思科 ISE 中的网络部署

注释 此产品的文档集力求使用无偏见语言。在本文档集中，无偏见定义为不暗示基于年龄、残障、性别、种族身份、族群身份、性取向、社会经济地位和交叉性的歧视的语言。由于产品软件的用户界面中使用的硬编码语言，基于 RFP 文档使用的语言或引用的第三方产品使用的语言，文档中可能存在例外情况。

Cisco ISE 网络架构

Cisco ISE 架构包括以下组件：

- 节点和角色类型
  - Cisco ISE 节点 - Cisco ISE 节点可以承担以下任意或所有角色：管理、策略服务、监控或 pxGrid
- 网络资源
- 终端

策略信息点表示外部信息传达给策略服务角色所在的点。例如，外部信息可以是轻量级目录访问协议 (LDAP) 属性。

Cisco ISE 部署术语

本指南在讨论 Cisco ISE 部署方案时使用以下术语：

术语	定义
服务	角色提供的特定功能，例如网络访问、分析、状态、安全组访问、监控和故障排除。
节点	单个物理或虚拟思科 ISE 设备。
节点类型	思科 ISE 节点可以承担下列任何角色：管理、策略服务、监控
角色	确定节点提供的服务。思科 ISE 节点可以承担以下任一或全部角色：。通过管理用户界面可使用的菜单选项取决于节点承担的角色和人员。
角色	确定节点是独立节点、主要节点还是辅助节点，并且仅适用于管理和监控节点。

分布式部署中的节点类型和角色

Cisco ISE 节点可以根据它承担的角色提供各种服务。部署中的每个节点均可承担管理、策略服务、pxGrid 和监控角色。在分布式部署中，您可以在网络中使用以下节点组合：

- 实现高可用性的主要和次要管理节点
- 实现自动故障切换的监控节点对
- 实现会话故障切换的一个或多个策略服务节点
- pxGrid 服务的一个或多个 pxGrid 节点

管理节点

通过具有管理角色的 Cisco ISE 节点，您可以在 Cisco ISE 上进行所有管理操作。它处理与诸如身份验证、授权和记帐等功能有关的所有系统相关配置。在分布式部署中，您最多可以具有两个运行管理角色的节点。管理角色可以承担独立、主要或辅助角色。

策略服务节点

承担策略服务角色的思科 ISE 提供网络访问、终端安全评估、访客接入、客户端调配和分析服务。此角色评估策略并作出所有决策。您可以让多个节点承担此角色。通常，分布式部署中可能有多个策略服务节点。驻留在同一高速局域网 (LAN) 中或负载均衡器后面的所有策略服务节点可以组合在一起，形成一个节点组。如果节点组中的一个节点发生故障，其他节点会检测到故障，并重置任何 URL 重定向会话。

分布式设置中至少有一个节点应当承担策略服务角色。

监控节点

具有监控角色的Cisco ISE 节点用作日志收集器，并且存储来自网络中所有管理节点和策略服务节点的日志消息。此角色提供可用于有效管理网络和资源的高级监控和故障排除工具。具有此角色的节点会将其收集的数据汇总和关联，并为您提供有意义的报告。通过 Cisco ISE，您最多可以拥有两个具有此角色的节点，并且这些节点可以承担主要角色或辅助角色，从而实现高可用性。主要和辅助监控节点收集日志消息。如果主监控节点断开连接，辅助监控节点会自动成为主监控节点。

分布式设置中至少有一个节点应承担监控角色。我们建议您不要在同一Cisco ISE 节点上启用监控和服务策略角色。我们建议监控节点仅专用于监控，以获取最佳性能。

pxGrid 节点

您可以使用思科 pxGrid 与其他网络系统（例如 ISE 生态系统合作伙伴系统）和其他思科平台共享思科 ISE 会话目录中的情景相关信息。pxGrid 框架也可用来在思科 ISE 与第三方供应商之间、在节点（例如共享标记）与策略对象之间交换策略和配置数据，还能进行其他信息的交换。思科 pxGrid 还允许第三方系统调通过自适应网络控制操作 (EPS) 来隔离用户/设备以应对网络或安全事件。可通过 TrustSec 主题将标签定义、值和说明等 TrustSec 信息从思科 ISE 传输到其他网络。可通过终端配置文件元主题，将具有完全限定名称 (FQN) 的终端配置文件从思科 ISE 传输到其他网络。思科 pxGrid 还支持标签和终端配置文件的批量下载。

您可以通过 pxGrid 发布和订用 SXP 绑定（IP-SGT 映射）。有关 SXP 绑定的详细信息，请参阅思科身份服务引擎管理员指南中的“源组标记协议”部分。

在高可用性配置中，思科pxGrid 服务器通过 PAN 在节点之间复制信息。当 PAN 断开连接时，pxGrid 服务器会停止处理客户端注册和订用。您需要手动升级 PAN，以激活 pxGrid 服务器。

独立和分布式 ISE 部署

具有单个 Cisco ISE 节点的部署称为独立部署。此节点运行管理、策略服务和监控角色。

具有多个Cisco ISE 节点的部署称为分布式部署。要支持故障切换和提高性能，您可以分布式方式设置具有多个 Cisco ISE 节点的部署。在 Cisco ISE 分布式部署中，管理和监控活动会进行集中，而处理则分布在多个策略服务节点上。根据您的性能需求，您可以扩展您的部署。Cisco ISE 节点可以承担以下任何角色：管理、策略服务和监控。

分布式部署方案

- 小型网络部署
- 中型网络部署
- 大型网络部署

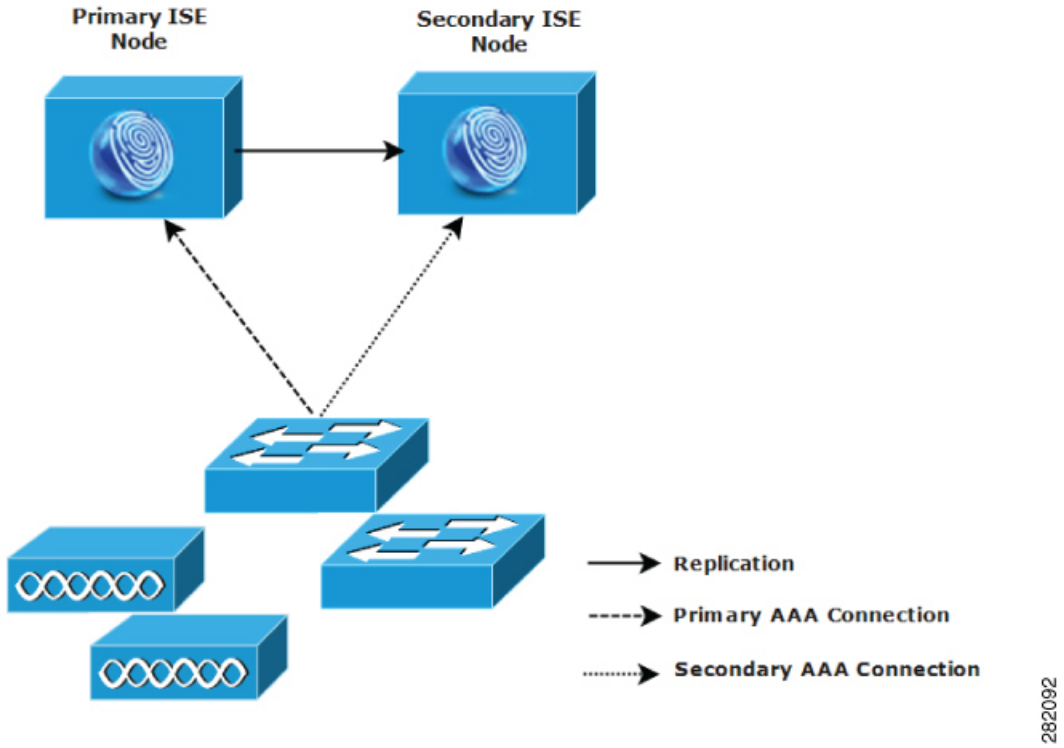
小型网络部署

最小的 Cisco ISE 部署包含两个 Cisco ISE 节点，其中一个 Cisco ISE 节点在小型网络中用作主要设备。

主要节点提供此网络模型所需的所有配置、身份验证和策略功能，并在备份角色中提供辅助 Cisco ISE 节点功能。辅助节点支持主要节点，并会在主要节点与网络设备、网络资源或 RADIUS 之间的连接断开时维持网络正常工作。

客户端与主思科 ISE 节点之间的集中式身份验证、授权和记帐 (AAA) 操作使用 RADIUS 协议来执行。Cisco ISE 会将驻留在主要 Cisco ISE 节点上的所有内容与辅助 Cisco ISE 节点同步或复制这些内容。因此，辅助节点与主要节点的状态保持一致。在小型网络部署中，通过此类型的配置模式，您可以使用此类型的部署或类似方法在所有 RADIUS 客户端上同时配置主要节点和辅助节点。

图 *1:* 小型网络配置



随着网络环境中设备、网络资源、用户和AAA客户端数量的增加，您应从基本的小模式更改部署配置并更多地使用分离式或分布式部署模式。

分离式部署

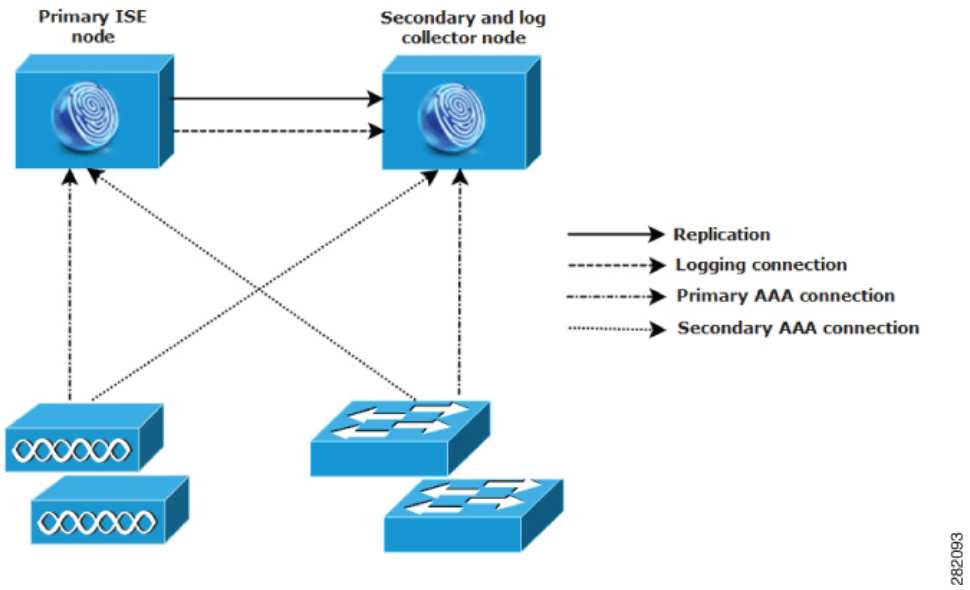
在分离式 Cisco ISE 部署中，您将按照小型 Cisco ISE 部署中所述继续维护主要节点和辅助节点。但是， AAA 负载会在两个 Cisco ISE 节点之间进行拆分，以优化 AAA 工作流程。如果 AAA 连接有任何问题，则每个Cisco ISE 设备（主要或辅助）需要能够处理全部工作负载。主要节点和辅助节点在正常网络操作过程中均不处理任何 AAA 请求，因为此工作负载分布在两个节点之间。

以此方式拆分负载的功能会直接减少系统中每个Cisco ISE 节点上的压力。此外，拆分负载可提供更好的加载，同时辅助节点的功能状态会在正常网络操作过程中得以维护。

在分离式Cisco ISE 部署中，每个节点可以执行各自的特定操作（例如网络准入或设备管理），并且在发生故障的情况下仍然执行所有 AAA 功能。如果您有两个 Cisco ISE 节点，分别用于处理身份验证请求和从AAA 客户端收集记帐数据，则建议您将其中一个Cisco ISE 节点设置为用作日志收集器。

此外，分离式 Cisco ISE 部署设计具有优势，因为它允许增长。

图 2: 分离式网络部署



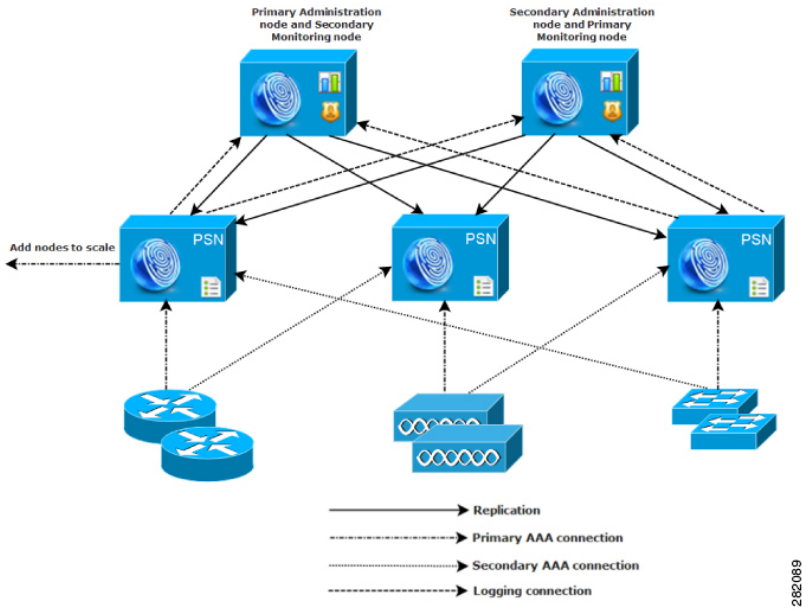
中型网络部署

随着小型网络的增长，您可以通过添加 Cisco ISE 节点创建中型网络来跟上步伐和管理网络增长。在中型网络部署中，您可以将新节点专用于所有 AAA 功能，并将原始节点用于配置和日志记录功能。

注释 在中型网络部署中，不能在运行管理角色和/或监控角色的节点上启用策略服务角色。需要专用策略服务节点。

随着网络中日志流量的增加，您可以选择将一个或两个辅助 Cisco ISE 节点专用于网络中的日志收集。

图 *3:* 中型网络部署



大型网络部署

集中日志记录

我们建议您对大型 Cisco ISE 网络使用集中日志记录。要使用集中日志记录，您必须先设置担任监控角色（用于监控和日志记录）的专用日志记录服务器，以处理大型繁忙网络可能会生成的高系统日志流量。

由于会针对出站日志流量生成系统日志消息，因此任何符合 RFC 3164 的系统日志设备都可以用作出站日志记录流量的收集器。通过专用日志记录服务器，您可以使用 Cisco ISE 中提供的报告和警报功能支持所有 Cisco ISE 节点。

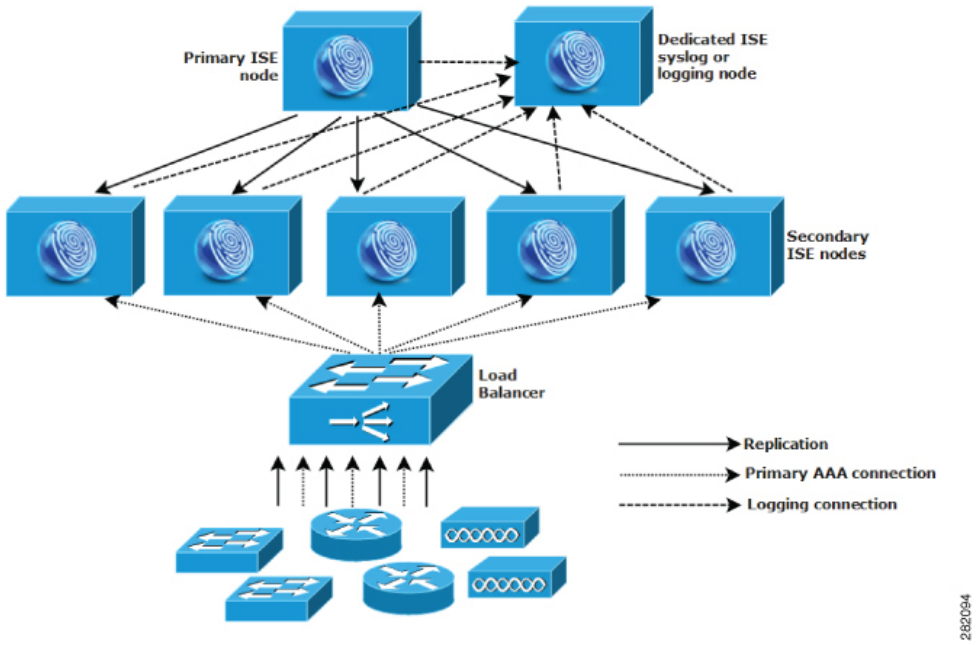
您也可以考虑使用设备将日志发送到 Cisco ISE 节点上的监控角色以及通用系统日志服务器。如果 Cisco ISE 节点上的监控角色关闭，则添加通用日志服务器可提供冗余备份。

负载均衡器

在大型集中式网络中，您应该使用负载均衡器，以此简化 AAA 客户端的部署。使用负载均衡器只需单个条目即可表示多个 AAA 服务器，并且负载均衡器会优化 AAA 请求至可用服务器的路由。

但是，只有一个负载均衡器可能会发生单点故障。要避免此潜在问题，请部署两个负载均衡器，以确保采取冗余和故障切换措施。此配置要求您在各 AAA 客户端中设置两个 AAA 服务器条目，并且此配置会在整个网络保持一致。

图 *4:* 大型网络部署

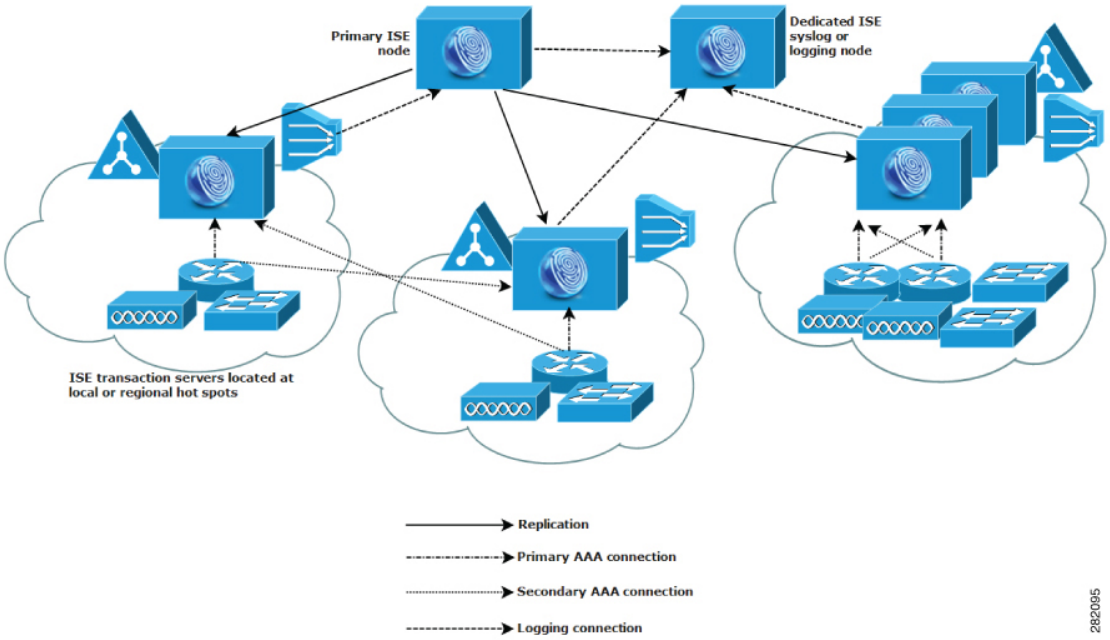


离散网络部署

离散 Cisco ISE 网络部署对于具有主园区且在其他位置有区域、国家或办事处场所的组织最有用。主园区是主网络驻留所在的位置，连接到其他 LAN，规模从小到大不等，并且支持不同地理区域和位置中的设备及用户。

大型远程站点可具有各自的 AAA 基础设施，以实现最佳 AAA 性能。集中管理模式有助于维护一致、同步的 AAA 策略。集中配置模式将主要 Cisco ISE 节点与辅助 Cisco ISE 节点结合使用。我们仍建议您在 Cisco ISE 节点上使用单独的监控角色，但是，各远程位置应保留其特有的网络要求。

图 *5:* 离散部署



规划具有多个远程站点的网络的注意事项

- 验证使用的是中央数据库还是外部数据库，例如 Microsoft Active Directory 或轻量级目录访问协议 (LDAP)。每个远程站点应具有同步的外部数据库实例，可供 Cisco ISE 访问以优化 AAA 性能。
- AAA 客户端的位置非常重要。您应使 Cisco ISE 节点的位置尽可能接近 AAA 客户端，以减少网络延迟影响以及由 WAN 故障导致无法访问的可能性。
- Cisco ISE 对某些功能（例如备份）具有控制台访问权限。请考虑在每个站点使用终端，从而允许进行直接、安全的控制台访问，以此绕过对每个节点进行网络访问。
- 如果小型远程站点距离接近并具有到其他站点的可靠 WAN 连接，请考虑使用 Cisco ISE 节点作为本地站点的备份以提供冗余。
- 应在所有 Cisco ISE 节点上正确配置域名系统 (DNS)，以确保对外部数据库的访问。

每个部署模式的最大支持会话数

下表列出了每个部署模式的最大支持会话数。

表 *1:* 每个部署模式支持的最大会话数

部署模式	平台	最大会话数
独立（所有角色位于单个节点上）	3615	10,000
	3655	25,000
	3695	50,000
	3515	7500
	3595	20,000
基本 2 节点部署（冗余）	3615	10,000
	3655	25,000
	3695	50,000
	3515	7500
	3595	20,000
混合分布式部署（管理和 MnT 位于同一设备上；策略服务位于专用设备上）	3615 作为 PAN 和 MnT	10,000
	3655 作为 PAN 和 MnT	25,000
	3695 作为 PAN 和 MnT	50,000
	3515 作为 PAN 和 MnT	7500
	3595 作为 PAN 和 MnT	20,000
专用（PAN、MnT、PXG 和 PSN 节点）	3595 作为 PAN 和 MnT	500,000
	3655 作为 PAN 和 MnT	500,000
	3695 作为 PAN/MnT	2,000,000

表 *2:* 每个 *PSN* 的最大活动会话数

每个 **PSN** 的扩展[1]	最大活动会话数
SNS 3615	10,000
SNS 3655	50,000
SNS 3695	100,000
SNS 3515	7500
SNS 3595	40,000

[1] 专用策略节点（最大会话数受部署总规模限制）

SNS 3500/3600 系列设备的部署规模和扩展建议

表 *3: SNS 3500/3600* 系列设备的最大 *RADIUS* 扩展

部署模式	平台	专用 PSN 的最大数量	每个部署的最大 RADIUS 会话数
独立式	3515	0	7500
	3595	0	20,000
	3615	0	10,000
	3655	0	25,000
	3695	0	50000
PAN 和 MnT 位于同一节点和专用 PSN 上	3515 作为 PAN 和 MnT	5	7500
	3595 作为 PAN 和 MnT	5	20,000
	3615 作为 PAN 和 MnT	5	10,000
	3655 作为 PAN 和 MnT	5	25,000
	3695 作为 PAN 和 MnT	5	50,000
专用（PAN、MnT、PXG 和 PSN 节点）	3595 作为 PAN 和 MnT	50	500,000
	3655 作为 PAN 和 MnT	50	500,000
	3695 作为 PAN 和 MnT	50	2,000,000

支持 Cisco ISE 功能所需的交换机和无线局域网控制器配置

要确保 Cisco ISE 能够与网络交换机互操作，并且来自 Cisco ISE 的功能可跨网段成功实施，您必须使用某些所需的网络时间协议 (NTP)、RADIUS/AAA、IEEE 802.1X、MAC 身份验证绕行 (MAB) 和其他设置来配置网络交换机。

ISE 社区资源

有关使用 WLC 设置思科 ISE 的信息，请参阅使用 WLC 设置思科 ISE 视频。