了解ISE节点复制警报并对其进行故障排除

目录

简介

本文档介绍思科身份服务引擎®(ISE)中的复制警报及其故障排除。

先决条件

要求

思科建议您了解思科身份服务引擎®(ISE)。

使用的组件

本文档中的信息基于这些硬件与软件版本。

- 思科身份服务引擎®(ISE)3.4及更高版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

ISE复制警报

思科ISE中的复制警报提供整个部署中复制框架的运行状况和同步状态的可视性。这些警报有助于确定可能影响数据一致性、节点通信或复制过程的条件，使管理员能够检测并解决问题，以免它们影响系统操作。了解复制警报的用途和重要性对于维护正常的ISE部署以及确保配置和操作数据在所有节点间保持同步至关重要。

ISE节点复制警报

复制失败

当部署中的辅助节点无法使用由部署中的主管理节点复制的消息时，会生成“复制失败”警报。此警报表示复制过程失败，受影响的节点不再具有最新配置或操作数据。

与特定于证书的复制警报不同，此警报表示常规复制框架中的故障，并且可能会影响部署中的多个配置对象和服务。

警报原因

当思科ISE无法成功传输或应用复制数据时，可能会出现复制失败警报。常见原因包括：

- 网络通信问题：数据包丢失、高网络延迟、防火墙限制、路由问题或MTU不匹配会中断ISE节点之间的通信。
- 复制服务问题：RabbitMQ、JGroups或其他内部复制服务不可用，正在重新启动或不能正常工作。
- 节点通信问题：目标节点脱机、重新启动、取消注册、与部署断开连接或无法访问。
- 数据库同步问题：由于数据库错误或同步失败，目标节点无法提交复制的数据。
- 系统资源限制：高CPU利用率、内存压力、磁盘空间不足，或磁盘I/O过大延迟复制处理。

- DNS或主机名解析问题：错误的前向或反向DNS解析导致节点之间无法成功通信。
- 版本或部署不一致：如果节点未在受支持的软件版本上运行，或者在升级或节点注册后部署处于不一致状态，则复制失败。
- Admin Certificate Expiry:ISE节点的管理员证书已过期/已损坏/无效，因此节点之间的通信处于危险状态，导致复制失败。
- 队列链路错误：部署或受影响的节点显示队列链路错误，其中ISE消息证书/ISE根CA链在端口8671上损坏或无效。
- Stunnel服务已禁用/脱机：Stunnel服务在分布式部署的所有节点中运行。禁用/未运行Stunnel服务的状态会导致“复制失败”警报。
- 复制端口被阻止：必须在部署中的节点与网络之间打开端口12001、8671、443、8443和6379，以便在部署中进行无缝复制。

警报的影响

影响取决于要复制的数据类型。复制失败可能导致跨ISE节点的配置不一致、管理更改传播延迟、策略过时、网络设备或身份信息丢失、证书同步失败和不一致的终端数据。如果复制在较长的一段时间内仍不成功，则整个部署中的管理操作和策略一致性可能会受到影响。

复制已停止

当主管理节点无法将信息复制到部署的辅助节点时，会生成“复制已停止”警报。此警报表示复制过程失败，受影响的节点不再具有最新配置或操作数据。

警报原因

当主管理节点无法成功传输复制的数据时，可能会出现“Replication Stopped”警报。常见原因包括：

- 网络通信问题：数据包丢失、高网络延迟、防火墙限制、路由问题或MTU不匹配会中断ISE节点之间的通信。
- 复制服务问题：RabbitMQ、JGroups或其他内部复制服务不可用，正在重新启动或在主管理节点中无法正常工作。
- 系统资源限制：主管理节点中的CPU使用率高、内存压力大、磁盘空间不足或磁盘I/O过大会延迟复制处理。
- DNS或主机名解析问题：错误的前向或反向DNS解析导致节点之间无法成功通信。

- 版本或部署不一致：如果节点未在受支持的软件版本上运行，或者在升级或节点注册后部署处于不一致状态，则复制失败。
- Admin Certificate Expiry:ISE节点的管理员证书已过期/已损坏/无效，因此节点之间的通信处于危险状态，导致复制失败。
- 队列链路错误：部署或受影响的节点显示队列链路错误，其中ISE消息证书/ISE根CA链在端口8671上损坏或无效。
- Stunnel服务已禁用/脱机：Stunnel服务在分布式部署的所有节点中运行。禁用/未运行Stunnel服务的状态会导致“复制失败”警报。
- 复制端口被阻止：必须在部署中的节点与网络之间打开端口12001、8671、443、8443和6379，以便在部署中进行无缝复制。

警报的影响

当复制停止时，部署中的节点不再从主管理节点接收配置更新。这会导致策略不一致、网络设备定义过时、终端信息丢失、证书同步延迟以及整个部署中的配置不匹配。如果复制操作在较长的一段时间内保持停止状态，则在主PAN上进行的管理更改在同步恢复前无法在受影响的节点上生效。

对复制失败和复制停止警报进行故障排除

缓慢复制警报

每当在主PAN上进行配置更改时， Cisco ISE将更改放在复制队列中并将其同步到辅助节点。在正常情况下，复制在短时间内完成。但是，如果复制队列开始建立或目标节点处理复制请求的时间比预期长，思科ISE会生成慢速复制警报。

思科ISE将这些警报分为三个严重性级别：

- 缓慢复制信息
- 复制速度缓慢警告
- 缓慢复制错误

警报原因

“慢速复制”警报通常由于延迟复制处理的临时情况而生成。常见原因包括：

- 临时系统资源利用率：短时间的高的CPU利用率、内存使用率或增加的磁盘I/O可能会延迟复

制处理。

- 网络延迟:网络延迟的短暂增加或ISE节点之间的微小数据包丢失可能会减缓数据传输速度。
- 大型配置更改：批量终端导入、策略更新、证书导入或其他大型管理更改会增加要复制的数据量。
- 后台系统操作：备份、恢复、清除、补丁安装或升级活动会暂时增加系统负载。
- 复制队列积压：在短时间内执行多次配置更改可能会暂时增加复制队列。
- 临时服务延迟：RabbitMQ、JGroups或数据库服务在继续正常运行的同时会遇到短暂的处理延迟。

缓慢复制警报 — 信息

当挂起的邮件计数超过10000或复制邮件所用时间超过一小时时，会检测到慢速或停滞的复制。

验证：验证挂起的同步消息计数。导航到Administration > System > Deployment，选择受影响的节点，然后单击Information(i)图标查看待定复制消息的数量。

缓慢复制警报 — 警告

当挂起的邮件计数大于20000或复制邮件所花费的时间超过三个小时时，会检测到慢速或停滞的复制。

验证：验证挂起的同步消息计数。导航到Administration > System > Deployment，选择受影响的节点，然后单击Information(i)图标查看待定复制消息的数量。

缓慢复制警报 — 错误

当挂起的邮件计数大于40000或复制邮件所用时间超过五小时时，会检测到慢速或停滞的复制。

验证：验证挂起的同步消息计数。导航到Administration > System > Deployment，选择受影响的节点，然后单击Information(i)图标查看待定复制消息的数量。

节点复制警报故障排除

1.验证节点的部署状态

要使证书复制成功，辅助节点必须处于Connected状态（在Cisco ISE部署中）。导航到Administration > System > Deployment并验证受影响节点的状态。将鼠标悬停在节点状态旁边的信息(i)图标上，以查看同步详细信息和任何待处理的复制消息。

为每个节点显示的同步状态表示其当前复制和连接状态：

- 绿色 — 节点与部署同步，复制正常运行。
- 黄色 — 节点不同步，节点注册失败，或群集连接已丢失。此状态表明该节点在过去五分钟内无法被集群访问。
- 红色 — 无法访问该节点，无法通过网络连接检查（例如ICMP ping或HTTPS）与其联系。

如果节点显示Yellow或Red状态，则表明存在影响该节点的复制或连接问题。此外，验证节点信息中显示的复制消息计数。挂起的消息计数必须为5,000或更少。包含5,000多条待处理消息的队列表示复制队列已累积，这可能会延迟或阻止复制成功。

2.验证部署中的队列链路警报

在Cisco ISE中成功复制取决于RabbitMQ消息服务和JGroups集群通信框架的可用性和通信。如果任一组件遇到通信问题，思科ISE会生成队列链路错误，这可能会中断部署节点之间的复制。

要验证警报状态，请导航到操作>控制面板>警报，并检查受影响节点上的队列链接错误。

如果存在队列链路错误，请续订思科ISE 根CA证书，因为与证书相关的通信故障通常会导致队列链路错误。解决证书问题后，复制通常会自动恢复，无需额外干预。

注意：有关队列链路错误的详细信息，请参阅ISE队列链路错误文档。

3.检验网络延迟和连通性

思科ISE复制依赖于部署节点之间的稳定网络连接。高网络延迟或间歇性连接会延迟复制，并可能导致同步失败，尤其是在地理位置分散的部署中。

使用ping等连接测试检验受影响节点之间的网络延迟。为了进行可靠的复制，节点之间的往返延迟必须保持在大约300毫秒内。延迟持续超过此阈值可能会对复制性能和同步产生负面影响。另请验证，不存在影响部署节点之间通信的间歇性网络中断、数据包丢失或防火墙限制。

4.验证系统资源利用率

高系统资源利用率可能会影响思科ISE性能和延迟复制任务。过多的CPU、内存或磁盘使用率可能会阻止复制进程成功完成。

验证受影响的节点是否有足够的可用系统资源，以及资源利用率是否保持在建议的运行限制内。如果资源利用率始终很高，请分配更多资源或减少节点上的工作负载，以恢复正常的复制性能。

注意：请参阅性能和可扩展性指南，了解思科ISE部署的推荐硬件大小和资源分配指南。

5.验证部署和网络中的端口可用性

思科ISE复制要求特定的TCP端口在部署中的所有节点之间保持打开状态，以确保不间断通信和成功复制。如果任何这些端口被防火墙、访问控制策略或网络设备阻止，则可能会发生复制失败或同步问题。

验证这些TCP端口是否打开以及是否可在所有思科ISE节点之间到达：

- TCP 443 - HTTPS通信
- TCP 8443 -管理通信
- TCP 12001 - JGroups群集通信和复制
- TCP 6379 — 内部报文传送服务
- TCP 8671 - Cisco ISE消息(RabbitMQ)

登录思科ISE CLI并运行show ports命令验证节点中允许的上述端口。

确认所需的端口在思科ISE节点上启用，并确保允许它们通过网络路径。验证中间防火墙、安全设备或网络策略是否阻止部署节点之间这些端口上的通信。

6.检验DNS解析

思科ISE复制依赖于部署中的所有节点之间的成功通信。要使节点间通信正常工作，节点必须可访问，并且必须配置转发和反向DNS解析并正常工作。DNS解析问题可能会阻止节点通信，从而导致复制失败。

要验证ISE节点中的DNS解析，请登录思科ISE CLI并使用nslookup命令验证部署中每个节点的正向和反向DNS解析。

例如：

- 转发DNS查找：命令nslookup www.example.com必须返回对应思科ISE节点的IP地址。
- 反向DNS查找：命令nslookup 10.x.x.1必须返回对应思科ISE节点的完全限定域名(FQDN)。

7.管理员和ISE消息传递证书验证

思科ISE使用管理员证书和ISE消息传递证书建立复制所需的安全节点间通信。如果任一证书为invalid、expired、corrupted或untrusted，则部署节点之间的复制可能会失败。

要验证证书状态，请导航到Administration > System > Certificates，选择受影响的节点，然后查看Admin和ISE消息证书。验证证书有效、未过期、受信任且处于正常状态。

如果Admin证书或ISE消息证书无效、已损坏或已过期，请替换或更新证书。解决证书问题后，在节点之间重新建立安全通信后，复制将恢复。

注意：有关证书续订的详细信息，请参阅ISE队列链接错误和在ISE中安装证书。

8.验证ISE Stunnel服务的状态

思科ISE中的Stunnel服务是一种内部服务，为ISE组件和外部服务之间的通信提供安全SSL/TLS隧道。ISE使用Stunnel作为封装，将SSL/TLS加密添加到通过普通TCP通信的服务中，而不是在每个应用中独立实施TLS加密。这提高了安全性，同时简化了安全通信的实施。

Stunnel服务必须在Cisco ISE部署中的所有节点上处于Running状态，以便复制正常运行。该服务依赖于有效的ISE管理员和ISE消息证书以在复制过程中在节点之间建立安全TLS通信。可使用命令show tech-support从Cisco ISE CLI验证服务状态 | include stunnel

复制警报的日志收集

这些是在debug模式下设置的常见组件，用于隔离和排除思科ISE中的复制警报。

- 复制部署（replication.log和ise-psc.log）
- Replication-JGroup（replication.log和ise-psc.log）
- 复制跟踪器(tracking.log)
- hibernate(hibernate.log)
- JMS(replication.log)

参考

- 思科身份服务引擎管理员指南，版本3.5
- 在ISE上排除故障并启用调试
- 收集身份服务引擎上的支持捆绑包

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。