了解ISE证书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。

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证书复制警报

证书复制失败

当思科ISE无法将证书相关数据从主要管理节点(PAN)复制到部署中的一个或多个节点时，会生成证书复制失败警报。每当在主PAN上导入、生成、续订或修改证书时，ISE会自动复制证书及其相关配置，以在所有节点之间保持一致性。此警报表示复制过程不成功，导致受影响节点上的证书配置不一致。

警报原因

当思科ISE无法在一个或多个节点上成功传输、验证或安装与证书相关的数据时，可能会发生Certificate Replication Failed警报。常见原因包括

- 网络通信问题：数据包丢失、高网络延迟、防火墙限制阻止复制流量、ISE节点之间的路由问题或MTU不匹配导致数据包分段或丢弃可能会中断证书复制。
- 复制服务问题：如果RabbitMQ、JGroups或其他内部复制服务不可用、重新启动或无法正常工作，则证书复制可能会失败。
- 证书验证失败：如果证书链不完整、CA或中间证书丢失、证书过期或损坏，或者证书包含不支持的密钥用法或无效格式，复制可能会失败。
- 节点通信问题：如果目标节点脱机、重新启动、取消注册、从部署断开连接或无法访问，则无法完成证书复制。
- 磁盘空间不足:目标节点没有足够的可用磁盘空间来导入和安装复制的证书。
- 内部数据库问题：如果ISE配置数据库无法存储或更新证书元数据，复制可能会失败。

警报的影响

此警报的影响取决于复制的证书类型和依赖它的服务。失败的证书复制可能导致ISE节点之间的证书配置不一致、HTTPS证书不匹配、EAP身份验证失败、pxGrid信任建立问题、SCEP注册或证书调配失败、受信任证书存储中的不一致以及外部集成的TLS验证失败。

证书复制暂时失败

当思科ISE暂时无法将证书相关数据从主要管理节点(PAN)复制到部署中的一个或多个节点时，生成证书复制暂时失败警报。与“证书复制失败”警报不同，此警报表示复制失败被视为暂时的，思科ISE会在解决基础条件时自动重试复制操作。

警报原因

警报通常由于临时阻止证书复制的瞬态情况而生成。常见原因包括：

- 临时网络通信问题：短暂的网络中断、数据包丢失、高延迟、防火墙延迟或ISE节点之间的临时路由问题。
- 复制服务初始化或重新启动：RabbitMQ、JGroups或其他内部复制服务正在重新启动或暂时不可用。
- 临时节点不可用：目标节点正在启动、重新启动应用服务、重新加入部署或暂时无法访问。
- 临时系统资源限制：高CPU利用率、内存压力或磁盘I/O争用会暂时延迟复制处理。
- 并发管理操作：当正在进行另一个证书导入、备份、恢复、修补程序安装或部署同步时，证书复制可能会延迟。
- 临时数据库或复制队列延迟：内部数据库操作或复制队列临时正忙于处理其他同步请求。

警报的影响

在大多数情况下，此警报对操作的影响最小，因为思科ISE会自动重试复制操作。但是，在复制成功完成之前，节点之间可能存在临时不一致，包括：

- 新导入或更新证书的延迟传播
- 部署中的临时证书配置不匹配
- 受影响节点上基于证书的服务的延迟可用性
- HTTPS、EAP、pxGrid或SCEP服务中的临时延迟（如果它们依赖于复制的证书）

如果警报持续或重复发生，则会导致“证书复制失败”警报。

排除ISE证书复制警报故障

这些是故障排除或验证ISE中的证书复制警报时要验证的常见因素。

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.确认受影响节点上尚未存在证书

如果辅助节点上已存在正在复制的证书，则证书复制可能会失败。

导航到Administration > System > Certificates，选择受影响的节点，然后验证是否已安装证书。如果存在证书，请检查其属性，确保它与正在复制的证书匹配，并确定是否存在任何重复或冲突的证书。

5.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。

6.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。

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）。