilitare a seconda delle esigenze.

Nota: È importante distinguere la replica dell'endpoint dalla replica della sessione. La replica degli endpoint sincronizza i record del database degli endpoint persistenti (ad esempio indirizzi MAC, gruppi di endpoint e informazioni di profiling), mentre la replica delle sessioni sincronizza le informazioni delle sessioni di runtime per supportare l'applicazione dei criteri e la continuità operativa. Questi meccanismi operano in modo indipendente e svolgono diverse funzioni all'interno dell'architettura Cisco ISE.

Problemi comuni di replica dei nodi

Scenario 1: Registrazione del nodo non riuscita a causa di un errore di risoluzione DNS

Registrazione del nodo non riuscita. Motivo dell'errore: impossibile risolvere il nome host. Controllare la configurazione DNS.

Passaggi da verificare

- Verificare che il server DNS valido sia configurato nel nodo di amministrazione primario e nel nodo autonomo. Verificare la configurazione del server DNS utilizzando il comando show

running-config | includi name-server
- Convalidare la risoluzione DNS diretta e inversa nel nodo di amministrazione primario e nel nodo autonomo utilizzando il comando nslookup FQDN del nodo per la ricerca DNS diretta e l'indirizzo IP nslookup del nodo per la ricerca DNS inversa.
- Verificare la raggiungibilità del server DNS dal nodo di amministrazione primario e dal nodo standalone utilizzando il comando ping DNS server IP dalla CLI dei nodi ISE.

Scenario 2: Registrazione del nodo non riuscita a causa della scadenza del certificato di amministrazione

Registrazione del nodo non riuscita. Motivo dell'errore: errore durante il caricamento dei certificati. Nodo non raggiungibile in questo momento. Riprova più tardi".

Passaggi da verificare

- Convalidare i certificati amministrativi del nodo di amministrazione principale e del nodo autonomo per garantire la validità e lo stato del certificato. Passare a Amministrazione > Sistema > Certificati, selezionare il nodo e verificare la validità e lo stato del certificato Amministratore.
- Se il certificato Admin è scaduto, sostituirlo o rinnovarlo e assicurarsi che l'utilizzo Admin sia assegnato.

Scenario 3: Registrazione del nodo non riuscita a causa di una mancata corrispondenza delle versioni

Registrazione del nodo non riuscita. Motivo dell'errore: mancata corrispondenza dei dettagli di versione/patch.

Passaggi da verificare

- Convalidare la versione del software insieme alla patch del nodo Admin primario e del nodo standalone utilizzando il comando show version per verificare che i dettagli della versione corrispondano.

Componenti per i log di debug

Questi sono i componenti comuni da impostare in modalità debug per isolare e risolvere i problemi 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)
- ca-service (caservice.log)
- admin-ca (ise-psc.log)

Riferimento

- Risoluzione dei problemi e abilitazione dei debug su ISE
- ISE - Errore collegamento coda
- Guida dell'amministratore di Cisco Identity Services Engine, versione 3.4
- Guida dell'amministratore di Cisco Identity Services Engine, versione 3.5

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).