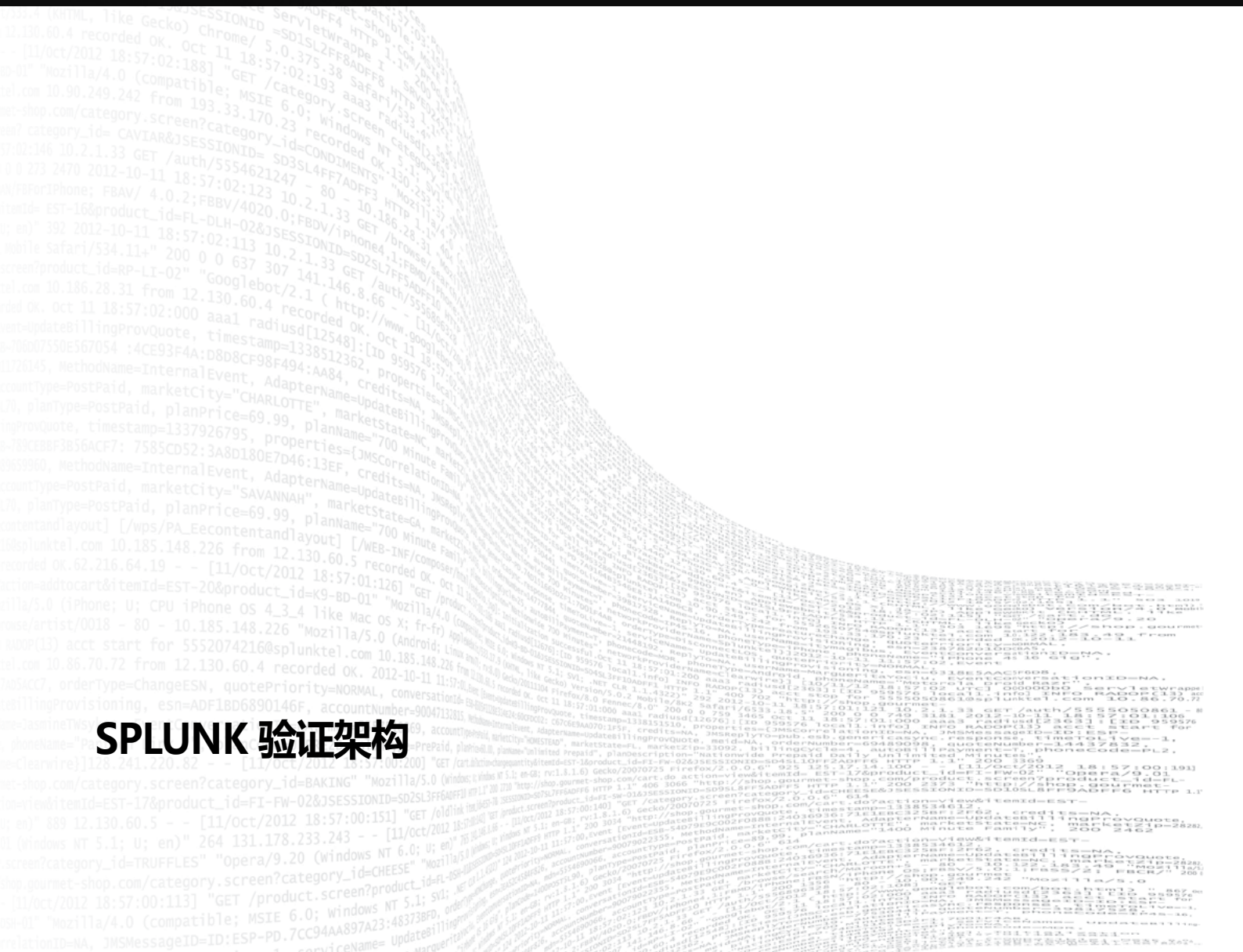
SPLUNK 验证架构



目录

引言

Splunk 验证架构（SVA）是经验证可确保稳定、高效及可重复 Splunk 部署的参考架构。Splunk 的许多现有客户都曾经历快速采用及扩容，导致他们在尝试扩展时面临若干挑战。同时，Splunk 的新客户日益希望获得指引及经认证的架构，以确保他们的初始部署具有稳固的基础。我们已开发出 SVA，帮助客户满足这些不断增长的需求。

不论您是 Splunk 的新客户还是现有客户，SVA 都可帮助您构建能够更轻松维护及更简单地进行故障检修的环境。SVA 的设计旨在尽可能为您提供最佳的结果，同时最大限度地降低您的总拥有成本。此外，您的整个 Splunk 基础将基于可重复的架构，让您能够根据您的需求变化扩展部署。

SVA 可提供将各种组织要求纳入考虑的拓扑选项，因此您可以轻松了解及找到最符合您要求的拓扑。Splunk 验证架构选择流程可帮助您将您的特定要求与最符合您组织需求的拓扑匹配。如果您是 Splunk 的新客户，我们建议您为您的初始部署实施经验证的架构。如果您是现有客户，我们建议您探索与经验证架构拓扑结合的选项。除非您有必须构建定制架构的独特要求，否则，经验证的架构将很有可能满足您的需求，同时确保成本效益。

本白皮书将为您提供 SVA 概览。在本白皮书内，您将会找到完成 SVA 选择流程所需的资源，包括要求问卷、部署拓扑图、设计原则以及一般指引。

如果您在实施 Splunk 验证架构时需要帮助，请联系 Splunk 专业服务部（https://www.splunk.com/en_us/support-and-services/splunk-services.html）。

文档结构

SVA 内容分为三个主要部分：

1. 索引和搜索拓扑
2. 数据收集架构组件
3. 设计原则和最佳实践

索引和搜索涵盖提供 Splunk 部署的核心索引和搜索能力的架构层。数据收集组件部分可指导您根据您的要求选择合适的数据收集机制。

设计原则和最佳实践适用于您的整个架构，可帮助您在处理部署细节时作出正确的选择。

使用 Splunk 验证架构的原因

实施经验证架构能使您更自信地设计和部署 Splunk。SVA 可帮助您解决组织面临的部分最常见挑战，包括：

性能

- 组织希望看到性能和稳定性得到改进。

复杂性

- 组织有时会陷入定制部署的陷阱，尤其是当他们过于快速或有机增长时。在这些情况下，可能会对环境引入不必要的复杂性。当组织尝试扩展时，该复杂性可能会成为严重的障碍。

效率

- 为获得 Splunk 部署的最大益处，组织必须提高运营效率及加快实现价值。

成本

- 组织寻求各种方法降低总拥有成本（TCO），同时满足他们的所有要求。

灵活性

- 组织在扩展及增长时需要适应变化。

维护

- 为减少维护工作，通常需要优化环境。

可扩展性

- 组织必须能够高效及无缝扩展。

验证

- 组织内的利益相关者想要确保他们的 Splunk 部署基于最佳实践构建。

Splunk 验证架构的支柱

Splunk 验证架构基于以下基础支柱构建。若要了解关于这些设计支柱的更多信息，请参阅下文附录 "A"。

可用性	性能	可扩展性	安全性	可管理性
系统**可持续运行**，能够从计划及非计划中断恢复。	系统**能够在不同的使用模式**下维持最佳的服务水平。	系统的设计旨在可在所有层扩展，使您可有效**处理增加的工作负载均衡**。	系统**设计旨在可保护数据、配置及资产**，同时持续实现价值。	系统**可集中操作，可跨所有层管理**。

这些支柱直接支持 Splunk 卓越中心模式的**平台管理及支持**服务。

Splunk 验证架构的特色

请注意，SVA 并不包含部署技术或部署分级。原因如下：

- 操作系统及服务器硬件等部署技术被视为 SVA 环境下的实施选择。不同客户具有不同的选择，因此无法一概而论。
- 部署分级需要评估数据摄取数量、数据类型、搜索量以及搜索使用案例，这是特定于客户的数据，对基础部署架构本身并无意义。当您建立部署架构后，现有分级工具可帮助您完成该流程。Splunk 存储分级（https://splunk-sizing.appspot.com/）是可用的工具之一。

SVA 将提供：	SVA 不提供：
✓ 群集及非群集部署选项。 ✓ 参考架构图。 ✓ 帮助您选择合适架构的指引 ✓ 层特定建议 ✓ 构建您的 Splunk 部署的最佳实践	✗ 实施选择（操作系统、裸机 VS 虚拟 VS 云等）。 ✗ 部署分级 ✗ 对您的架构的规范性认可。注：SVA 可提供建议和指引，使您最终能够为您的组织做出正确的决定。 ✗ 针对每个可能的部署场景的拓扑建议在某些情况下，由于独特的因素，可能需要开发定制架构。Splunk 专家可帮助提供您需要的任何定制解决方案。如果您是现有客户，请联络您的 Splunk 客户团队。如果您是 Splunk 的新客户，请点击此处（https://www.splunk.com/en_us/talk-to-sales.html）联络我们。

角色与职责

Splunk 验证架构与决策者和管理员关心的问题高度相关。企业架构师、顾问、Splunk 管理员以及管理服务供应商均应参与 SVA 选择流程。 下文载有关于这些角色的描述：

角色	描述
企业架构师	负责构建 Splunk 部署，以满足企业需求。
顾问	负责为 Splunk 架构、设计和实施提供服务。
Splunk 工程师	负责管理 Splunk 生命周期。
管理服务供应商	作为一项服务为客户部署及运行 Splunk 的实体。

Splunk 验证架构选择流程概览

Splunk 验证架构选择流程可帮助您识别符合您的组织的所有需求的最简单及最流畅的架构。

选择流程中的步骤	目标	考虑事项
第 1 步：为以下内容界定要求： a) 索引及搜索 b) 数据收集机制	界定要求。	• 决策者、利益相关者及管理员应合作识别及界定您的组织的需求 • 如果您已经有部署，您可评估您当前的架构，以确定需要怎么做才能移至经验证的模型。 若要查看可帮助您界定要求的问卷，请参阅下文第 1 步。
第 2 步：为以下内容选择拓扑： a) 索引及搜索 b) 每个数据收集机制	选择符合所识别要求的拓扑。	• 您可选择最符合您的要求的拓扑。 • 坚持简单原则，根据 SVA 的指引，可拥有更轻松的扩展路径。 若要查看拓扑选项的示意图及说明，请参阅下文第 2 步。
第 3 步：应用设计原则和最佳实践	将您的设计原则按优先顺序排好，审查层特定实施最佳实践。	• 每个设计原则都加强 Splunk 验证架构的一或多个支柱。 • 您可根据您的组织需求设定设计原则的优先次序。 • 层特定建议可为您的拓扑实施提供指导。 若要查看设计原则明细，请参阅下文第 3 步。

第 1a 步:界定您的索引及搜索要求

若要选择适当的部署拓扑，您需要深入分析您的要求。当您界定要求后，您将能够选择最简单及最具成本效益的方式部署 Splunk。您在下方会找到一个调查问卷，该问卷可帮助您界定您的部署索引和搜索层的关键要求领域。

该要求问卷聚焦于对您的部署拓扑有直接影响的领域。因此，我们强烈建议您记录您对以下问题的回答，然后再选择拓扑。

须考虑的事项

查看您的使用案例

在您界定要求时，您应思考您的 Splunk 架构的预期使用案例。例如，用于部门发展运营使用案例的拓扑通常比关键任务使用案例的拓扑简单（虽然并非始终如此）。您应全面考虑涉及以下内容的使用案例：

- 搜索
- 可用性
- 合规要求（如果您需要始终获得 100% 的数据保真度及可用性，这尤为重要）
- 其他特定于您的组织的使用案例场景

取决于您的使用案例场景，您的部署可能需要提供额外的架构特征。

考虑未来增长

您需要考虑您的迫切需求，以界定您的要求。但是，您还应考虑未来增长及可扩展性。扩展部署可能需要开支、额外的人手或其他您现在就需要开始规划的资源。

拓扑类别

以下内容对 SVA 拓扑类别极为关键。这些类别用于下方的问卷。您还可在 SVA 选择流程的后续步骤看到对这些类别的引用。

索引层类别

类别代码	解释
S	类别 "S" 表示单服务器 Splunk 部署的索引器
D	类别 "D" 表示需要带有至少 2 个索引器的分布式索引器层
C	类别 "C" 表示需要群集索引器层（需要复制数据）
M	类别 "M" 表示需要带多个站点的群集索引器层

搜索层类别

类别代码	解释
1	类别 "1" 表示单搜索投可满足要求
2	类别 "2" 表示需要多个搜索头才能满足要求
3	类别 "3" 表示需要搜索头群集才能满足要求
4	类别 "4" 表示需要跨多个站点的搜索头群集（“延伸” SHC）才能满足要求

类别代码	解释
+10	类别 "+10" 表示需要专用搜索头（群集）支持 Enterprise Security 应用将 10 添加至搜索层拓扑类别，仔细阅读该应用特定要求的拓扑说明。

问卷 1：界定您的索引及搜索层要求

♦ 有关拓扑类别代码的解释，见上文图例说明。如果您对多个问题回答“是”，请对编号最高的问题使用拓扑类别代码。

#	问题	考虑事项	对拓扑的影响	索引器层拓扑类别♦	搜索层拓扑类别♦
1	您的预期日常数据摄取量是否少于 300GB/天？	考虑日常摄取量的短期增长（6-12 个月）	取决于对可用性相关问题的回答，可选择单服务器部署	S	1
2	您是否需要高可用性，以进行数据收集/索引？	如果您并未计划使用 Splunk 监控需要连续数据摄取的使用案例，临时中断输入数据流属可接受（假设并无丢失日志数据）。	需要分布式部署，以支持连续摄取	D	1
3	假设使用搜索头运行搜索：您的数据是否需要始终完全可搜索，即，您无法承受搜索结果的完整性受到影响的后果？	例如，如果您的使用案例是利用聚合函数计算性能指标和一般使用监控，单个索引器中断可能不会对大量事件的统计造成重大影响。 如果您的使用案例是安全审核及威胁检测，您可能不希望搜索结果出现盲点。	需要复制因子至少为二 (2) 的群集索引器。注：虽然复制因子达到 2 可以为单个索引节点故障提供最低防护，但建议（及默认）的复制因子是 3。	C	1
4	您是否运行多个数据中心，并需要在数据中心中断时自动恢复您的 Splunk 环境？	灾难恢复要求可能指示通过两个设施（主动/主动）实现连续运行或规定手动灾难恢复的 RTO/RPO 目标。	连续运行需要多站点索引器群集及至少两个主动搜索头，以确保数据摄取/索引层和搜索层都能实现故障转移。	M	2
5	假设执行连续无损失数据摄取，您是否需要面向用户的搜索层的高可用性？	若 Splunk 用于连续近实时监控，搜索层中断可能无法容忍。其他使用案例可能也是如此（当然也可能不是）。	需要冗余搜索头（可能需要搜索头群集）	D/C/M	3

#	问题	考虑事项	对拓扑的影响	索引器层拓扑类别♦	搜索层拓扑类别♦
6	您是否需要支持大量并行用户及/或重要的计划搜索工作负载？	若并行用户/搜索超过 50 个，一般需要对搜索层进行水平式扩展。	可能需要在搜索层使用搜索头群集的拓扑	D/C/M	3
7	在多数据中心环境，您是否需要在站点之间同步用户项目（搜索、仪表板和其他知识对象）？	这将决定用户在站点中断时是否有现行及一致的体验。	需要具有适当配置的跨站点“延伸”的搜索头群集。**重要提示：**虽然延伸 SHC 可在发生全站点故障时为用户改善搜索可用性，但无法保证始终在两个站点之间复制所有项目。这可能会影响依赖一致及现行项目的特定应用程序，例如，Splunk App for Enterprise Security。搜索头群集本身无法提供完整的灾难恢复解决方案。SHC 的其他益处仍将适用。	M	4
8	您是否计划部署 Splunk App for Enterprise Security (ES)？	请确保您已阅读并理解各个拓扑文档所载的 Splunk App for Enterprise Security 的特定限制。	ES 需要专用搜索头环境（单独或群集）。	D/C/M	+10
9	您是否有受数据保管法规限制的地理分散式环境？	部分国家的法规不允许国内产生的数据离开该国的系统	该等法规禁止部署中央 Splunk 索引层，并要求 Splunk/合作伙伴与深入考虑部署细节的客户合作开发定制架构。换言之，并无 SVA 可满足该要求。	自定义	自定义
10	您是否有禁止将特定日志数据在共享服务器/索引器归置的高度限制性安全政策？	基于公司政策，可能不允许高度敏感型日志数据与低风险数据集共同归置于相同的物理系统/相同的网络区内。	需要多个独立索引环境，可能需要共享混合搜索层。这超出 SVA 的范围，需要定制架构开发。	自定义	自定义

如何确定您的拓扑类别代码

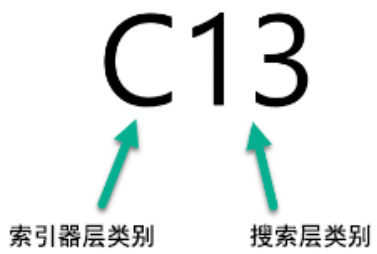
基于您对上文调查问卷的回答，您可获得综合拓扑类别指示，让您能够识别符合您需求的最佳拓扑。指示及示例在下文提供。

指示

1. 写下您回答“是”的问题。
2. 如果您对多个问题回答“是”，请对编号最高的问题采用拓扑建议。如果您看到多个拓扑选项（例如，"D/C/M"），请查阅先前的问题，以确定最适合您的选项。
3. 您的拓扑类别代码将以代表索引器层的字母为开头（例如，"C" 或 "M"）。该字母后跟代表搜索层的数字（例如，"1" 或 "13"）。

示例 1

假设您对问题 3、5 和 8 回答“是”。您将获得拓扑类别 "C13"，表示需要带两个搜索头群集的群集索引层。



示例 2

假设您只对问题 1 回答“是”。您将获得拓扑类别 "S1"，表示单服务器 Splunk 部署是您的理想拓扑。

第 2a 步：选择索引及搜索拓扑

拓扑一般分为非群集和群集部署。非群集部署只需最少数量的分离组件，具有卓越的可扩展性特征。请记住，即使非群集部署的可用性及灾难恢复功能较低，该部署选项仍可能是您的组织的最佳选择。

请牢记：SVA 选择流程的主要目标是让您能够构建所需的架构，而无需引入不必要的组件。

注

虽然您可能会选择实施提供超过您当前所需的额外利益的拓扑，但请记住，这可能会导致不必要的成本。此外，引入额外的复杂性通常会降低运作效率。

关于拓扑图的重要提示

拓扑图中的图标代表 **Splunk 功能角色**，并不表示专用架构将运行这些功能。有关哪些 Splunk 角色可归置于同一架构/服务器的指引，请参阅《附录》。

使用您的拓扑类别代码

强烈建议您在选择拓扑选项前完成要求问卷，以确定您的拓扑类别代码。如果您尚未执行该操作，请返回上一步并完成相关操作。当您确定拓扑类别代码后，您将能够识别最适合您的要求的部署选项。

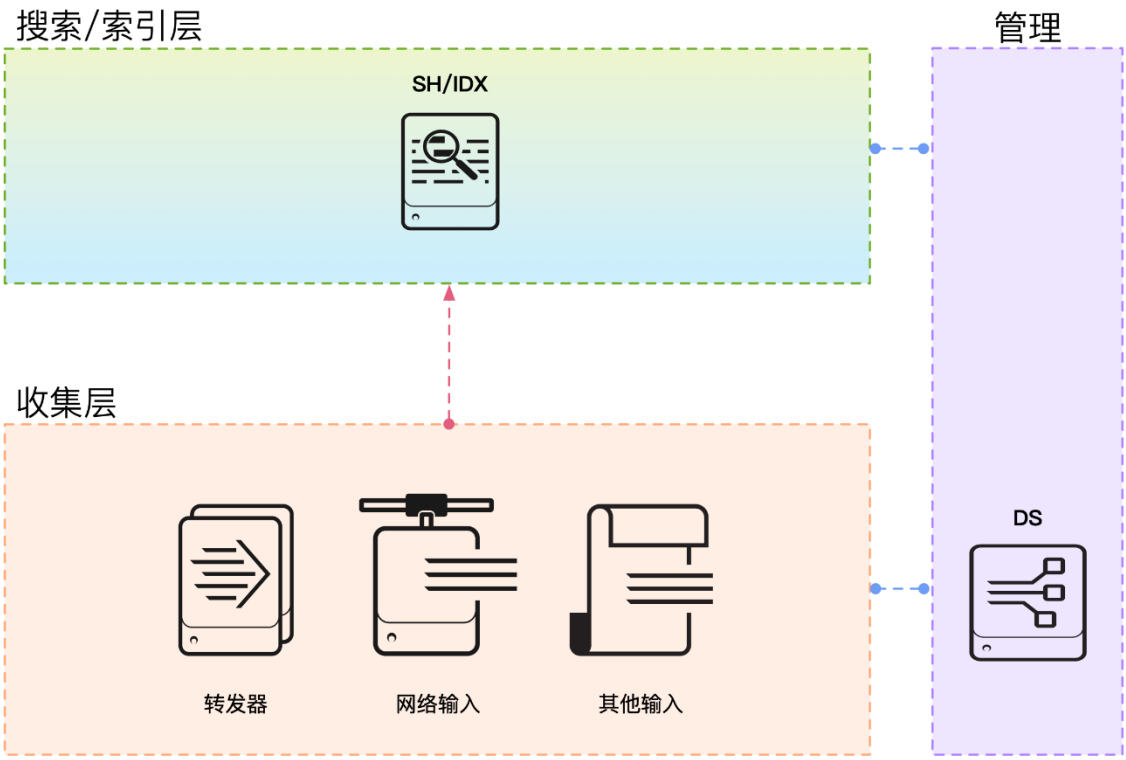
非群集部署选项

您在下方将会找到以下拓扑选项：

部署类型	拓扑类别代码
单一服务器部署	S1
分布式非群集部署	D1 / D11

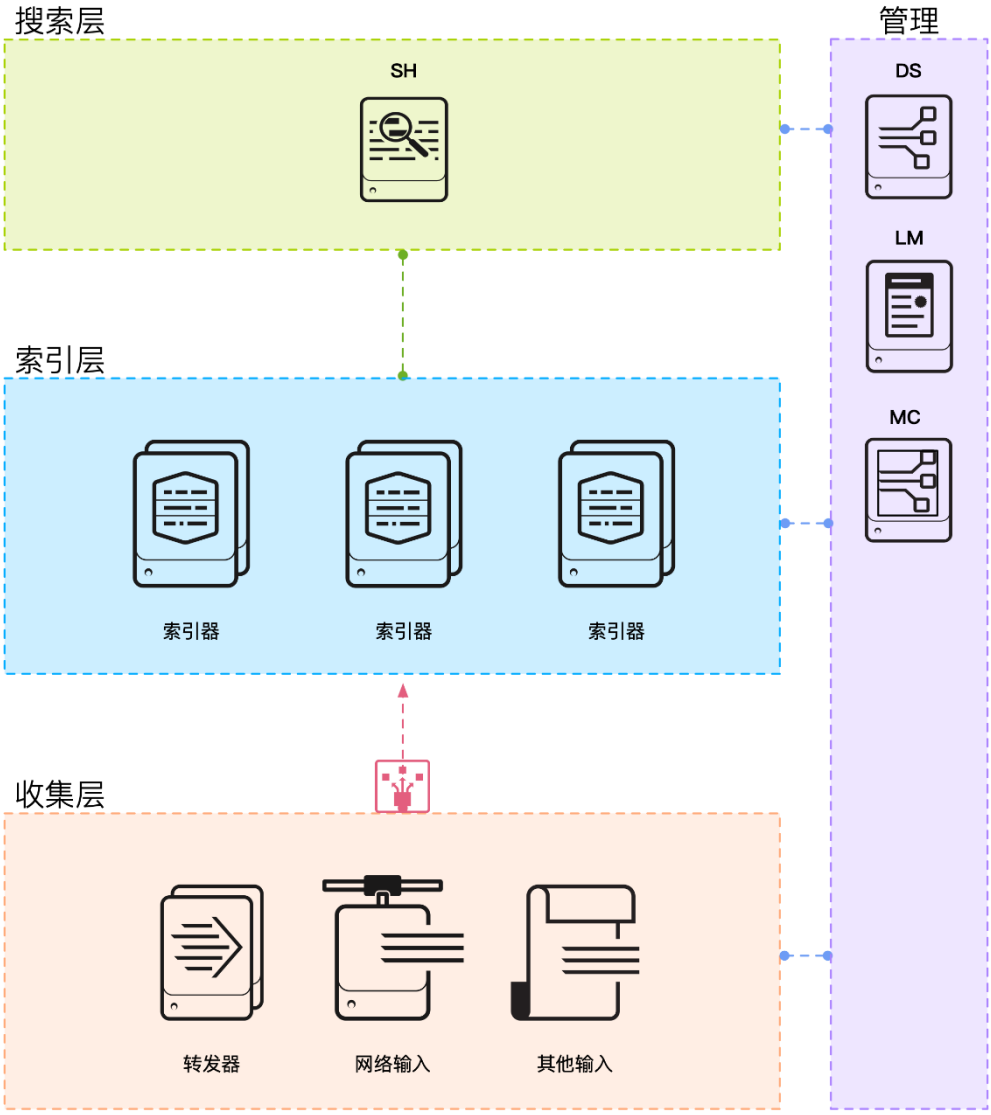
若要查看拓扑组件的说明，请参阅下文附录 "B" 。

单一服务器部署 (S1)



单一服务器部署的描述	限制
如果您的环境符合以下标准，该部署拓扑可为您提供极具成本效益的解决方案：a）您并无为您的 Splunk 部署提供高可用性或自动灾难恢复的要求；b）您的日常数据摄取量低于 300GB/天，且 c）您的非关键搜索使用案例的用户数量较少。 该拓扑一般用于小型、非业务关键使用案例（通常为部门性质）。适当的使用案例包括数据载入测试环境、小型开发运营使用案例、应用测试和集成环境，以及类似场景。 该拓扑的主要优点包括易于管理、良好的搜索性能（数据量较少）以及固定 TCO。	• 搜索/索引无高可用性 • 可扩展性受硬件容量限制（迁移至分布式部署的直接迁移路径）

分布式非群集部署 （D1 / D11）



分布式非群集部署 (D1 / D11) 的描述	限制
在以下任一情况下，您需要迁移至分布式拓扑：a) 您要发送至 Splunk 的日常数据量超过单一服务器部署的容量；或 b) 您想要/需要提供高度可用的数据摄取。部署多个独立索引器能让您线性扩展您的索引能力，从而提高数据摄取的可用性。 随着您增加索引器节点，TCO 将以可预测及线性的方式增加。建议引入监控控制台 (MC) 组件，这样您可以监控您的分布式部署的运行状况及能力。此外，MC 可提供中央警报系统，将您的部署的异常状况通知您。 每次添加新索引器时，需要使用可用的搜索对等节点列表手动配置搜索头。**ES 客户须知：**如果您的类别代码是 D1（即，您计划部署 Splunk App for Enterprise Security），需要**单独的专用**搜索头部署该应用（这并未在拓扑图显示）。 每次添加新索引器时，需要使用目标索引器列表（通过部署服务器）配置收集层。 该部署拓扑可线性扩展至超过 1000 个索引器节点，从而可支持极高的数据摄取及搜索量。 可通过跨多个索引器的并行搜索执行（映射/化简），对大型数据集维持搜索性能。 虽然并未专门划分为单独的拓扑，但搜索头群集可用于提高搜索层的搜索能力（详见拓扑 C3/C13 的搜索层）。	• 搜索层无高可用性 • 索引层的可用性有限，节点故障可能会导致历史搜索的搜索结果不完整。

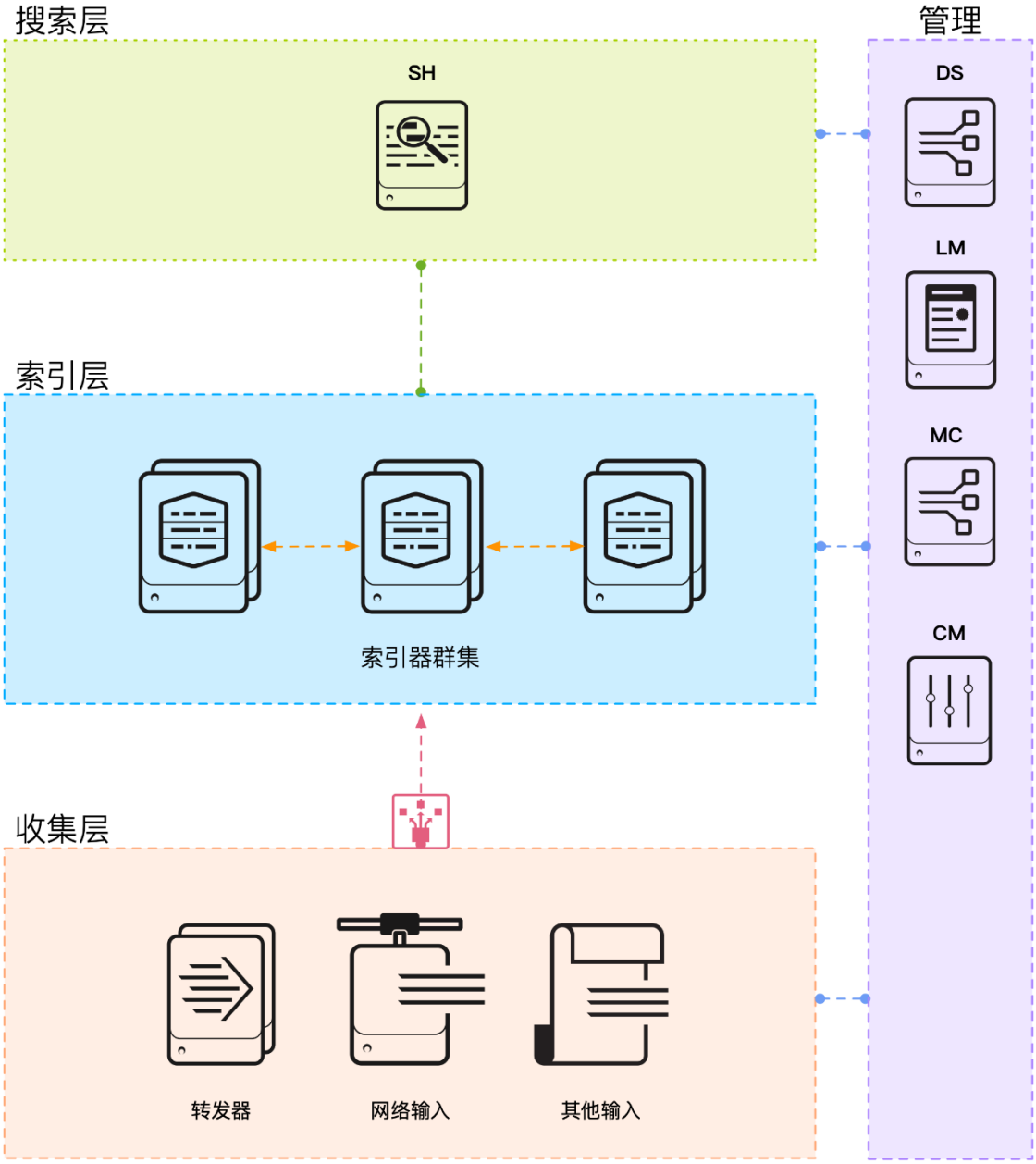
群集部署选项

您在下方将会找到以下拓扑选项：

部署类型	拓扑类别代码
分布式群集部署 - 单个站点	C1 / C11
分布式群集部署 + SHC - 单个站点	C3 / C13
分布式群集部署 - 多站点	M2 / M12
分布式群集部署 + SHC - 多站点	M3 / M13
分布式群集部署 + SHC - 多站点	M4 / M14

若要查看拓扑组件的说明，请参阅下文附录 "B" 。

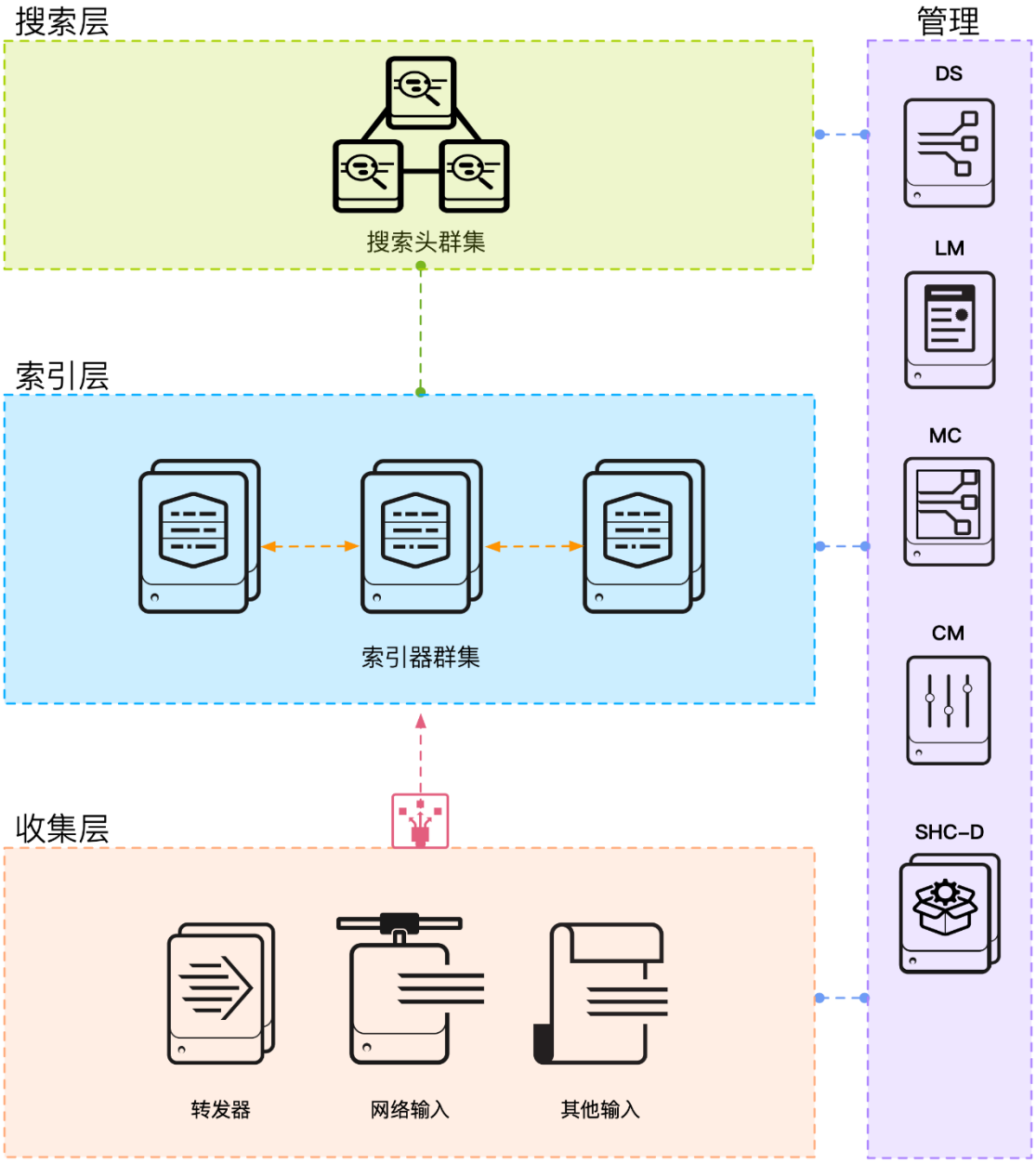
分布式群集部署 – 单个站点（C1 / C11）



分布式群集部署 – 单个站点（C1 / C11）的描述	限制
该拓扑根据适当配置的数据复制政策引入索引器群集。在索引器对等端点出现故障的情况下，这可提供高数据可用性。但是，您应注意，这仅适用于索引层，并不提供搜索头故障防护。 **ES 客户须知：**如果您的类别代码是 C11（即，您计划部署 Splunk App for Enterprise Security），需要**单独的专用**搜索头部署该应用（这并未在拓扑图显示）。 该拓扑需要名为群集主服务器（CM）的额外 Splunk 组件。CM 负责所配置的数据复制政策的协调及执行。CM 还可充当可用群集节点（索引器）的权威来源。搜索头配置可通过配置 CM 而非各个搜索对等节点的方式简化。	• 搜索层无高可用性 • 索引器群集中的唯一存储桶总数限制为 5MM（V6.6+），桶总数为 15MM。 • 若数据中心中断，则无自动灾难恢复能力

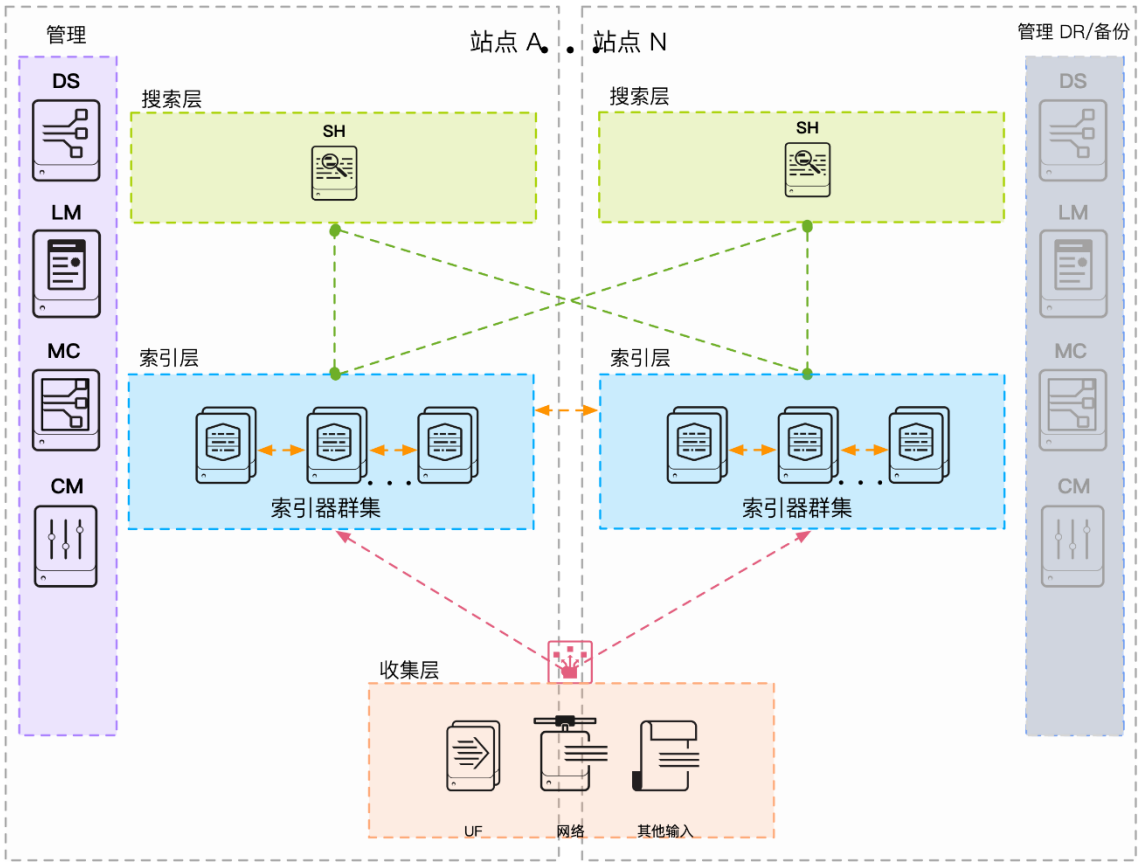
分布式群集部署 – 单个站点（C1 / C11）的描述	限制
您可选择将转发层配置为通过 CM 发现可用的索引器。这可简化转发层管理。 请注意，数据以不确定的方式在群集内复制。您无法控制每个事件所要求的副本的存储位置。此外，虽然可扩展性为线性，但存在与群集总容量有关的限制（在理想状况下，可搜索数据约为 50PB）。 我们建议部署监控控制台（MC），以监控您的 Splunk 环境的状况。	

分布式群集部署 + SHC – 单个站点（C3 / C13）



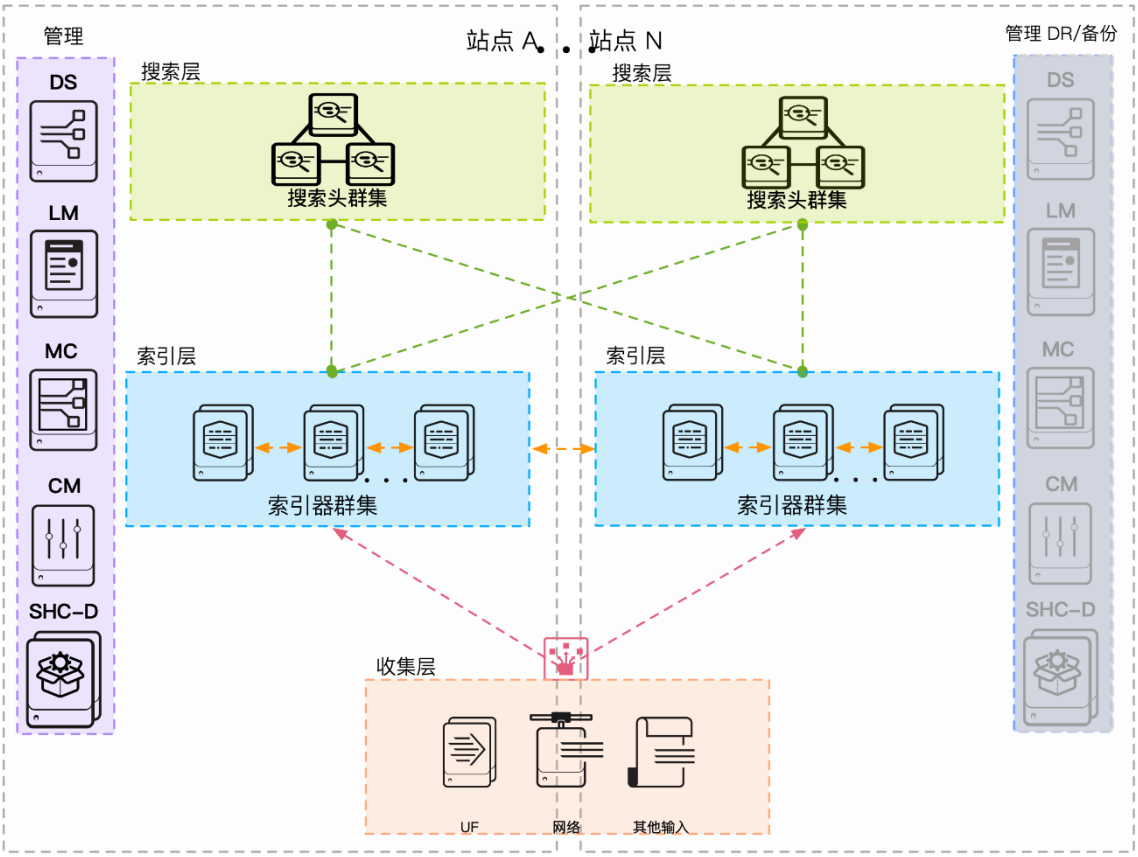
分布式群集部署 + SHC – 单个站点（C3 / C13）的描述	限制
该拓扑加入了水平可扩展性，消除了搜索层的单一故障点。至少需要 3 个搜索头才能实施 SHC。 为管理 SHC 配置，每个 SHC 需要一个名为搜索头群集部署器的额外 Splunk 组件。必须安装该组件，才能在群集中部署配置文件变动。搜索头群集部署器并无高可用性要求（无运行时间角色）。 SHC 可提供特定的机制，将可用搜索能力增至超过单个搜索头能够提供的范围。此外，SHC 允许在群集内进行计划搜索工作负载分配。在发生搜索头故障时，SHC 还可提供最佳的用户故障转移。 需要面向 SHC 成员配置支持粘滞会话的网络负载均衡器，以确保在群集内实现适当的用户负载均衡。 **ES 客户须知：**如果您的类别代码是 C13（即，您计划部署 Splunk App for Enterprise Security），需要一个**专用**搜索头群集部署该应用（这并未在拓扑图显示）。取决于您的容量和组织需求，搜索层可包含群集及非群集搜索头（同样没有在拓扑图显示）。	• 若数据中心中断，则无灾难恢复能力 • ES 需要专用 SH/SHC • 支持在 SHC 管理 ES 部署，但较为困难（涉及 PS） • SHC 的节点不能超过 100 个

分布式群集部署 – 多站点（M2 / M12）



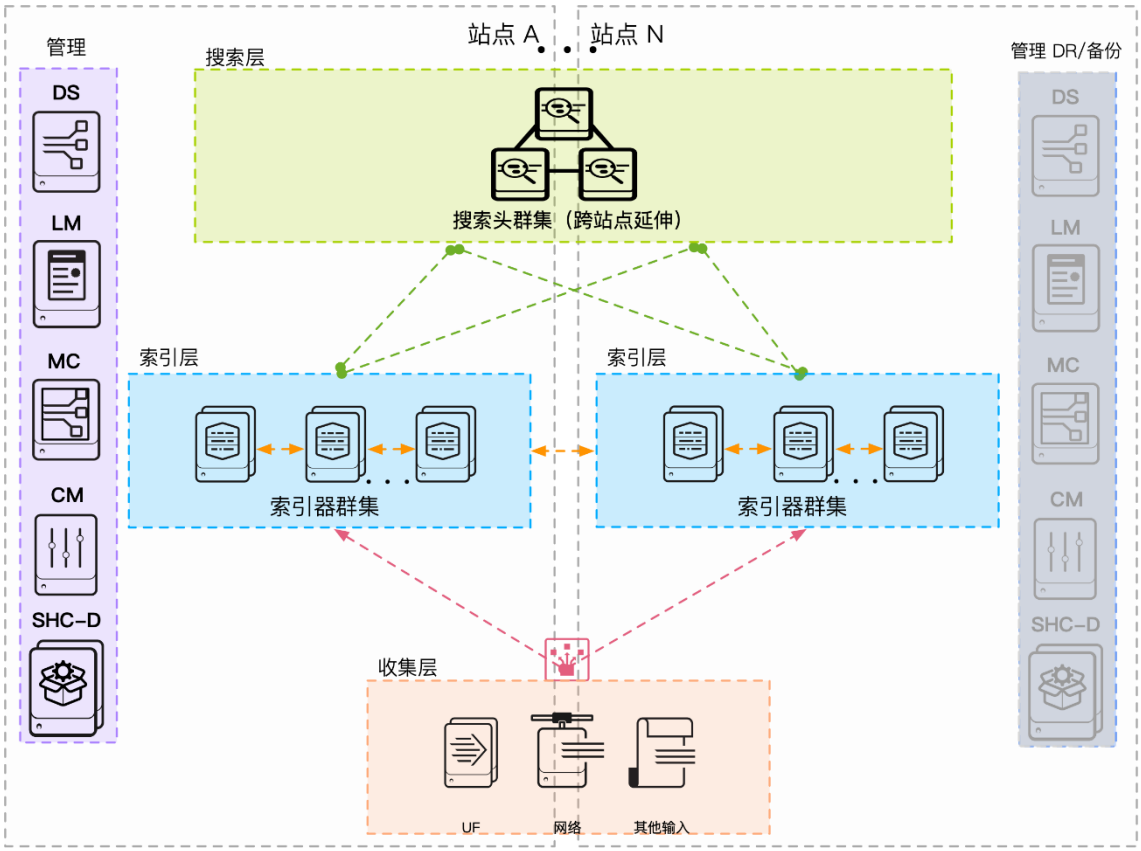
分布式群集部署 – 多站点（M2 / M12）的描述	限制
若要在发生灾难事件（如，数据中心中断）时提供近乎自动的灾难恢复，多站点群集是理想的部署架构选择。健康的多站点群集需要 Splunk 文档中所述的可接受站点间网络延迟。 该拓扑让您能够**确定性**地将数据复制至两组或以上的索引器集群节点。您将能够配置站点复制及搜索因子。该站点复制因子能让您指定副本将发送到的位置，并确保跨多个站点分发数据。 它仍由单个群集主节点管理，该节点在发生灾难时必须能够故障转移至灾难恢复站点。 多站点群集可跨多个物理隔离分布式站点提供数据冗余，确保地理隔离式分配的可能性。 用户可自动故障转移至灾难恢复站点，以确保可用性。但是，该拓扑并不提供跨站点自动同步搜索层配置和运行时间项目的机制。 可利用跨站点的可用搜索对等节点（索引器）能力进行主动/主动模式的搜索执行。在可能的情况下，可配置站点相关性，确保登录至特定站点的搜索头的用户仅搜索本地索引器。 **ES 客户须知：**如果您的类别代码是 M12（即，您计划部署 Splunk App for Enterprise Security），需要**单独的专用**搜索头部署该应用（这并未在拓扑图显示）。 对于 ES 搜索头，故障转移涉及在仅在灾难恢复情况下激活及使用的故障转移站点设置“影子”搜索头。请联系 Splunk 专业服务，为您的 Enterprise Security 部署设计和实施站点故障转移机制。	• 不会**跨站点**共享可用的搜索头能力，且不会跨站点复制搜索项目 • 若发生站点故障，管理功能失效需要在 Splunk 之外处理 • 索引复制的跨站点延迟必须在建议限制内

分布式群集部署+ SHC – 多站点 (M3 / M13)



分布式群集部署+ SHC – 多站点 (M3 / M13) 的描述	限制
该拓扑加入了水平可扩展性，消除了每个站点的搜索层的单一故障点。至少需要 3 个搜索头才能实施 SHC（每个站点）。 为管理 SHC 配置，**每个** SHC 需要一个名为搜索头群集部署器的额外 Splunk 组件。必须安装该组件，才能在群集中部署配置文件变动。搜索头群集部署器并无高可用性要求（无运行时间角色）。 SHC 可提供以下益处：a) 将可用搜索能力增至超过单个搜索头能够提供的范围；b) 在群集内进行计划搜索工作负载分配；及 c)在发生搜索头故障时，可提供最佳的用户故障转移。 在每个站点中，需要面向 SHC 成员配置支持粘滞会话的网络负载均衡器，以确保在群集内实现适当的用户负载均衡。 **ES 客户须知：**如果您的类别代码是 M13（即，您计划部署 Splunk App for Enterprise Security），需要包含在一个站点内的一个专用搜索头群集部署该应用（这并未在拓扑图显示）。若要从站点故障中恢复 ES SH 环境，可使用第三方技术执行搜索头实例的故障转移，或者可配置 ES SH“热备份”及与主 ES 环境同步。强烈建议您在 HA/DR 环境中部署时咨询 Splunk 专业服务部。	• 无跨站点的搜索项目复制，SHC 彼此独立 • 索引复制的跨站点延迟必须在文档限制内 • SHC 的节点不能超过 100 个

分布式群集部署+ SHC – 多站点 (M4 / M14)



分布式群集部署+ SHC – 多站点 (M4 / M14) 的描述	限制
这是最复杂的经验证架构，其设计用于具有严格的高可用性及灾难恢复要求的部署。我们强烈建议您让 Splunk 专业服务部参与，以确保正确部署。若正确部署，该拓扑能够为数据收集、索引和搜索提供您的 Splunk 基础架构的持续操作。 该拓扑涉及实施跨一个或多个站点的“延伸”搜索头群集。在发生搜索对等节点或数据中心故障时，可为用户提供最佳的故障转移。搜索项目和其他运行时间知识对象在 SHC 中复制。需要谨慎部署，以确保能够跨站点复制，因为 SHC 本身并不能感知站点（即，项目复制不确定）。 可配置站点相关性，确保站点之间的 WAN 链接仅在本地搜索无法满足要求时使用。 需要面向 SHC 成员配置支持粘滞会话的网络负载均衡器，以确保在群集内实现适当的用户负载均衡。 **ES 客户须知：**如果您的类别代码是 M14（即，您计划部署 Splunk App for Enterprise Security），需要包含在一个站点内的一个专用搜索头群集部署该应用（这并未在拓扑图显示）。ES 需要提供一致的运行时间项目集，当发生站点中断时，这在延伸 SHC 中无法保证。若要从站点故障中恢复 ES SH 环境，可使用第三方技术执行搜索头实例的故障转移，或者可配置 ES SH “热备份”及与主 ES 环境同步。强烈建议您在 HA/DR 环境中部署时咨询 Splunk 专业服务部。	• 跨站点网络延迟必须在文档限制内 • 若只有少数群集成员幸存，SHC 故障转移可能需要手动操作

第 1b 步:界定您的数据收集要求

数据收集层是 Splunk 部署的核心组件。它使您环境中的任何设备能够向索引层发送数据进行处理，从而可在 Splunk 中搜索。此处最重要的因素是确保以最高效及可靠的方式进行发送及索引，因为这对您的 Splunk 部署的成功及性能至关重要。

请考虑您的数据收集层架构的以下方面：

- 数据的来源。数据是来自日志文件、系统日志来源、网络输入、操作系统事件记录设施、应用程序、消息总线还是其他地方？
- 数据摄取延迟及吞吐量要求
- 您的索引层内理想的跨索引器事件分配
- 容错及自动恢复（高可用性）
- 安全和数据主权要求

SVA 的这一部分重点简述常用的数据收集方法。这部分还讨论各个数据收集方法的架构及最佳实践，提出在作出您的实施选择时应考虑的潜在问题。

重要架构考虑事项以及它们为何如此重要

鉴于数据收集层的重要作用，必须了解设计该架构涉及的主要考虑事项。

虽然有些考虑事项可能与您的要求无关，在下表中以粗体显示的考虑事项将描述与每个环境相关的基础项目。

考虑事项	为何它如此重要？
适当摄取数据（时间戳、自动换行、截断）	理想的跨索引器事件分配的重要性难以尽述。当所有可用的索引器均衡利用时，索引层的工作效率最高。这对于数据摄取和搜索性能都是如此。如果单个索引器的数据摄取处理量远超其他索引器，这会对搜索响应时间带来不利影响。对于本地磁盘存储有限的索引器，不均匀的事件分配也可能会导致数据在达到配置的数据保留政策要求前过早失效。
数据以最佳方式跨可用的索引器分配	若由于事件时间戳和自动换行并未正确配置，导致数据未能适当摄取，则搜索该数据将变得极为困难。这是因为必须在搜索时强制执行事件边界。时间戳提取配置缺失或不正确会导致多余的隐性时间戳分配。这会使您的用户困惑，增加从您的数据获取价值的难度。
所有数据均可靠地到达索引层，且无损失	任何为可靠分析目的收集的日志数据必须完整有效，以便基于该数据执行的搜索可提供有效准确的结果。
所有数据均在延迟最少的情况下到达索引层	数据摄取延迟会增加潜在重要的事件发生与搜索该事件及作出反应之间的时间。对于设计向员工触发警报或引发自动化行动的监控使用案例，最大程度地减少摄取延迟通常极为重要。
确保数据在传输期间的安全	若数据为敏感数据或必须在通过非受信网络发送时加以保护，可能需要对数据进行加密，以防止第三方未经授权拦截。一般而言，我们建议，Splunk 组件之间的所有连接采用 SSL 支持连接。
最大限度地减少网络资源的使用	必须尽可能减少日志数据收集的网络资源影响，以确保不影响其他关键业务网络流量。对于专线网络，减少网络使用还可降低您的部署的 TCO。
验证/授权数据源	为防止流氓数据源影响您的索引环境，请考虑实施连接验证/授权。这可以通过使用网络控制或采用应用程序级机制（如，SSL/TLS）实施。

本文档中的指引重点讲述支持理想事件分配的架构，因为它对您的部署至关重要。如果 Splunk 环境不能提供预期的搜索性能，在几乎所有情况下都是由于未能达到最低存储性能要求及/或限制利用搜索并行化的事件分配不均匀所致。

既然您已经了解最重要的架构考虑事项，我们现在来弄清您需要满足的哪些具体的数据收集要求。

问卷 2：界定您的数据收集要求

通过回答以下问题，您可以获得您的部署所需的数据收集组件列表。您可以使用最右栏的按键，在下文查看关于每个组件的更详细信息。

#	问题	考虑事项	对拓扑的影响	相关数据收集组件
1	您是否需要在端点监控本地文件或执行数据收集脚本？	这是几乎所有 Splunk 部署场景的核心要求。	您需要在您的端点安装通用转发器并集中管理其配置。	UF
2	您是否需要从您无法安装软件的设备（电器、网络交换机等）收集通过系统日志发送的日志数据？	系统日志是不允许安装定制软件的专用设备常用的普适运输协议。	您需要充当收集点的系统日志服务器基础架构。	系统日志 HEC

3	您是否需要支持从登录到 API 的应用程序收集日志数据而非写入本地磁盘？	在端点写入日志文件需要提供磁盘空间及管理这些日志文件（轮换、删除等）有些客户不想采用这种模式，而想要使用可用的日志库直接记录到 Splunk。	您需要使用 Splunk HTTP 事件收集器 (HEC) 或可充当日志接收器的其他技术。	HEC
4	您是否需要收集来自流事件数据供应商的数据？	许多企业已采用事件中心模式，在该模式下，中央流数据平台（如，AWS Kinesis 或 Kafka）充当日志数据生产者与消费者之间的消息传输。	您需要整合流数据供应商和 Splunk。	KAFKA KINESIS HEC
5	您是否有不可动摇的防止日志生产商直接与索引层建立 TCP 连接的安全政策？	有时，网络拓扑包含彼此之间有限制性防火墙规则的多个网络区，一般无法允许 Splunk 端口的流量在各个网络区之间流动。为各个源/目标 IP 地址配置和维护防火墙规则可能非常麻烦。	您需要允许流量在各个网络区之间流动的中介转发层。	IF
6	您是否需要使用程序化方法（如，调用 REST API 或查询数据库）收集日志数据？	Splunk 提供多种模块化输入，可允许为众多不同的数据摄取使用案例针对 API 执行脚本，包括从关系数据库收集数据的 DBX。	您的数据收集层需要实施一或多个带 Splunk Heavy Forwarder 的数据收集节点 (DCN)。	DCN
7	您是否需要将数据（子集）路由至除 Splunk 外的其他系统？	某些使用案例需要将 Splunk 内已建立索引的数据也转发到其他系统。转发的数据通常只包含源数据的子集，或在转发前必须更改数据。	您可能需要根据使用案例的具体情况构建带 Heavy Forwarder 的中介转发层，以支持基于事件的路由及过滤。或者，您可以使用 Splunk App for CEF 中的 cefout 命令在索引后转发数据。	HF
8	您是否有存在网络带宽限制的远程站点，需要在通过网络发送数据前对数据进行大量过滤？	在传输前过滤数据需要解析（重载）转发器。HWF 使用的出站网络带宽约为 UF 的 5 倍，因此，过滤仅在需要滤出大量事件时才有意义（经验法则：>50% 的源数据）。在理想情况下，您应调整您的记录粒度，以实现所需的日志数量削减。	如果您无法在源头减少日志数量，您需要在远程站点部署中介 HF，以根据配置解析源数据及滤出事件。	IF HF
9	您是否需要在将敏感数据为索引目的通过公共网络发送前对其进行掩码/模糊化处理？	有时，通过 SSL 保护转发器流量不足以保护通过公共网络传输的敏感数据，必须在传输前对事件的各个部门进行掩码（SSN、CC 数据等）。在理想情况下，此类数据掩码在产生日志数据的应用程序中完成。	如果您无法在产生应用程序中掩码数据，您需要在站点部署中介 HF，以便在数据发送至索引器之前根据配置解析源数据及应用所需的掩码规则。	IF HF
10	您是否需要使用 statsd 或 collectd 捕获指标？	Statsd 和 collectd 是用于收集来自主机系统及应用程序的指标的普适技术。	Splunk 支持利用 UF、HF 或 HEC 输入这些索引的特定索引类型及收集方法。	指标

11	您是否需要确保任何数据收集组件的高可用性？	可用性一般不适用于端点，但可能是其他数据收集组件（如，中介转发器或数据收集节点）的关注点。	需要考虑中断将如何影响各个组件的可用性以及如何解决该问题。	高可用性

第 2b 步:选择您的数据收集组件

在您完成问卷后，您将获得满足您的部署要求所需的数据收集组件列表。这部分将更详细讨论各个数据收集架构组件。在开始之前，我们将简要提供一些通用指南。

关于转发架构的通用指南

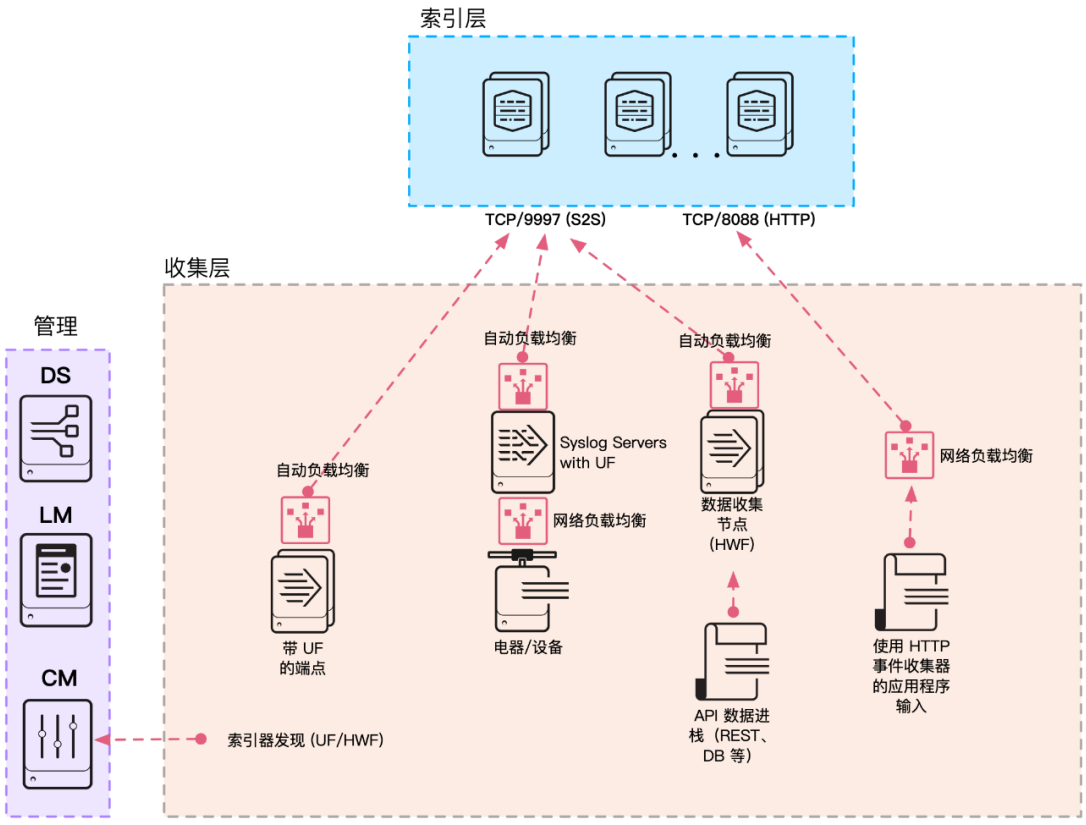
在理想情况下，数据收集层应尽可能“扁平”。这意味着，数据源通过通用转发器在本地收集，并直接转发至索引层。这是最佳实践，因为它可最大限度地减少数据摄取延迟（搜索时间），确保跨可用索引器的适当事件分配。遵循该最佳实践可确保轻松管理及简化操作。我们经常会看到客户部署中介转发层。一般而言，应避免该操作，除非在其他情况下无法满足要求。由于中介转发器的潜在影响，本文档将在单独的章节详细讨论该主题。

存在不允许安装通用转发器（换言之，网络设备、电器）的端点以及使用系统日志协议的日志。用于收集此类数据源的单独的最佳实践架构在“系统日志数据收集”一节介绍。

对于必须使用程序化方法（API、数据库访问）收集的数据源，建议基于完整的 Splunk 企业安装部署数据收集节点（DCN）。这一般也称之为重型转发器。建议您不要在除开发环境以外任何环境的搜索头层运行这些类型的输入。

下图显示反映该指南的一般数据收集架构。

数据收集拓扑概览



上图显示管理层的部署服务器（DS），该服务器用于管理数据收集组件的配置。此外，此处显示许可证主服务器（Lm），因为数据收集节点需要访问 LM，以启用 Splunk Enterprise 的功能。群集主服务器（CM）（若可用）可由转发器用于发现索引器，从而无需管理在转发器输出配置中可用的索引器。

在上图中，AutoLB 代表 Splunk 内置自动负载均衡机制。该机制用于为使用 Splunk 专用 S2S 协议（默认端口 9997）发送的数据确保适当的事件分配。说明：目前不支持亦不建议为 S2S 流量使用外部网络负载均衡器。

若要为来自采用行业标准协议（如，HTTP 或系统日志）通信的数据源的流量实现负载平衡，使用网络负载均衡器可确保在索引层内的各个索引器之间实现均衡负载及事件分配。

（UF）通用转发器

通用转发器（UF）是满足来自您的环境中系统的大量数据收集要求的最佳选择。它是专用的数据收集机制，只需极少的资源。UF 应为收集和转发日志数据的默认选择。UF 可提供：

- 检查点/重启功能，确保无损数据收集。
- 可最大程度地减少网络带宽使用的高效协议。
- 节流能力。
- 跨可用索引器的内置负载均衡。
- 使用 SSL/TLS 的可选网络加密。
- 数据压缩（仅可在没有 SSL/TLS 的情况下使用）
- 多个输入方法（文件、Windows 事件日志、网络输入、脚本输入）。
- 有限的事件过滤能力（仅限 Windows 事件日志）。
- 并行摄取管道支持，提高吞吐量/减少延迟。

除适用于良好构建数据（json、csv、tsv）的少量例外情况外，UF 不会将日志源解析为事件，因此它无法执行需要理解日志格式的任何操作。它还随附精简版 Python，因此与任何需要完整 Splunk 堆栈策略才能运行的模块化输入应用不兼容。

在 Splunk 环境的端点和服务器部署大量 UF（100s 至 10,000s）及集中管理（通过 Splunk 部署服务器或第三方配置管理工具（如，Puppet 或 Chef））属正常现象。

(HF) 重型转发器

重量级转发器（HWF）是完整的 Splunk Enterprise 部署，将其配置以在索引禁用时充当转发器。HWF 通常不执行其他 Splunk 角色。UF 和 HWF 之间的主要区别是 HWF 含有完整的解析管道，可执行与索引器相同的功能，而无需在磁盘上实际写入事件及编制索引。这使 HWF 能够理解和基于个别实践行动，例如，基于事件数据对数据掩码或执行过滤及路由。由于它是完整的 Splunk Enterprise 安装，因此，它可托管需要完整 Python 堆栈才能为数据收集正常运行的模块化输入或充当 Splunk HTTP 事件收集器（HEC）的端点。HWF 执行以下功能：

- 将数据解析为事件。
- 基于个别事件数据的过滤器及路由。
- 具有比 UF 更大的资源占用空间。
- 具有比 UF 更大的网络带宽占用空间（约 5 倍）。
- 用于管理的 GUI。

一般而言，HWF 不会为数据收集目的安装在端点。相反，它们用于单独的系统，实施数据收集节点（DCN）或中介转发层。**仅当无法以 UF 满足来自其他系统的数据收集要求时使用 HWF。**

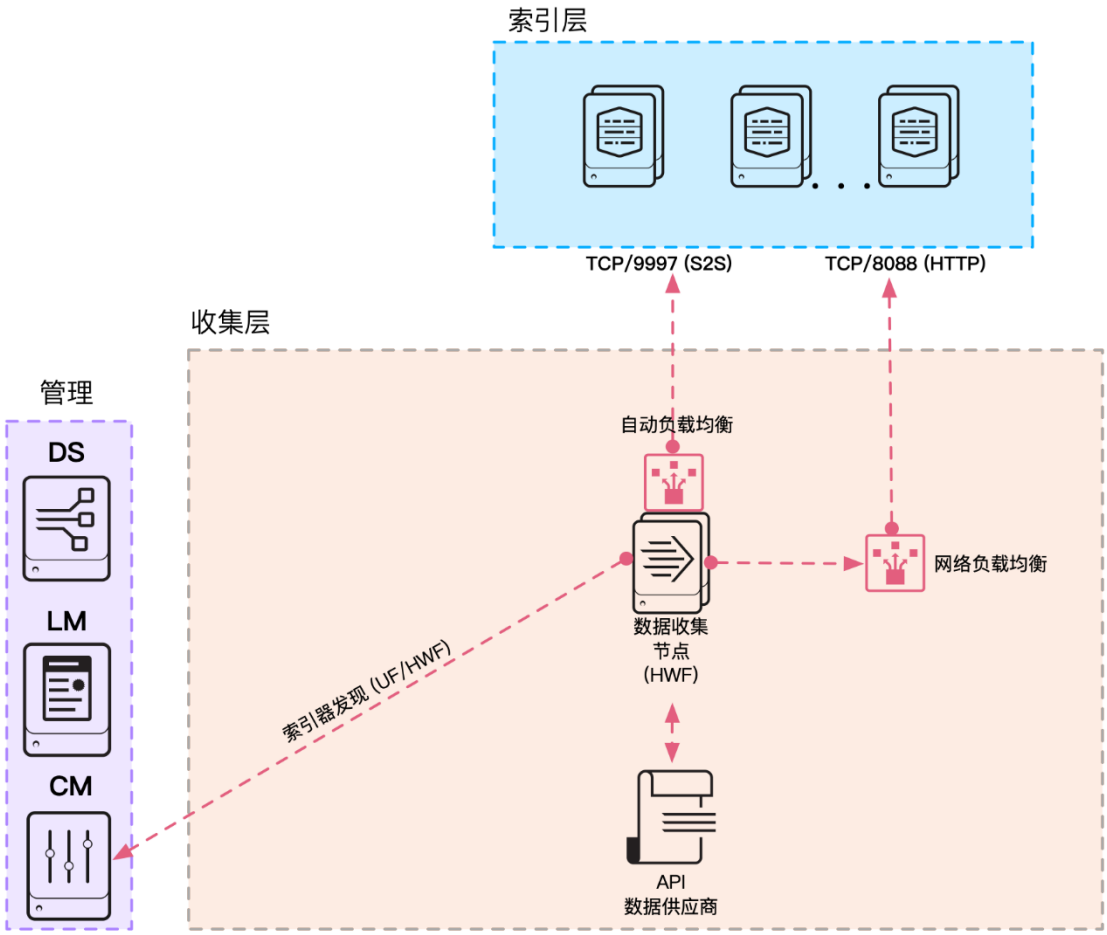
这些要求示例包括：

- 为将数据摄取到 Splunk 的目的从 RDBMS 读取数据（数据库输入）。
- 从可通过 API（云服务、VMWare 监控、专用系统等）访问的系统收集数据。
- 提供专用层托管 HTTP 事件收集器服务。
- 实施需要解析转发器进行路由/过滤/掩码的中介转发层。

(DCN) 重型转发器作为数据收集节点

有些数据源需要使用某种 API 收集。这些 API 可包含 REST、网络服务、JMS 及/或 JDBC 作为查询机制。Splunk 以及第三方开发商可提供允许这些 API 交互的各种应用程序。最常见的情况下，这些应用使用 Splunk 模块化输入框架实施，该框架需要完整的 Splunk 企业软件安装才能正常运行。实现该使用案例的最佳实践是部署一个或多个服务器，充当作为数据收集节点 (DCN) 配置的重型转发器。

数据收集节点拓扑

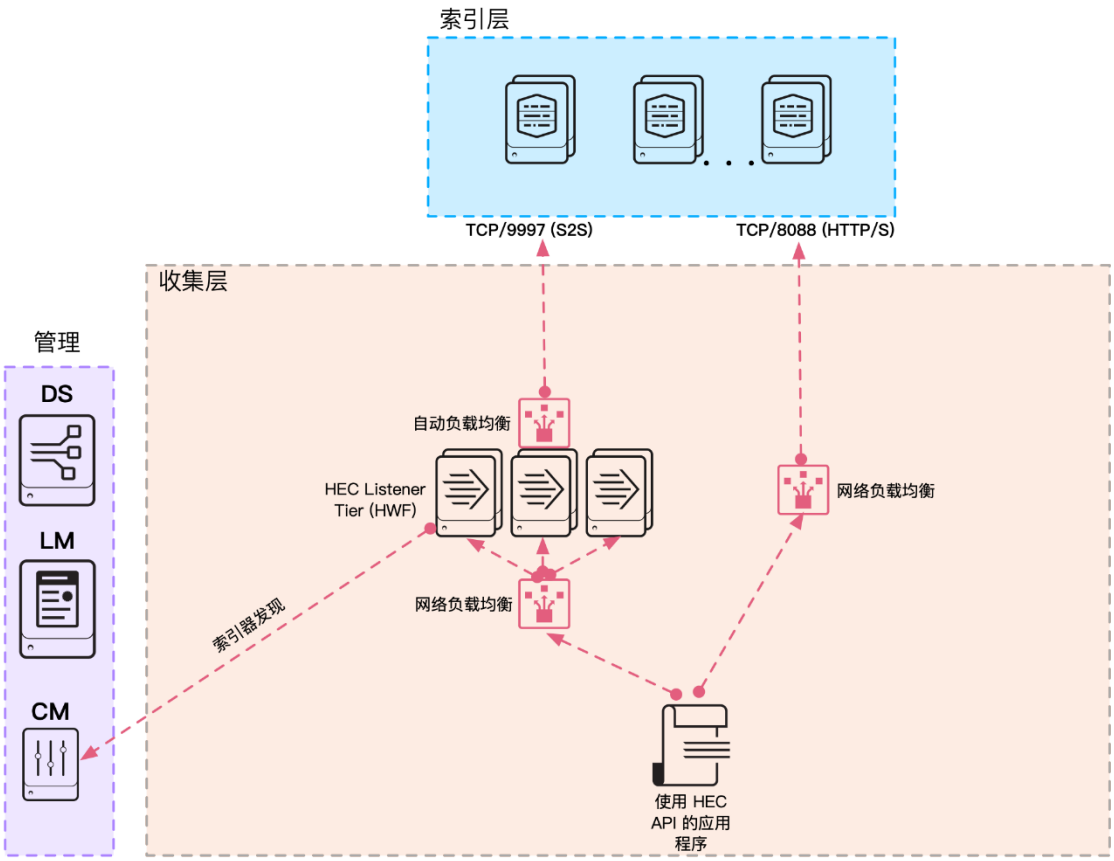


(HEC) HTTP 事件收集器

HEC 可提供在服务器侧接受 HTTP/S 连接及在客户端接受 API 的侦听器服务，允许应用直接向索引层或由一个或多个重型转发器组成的专用 HEC 接收器层发布日志数据有效负载。HEC 提供两个支持以原始格式或 JSON 格式发送数据的端点。使用 JSON 可在事件有效负载中包含额外的元数据，从而可在后续搜索数据时提供更高的灵活性。

下图对 HEC 的两个部署选项进行图解：

HEC 拓扑选择



管理层包含（HF 要求的）许可证主服务器以及部署服务器，以管理侦听组件上的 HTTP 输入。说明：若索引层群集且直接接收 HEC 流量，HEC 配置通过群集主服务器而非部署服务器管理。

您的部署拓扑选择很大程度上取决于您的特定需求。专用 HEC 侦听器层为您的部署引入另一个架构组件。从积极方面讲，它可独立扩展，就管理而言，可与索引层隔离。而且，由于专用 HEC 层需要 HF，它可解析所有进站流量，使索引器无需处理该工作负载。

另一方面，直接在索引器上托管 HEC 侦听器可能能够确保更佳的跨索引层事件分布，因为 HTTP 是所有网络负载均衡器都能易于理解的协议，适当的负载均衡政策有助于确保首选最不繁忙的索引器。

基于部署尽可能简单的架构满足您的要求的精神，我们建议您考虑在索引器上托管您的 HEC 侦听器（假设您有足够的系统容量这么做）。该决定可在需要时轻易推翻，只需部署容量及配置适当的 HF 层及将 LB 配置更改为使用 HF 的 IP 地址而非索引器即可。该变化对客户端应用程序应当透明化。

说明：如果您要求为通过 HEC 发送的数据确认索引器，建议使用专用 HEC 侦听器层减少反复重启索引器导致的重复消息。

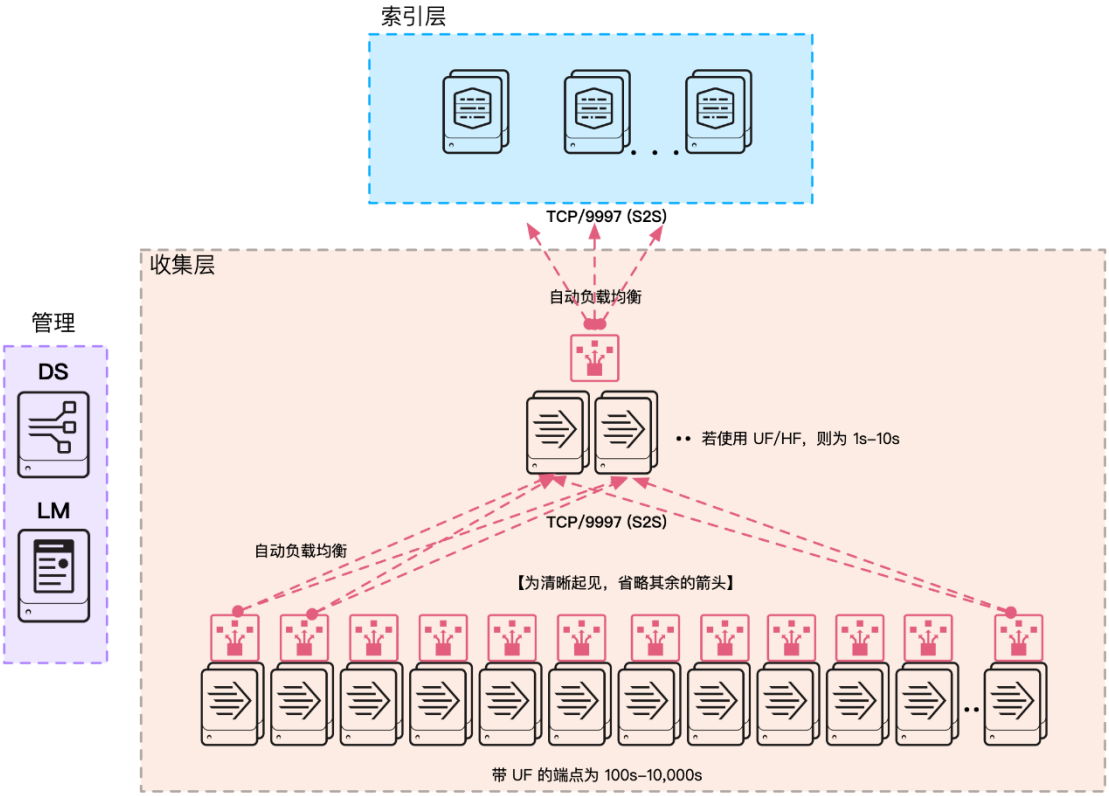
说明：该 HEC 部署架构可为稍后讨论的其他数据收集组件提供传输，尤其是系统日志和指标数据收集。

（IF）中介转发层

在某些情况下，需要中介转发器进行数据转发。中介转发器从端点接收日志流并将其转发至索引器层。中介转发器引入需要谨慎设计的架构挑战，以免对整个 Splunk 环境造成不利影响。最突出的是，中介转发器可集中端点转发器的连接（从 100s 到 10,000s），使用更少的连接转发至索引器。这会严重影响索引层的数据分配，因为在任何指定的时间点只有部分索引器接收流量。但是，这些负面影响可通过适当调整和配置减轻。

下图对该挑战进行了很好的图解：

中介转发拓扑



在单中介转发器场景，所有端点连接至该单一转发器（可能有数千个），而该中介转发器在任何指定时间仅连接一个索引器。这并非最佳场景，因为可能会出现以下后果：

- 来自许多端点的大量数据流同时通过单个管道，该管道消耗您的系统和网络资源。
- 在发生 IF 故障时，仅为端点实现有限的故障转移目标（您的中断风险与 IF 的数量成反比）。
- 在任何指定时间点只有少量索引器得到服务。短时搜索无法从并行化获得并应可获得的益处。

中介转发器还会向您的部署添加额外的架构层，导致管理和故障检修复杂化，增加前往数据摄取路径的延迟。应尽可能避免使用中介转发层，除非这是满足您要求的唯一选择。如果您符合以下条件，可考虑使用中介层：

- 有需要在通过网络发送至索引器前截断/移除的敏感数据。其中一个示例为你使用公共网络的场景。
- 严格的安全政策不允许端点与索引器之间的直接连接（如，多区网络或基于云的索引器）。
- 在端点与索引器之间有需要过滤大量事件子集的带宽限制。
- 要求是以基于事件的路由通往动态目标。

考虑任何中介转发层的调整及配置需要，以确保该层的可用性，提供足够的处理容量处理所有流量，并且支持跨索引器的良好事件分配。IF 层有以下要求：

- 整体需要大量数据处理管道。
- 具有冗余 IF 基础架构。
- 可适当调整 Splunk 负载均衡配置。例如，autoLBVolume、EVENT_BREAKER、EVENT_BREAKER_ENABLE，必要时可强制执行 TimeBasedAutoLB。

一般指南建议配置相当于索引层的索引器数量两倍的 IF 处理管道。

说明：处理管道与实体 IF 服务器并不等同。提供足够的系统资源。例如，CPU 核、内存及 NIC 带宽可用，单个 IF 可配置带有多个处理管道。

如果您需要 IF 层 （见问卷），请默认使用该层的 UF，因为它们可以较低的资源占用空间为系统及网络提供较高的吞吐量。如果您的 UF 容量不足以满足您的需求，请使用 HF。

（系统日志）系统日志数据收集

系统日志协议可为企业中的日志数据提供普适来源。大部分可扩展及可靠的数据收集层都含有系统日志摄取组件。有很多方法可以将系统日志数据导入 Splunk。请考虑以下方法：

- **通用转发器 (UF)/重型转发器 (HF)**：使用 Splunk UF 或 HF 监控（摄取）系统日志服务器输出的文件（如 rsyslog 或 syslog-ng）。
- **通往 HEC 的系统日志代理**：使用能够输出至 Splunk 的 HEC 的系统日志代理。（有可将 rsyslog 和 syslog-ng 输出至 HEC 的第三方模块）。
- **直接 TCP/UDP 输入**：Splunk 能够侦听 TCP 或 UDP 端口（默认端口为 UDP 514）并摄取此处的数据源（不建议用于生产用途）。

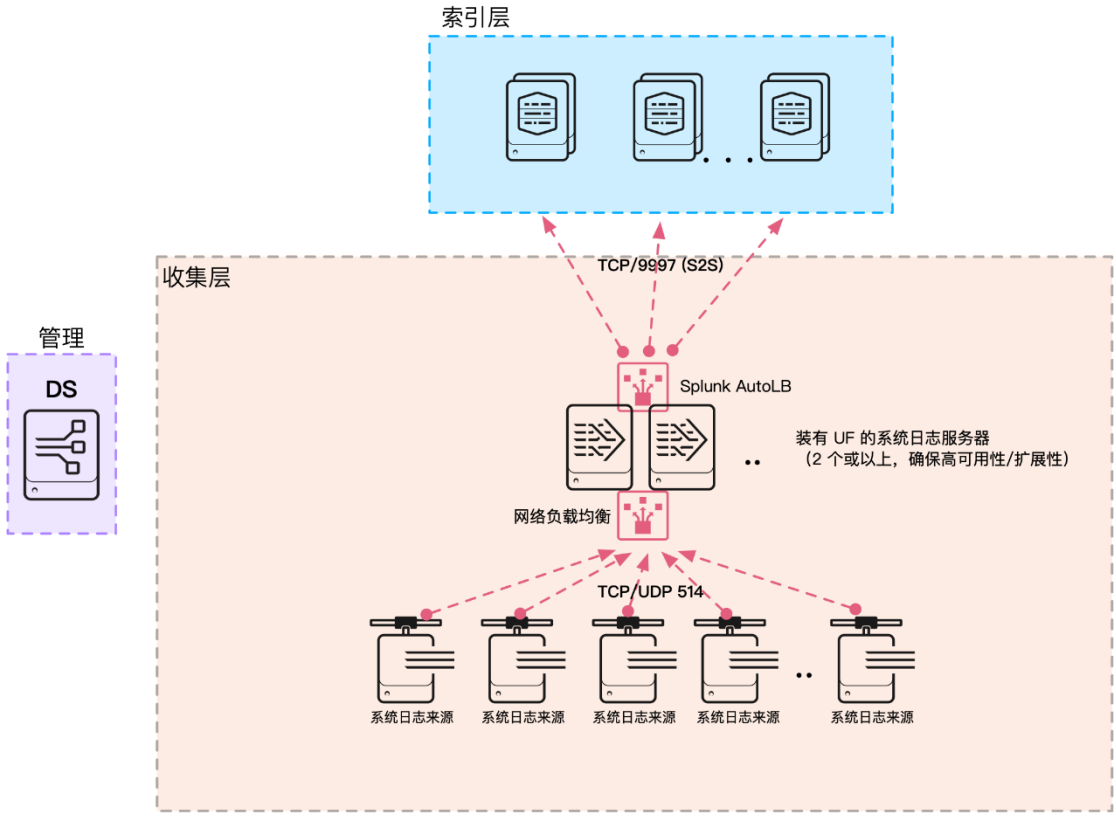
系统日志（与 SCD 共同进行文件监控）

Splunk 可使用监控，通过 UF/HF 上的 inputs.conf 处理由系统日志收集守护进程 (SCD) 写入端点磁盘的系统日志源。最常见的 rsyslog、syslog-ng 和 Fastvue 可提供能够在低容量环境及大型分布式环境中扩展及轻松整合并管理的商业免费解决方案。

若要了解关于如何配置监控器的更多信息，请参阅数据导入中的监控文件和目录。

该架构以与通用转发器在任何其他端点操作相同的方式支持适当的数据载入。您可将 SCD 配置为识别多个不同的日志类型及以适当的文件和目录输出日志事件，方便 Splunk 转发器提取。这可通过将日志写入磁盘，增加系统日志的日志数据流的持久性，减少因使用不可靠的 UDP 作为传输路径发送消息导致的数据损失风险。

使用 UF 的系统日志数据收集拓扑



下图显示使用端口 514 上的 TCP 或 UDP 发送数据至系统日志服务器的负载均衡池的系统日志源。多个服务器可却确保收集层的高可用性，并可防止数据在维护操作期间丢失。每个系统日志服务器都配置为对系统日志流应用将系统日志事件写入每个源类型（防火墙事件、操作系统的系统日志、网络交换机、IPS 等）的专用文件/目录的规则。每个服务器部署的 UF 监控这些文件并将数据转发至索引层，以处理至相应的索引中。Splunk AutoLB 用于跨可用的索引器均匀分发数据。

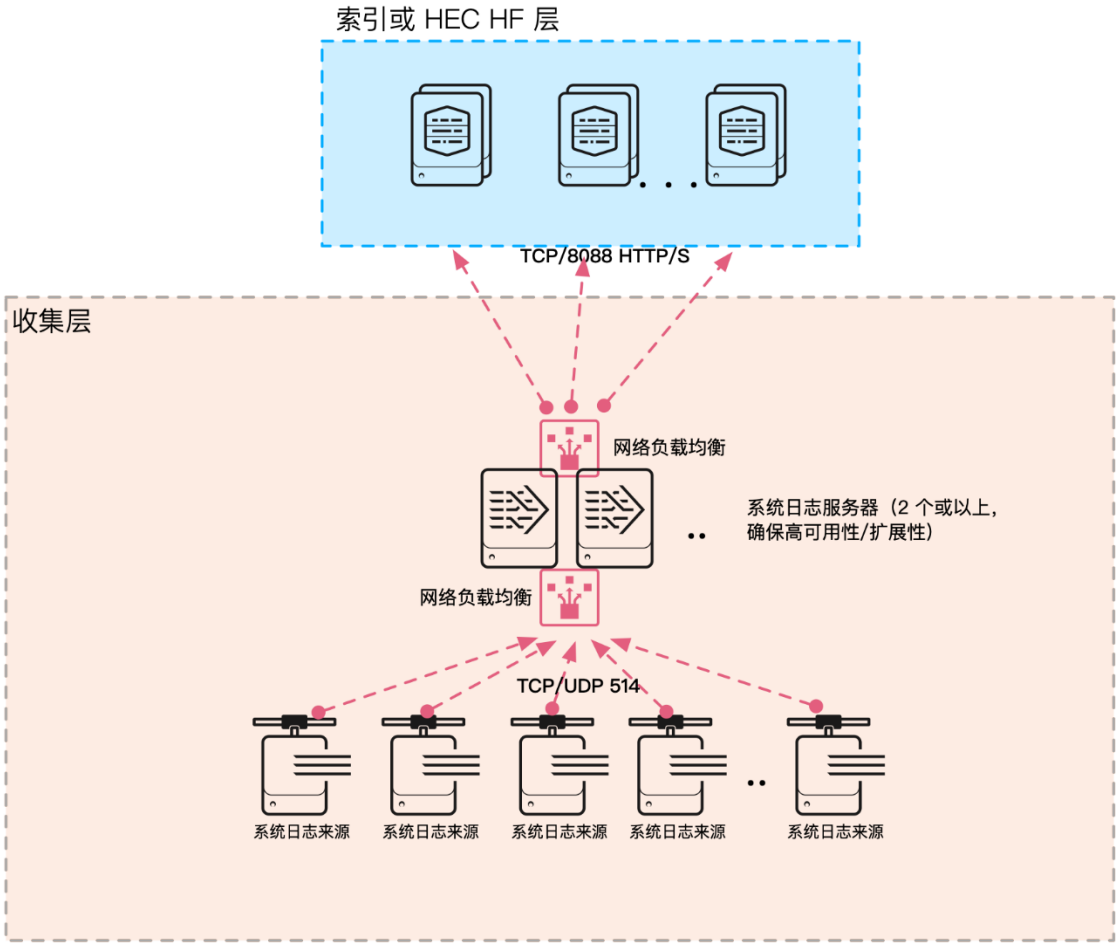
管理层中显示的部署服务器可用于集中管理 UF 配置

通往 HEC 的系统日志代理

增加 HEC 的采用量之后，将有更多的部署使用它们的 HEC 部署摄入系统日志。若要了解更多信息，请查看 Splunk 博客帖子 Syslog-ng 与 HEC：Splunk 中的可扩展聚合数据收集。

下图显示在端口 514 使用网络负载均衡器向系统日志服务器场发送数据的系统日志源。可应用具有定制系统日志目的地的适当系统日志策略（使用 HEC API 的 python 脚本），将事件发送至 HEC 侦听器，采用网络流量负载均衡器进行索引：

使用 HEC 的系统日志数据收集拓扑



该拓扑的优点是无需部署和配置 UF/HF。HTTP 负载均衡器可充当索引器上的 HEC 侦听器（或专用的 HEC 侦听器层），确保数据跨 HEC 端点均匀分布。以“最少连接”策略配置该负载均衡器。

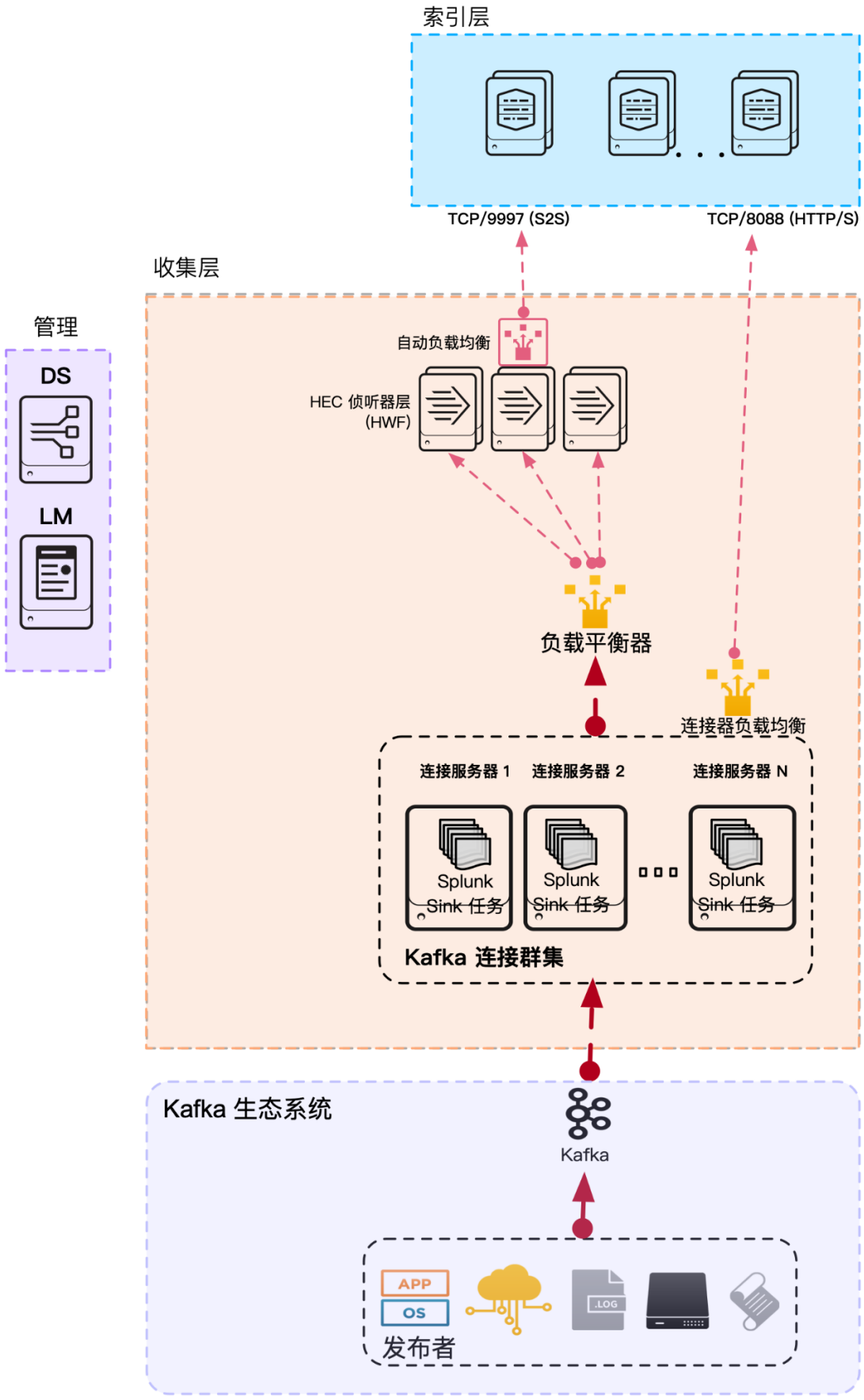
Splunk UDP 输入

Splunk 可使用 UF 或 HF 上的直接 UDP 输入接收来自系统日志的数据。若要了解关于配置 TCP 和 UDP 端口的更多信息，请参阅《数据导入》中的从 TCP 和 UDP 端口获取数据接收端口 514 的事件的能力取决于作为根运行的 UF/HF 的能力。此外，该代理必须所有时间 100% 可用，以免出现数据丢失。转发器可能会频繁重启以应用配置变更，这可能会导致数据丢失。因此，**这不被视为生产部署的最佳实践**。

(KAFKA) 使用来自 Kafka 主题的日志数据

Splunk 为使用来自 Kafka 主题的日志数据提供支持的接收器连接器，名为 "Splunk Connect for Kafka"。详细的产品文档信息请参阅 Splunk Connect for Kafka 手册中的 Apache Kafka Connect。Splunk Connect for Kafka 软件包安装到适当大小的 Kafka Connect 群集（位于 Splunk 外），在这里，它可以根据配置订阅主题并使用 HEC 发送使用的事件，以便进行索引。

使用 Kafka 和 HEC 的数据收集拓扑

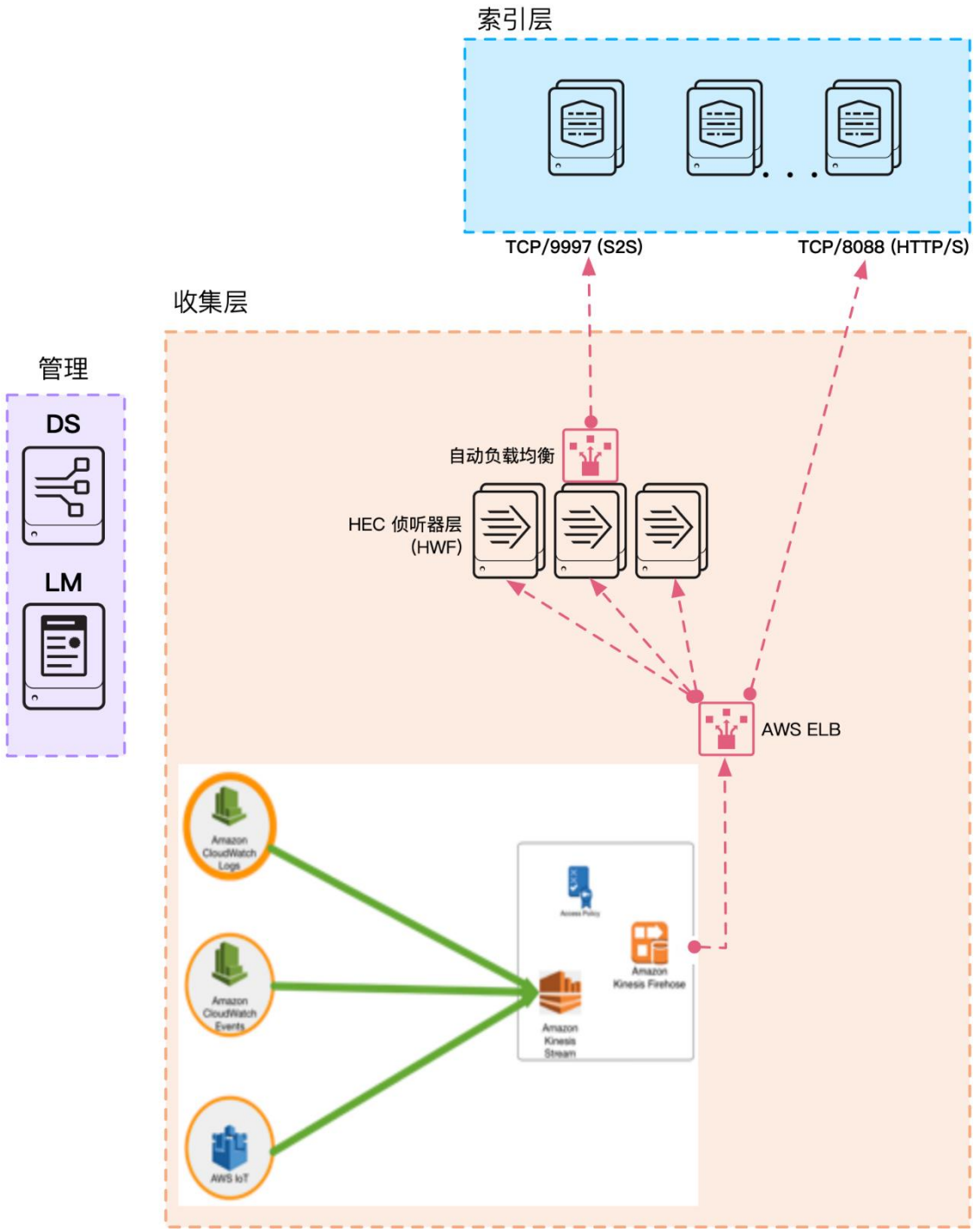


下图显示向 Kafka 总线发送讯息的 Kafka 发布器。Kafka Connect 群集托管的任务通过 Splunk Connect for Kafka 使用这些讯息，并使用网络负载均衡器将数据发送至 HEC 侦听服务。再一次，HEC 侦听服务可直接托管在索引器或专用 HEC 侦听器层。详情请参阅 HEC 部分。仅当专用 HF 层部署为托管 HEC 侦听器时才需要管理层组件。

(KINESIS) 使用来自 Amazon Kinesis Firehose 的日志数据

Splunk 和 Amazon 已在 Kinesis 和 Splunk HEC 之间实施整合，使您可将来自 AWS 的流数据直接传输至 HEC 端点（可通过您的 AWS 控制台配置）。这可由 Splunk Add-On for Kinesis Firehose 进行补充，该组件可为来源于 AWS 的不同数据来源提供遵循 CIM 的知识。

使用 Amazon Kinesis 的数据收集拓扑



此图显示使用 Kinesis 流发送至 Firehose 的 AWS 日志源，经适当配置，该组件可通过 AWS ELB 将数据发送至 HEC 侦听服务。再一次，HEC 侦听服务可直接托管在索引器或专用 HEC 侦听器层。详情请参阅 HEC 部分。

仅当专用 HF 层部署为托管 HEC 侦听器时才需要所示的管理层组件。

（指标）指标收集

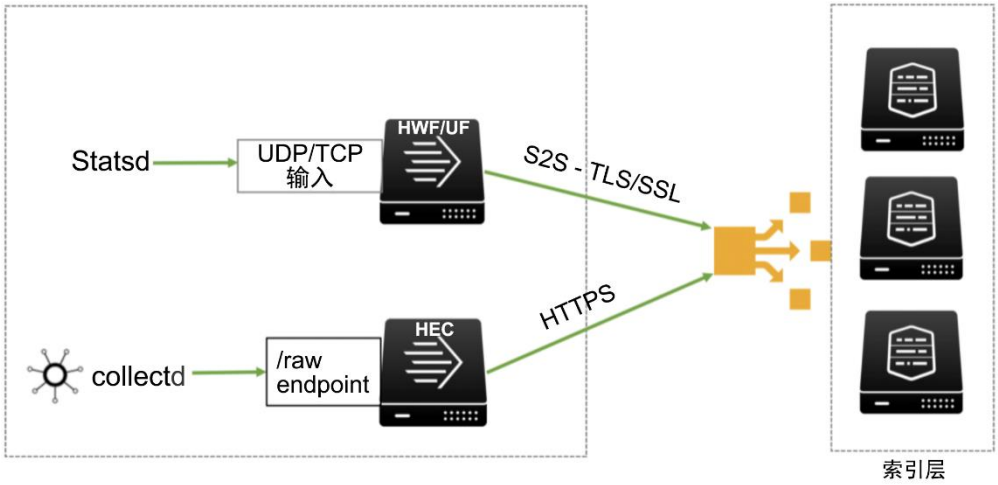
Splunk 能够接收和收集来自不同第三方软件的系统和应用性能数据或指标数据。Splunk 平台中的指标使用已为指标存储及检索优化的定制索引类型。

可以通过不同的方式使用指标数据，收集方法基于所用技术。最常用的指标收集形式是采用软件守护进程（如 **collectd**、**statsd**）或使用定制的指标数据文件及有效的数据源配置。

当使用 **statsd** 和 **collectd** 等代理时，主要有两种方法将指标输入 Splunk。使用**直接 TCP/UDP** 输入或通过 **HEC**。

由于 **HEC** 端点的弹性及可扩展性以及可轻松水平扩展收集层的能力，使用 **HEC** 被视为最佳实践。

指标数据收集拓扑



Statsd 目前支持 **UDP** 和 **TCP** 传输，您可将它用作 Splunk 转发器或索引器的直接输入。但是，将 TCP/UDP 流量直接发送至转发器并非生产环境中的最佳实践，因为架构不具弹性且易于受所需的 Splunk 转发器重启导致的事件丢失影响（见系统日志收集）。

转发层组件的高可用性（HA）考虑事项

在数字世界中，有关于高可用性（HA）的常用概念。但是，其含义可能随组织而异，更符合灾难恢复（DR）而非高可用性定义。这两个概念虽然相似，但有不同的含义。HA 是系统特征，旨在确保达到议定水平的运行性能，通常是指高于正常时段的运行时间。DR 涉及一整套用于确保重要技术架构及系统在发生灾难后能够恢复及继续运行的策略、工具和程序。

下文概述中间/聚合层的不同 HA 形式。

中间层

- 对于具有中间/聚合层部署的客户，转发器的高可用性对任务非常关键。在应用层，Splunk 目前并无高可用性的原生支持方法。有其他策略在并非 Splunk 原生的操作系统层提供高可用性。常用解决方案包括 VMWare VMotion、AWS 自动扩展组以及 Linux 群集。请联络您的 Splunk 架构师，讨论对您可用的其他设计选项。
- 对于对专用 HEC 层有高可用性要求的环境，在多个 Splunk 重型转发器之前使用网络流量负载均衡器（NTLB）（如，NGINX）是最佳实践。这可提供最大吞吐量、扩展性及可用性优势。您有专用的 HTTP 事件收集器实例池，其唯一工作是接收和转发数据。您可添加更多 HEC 实例，而无需添加更多索引器。如果您的索引器成为瓶颈，可添加额外的索引器。
- 对于对系统日志收集有高可用性要求的环境，使用由负载均衡解决方案托管的群集（虚拟）IP 地址服务的多个系统日志服务器是最佳实践，可提供最大吞吐量、扩展性及可用性。您有

专用的 Splunk 实例池，其唯一工作是接收和转发数据。您可添加更多实例，而无需添加更多索引器。如果您的索引器成为瓶颈，可添加额外的索引器。

转发层

- 在转发（端点）层，代理本身的高可用性取决于相关操作系统。您至少应确保实施转发功能的任何服务能够在主机操作系统重启时自动重启。此外，转发器的最佳实践涉及从转发器到多个索引器配置和适当使用 AutoLB。这还涉及使用索引器确认，以确保数据抵达索引层。

第 3 步：应用设计原则和最佳实践

在下文您会找到按部署层划分的设计原则和最佳实践。

部署层

SVA 设计原则涵盖以下所有部署层：

层	定义
搜索	• 搜索头
索引	• 索引器
收集	• 转发器 • 模块化输入 • 网络 • HEC（HTTP 事件收集器） • 等
管理/实用工具	• CM • DS • LM • DMS • SHC-D

根据最佳实践设计您的拓扑

您需要牢记您的要求和拓扑，以便为您的部署选择适当的设计原则和最佳实践。因此，您应仅在完成上述 Splunk 验证架构选择流程的第 1 步和第 2 步之后考虑最佳实践。

最佳实践：层特定建议

在下文您会找到各个部署层的设计原则和最佳实践建议。每个设计原则都加强一或多个 SVA 支柱：可用性、性能、可扩展性、安全及可管理性。

搜索层建议

设计原则/最佳实践 （您的要求将确定哪些实践适用于您）		SVA 支柱				
		可用性	性能	可扩展性	安全性	可管理性
1	将搜索层尽可能靠近索引层（就网络而言） 搜索与索引层之间的任何延迟都会直接影响搜索性能		✓			
2	避免使用多个独立的搜索头 独立的搜索头不允许共享用户创建的 Splunk 工件。它们在跨搜索层利用资源方面的扩展性不佳。除非有配置隔离搜索头环境的特定需要，否则，您可以选择更好的扩展选项。	✓		✓	✓	✓
3	在扩展搜索层时利用搜索头群集 搜索头群集可跨群集复制用户工件，允许跨所有群集组件智能安排搜索工作负载。它还提供高可用性解决方案。	✓		✓		
4	将所有搜索头的内部日志转发至索引层 所有索引数据应仅存储在索引层。这样，无需在搜索头层提供高性能存储，且可简化管理。注：这也适用于任何其他 Splunk 角色。		✓			✓
5	在可能时考虑使用 LDAP 认证 为认证目的集中管理用户身份是一般企业最佳惯例，可简化您的 Splunk 部署的管理，提高安全性。				✓	✓
6	确保有足够的核，满足并行搜索需求。 每个搜索都需要一个 CPU 核执行。若没有核运行搜索，该搜索将排队，导致用户的搜索延迟。说明：同样适用于索引层	✓	✓	✓		
7	尽可能使用计划的搜索时间窗/理顺计划的搜索负载 计划的搜索通常在特定的时间点（整点、整点后第 5/15/30 分钟、午夜）运行。提供您的搜索可运行的时间窗有助于避免搜索并发性热点。		✓	✓		

9	限制独立搜索头群集的数量，以免索引层过载 搜索工作荷载仅可在 SH 环境内自动管理。独立 SHC 可能会产生比超出索引器（搜索对等节点）层处理能力的并行搜索工作负载。在规划独立搜索头的数量时同样如此。	✓		✓		
10	在构建搜索头群集时，使用奇数节点（3、5、7 等） 使用基于多数的协议执行 SHC 队长选举。奇数的节点可确保 SHC 不会在网络故障时分为数量均匀的节点。	✓				✓

索引层建议

设计原则/最佳实践 （您的要求将确定哪些实践适用于您）		支柱				
		可用性	性能	可扩展性	安全性	可管理性
1	在具有相关能力的服务器上启用并行管道 并行化功能有助于利用本应闲置的可用系统资源。请注意，在启用摄取并行化功能前，必须确保 I/O 性能足够。		✓	✓		
2	考虑为 HOT/WARM 卷和摘要使用 SSD SSD 已达到经济价格，可消除通常会导致搜索性能不佳的 IO 限制。		✓			
3	将索引层尽可能靠近搜索层（就网络而言） 减少网络延迟可为用户的搜索体验带来积极的影响。		✓			
4	在需要历史数据/报告高可用性时使用索引复制 索引复制可确保在群集中提供多个事件副本，以防搜索对等节点故障。调整副本数量（复制因子）以匹配您的 SLA。	✓				
5	使用监控控制台确保良好的数据载入实践（如，为每个数据源适当及明确界定自动换行、时间戳提取、TZ、源、源类型及主机）		✓	✓		✓

	明确配置数据源及依赖 Splunk 的自动检测能力经证明有利于提高数据摄取能力及减少索引延迟，尤其是在高容量部署中。					
6	考虑在具有卓越处理能力的索引器中配置批模式搜索并行化 利用搜索并行化功能可对若干类型搜索的搜索性能产生重大影响，让您可利用本可能无法使用的系统资源。		✓	✓		
7	监控跨索引器节点（=搜索对等节点）数据均衡分配。 跨搜索对等节点的事件/数据分配是搜索性能及强制执行适当数据保管策略的关键影响因素。		✓	✓		✓
8	在分布式/群集部署中禁用索引器的网络 UI。 并无直接在索引器上访问网络 UI 的合理需要。		✓		✓	✓
9	考虑对知名数据源使用 Splunk 预建技术加载项 您无需构建自身的配置以确保对知名数据源采用数据载入最佳实践，Splunk 提供的技术附件易于安装及管理，可确保最佳实施。		✓			✓
10	监控关键索引器指标 Splunk 可为您提供监控控制台，该监控控制台可提供关于您的索引层如何运行的关键性能数据。这包括 CPU 和内存使用情况以及内部组件的详细指标（流程、管道、排队、搜索）	✓	✓			

收集层建议

设计原则/最佳实践 （您的要求将确定哪些实践适用于您）		**支柱**				
		可用性	**性能**	**可扩展性**	**安全性**	**可管理性**
1	在可能的情况下使用 UF 转发数据。重型转发器的使用仅限于需要的使用案例。 内置 autoLB、能够重启、可集中配置、资源需求较低		✓			✓

2	在传输许多 UF 时，使用至少相当于索引器数量两倍的中介转发管道 将大电量端点转发器跨少量中介转发器多路传输会影响跨索引器的均衡事件分配，从而影响搜索性能。**仅在绝对必需时部署中介转发器。**	✓	✓			
3	考虑使用 SSL 保护 UF-IDX 流量				✓	
4	使用原生 Splunk LB 向索引层分配数据 当前并未支持转发器与索引器之间的网络负载均衡器。	✓		✓		
5	使用专用系统日志服务器进行系统日志收集 系统日志服务器可基于源和可用适当源类型配置，通过通用转发器将 TCP/UDP 流量持续发送至磁盘，以便处理。所需的转发器重启不会导致数据丢失。	✓				✓
6	使用 HEC 进行无代理收集（而非原生 TCP/UDP） HTTP 事件收集器 (HEC) 是允许通过 HTTP[/S] 协议发布事件的侦听服务。它可在索引器上直接启用，或配置在重型转发器层；两者都由负载均衡器提供服务。	✓				✓

管理/实用工具层建议

设计原则/最佳实践 （您的要求将确定哪些实践适用于您）		**支柱**				
		可用性	**性能**	**可扩展性**	**安全性**	**可管理性**
1	对于小型环境，考虑将 LM、CM、SHC-D 和 MC 整合于单个实例。 这些服务器角色的资源需求极低，是极佳的托管备选方案。在大型索引器群集，CM 可能需要专用服务器，以高效管理群集。					✓
2	对于大中型部署，考虑为 DS 使用单独实例					✓

	当通过部署服务器管理大量转发器时，资源需求将增加，需要专用服务器维持服务。					
3	对于超大型部署，考虑在 LB 后面配置多个 DS 说明：这可能需要 Splunk 专业服务部的帮助，以确保安装及配置正确	✅		✅		✅
4	确定 DS phoneHomeIntervalInSecs 是否可撤销 60 秒默认设置 更长的电话回归时间间隔可对 DS 的可扩展性产生积极影响。			✅		
5	使用专用/安全 DS，避免客户端通过应用部署遭到利用 任何可访问部署服务器的人都可更改该 DS 管理的 Splunk 配置，包括可能对转发器端点部署恶意应用。适当保护该角色属谨慎行为。				✅	
6	使用监控控制台 (MC) 监控部署的健康状态以及有关健康问题的警报。 监控控制台可提供预建的 Splunk 特定监控解决方案，且包含可向您提供有关环境健康状况的可扩展平台警报。	✅	✅			✅

总结及后续步骤

该白皮书已提供有关 Splunk 验证架构的简介。经验证架构可确保以最具成本效益、可管理及可扩展的方式满足您组织的要求。SVA 可提供基于以下基础支柱的最佳实践和设计原则：

- 可用性
- 性能
- 可扩展性
- 安全性
- 可管理性

该白皮书还讲述了 3 步 Splunk 验证架构选择流程：1）界定要求；2）选择拓扑；及 3）应用设计原则及最佳实践。既然您已经熟悉了 Splunk 验证架构的众多优点，我们希望您已准备好开始为您的组织选择合适的部署拓扑的流程。

后续步骤

那么，选择经验证架构之后该做什么呢？您的工作环境之旅的后续步骤包括：

定制

- 考虑您的拓扑可能需要的任何必要的定制，以满足特定要求

部署模式

- 决定部署模式（裸机、虚拟、云）

系统

- 根据 Splunk 系统要求选择您的技术（服务器、存储、操作系统）。

调整

- 收集所需的所有相关数据，以调整您的部署（数据摄取、预期搜索量、数据保留需要、复制等） Splunk Storage Sizing（https://splunk-sizing.appspot.com/）是可用的工具之一。

人手安排

- 评估您实施及管理部署所需的人手。这是构建 Splunk Center of Excellence 的重要部分。

我们可在经验证架构的整个流程及后续步骤为您提供帮助。若有任何疑问，请随时联络您的 Splunk 客户团队。您的客户团队可获取 Splunk 的全套技术及架构资源，并乐于为您提供进一步的信息。

祝您使用 Splunk 愉快！

附录

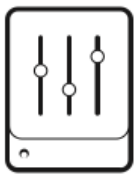
本部分包含用于 SVA 的额外参考信息。

附录 "A":解释 SVA 支柱

支柱	描述	主要目标/设计原则
可用性	可持续运行，能够从计划及非计划中断恢复的能力。	1. 消除单点故障/增加冗余 2. 发现计划及非计划的故障/中断 3. 容忍计划/非计划的中断（最好是自动） 4. 计划持续升级
性能	有效使用可用资源，以在不同使用模式下维持最佳服务水平的能力。	1. 添加提高性能的硬件 – 计算、存储、内存。 2. “自下而上”消除瓶颈 3. 利用所有并行处理方法 4. 利用本地设置（即，减少组件分布） 5. 优化常见案例（80/20 规则） 6. 避免不必要的普遍性 7. 时移计算（预先计算、徐缓计算、共享/批量计算） 8. 以确定性及准确度换取时间（随机化、抽样）
可扩展性	确保系统设计可在所有层扩展及有效处理增加的工作负载的能力。	1. 垂直及水平扩展 2. 分开需要单独扩展的功能组件 3. 降低组件之间的依存性 4. 及早设计已知的未来增长 5. 在整个系统设计中引入层次结构
安全性	确保系统设计可保护数据及配置/资产，同时继续实现价值的能力。	1. 从一开始就设计安全的系统 2. 对所有通信采用先进的协议 3. 允许对事件数据进行广泛及细粒度访问 4. 采用集中式认证 5. 实施审核程序 6. 减少攻击或恶意应用的影响范围

支柱	描述	主要目标/设计原则
可管理性	确保系统设计可跨所有层集中操作及管理的能力。	1. 提供集中管理功能 2. 管理配置对象生命周期（源控制） 3. 衡量及监控/描述应用 (Splunk) 使用情况 4. 衡量及监控系统健康状况

附录 "B":拓扑组件

层	组件	图标	描述	说明
管理	部署服务器 (DS)		部署服务器管理转发器配置的配置。	应在专用实例中部署。可虚拟化，以确保轻松实现故障恢复。
	许可主机 (LM)		其他 Splunk 组件需要许可主机，以启用许可功能及跟踪日常数据摄取量。	许可主机角色的能力和可用性要求极低，可与其他管理功能一并托管。可虚拟化，以确保轻松实现故障恢复。
	监控控制台 (MC)		监控控制台可提供仪表板，监控您的环境的使用及健康状况。它还含有大量预装平台警报，该等警报可予以定制，提供运行问题通知。	在群集环境中，除在非群集部署中运行的许可主机和部署服务器外，MC 还可与主节点一并托管。可虚拟化，以确保轻松实现故障恢复。
	群集主机 (CM)		群集主机是群集部署中所有活动必需的协调器。	在带有大量索引数据桶（高数据量/保留）的群集中，群集主机可能需要运行专用服务器。可虚拟化，以确保轻松实现故障恢复。
	搜索头群集 Deployer (SHC-D)		引导 SHC 及管理部署至群集的 Splunk 配置需要搜索头群集 Deployer。	SHC-D 并非运行时间组件，系统要求极低。它可与其他管理角色一同托管。说明：每个 SHC 都需要其自身的 SHC Deployer 功能。可虚拟化，以确保轻松实现故障恢复。
搜索	搜索头 (SH)		搜索头可为 Splunk 用户提供 UI 及协调计划的搜索活动。	搜索头是分布式部署的专用 Splunk 实例。搜索头可虚拟化，以确保轻松实现故障恢复，但它们须部署适当的 CPU 及内存资源。

层	组件	图标	描述	说明
	搜索头群集 (SHC)		搜索头群集是由至少三个搜索头组成的群集。它可为搜索头层提供水平可扩展性，并在中断时实现对用户透明的失效备援。	搜索头群集需要专用的服务器（最好采用相同的系统规格）。搜索头群集成员可虚拟化，以确保轻松实现故障恢复，但它们须部署适当的 CPU 及内存资源。
索引	索引器		索引器是 Splunk 的核心与灵魂。他们处理和索引进站数据，同时充当搜索对等节点，满足搜索层发起的搜索请求。	索引器必须始终配置在分布式或群集部署中的专用服务器。在单服务器部署中，索引器还可提供搜索 UI 及许可主机功能。若能保证充足的资源，索引器在裸机服务器或专用高性能虚拟机中表现最佳。
数据收集	转发器及其他数据收集组件		数据收集涉及的任何组件的通用图标	包括通用及重型转发器、网络数据输入及其他形式的数据收集（HEC、Kafka 等）