pxGrid

pxGrid 和思科 ISE

Cisco pxGrid 是一个开放且可扩展的安全产品集成框架 (SPIF)，允许任意合作伙伴平台双向集成。

pxGrid 1.0 使用传统可扩展消息传送和网真协议 (XMPP) 实施方法。pxGrid 1.0 处于维护模式，很快将被删除。Cisco pxGrid 1.0 需要客户端 SDK 库（Java 或 C）才能使用 pxGrid。

pxGrid 2.0 使用 REST 和 WebSocket 接口。客户端使用 REST 处理控制消息、查询和应用数据，并使用 WebSocket 推送事件。有关 pxGrid 2.0 的详细信息，请参阅**欢迎学习思科平台交换网格 (pxGrid)**。

Cisco pxGrid 可以：

- 与其他网络系统（例如 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。
- 让第三方系统能调用自适应网络控制操作隔离用户和设备以应对网络或安全事件。标签定义、值和说明等 TrustSec 信息通过 TrustSec 主题从Cisco ISE 传输到其他网络。
- 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Cisco ISE 发送到其他网络。
- 批量下载标签和终端配置文件。
- 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 ISE 管理员指南》中“分段”一章中的安全组标签交换协议部分。
- Cisco pxGrid Context-in 使生态系统合作伙伴能够将主题信息发布到Cisco ISE。因此Cisco ISE 能够根据生态系统中识别的资产采取行动。有关 Cisco pxGrid Context-in 的详细信息，请参阅 pxGrid Context-In。

注释 pxGrid 1.0 处于维护模式，很快将被弃用。我们在 ISE 2.4 中引入了 pxGrid 2.0。我们强烈建议合作伙伴将其 pxGrid 客户端实施切换到 pxGrid 2.0。

pxGrid 概述

pxGrid 具有以下组件：

- 控制器：处理发现、身份验证和授权。
- 提供程序：返回查询结果或发布。
- Pubsub：为提供程序和使用者提供 pxGrid 服务。
- 用户：获得授权后，用户会从订阅的主题获取情景信息和警报。

pxGrid 提供以下功能：

- 发现：根据服务名称发现服务属性。当提供程序要求向 pxGrid 控制器“注册服务”时，流程开始。注册后，消费者使用“查找服务”发现提供商的位置。
- 身份验证：pxGrid 控制器验证 pxGrid 客户端有否有权访问服务。凭证为用户名和密码或证书（首选）。
- 授权：当 pxGrid 收到操作请求时，它会与 pxGrid 控制器协商以授权请求。pxGrid 将客户端分配到预定义的组。

pxGrid 1.0 的高可用性

使用 pxGrid 1.0 时，您可以配置两个在主/备模式下运行 pxGrid 角色的节点。Cisco 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。您必须手动升级 PAN 才能激活 pxGrid 服务器。

您可以使用 CLI 命令 **show application status ise** 查看 pxGrid 进程。以下与 pxGrid 1.0 相关的进程是：

- pxGrid Infrastructure Service
- pxGrid Publisher Subscriber Service
- pxGrid Connection Manager
- pxGrid 控制器

在活动 pxGrid 1.0 节点上，这些进程显示为“正在运行”(Running)。在备用 pxGrid 1.0 节点上，它们显示为“已禁用”(Disabled)。如果活动 pxGrid 1.0 **show logging application pxgrid.state**节点关闭，备用 pxGrid 节点会检测到此丢失情况，并启动四个 pxGrid 进程。在几分钟内，这些进程显示为“正在运行”(Running)，并且备用节点变为活动节点。您可以通过运行 CLI 命令 **show logging application pxgrid** 验证此节点上的 pxGrid 是否处于备用状态。

Cisco ISE 会自动故障转移到辅助 pxGrid 节点。如果您将原始主 pxGrid 节点重新连接到网络，原始主 pxGrid 节点将继续担当辅助角色，并且不会升级回主角色，除非您关闭当前的主节点。

pxGrid 2.0 的高可用性

pxGrid 2.0 节点在主动/主动配置下运行。为实现高可用性，部署中应至少有两个 pxGrid 节点。大型部署最多可以有四个节点，以增加规模和冗余。我们建议您为所有节点配置 IP 地址，以便在一个节

点关闭时，该节点的客户端连接到工作节点。当 PAN 关闭时，pxGrid 服务器会停止处理激活。手动升级 PAN 才能激活 pxGrid 服务器。有关 pxGrid 部署的详细信息，请参阅 **ISE 性能和扩展**。

所有 pxGrid 服务提供商客户端会在 7.5 分钟内定期向 pxGrid 控制器重新注册。如果客户端未重新注册，PAN 节点会认定它处于非活动状态，并删除该客户端。如果 PAN 节点关闭超过 7.5 分钟，当它恢复正常运行时，它将删除时间戳值早于 7.5 分钟的所有客户端。所有这些客户端都必须再次向 pxGrid 控制器注册。

pxGrid 2.0 客户端使用 WebSocket 和基于 REST 的 API 进行发布/订阅和查询。这些 API 由端口 8910 上的 ISE 应用服务器提供。通过 **show logging application pxgrid** 显示的 pxGrid 进程不适用于 pxGrid 2.0。

丢失检测

在Cisco ISE 3.0 中，我们向 pxGrid 主题添加了序列 ID。如果传输中断，用户可以通过检查 ID 序列中的缺口来识别这种情况。用户注意到主题序列 ID 发生变化，根据最后一个序列号的日期请求数据。如果发布者关闭，则当它恢复时，主题序列从 0 开始。当用户看到序列 0 时，必须清除缓存并开始批量下载。如果用户关闭，发布者会继续分配顺序 ID。当用户重新连接后发现序列 ID 出现缺口时，用户会从最后一个序列号的时间开始请求数据。丢失检测配合 Session Directory 和 TrustSec 配置运行。对于 Session Directory，当客户端检测到丢失时，必须清除缓存并开始批量下载。

如果您现有的应用不使用序列ID，则不必使用它们。但是，使用它们有助于检测丢失情况并从丢失中恢复。

Session Directory 会话是批处理的，在每个通知间隔内由 MnT 异步发布到 `/topic/com.cisco.ise.session`。

Trust Sec Config Security Group 安全组的更改将发布到 `/topic/com.cisco.ise.config.trustsec.security.group`。

丢失检测仅受 pxGrid 2.0 支持，默认情况下处于启用状态。

要查看使用丢失检测的代码示例，请参阅https://github.com/cisco-pxgrid/pxgrid-rest-ws/tree/master/java/src/main/java/com/cisco/pxgrid/samples/ise。

监控和调试

以下日志可用于 pxGrid：

- pxgrid.log：pxGrid 1.0 进程活动
- pxgrid-server.log：pxGrid 2.0 活动和错误
- pxgrid-cm.log：pxGrid 1.0 连接日志
- pxgrid-controller.log：pxGrid 1.0 控制消息日志
- pxgrid-jabberd.log：pxGrid 1.0 XMPP 服务器日志
- pxgrid-pubsub.log：pxGrid 1.0 XMPP Pubsub 日志

日志 (Log) 页面显示所有 pxGrid 2.0 管理事件。事件信息包括客户端和功能名称，以及事件类型和时间戳。导航至**管理 (Administration) > pxGrid 服务 (pxGrid Services) > 诊断 (Diagnostics) > 日志 (Log)** 以查看事件列表。您还可以清除日志并重新同步或刷新列表。

pxGrid 摘要页面

“摘要”(Summary) 页面显示当前 pxGrid 2.0 环境的统计信息。

- 当前连接 (Current Connections)：列出与控制器的连接
- 控制消息 (Control Messages)：身份验证、授权和服务发现
- REST API：使用 WebSocket 或 XMPP 连接的客户端数量
- Pubsub 吞吐量 (Pubsub Throughput)：发布到客户端的数据量
- 客户端 (Clients)：通过 REST 或 WebSocket 连接的客户端
- 错误数 (Errors)：导致客户端请求重新启动数据传输的传输错误数

pxGrid 客户端管理

当新客户端连接到 pxGrid 时，管理员必须访问此页面以批准客户端，然后客户端才能参与网格。但是，如果在**设置 (Settings)** 页面上启用了自动批准基于证书的帐户，则无需手动审批。

- **客户端 (Clients)**：同时列出 pxGrid 1.0 和 2.0 的外部客户端帐户。
- **pxGrid 策略 (pxGrid Policy)**：列出客户端可以订阅的可用服务。您可以编辑策略以更改哪些组可以访问该策略。您还可以为尚无策略的服务创建新策略。
- **组 (Groups)**：默认组为 EPS 或 ANC。您可以添加更多组，并使用它们限制对服务的访问。

  pxGrid 客户端可以通过使用 REST API 发送用户名向 pxGrid 控制器注册。在客户端注册时，pxGrid 控制器为 pxGrid 客户端生成密码。管理员可以批准或拒绝连接请求。
- **证书 (Certificates)**：您可以生成新证书以使用Cisco ISE 内部证书颁发机构。

  有关为 pxGrid 创建证书的信息，请参阅：
  - 随思科 pxGrid 部署证书 - 使用自签证书和思科 ISE 2.0/2.1/2.2 更新
  - 随思科 pxGrid 部署证书 - 使用外部 CA 和思科 ISE 2.0/2.1/2.2 更新

控制 pxGrid 策略

您可以创建 pxGrid 授权策略来控制对 pxGrid 客户端可访问服务的访问。这些策略控制哪些服务可供 pxGrid 客户端使用。

您可以创建不同类型的组，并将 pxGrid 客户端的可用服务映射到这些组。使用**客户端管理 > 组 (Client Management > Groups)** 窗口中的**管理组 (Manage Groups)** 选项添加新组。您可以在“策略”(Policies) 窗口中查看使用预定义组（例如 EPS 和 ANC）的预定义授权策略。

要为 pxGrid 客户端创建授权策略，请执行以下操作：

SUMMARY STEPS

1. 从**管理 (Administration)** 中选择 **pxGrid 服务 (pxGrid Services) > 客户端管理 (Client Management) > 策略 (Policy)**，并点击**添加 (Add)** 按钮。
2. 从**服务 (Service)** 下拉列表中选择服务：
3. 从**操作 (Operation)** 下拉列表中，选择以下选项之一：
4. 从**组 (Groups)** 下拉列表中，选择要映射到此服务的组。
5. 点击**提交 (Submit)**。

DETAILED STEPS

步骤 1 从**管理 (Administration)** 中选择 **pxGrid 服务 (pxGrid Services) > 客户端管理 (Client Management) > 策略 (Policy)**，并点击**添加 (Add)** 按钮。

步骤 2 从**服务 (Service)** 下拉列表中选择服务：

- com.cisco.ise.radius
- come.cisco.ise.sxp
- com.cisco.ise.trustsec
- com.cisco.ise.session
- com.cisco.ise.system
- com.cisco.ise.mdm
- com.cisco.ise.config.trustsec
- com.cisco.ise.config.profiler
- com.cisco.ise.pxgrid.admin
- com.cisco.ise.config.deployment.node
- com.cisco.ise.endpoint
- com.cisco.ise.config.anc
- com.cisco.ise.dnac
- com.cisco.ise.config.upn
- com.cisco.ise.pubsub

步骤 3 从**操作 (Operation)** 下拉列表中，选择以下选项之一：

- <ANY>
- 发布

- publish /topic/com.cisco.ise.session
- publish /topic/com.cisco.ise.session.group
- publish /topic/com.cisco.ise.anc
- <CUSTOM> - 如果选择此选项，可以指定自定义操作。

步骤 4 从**组 (Groups)** 下拉列表中，选择要映射到此服务的组。

预定义组（例如 EPS 和 ANC）和手动添加的组列在此下拉列表中。

步骤 5 点击**提交 (Submit)**。

启用 pxGrid 服务

开始之前

- 至少在一个节点上启用 pxGrid 角色，以查看Cisco pxGrid 客户端发送的请求。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **pxGrid 服务 (pxGrid Services)**。

步骤 2 选中该客户端旁边的复选框，然后点击**通过 (Approve)**。

步骤 3 点击**刷新 (Refresh)** 查看最新的状态。

步骤 4 选择要启用的功能，并点击**启用 (Enable)**。

步骤 5 点击**刷新 (Refresh)** 查看最新的状态。

pxGrid 诊断

- XMPP：**管理 (Administration) > pxGrid 服务 (pxGrid Services) > 诊断 (Diagnostics) > XMPP** 页面列出了外部和内部 pxGrid 1.0 客户端。此外还列出了功能。
- Websocket：**管理 (Administration) > pxGrid 服务 (pxGrid Services) > 诊断 (Diagnostics) > Websocket** 页面列出了外部和内部 pxGrid 2.0 客户端。它还列出了可用 pxGrid 2.0 主题，以及发布或订阅每个主题的客户端。
- 日志：**管理 (Administration) > pxGrid 服务 (pxGrid Services) > 诊断 (Diagnostics) > 实时日志 (Live Logs)** 页面列出了管理事件。
- 测试：在**管理 (Administration) > pxGrid 服务 (pxGrid Services) > 诊断 (Diagnostics) > 测试 (Tests)** 页面上，运行状况监控测试将验证客户端能否访问会话目录服务。点击**开始测试 (Start Test)** 按钮时，我们将创建一个内部 pxGrid 2.0 客户端。此客户端会查询批量会话下载 REST API，然后订阅会话主题。它侦听该主题几分钟，然后终止。测试完成后，可以显示测试活动的日志。

pxGrid 设置

- **自动批准新的基于证书的帐户 (Automatically approve new certificate-based accounts)**：默认情况下关闭，可以让您控制与 pxGrid 服务器的连接。仅当您信任环境中的所有客户端时，才选中此设置。
- **允许创建基于密码的帐户 (Allow password based account creation)**：选中此复选框可为 pxGrid 客户端启用基于用户名/密码的身份验证。如果启用此选项，系统不会自动批准 pxGrid 客户端。

生成思科 pxGrid 证书

开始之前

某些版本的Cisco ISE 具有使用 NetscapeCertType 的Cisco pxGrid 证书。建议您生成新证书。

- 要执行以下任务，您必须是超级管理员或系统管理员。
- 必须从主 PAN 生成Cisco pxGrid 证书。
- 如果Cisco pxGrid 证书使用了使用者替代名称 (SAN) 扩展名，请确保将使用者身份的 FQDN 包含为 DNS 名称条目。
- 创建使用数字签名用法的证书模板，并使用该模板生成新的Cisco pxGrid 证书。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **pxGrid 服务 (pxGrid Services)** > **客户端管理 (Client Management)** > **证书 (Certificates)**。

步骤 2 从**我想 (I want to)** 下拉列表中选择以下选项之一：

- **生成无证书签名请求的单个证书 (Generate a single certificate without a certificate signing request)**：如果选择此选项，则必须输入通用名称 (CN)。
- **生成单个证书（带证书签名请求）Generate a single certificate (with a certificate signing request)**：如果选择此选项，则必须输入证书签名请求详细信息。
- **生成批量证书 (Generate bulk certificates)**：可以上传包含所需详细信息的 CSV 文件。
- **下载根证书链 (Download Root Certificate Chain)**：下载根证书，并将其添加到受信任证书存储区。必须指定主机名和证书的下载格式。

步骤 3 **通用名称 (CN) (Common Name (CN))**：（如果选择**生成单个证书（无证书签名请求）(Generate a single certificate (without a certificate signing request))** 选项，则必须选择此选项。）输入 pxGrid 客户端的 FQDN。

步骤 4 **证书签名请求详细信息 (Certificate Signing Request Details)**：（如果选择**生成单个证书（无证书签名请求）(Generate a single certificate (without a certificate signing request))** 选项，则必须选择此选项。）输入完整的证书签名请求详细信息。

步骤 5 **说明**：（可选）可以输入此证书的说明。

步骤 6 **证书模板 (Certificate Template)**：点击 **pxGrig_Certificate_Template** 链接可下载证书模板，并根据您的要求进行编辑。

步骤 7 **使用者备用名称 (SAN) (Subject Alternative Name (SAN))**：可以添加多个 SAN。可提供以下选项：

- **IP 地址 (IP address)**：输入要与证书关联的Cisco pxGrid 客户端的 IP 地址。
- **FQDN**：输入 pxGrid 客户端的完全限定域名。

注释　如果选定**生成批量证书 (Generate Bulk Certificate)** 选项，则不会显示此字段。

步骤 8 从**证书下载格式 (Certificate Download Format)** 下拉列表中选择以下选项之一：

- **加强隐私电子邮件 (PEM) 格式的证书和 PKCS8 PEM 格式的密钥（包括证书链）(Certificate in Private Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain))**：根证书、CA 中间证书和终端实体证书均采用 PEM 格式。PEM 格式的证书是采用 BASE64 编码的 ASCII 文件。每个证书的开头采用“-------证书开始 (BEGIN CERTIFICATE) -----”标签，结尾采用“-----证书结束 (END CERTIFICATE) ----”标签。终端实体的私钥使用 PKCS* PEM 存储。其开头采用“-----加密私钥开始 (BEGIN ENCRYPTED PRIVATE KEY) ----”标签，结尾采用“-----加密私钥结束 (END ENCRYPTED PRIVATE KEY) ----”标签。
- **PKCS12 格式（包括证书链；证书链和密钥的文件）(PKCS12 format (including certificate chain; one file for both the certificate chain and key))**：CA 根证书、CA 中间证书以及终端实体的证书和私钥存储在一个加密文件时，所采用的二进制格式。

步骤 9 **证书密码 (Certificate Password)**：输入证书的密码，并在下一字段中再次输入以确认密码。

步骤 10 点击**创建 (Create)**。

您创建的证书在Cisco ISE 的**已颁发证书 (Issued Certificates)** 窗口中可见。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书颁发机构 (Certificate Authority)** > **已颁发证书 (Issued Certificates)**。证书也会下载到浏览器的“下载”目录中。

注释 从Cisco ISE 2.4 补丁 13 开始，pxGrid 服务的证书要求变得更加严格。如果您使用Cisco ISE 默认自签名证书作为 pxGrid 证书，则Cisco ISE 可能会在应用Cisco ISE 2.4 补丁 13 或更高版本后拒绝此证书。这是因为此证书的旧版本具有指定为 **SSL 服务器 (SSL Server)** 的 **Netscape 证书类型 (Netscape Cert Type)** 扩展，此扩展现在会失败（现在还需要客户端证书）。

任何具有不合规证书的客户端都无法与Cisco ISE 集成。使用内部 CA 颁发的证书或生成具有正确使用扩展名的新证书：

- 证书中的**密钥使用 (Key Usage)** 扩展必须包含**数字签名 (Digital Signature)** 和**密钥加密 (Key Encipherment)** 字段。
- 证书中的**扩展密钥使用 (Extended Key Usage)** 扩展必须包含**客户端身份验证 (Client Authentication)** 和**服务器身份验证 (Server Authentication)** 字段。
- 不需要 **Netscape 证书类型 (Netscape Certificate Type)** 扩展。如果要包含此扩展，则必须在扩展中同时添加 **SSL 客户端 (SSL Client)** 和 **SSL 服务器 (SSL Server)**。
- 如果使用的是自签名证书，则**基本约束 CA (Basic Constraints CA)** 字段必须设置为 True，并且**密钥使用 (Key Usage)** 扩展必须包含**密钥证书签名 (Key Cert Sign)** 字段。