Problemen met ISE-replicaties begrijpen en oplossen

Inhoud

Inleiding

Dit document beschrijft Replicatie en de probleemoplossing in Cisco Identity Services Engine® (ISE).

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van Cisco Identity Services Engine® (ISE).

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende hardware- en softwareversies.

- Cisco Identity Services Engine 3.4 en hogere versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Replicatie in Cisco ISE

Replicatie in ISE is het proces waarbij configuratie- en operationele gegevens over meerdere knooppunten in een implementatie worden gesynchroniseerd om ze consistent te houden.

Primaire beheerknooppunt is verantwoordelijk voor het repliceren van de wijzigingen die zijn aangebracht in de implementatie naar alle andere (secundaire) knooppunten in de implementatie.

Cisco ISE maakt gebruik van JGroups, een betrouwbaar kader voor groepscommunicatie, als onderdeel van de replicatiearchitectuur. JGroups stelt de knooppunten in een ISE-implementatie in staat met elkaar te communiceren en replicatiegegevens uit te wisselen. Het biedt het berichtenframework dat helpt bij het leveren van configuratie- en database-updates tussen nodes terwijl de synchronisatie in de implementatie wordt gehandhaafd.

- JGroups is een communicatiekader dat door Cisco ISE wordt gebruikt voor replicatie; het slaat de gerepliceerde gegevens zelf niet op.
- Niet alle gegevens binnen Cisco ISE worden gerepliceerd via JGroups. Verschillende diensten gebruiken verschillende communicatiemechanismen op basis van het type gegevens dat wordt overgedragen.
- Als de replicatie tijdelijk wordt onderbroken, kunnen sommige Cisco ISE-services blijven werken met lokaal beschikbare gegevens totdat de synchronisatie is hersteld.

Voorbeelden van methoden voor gegevensoverdracht

gegevens	communicatiemethode

Configuratie- en replicatieberichten	JGroups
Ondersteuningsbundelcollectie	HTTPS-API (TCP-poort 443)
Foutopsporingsconfiguratie	HTTPS-API (TCP-poort 443)
Live logboeken en rapporten	RabbitMQ of UDP, afhankelijk van de implementatie configuratie

Belangrijkste vereisten en validatiecontroles voor Cisco ISE-replicatie

- DNS-resolutie: Forward en reverse DNS-lookups moeten succesvol worden opgelost voor alle Cisco ISE-nodes die deelnemen aan de implementatie. De juiste DNS-resolutie is vereist voor knooppuntcommunicatie en replicatiebewerkingen.
- NTP-synchronisatie: alle Cisco ISE-knooppunten moeten worden gesynchroniseerd met een betrouwbare NTP-bron om een consistente systeemtijd tijdens de implementatie te behouden. Tijdsynchronisatie is essentieel voor replicatie en certificaatvalidatie.
- Certificaten: Het beheercertificaat dat op elke Cisco ISE-node is geïnstalleerd, moet geldig en vertrouwd zijn. Replicatieprocessen zijn gebaseerd op het Admin-certificaat voor veilige communicatie tussen nodes.
- Poortvereisten: netwerkconnectiviteit moet communicatie mogelijk maken via de poorten die nodig zijn voor replicatie en internodeservices:

dienst	Protocol / poort
HTTPS (SOAP)	TCP/443
Gegevenssynchronisatie en -replicatie (JGroups)	TCP/12001
administratieve toegang	TCP/8443

ISE-berichtenservice (SSL)	TCP/8671
Synchronisatie van eigendom van Profiler-eindpunt	TCP/6379

- Netwerkbereikbaarheid: de netwerkconnectiviteit tussen Cisco ISE-nodes moet stabiel zijn en de latentie mag niet langer zijn dan 300 ms. Het controleren van de latentie en het pakketverlies tussen nodes zorgt voor betrouwbare replicatie.
- Queue Link Status: Cisco ISE Messaging Certificaten worden gebruikt om inter-node communicatie over TCP poort 8671 te beveiligen. Ongeldige of beschadigde berichtencertificaten kunnen leiden tot fouten in de wachtrijkoppeling en replicatiefouten. In dergelijke scenario's moet het ISE Root CA-certificaat of ISE Messaging Certificates worden geregenereerd.
- ISE Stunnel Service: De Cisco ISE Stunnel-service werkt in gedistribueerde implementaties en vergemakkelijkt veilige communicatie tussen knooppunten. De service moet op alle toepasselijke knooppunten worden uitgevoerd om replicatie te ondersteunen. De servicestatus kan worden geverifieerd vanuit de Cisco ISE CLI met behulp van de opdracht: Toon technische ondersteuning | Inclusief stunnel
- ISE-patch en -versie: de primaire beheernode en de verbindende node (zelfstandige node) moeten dezelfde versie en hetzelfde patchniveau hebben voor de registratie en synchronisatie van de node om naadloos te kunnen werken.

Fases van replicatie in Cisco ISE

Replicatie in Cisco ISE bestaat uit drie afzonderlijke fasen die samenwerken om synchronisatie tussen alle knooppunten in de implementatie tot stand te brengen en te behouden. Elke fase dient een specifiek doel, te beginnen met knooppunt onboarding, gevolgd door de eerste database synchronisatie, en ten slotte de continue uitwisseling van incrementele updates om alle knooppunten gesynchroniseerd te houden.

- Node-registratie
- Volledige synchronisatie
- Incrementele synchronisatie omhoog

Node-registratie in Cisco ISE begrijpen

Node registration is het proces waarbij een Cisco ISE-node zich aansluit bij een bestaande implementatie en communicatie tot stand brengt met de Primary Administration Node (PAN).

Tijdens de registratie van de node:

Stap 1: De verbindende node (zelfstandige node) initieert de communicatie met de primaire node voor beheer.

Stap 2: De wederzijdse certificaatvalidatie wordt uitgevoerd met behulp van het Cisco ISE-beheercertificaat.

Stap 3: DNS-resolutie, NTP-synchronisatie, netwerkbereikbaarheid en vereiste poorttoegankelijkheid worden gevalideerd als onderdeel van het communicatieproces.

Stap 4: De primaire beheerknooppunt controleert of de zelfstandige knooppunt/verbindende knooppunt een compatibele Cisco ISE-versie en patchniveau uitvoert.

Stap 5: Implementatiegegevens, knooppuntrollen en vertrouwensrelaties worden uitgewisseld.

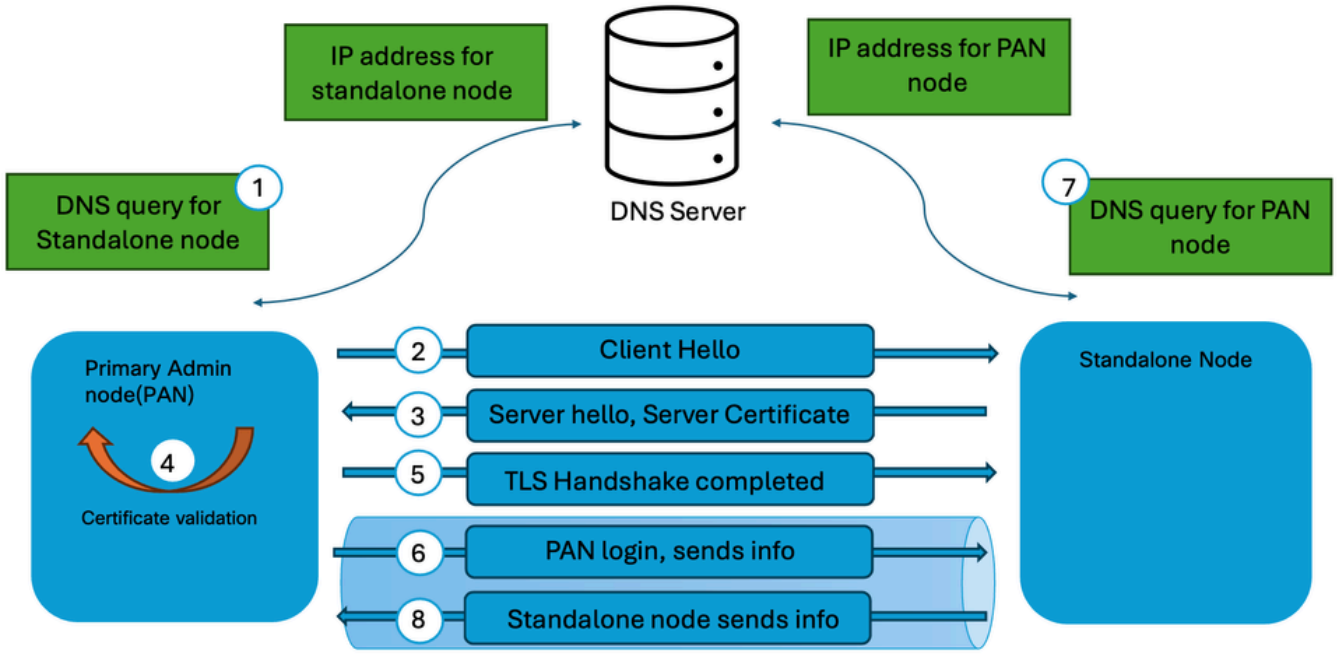
Stap 6: Databasereplicatieservices worden geïnitialiseerd en voorbereid voor synchronisatie.

Als de registratie van de node succesvol is voltooid, wordt de node een vertrouwd lid van de implementatie en kunnen replicatieprocessen worden gestart.

Belangrijkste kenmerken

- Dit gebeurt wanneer een nieuw knooppunt aan de implementatie wordt toegevoegd.
- Creëert vertrouwens- en communicatiekanalen.
- De volledige configuratiedatabase wordt niet onmiddellijk overgedragen.
- Het dient als voorwaarde voor latere synchronisatie-bewerkingen.

Raadpleeg Knooppuntenregistratieproces in Cisco ISE begrijpen voor een gedetailleerde uitleg van het knooppuntenregistratieproces.



Node-registratieproces

Opmerking: de node die aan de implementatie wordt toegevoegd, moet een zelfstandige node zijn. Bovendien moet de primaire beheernode (PAN) de primaire beheerrol hebben ingeschakeld in de implementatie om de registratie van de node in Cisco ISE mogelijk te maken.

Volledige synchronisatie in Cisco ISE begrijpen

Volledige synchronisatie is een volledig databasereplicatieproces waarbij de volledige configuratiedatabase van het primaire PAN naar een andere node wordt overgebracht. Bij volledige synchronisatie worden niet alleen gewijzigde records overgedragen. In plaats daarvan wordt de volledige configuratiedataset opnieuw opgebouwd op de ontvangende node.

Een volledige synchronisatie kan plaatsvinden in scenario's zoals:

- Initiële synchronisatie na noderegistratie.
- Herstel van replicatiefouten.
- Aanzienlijke inconsistenties in de database.
- Een node opnieuw aansluiten bij de implementatie.
- Handmatige synchronisatie gestart via Cisco TAC-procedures voor probleemoplossing.
- Interne replicatiemechanismen die bepalen dat stapsgewijze synchronisatie niet langer de consistentie van de database kan herstellen.

Tijdens volledige synchronisatie:

Stap 1: Het primaire knooppunt voor beheer bereidt een volledige momentopname van de database voor.

Stap 2: Configuratiegegevens worden verpakt in het .dmp-bestand en verzonden naar de ontvangende node.

Stap 3: Bestaande gerepliceerde gegevens op de ontvangende node worden gevalideerd en bijgewerkt.

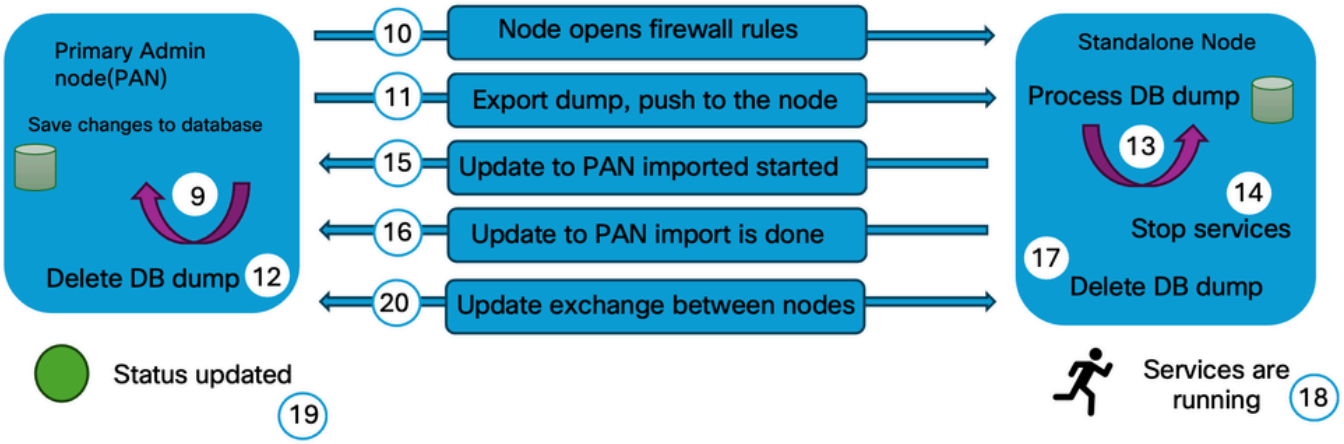
Stap 4: De volledige configuratiedatabase wordt opnieuw opgebouwd zodat deze overeenkomt met de primaire beheerdersknooppunt.

Stap 5: Replicatiestatus wordt geverifieerd na voltooiing.

Omdat bij een volledige synchronisatie aanzienlijk meer gegevens nodig zijn dan bij een stapsgewijze synchronisatie, zijn extra verwerkingstijd en netwerkbronnen nodig.

Kenmerken van volledige synchronisatie

- Hiermee wordt de volledige configuratiedatabase overgedragen.
- Verbruikt meer bandbreedte en systeembronnen.
- Het duurt langer dan incrementele synchronisatie.
- Herstelt de consistentie van de database wanneer afwijkingen worden gedetecteerd.
- Dit gebeurt meestal minder vaak dan incrementele synchronisatie.



Volledige synchronisatie

Begrijp incrementele synchronisatie in Cisco ISE

Incrementele synchronisatie is het mechanisme voor continue replicatie dat door Cisco ISE wordt gebruikt om configuratiewijzigingen te distribueren nadat knooppunten zich met succes bij de implementatie hebben aangesloten. Wanneer een beheerder een configuratiewijziging aanbrengt op het PAN, wordt de volledige database niet overgedragen door Cisco ISE. In plaats daarvan worden alleen de gewijzigde records gerepliceerd naar de abonneeknooppunten.

Voorbeelden van veranderingen die worden gerepliceerd door incrementele synchronisatie zijn:

- Beleidswijzigingen
- Toevoegingen of updates voor netwerkapparaten
- Wijzigingen in de eindpuntgroep
- Updates van autorisatieprofiel
- Certificaatgerelateerde configuratiewijzigingen
- Updates van de bronconfiguratie van de identiteit

Het incrementele synchronisatieproces werkt continu en is ontworpen om de consistentie van alle knooppunten te behouden terwijl het gebruik van bandbreedte en de overhead voor replicatie worden geminimaliseerd.

Voordelen van incrementele synchronisatie

- Vermindert replicatieverkeer.
- Minimaliseert de synchronisatietijd.
- Maakt snelle verspreiding van configuratiewijzigingen mogelijk.
- Behoudt vrijwel realtime consistentie in de implementatie.

Replicatieworkflow

Stap 1: Configuratiewijziging vindt plaats op de primaire beheernode.

Stap 2: Wijziging wordt naar de database van de primaire beheernode geschreven.

Stap 3: Replicatieservices identificeren de gewijzigde records.

Stap 4: Primair administratieknooppunt schrijft de nieuwe gebeurtenissen / wijzigingen in een transactietabel.

Stap 5: Scheid threads van PAN en publiceer de informatie / wijzigingen in de secundaire knooppunten in de implementatie.

Stap 6: Secundaire knooppunten in de implementatie ontvangen de wijzigingen van de primaire beheerknooppunt.

Stap 7: Secundaire knooppunten in de implementatie passen de wijzigingen toe die zijn ontvangen van de primaire beheerknooppunt.

Stap 8: Replicatiestatus wordt bijgewerkt na succesvolle voltooiing.

Onder normale bedrijfsomstandigheden vindt de meeste replicatieactiviteit in Cisco ISE plaats door incrementele synchronisatie.

Opmerking: als een secundair knooppunt ontbrekende replicatieberichten identificeert, wordt een verzoek gestart aan het primaire beheerknooppunt (PAN) om de ontbrekende berichten op te halen en de synchronisatie te behouden

---

Overzicht van replicatiesequentie en synchronisatiestatus

De algehele replicatieworkflow in een Cisco ISE-implementatie kan als volgt worden samengevat:

1. Node Registration: zorgt voor vertrouwen en voegt de node toe aan de implementatie.

2. Eerste volledige synchronisatie: de volledige configuratiedatabase wordt overgebracht naar de nieuw geregistreerde node.

3. Stapsgewijze synchronisatie: Voortdurend propageren van configuratiewijzigingen tijdens de normale werking.

4. Volledige synchronisatie (indien vereist): bouwt de consistentie van de database opnieuw op als replicatieproblemen of databasemismatches worden gedetecteerd.

Met deze gefaseerde aanpak kan Cisco ISE een consistente configuratiedatabase voor alle

knooppunten onderhouden en tegelijkertijd het netwerkgebruik en de replicatieprestaties optimaliseren.

Synchronisatiestatus

De synchronisatiestatus die voor elk knooppunt wordt weergegeven, geeft de huidige replicatie- en connectiviteitsstatus aan:

- Groen – De node wordt gesynchroniseerd met de implementatie en de replicatie functioneert normaal.
- Geel – De node is niet gesynchroniseerd, de registratie van de node is mislukt of de clusterconnectiviteit is verloren gegaan (de node is de afgelopen vijf minuten niet bereikbaar geweest voor het cluster).
- Rood – De node is fysiek onbereikbaar en kan niet worden gecontacteerd via netwerkconnectiviteitscontroles (bijvoorbeeld ICMP-ping en HTTPS).

Opmerking: als replicatie niet correct plaatsvindt, kunt u handmatig synchroniseren met de secundaire knooppunten met de primaire beheerknooppunt door u aan te melden bij de primaire beheerknooppunt, naar Beheer > Systeem > Implementatie > selecteer de knooppunt en klik op Synchroniseren.

Eindpuntreplicatie

Endpoint Replication is het proces waarbij ISE de eindpuntdatabasegegevens synchroniseert tussen alle Policy Service Nodes (PSN's) en de Primary Administration Node (PAN) om een consistent beeld van de identiteit van het eindpunt tijdens de implementatie te behouden.

- Cisco ISE onderhoudt een gecentraliseerde endpointdatabase die informatie opslaat over apparaten die verbinding maken met het netwerk. Deze informatie omvat zowel statisch geconfigureerde eindpunten als dynamisch aangeleerde eindpunten door middel van authenticatie, profilering, houdingsbeoordeling of integratie met externe identiteitsbronnen.

- Wanneer eindpuntinformatie wordt gemaakt of gewijzigd, repliceert Cisco ISE de wijzigingen naar andere knooppunten in de implementatie. Deze synchronisatie stelt elke Policy Service Node in staat om authenticatie- en autorisatieverzoeken te evalueren met behulp van dezelfde eindpuntinformatie, ongeacht welke PSN het verzoek verwerkt.

- Endpoint-replicatie wordt automatisch afgehandeld door Cisco ISE en maakt deel uit van het algemene databasereplicatiemechanisme. Beheerders zijn niet verplicht om handmatig de eindpuntsynchronisatie te starten tijdens normale bewerkingen.

Hoe Endpoint Replication werkt

- Eindpuntupdate: een eindpunt wordt gemaakt of bijgewerkt door middel van verificatie, profilering, houding of handmatige configuratie.
- Wijzigingsdetectie: Cisco ISE detecteert de eindpuntwijziging en bereidt deze voor op replicatie.
- Replicatie: de bijgewerkte eindpuntinformatie wordt gerepliceerd naar de andere knooppunten in de implementatie met behulp van het ISE-replicatieframework.
- Databasesynchronisatie: de secundaire knooppunten werken hun lokale eindpuntdatabase bij met de gerepliceerde informatie.
- Consistente beleidshandhaving: zodra de synchronisatie is voltooid, gebruiken alle Beleidsserviceknooppunten dezelfde eindpuntinformatie voor authenticatie- en autorisatiebeslissingen.

Vanaf Cisco ISE Release 3.3 worden dynamisch ontdekte eindpunten niet automatisch gerepliceerd naar alle nodes. Deze functie kan worden in- of uitgeschakeld vanuit het venster Endpoint Replication. Navigeer naar Beheer > Systeem > Instellingen > Eindpuntreplicatie, in- of uitschakelen volgens de vereiste.

Opmerking: Het is belangrijk om endpointreplicatie te onderscheiden van sessiereplicatie. Eindpuntreplicatie synchroniseert permanente eindpuntsdatabaserecords (zoals MAC-adressen, eindpuntgroepen en profielinformatie), terwijl sessiereplicatie runtime-sessieinformatie synchroniseert om de handhaving van het beleid en de operationele continuïteit te ondersteunen. Deze mechanismen werken onafhankelijk en dienen verschillende functies binnen de Cisco ISE-architectuur.

Veel voorkomende problemen met knooppuntreplicatie

Scenario 1: Node-registratie mislukt vanwege DNS-resolutiefout

Node registratie is mislukt met de fout reden als "hostnaam kan niet worden opgelost.Controleer uw DNS-configuratie".

Stappen om te verifiëren

- Controleer of de geldige DNS-server is geconfigureerd in de primaire beheernode en de

zelfstandige node. Controleer de DNS-serverconfiguratie met behulp van de opdracht show running-config | include name-server
- Valideer de voorwaartse en omgekeerde DNS-resolutie in de primaire beheerknooppunt en de zelfstandige knooppunt met behulp van de opdracht nslookup FQDN van de knooppunt voor voorwaartse DNS-lookup en het nslookup-IP-adres van de knooppunt voor omgekeerde DNS-lookup.
- Valideer de bereikbaarheid van de DNS-server vanaf de primaire beheerknooppunt en de zelfstandige knooppunt met behulp van de opdracht ping DNS-server IP van de CLI van de ISE-knooppunten.

Scenario 2: Node-registratie mislukt vanwege verlopen beheerderscertificaat

Node registratie is mislukt met de fout reden als "Fout bij het laden van certificaten. Knooppunt niet bereikbaar op dit moment. Probeer het later nog eens."

Stappen om te verifiëren

- De beheercertificaten van de primaire beheernode en de zelfstandige node valideren om de geldigheid en certificaatstatus te garanderen. Navigeer naar Beheer > Systeem > Certificaten, selecteer de node en controleer de geldigheid en status van het beheercertificaat.
- Als het beheerderscertificaat is verlopen, vervangt of verlengt u het certificaat en zorgt u ervoor dat het beheerdergebruik wordt toegewezen.

Scenario 3: Node registratie mislukt vanwege versie mismatch

Node registratie mislukt met de fout reden als "versie/patch details mismatch".

Stappen om te verifiëren

- Valideer de softwareversie samen met de patch van de primaire beheerknooppunt en de zelfstandige knooppunt met behulp van de opdrachtregelversie om ervoor te zorgen dat de versienummers overeenkomen.

Componenten voor foutopsporingslogs

Dit zijn de gemeenschappelijke componenten die moeten worden ingesteld in de debug-modus om replicatie in Cisco ISE te isoleren en problemen op te lossen.

- Replication-Deployment (replication.log en ise-psc.log)
- Replication-JGroup (replication.log en ise-psc.log)
- Replication Tracker (tracking.log)
- Sluimerstand (Hibernate.log)
- JMS (replication.log)
- CA-service (caservice.log)
- Admin-CA (ISE-PSC.log)

referentie

- Troubleshooten en foutsporing inschakelen op ISE
- ISE- Queue Link-fout
- Beheerdershandleiding voor de Cisco Identity Services-engine, release 3.4
- Beheerdershandleiding voor de Cisco Identity Services-engine, release 3.5

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.