Cisco 身份服务引擎性能和可扩展性指南

Revised: 2022 年 4 月 1 日

概述

本文档列出了 Cisco 身份服务引擎 (Cisco ISE) 的性能和可扩展性指标。

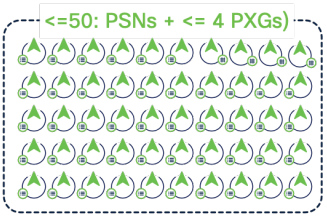
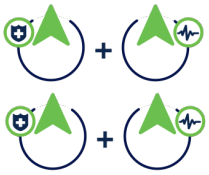
Cisco ISE 节点术语

思科 ISE 节点可以根据它承担的角色提供各种服务。通过管理员门户可用的菜单选项取决于思科 ISE 节点承担的职责和角色。

表 *1:* 不同类型的 *Cisco ISE* 节点

节点类型	说明
策略管理节点 (PAN)	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和配置。它用作查看所有管理操作，配置和情景数据的单一窗格。它将配置与部署中的其余节点同步。
策略服务节点 (PSN)	承担策略服务角色的思科 ISE 提供网络访问、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。
监控节点（MnT）	具有监控角色的思科 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。
pxGrid 节点	可以使用 Cisco pxGrid 与其他网络系统（例如 Cisco ISE 生态系统合作伙伴系统）和其他 Cisco 平台共享 Cisco ISE 会话目录中的情景相关信息。pxGrid 框架也可用来在 Cisco 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。

不同类型的 Cisco ISE 部署

Evaluation	小型部署	中型部署	大型部署
 • 同一设备或 VM 实例上的所有 ISE 角色（PAN + MnT + PSN + pxGrid）。 • 不建议用于生产。	 • 同一设备或 VM 实例上的所有 ISE 角色（PAN + MnT + PSN + pxGrid）。 • 双节点部署。一个节点作为主节点，另一个节点作为副节点，以实现冗余。	  • PAN + MnT + pxGrid 在同一节点上运行。 • 一个节点作为主节点，另一个节点作为副节点，以实现冗余。 • 专用节点上的 PSN。节点可以是 VM 或设备。 • 最多支持 6 个 PSN（适用于 Cisco ISE 3.0 及更高版本）。您可以在任何 PSN 上启用 pxGrid 角色，或将专用 pxGrid 节点添加到部署。	  • 所有 ISE 角色都是完全分布式的，在单独的 VM 或设备节点上运行。 • 最多支持 4 个 pxGrid 节点。 • 最多支持 50 个节点 (PSN + pxGrid)。

不同部署的最大并发活动终端最大数量

思科身份服务引擎 (ISE) 可以安装在思科 SNS 硬件或虚拟设备上。为了实现可与 Cisco ISE 硬件设备相媲美的性能和可扩展性，为虚拟机分配的系统资源应与为 Cisco SNS 3500 或 3600 系列设备分配的系统资源相当。

下面提供的身份验证值是近似值（大约 5%）。您可以根据以下内容确定部署所需的 PSN 数量：

- 最大并发活动终端的最大数量
- RADIUS 身份验证率
- TACACS+ 身份验证率

表 *2:* 基于 ***PSN*** 类型的最大并发活动终端最大数量

PSN 类型	Cisco SNS 3515	Cisco SNS 3595	Cisco SNS 3615	Cisco SNS 3655	Cisco SNS 3695
专用 PSN	7500	40,000	10,000	50,000	100,000
共享 PSN	5000	20,000	10,000	25,000	50,000

表 *3:* 不同部署的最大并发活动终端最大数量

部署类型	Cisco SNS 3515	Cisco SNS 3595	Cisco SNS 3615	Cisco SNS 3655	Cisco SNS 3695
	PAN 和 MnT	PAN 和 MnT	PAN 和 MnT	PAN 和 MnT	PAN 和 MnT
大规模部署	—	500,000	—	500,000	2,000,000
中型部署	7500	20,000	10,000	25,000	50,000
小型部署	7500	20,000	10,000	25,000	50,000

有关不同类型的部署的信息，请参阅 不同类型的 Cisco ISE 部署，第 3 页

注释

- 即使中型和小型部署中的并发活动终端数量相同，由于专用 PSN，中型部署可提供更高的性能。
- 这些值适用于所有类型的活动会话。
- 当任何部署的并发活动终端数量超过这些数量时，会话可能会被丢弃。

Cisco ISE 部署规模限制

属性 (Attribute)	上限
大型或专用部署中的最大 pxGrid 节点数上限	4
每个 pxGrid 节点的最大 pxGrid 用户数	200
已启用 SXP 服务的专用 PSN 节点	4
已启用 SXP 服务的每个 PSN 节点的最大 ISE SXP 对等体的最大数量	200
最大网络设备条目数（IP 地址和/或 IP 地址范围）	100,000
最大网络设备组数 (NDG)	10,000
最大 Active Directory 林数（加入点数）	50

属性 (Attribute)	上限
最大 Active Directory 控制器数量（WMI 查询）	100
最大内部用户数量	300,000
最大内部访客数量 注释　拥有超过500,000个访客用户可能会在用户身份验证中造成延迟。	1,000,000
最大用户证书数量	1,000,000
最大服务器证书数量	1,000
最大受信任的证书数量	1,000
最大用户门户数量（访客，自带设备，MDM，证书调配，安全评估，客户端调配）	600
最大并发活动终端的最大数量	2,000,000
最大策略集数量	200
最大身份验证规则数量	1000（策略集模式）
最大授权规则数量	策略集模式：3,000（3,200个授权配置文件） 不建议在单个策略集中包含超过 600 条授权规则。 注释　增加每个授权规则的条件数量可能会影响性能。
最大用户身份组数量	1,000
最大终端身份组数量	1,000
TrustSec 安全组标记 (SGT) TrustSec 安全组 ACL (SGACL) TrustSec IP-SGT 静态绑定（通过 SSH）	10,000 1,000 10,000
最大并发连接数	ERS API：100 OpenAPI：150
大型部署的最大被动 ID 会话数上限	3695 PAN，MnT：2,000,000 3595 PAN，MnT：500,000
主 PAN 与任何其他 Cisco ISE 节点（包括副 PAN、MnT 和 PSN）之间的最大网络延迟	300 毫秒
最大被动 ID 会话提供程序的最大数量	

属性 (Attribute)	上限
最大 AD 域控制器数量	100
最大 REST API 提供程序数	50
最大系统日志提供程序数	70
最大 pxGrid 用户数	50

RADIUS 性能

注释 Cisco 身份服务引擎 (ISE) 可以安装在 Cisco SNS 硬件或虚拟设备上。物理和虚拟部署都提供相同级别的性能。为了实现可与 Cisco ISE 硬件设备相媲美的性能和可扩展性，为虚拟机分配的系统资源应与为 Cisco SNS 3500 或 3600 系列设备分配的系统资源相当。

下表显示专用 PSN 节点的每秒身份验证。

身份验证方法	身份库	Cisco SNS 3515	Cisco SNS 3595	Cisco SNS 3615	Cisco SNS 3655	Cisco SNS 3695
PAP	内部	775	1100	900	1300	1300
PAP	Active Directory	250	275	275	300	300
PAP	LDAP	275	300	300	350	350
PEAP (MSCHAPv2)	内部	125	150	150	225	225
PEAP (MSCHAPv2)	Active Directory	100	150	150	175	175
PEAP (GTC)	内部	100	150	175	250	250
PEAP (GTC)	Active Directory	100	125	100	175	175
EAP-FAST (MSCHAPv2)	内部	375	400	375	550	550
EAP-FAST (MSCHAPv2)	Active Directory	175	225	200	275	300
EAP-FAST (GTC)	内部	300	450	350	450	450
EAP-FAST (GTC)	Active Directory	125	200	200	300	300
EAP-FAST (GTC)	LDAP	150	300	200	300	300
EAP-TLS	内部	125	150	175	225	250

身份验证方法	身份库	Cisco SNS 3515	Cisco SNS 3595	Cisco SNS 3615	Cisco SNS 3655	Cisco SNS 3695
EAP-TLS	Active Directory	125	175	150	200	200
EAP-TLS	LDAP	150	175	175	250	250
EAP TEAP	内部	75	100	100	175	200
MAB	内置	400	575	500	1000	1300
MAB	LDAP	300	500	400	600	600

TACACS + 性能

下表显示专用 PSN 节点的每秒事务数（TPS）。

场景	Cisco SNS 3515	Cisco SNS 3595	Cisco SNS 3615	Cisco SNS 3655	Cisco SNS 3695
TACACS + 功能：PAP	1800	2500	2800	3000	3200
TACACS + 功能：CHAP	2000	3200	2800	3200	3900
TACACS + 功能：启用	1000	1100	1000	1100	1100
TACACS + 功能：会话授权	1800	3000	2800	3000	3600
TACACS + 功能：命令授权	1800	2800	2800	3000	3900
TACACS + 功能：计费	2000	3000	3000	6000	9000

Cisco ISE 基于场景的性能

下表显示专用 PSN 节点的每秒事务数（TPS）。

场景	Cisco SNS 3515	Cisco SNS 3595	Cisco SNS 3615	Cisco SNS 3655	Cisco SNS 3695
终端安全评估身份验证	50	55	55	60	60
访客热点身份验证	50	100	75	125	150
访客赞助的身份验证	50	75	50	75	75
BYOD 激活单 SSID	10	12	12	15	15
BYOD 激活双 SSID	10	12	12	15	15
MDM	100	200	200	225	350

场景	Cisco SNS 3515	Cisco SNS 3595	Cisco SNS 3615	Cisco SNS 3655	Cisco SNS 3695
内部 CA 证书发放	40	45	45	50	50
每秒分析的新终端/每秒的配置文件更新	200	250	200	250	250
每秒处理的最大 PassiveID 会话数的最大值	1000	1000	1000	1000	1000
ERS：终端批量 API	50	75	75	100	100
ERS：访客批量 API	50	75	75	100	100
ERS：TrustSec 批量 API	5	5	5	10	10
TrustSec					
将 300 个 TrustSec 策略推送到 254 个 NAD 所需的时间（以秒为单位）	50	50	50	50	25
5000 TrustSec 策略通过 REST API 下载 2GB 数据所需的时间（以秒为单位）	50	50	50	50	25
SXP					
将 SXP 连接到 SXPSN 所需的时间（以毫秒为单位）	5	5	5	3	3
pxGrid					
使用 20,000 个会话批量下载 200 个 pxGrid 用户所需的时间（以秒为单位）	40	45	40	55	60

注释 当超过这些限制时，可能会导致性能下降，导致请求被丢弃。您必须调配 Cisco ISE 设备和虚拟机，同时记住每个部署的总容量和预期的高峰小时身份验证速率。

Cisco ISE 硬件平台

请注意以下问题：

- VM 设备规格应可与生产环境中运行的物理设备相比较。
- 您必须部署专用 VM 资源，不要在多个访客 VM 之间共享或超订用资源。
- 对于 VM 部署，由于超线程，核心数量是物理设备数量的两倍。例如，对于小型网络部署，您必须分配 16 个 vCPU 核心才能满足 SNS 3615（包含 8 个 CPU 核心或 16 个线程）的 CPU 规格。
- Cisco ISE 3.1 不支持 Cisco 安全网络服务器（SNS）3515 设备。

表 *4:* 不同硬件平台的规格

设备	Cisco SNS 3515	Cisco SNS 3595	Cisco SNS 3615	Cisco SNS 3655	Cisco SNS 3695
处理器	1 x Intel Xeon 2.4 GHz E5-2620 处理器	1 x Intel Xeon 2.6 GHz E5-2640 处理器	1 x Intel Xeon 2.10 GHz 4110 处理器	1 x Intel Xeon 2.10 GHz 4116 处理器	1 x Intel Xeon 2.10 GHz 4116 处理器
每个处理器的内核数量	6	8	8	12	12
内存	16 GB (2x8GB)	64 GB (4x16GB)	32 GB (2x16GB)	96 GB (6 x 16 GB)	256 GB (8 x 32 GB)
硬盘	1 x 600-GB 6Gb SAS 10K RPM	4 x 600-GB 6Gb SAS 10K RPM	1 x 600-GB 6Gb SAS 10K RPM	4 x 600-GB 6Gb SAS 10K RPM	8 x 600-GB 6Gb SAS 10K RPM
硬件 RAID	—	RAID 10 思科 12G SAS 模块化 RAID 控制器	—	RAID 10 思科 12G SAS 模块化 RAID 控制器	RAID 10 思科 12G SAS 模块化 RAID 控制器
网络接口	6 个 1GBase-T 接口	6 个 1GBase-T 接口	2 个 10Gbase-T 接口 4 个 1GBase-T 接口	2 个 10Gbase-T 接口 4 个 1GBase-T 接口	2 个 10Gbase-T 接口 4 个 1GBase-T 接口
电源	1 个 770W 电源	2 个 770W 电源	1 个 770W 电源	2 个 770W 电源	2 个 770W 电源

ISE 社区资源

有关如何规划 Cisco ISE 部署的信息，请参阅以下链接：

ISE 高级设计

ISE 规划和与部署要点清单

美洲总部
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

亚太区总部
CiscoSystems(USA)Pte.Ltd.
Singapore

欧洲总部
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco 在全球拥有 200 多个办事处。相关地址、电话和传真号码可见于
Cisco 位于 www.cisco.com/go/offices 上的网站。