了解ISE复制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。

思科ISE中的复制

ISE中的复制是跨部署中的多个节点同步配置和运行数据以保持一致的过程。

主管理节点负责将部署中所做的更改复制到部署中的所有其他（辅助）节点。

Cisco ISE使用JGroups（可靠的组通信框架）作为其复制架构的一部分。JGroups使ISE部署中的节点能够彼此通信并交换复制数据。它提供的消息传送框架有助于在节点之间传送配置和数据库更新，同时保持部署之间的同步。

- JGroups是Cisco ISE用于复制的通信框架；它本身不存储复制的数据。
- 并非思科ISE中的所有数据都通过JGroups进行复制。根据传输的数据类型，不同的服务使用不同的通信机制。
- 如果复制暂时中断，则某些Cisco ISE服务可以使用本地可用数据继续运行，直到恢复同步。

数据传输方法示例

数据	通信方法
配置和复制消息	JGroups
支持捆绑包集合	HTTPS API（TCP端口443）
调试配置	HTTPS API（TCP端口443）
实时日志和报告	RabbitMQ或UDP，取决于部署配置

思科ISE复制的关键必备条件和验证检查

- DNS解析：对于参与部署的所有思科ISE节点，必须成功解析转发和逆向DNS查找。节点通信和复制操作需要适当的DNS解析。
- NTP同步：所有思科ISE节点必须同步到可靠的NTP源，以在部署中保持一致的系统时间。时间同步对于复制和证书验证至关重要。
- 证书：每个思科ISE节点上安装的管理员证书必须有效且受信任。复制过程依赖管理员证书在节点之间进行安全通信。
- 端口要求：网络连接必须允许通过复制和节点间服务所需的端口进行通信：

服务	协议/端口
HTTPS(SOAP)	TCP/443
数据同步和复制(JGroups)	TCP/12001
管理访问	TCP/8443
ISE消息服务(SSL)	TCP/8671
分析器终端所有权同步	TCP/6379

- 网络连通性：思科ISE节点之间的网络连接必须稳定，且延迟不得超过300毫秒。检验节点之间的延迟和丢包有助于确保可靠的复制。
- 队列链路状态：思科ISE消息传送证书用于通过TCP端口8671保护节点间通信。无效或损坏的消息传递证书可能会导致队列链路错误和复制失败。在这种情况下，必须重新生成ISE根CA证书或ISE消息传递证书。
- ISE Stunnel服务：Cisco ISE Stunnel服务在分布式部署中运行，促进节点之间的安全通信。服务必须在所有适用节点上运行才能支持复制。可使用以下命令从Cisco ISE CLI验证服务状态：
  show tech-support | include stunnel
- ISE补丁和版本：主管理节点和加入节点（独立节点）必须具有相同的版本和补丁级别进行节点注册和同步，才能无缝工作。

思科ISE中的复制阶段

思科ISE中的复制包括三个不同的阶段，这些阶段共同建立和维护部署中所有节点的同步。每个阶段都有其特定的用途，首先是节点入网，然后是初始数据库同步，最后是持续交换增量更新以保持所有节点同步。

- 节点注册
- 完全同步
- 增量同步

了解思科ISE中的节点注册

节点注册是思科ISE节点加入现有部署并与主要管理节点(PAN)建立通信的流程。

在节点注册过程中：

步骤 1：加入节点（独立节点）发起与主管理节点的通信。

步骤 2：使用思科ISE管理员证书执行相互证书验证。

步骤 3：DNS解析、NTP同步、网络可达性和所需的端口可访问性都作为通信过程的一部分进行验证。

步骤 4：主管理节点验证独立节点/加入节点运行兼容的Cisco ISE版本和补丁级别。

步骤 5：交换部署信息、节点角色和信任关系。

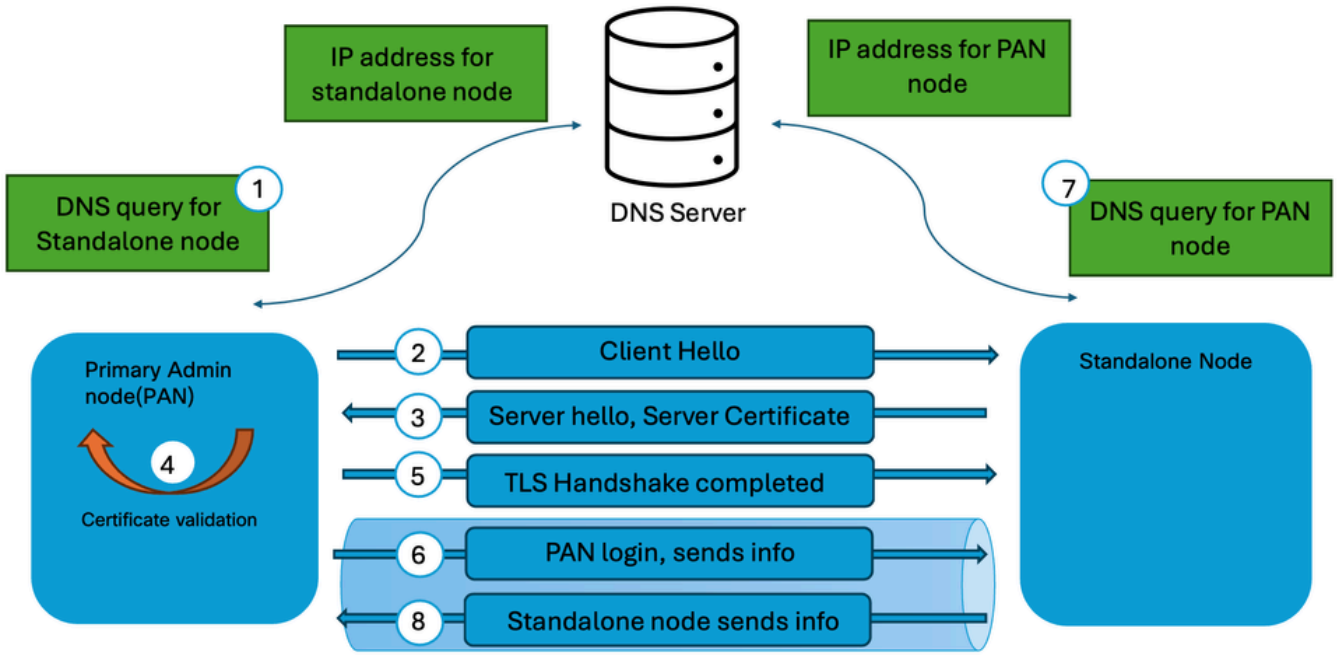
步骤 6：数据库复制服务已初始化并准备好进行同步。

成功完成节点注册会将节点设置为部署的受信任成员，并允许开始复制过程。

主要特征

- 在将新节点添加到部署时发生。
- 建立信任和通信渠道。
- 不会立即传输完整的配置数据库。
- 作为后续同步操作的先决条件。

有关节点注册过程的详细说明，请参阅[了解思科ISE中的节点注册过程]。



节点注册流程

注意：要添加到部署的节点必须是独立节点。此外，主要管理节点(PAN)必须在部署中启用主要管理角色，以允许在Cisco ISE中注册节点。

了解思科ISE中的完全同步

完全同步是一个完整的数据库复制过程，在此过程中，整个配置数据库从主PAN传输到另一个节点。完全同步不会只传输已修改的记录。相反，将在接收节点上重建整个配置数据集。

在以下情况下可能会发生完全同步：

- 节点注册后的初始同步。
- 从复制失败中恢复。
- 数据库严重不一致。
- 将节点重新加入部署。
- 通过Cisco TAC故障排除过程启动手动同步。
- 内部复制机制确定增量同步无法再恢复数据库一致性。

在完全同步期间：

步骤 1：主管理节点准备一个完整的数据库快照。

步骤 2：配置数据封装在.dmp文件中并传输到接收节点。

步骤 3：接收节点上的现有复制数据将进行验证和更新。

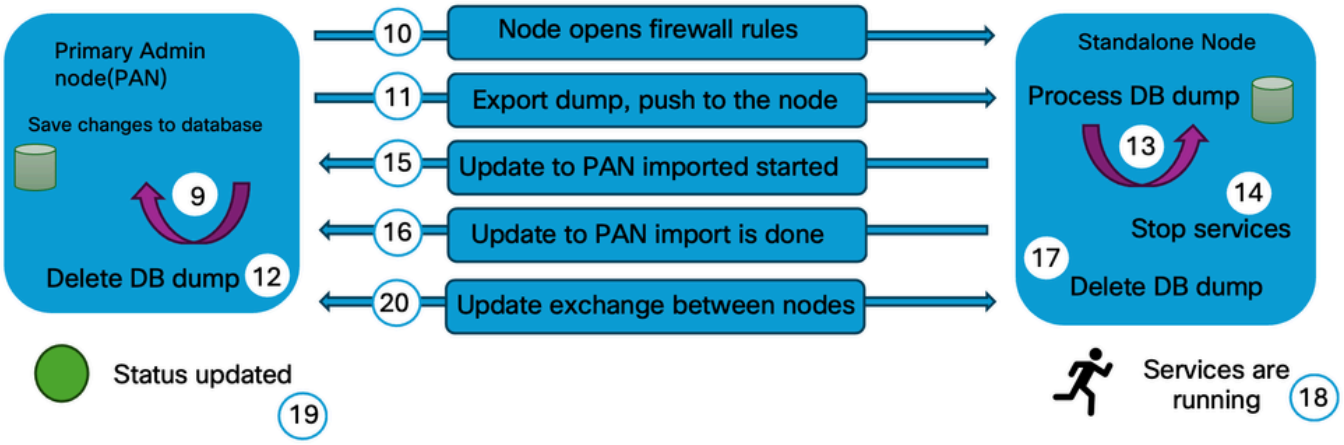
步骤 4：将重建整个配置数据库以匹配主管理节点。

步骤 5：复制状态会在完成后进行验证。

由于完全同步涉及的数据远远多于增量同步，因此它需要额外的处理时间和网络资源。

完全同步的特征

- 传输完整的配置数据库。
- 消耗更多带宽和系统资源。
- 比增量同步花费的时间长。
- 在检测到差异时恢复数据库一致性。
- 通常比增量同步发生频率低。



完全同步进程

了解思科ISE中的增量同步

增量同步是思科ISE在节点成功加入部署后用于分发配置更改的持续复制机制。当管理员在PAN上进行配置更改时，思科ISE不会传输整个数据库。相反，仅修改后的记录会复制到用户节点。

通过增量同步复制的更改示例包括：

- 策略修改
- 网络设备添加或更新
- 终端组更改
- 授权配置文件更新
- 与证书相关的配置更改
- 身份源配置更新

增量同步过程持续运行，旨在维护所有节点的一致性，同时最大限度地降低带宽利用率和复制开销。

增量同步的优点

- 减少复制流量。
- 最大程度地缩短同步时间。
- 允许快速传播配置更改。
- 在整个部署过程中保持接近实时的一致性。

复制工作流程

步骤 1：配置更改发生在主管理节点上。

步骤 2：更改会写入主管理节点数据库。

步骤 3：复制服务标识已修改的记录。

步骤 4：主管理节点将新事件/更改写入事务表中。

步骤 5：独立于PAN的线程将信息/更改发布到部署中的辅助节点。

步骤 6：部署中的辅助节点从主要管理节点接收更改。

步骤 7：部署中的辅助节点应用从主管理节点接收的更改。

步骤 8::复制状态在成功完成时更新。

在正常操作条件下，思科ISE中的大多数复制活动通过增量同步进行。

注意：如果辅助节点识别缺少的复制消息，它会向主管理节点(PAN)发起请求，以检索缺少的消息并保持同步

复制序列概述和同步状态

思科ISE部署中的整体复制工作流程可概述如下：

1.节点注册：建立信任并将节点添加到部署。

2.初始完全同步：将完整的配置数据库传输到新注册的节点。

3.增量同步：在正常操作过程中持续传播配置更改。

4.完全同步（如果需要）：如果检测到复制问题或数据库不匹配，则重建数据库一致性。

此阶段化方法使Cisco ISE能够跨所有节点维护一致的配置数据库，同时优化网络利用率和复制性能。

同步状态

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，或群集连接丢失（过去五分钟内群集无法访问该节点）。
- 红色 — 节点在物理上不可达，无法通过网络连接检查（例如，ICMP ping和HTTPS）与其联系。

注意：如果复制未正确进行，可以通过登录到主管理节点来执行与主管理节点的手动同步，导航到Administration > System > Deployment > select the node，然后单击Sync up。

终端复制

终端复制是ISE跨所有策略服务节点(PSN)和主管理节点(PAN)同步终端数据库信息以在部署中维护一致的终端身份视图的过程。

- 思科ISE维护一个集中终端数据库，存储有关连接到网络的设备的信息。此信息包括静态配置的终端和通过身份验证、分析、状态评估或与外部身份源集成动态了解的终端。
- 当创建或修改终端信息时，思科ISE将更改复制到部署中的其他节点。此同步使每个策略服务节点可以使用相同的终端信息评估身份验证和授权请求，而不管哪个PSN处理该请求。
- 终端复制由Cisco ISE自动处理，并构成整体数据库复制机制的一部分。在正常操作过程中，管理员不需要手动启动终端同步。

终端复制的工作原理

- 终端更新：终端通过身份验证、分析、状态或手动配置创建或更新。
- 变更检测：思科ISE检测终端更改并准备进行复制。
- 复制：使用ISE复制框架将更新的终端信息复制到部署中的其他节点。
- 数据库同步：辅助节点使用复制的信息更新其本地终端数据库。
- 一致的策略实施：同步完成后，所有策略服务节点使用相同的终端信息来进行身份验证和授权决策。

从思科ISE版本3.3中，动态发现的终端不会自动复制到所有节点。可以从终端复制窗口启用或禁用此功能。导航到Administration > System > Settings > Endpoint Replication，根据需要启用或禁用。

注意：必须将终端复制与会话复制区分开来。终端复制同步永久终端数据库记录（例如MAC地址、终端组和分析信息），而会话复制同步运行时会话信息以支持策略实施和操作连续性。这些机制独立运行，并在Cisco ISE架构内提供不同的功能。

常见节点复制问题

情形 1：由于DNS解析失败，节点注册失败

节点注册失败，错误原因为“主机名无法解析。请检查您的DNS配置”。

验证步骤

- 确保在主要管理节点和独立节点中配置了有效的DNS服务器。使用命令show running-config验证DNS服务器配置 | include name-server
- 使用用于正向DNS查找的节点的命令nslookup　FQDN和用于反向DNS查找的节点的nslookup ip address，验证主管理节点和独立节点中的正向和反向DNS解析。
- 从ISE节点的CLI使用命令ping　DNS服务器IP，验证从主要管理节点和独立节点的DNS服务器可达性。

方案 2：由于管理员证书过期，节点注册失败

节点注册失败，错误原因为“加载证书时出错。此时无法到达节点。请稍后重试”。

验证步骤

- 验证主要管理节点和独立节点的管理员证书，以确保有效性和证书状态。导航到 Administration > System > Certificates，选择节点，然后验证管理员证书的有效性和状态。
- 如果管理员证书已过期，请替换或更新证书，并确保分配了管理员用法。

情形 3：由于版本不匹配，节点注册失败

节点注册失败，错误原因为“版本/修补程序详细信息不匹配”。

验证步骤

- 使用命令show version验证软件版本以及主要管理节点和独立节点的补丁以确保版本详细信息匹配。

调试日志的组件

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中的复制故障。

- 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)
- ca-service(caservice.log)
- admin-ca(ise-psc.log)

参考

- 在ISE上排除故障并启用调试
- ISE — 队列链路错误
- 思科身份服务引擎管理员指南，版本3.4
- 思科身份服务引擎管理员指南，版本3.5

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）。