pxGrid

思科 pxGrid 节点

可以使用思科 pxGrid 与其他网络系统（例如思科 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) 来隔离用户和/或设备以应对网络或安全事件。可通过思科 TrustSec 主题将标签定义、值和说明等思科 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。

可通过思科 pxGrid 发布和订用 SXP 绑定（IP-SGT 映射）。有关 SXP 绑定的详细信息，请参阅安全组标记交换协议。

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 关闭时，思科 pxGrid 服务器会停止处理客户端注册和订用。需要手动升级 PAN，以激活思科 pxGrid 服务器。可以查看**思科 pxGrid 服务 (Cisco pxGrid Services)** 窗口（**管理(Administration)** > **pxGrid 服务 (pxGrid Services)**）以验证思科 pxGrid 节点当前处于主用状态还是备用状态。

在具有 pxGrid 角色的活动思科节点上，这些进程会显示为**正在运行 (Running)**。在备用思科 pxGrid 节点上，它们会显示为**备用 (Standby)**。如果活动 pxGrid 节点关闭，备用 pxGrid 节点会检测到此情况，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)**，备用节点成为活动节点。可以运行 CLI 命令 **show logging application pxgrid/pxgrid.state** 来验证思科 pxGrid 服务在此节点上是否处于备用状态。

对于 XMPP（可扩展消息传送和在线状态协议）客户端，思科 pxGrid 节点在活动-备用高可用性模式下工作，这意味着思科 pxGrid 服务在活动节点上处于**正在运行 (Running)** 状态，在备用节点上处于**已禁用 (Disabled)** 状态。

注释 在高可用性的思科 ISE 部署中，在活动-备用设置中工作的 pxGrid 角色节点显示，pxGrid 服务在活动节点上处于**正在运行 (running)** 状态，在备用节点上处于 **备用 (standby)** 状态。

要验证思科 ISE 节点上 pxGrid 服务的状态，请使用以下 CLI 命令：

```
show logging application pxgrid/pxgrid.state
```

启动面向辅助思科pxGrid节点的自动故障转移后，如果原始主思科pxGrid节点重新接入网络，则除非当前主节点关闭，否则原始主思科 pxGrid 节点将继续具有辅助角色，并且不会重新升级到主角色。

注释 有时，原始主思科 pxGrid 节点可能会自动重新升级回主角色。

在高可用性部署中，当主 pxGrid 节点关闭时，可能需要大约 3 到 5 分钟来切换到辅助 pxGrid 节点。我们建议客户端等待故障切换完成，然后再清除缓存数据，以防主思科 pxGrid 节点发生故障。

以下日志可用于思科 pxGrid 节点：

- pxgrid.log：状态变更通知。
- pxgrid-cm.log：有关客户端与服务器之间的发布者和/或用户以及数据交换活动的更新。
- pxgrid-controller.log：显示客户端功能、组和客户端授权的详细信息。
- pxgrid-jabberd.log：显示与系统状态和身份验证相关的所有日志。
- pxgrid-pubsub.log：显示与发布者和用户事件相关的所有信息。

注释 如果在节点上禁用思科 pxGrid 服务，则端口 5222 将关闭，但是端口 8910（由 Web 客户端使用）将正常工作，并将继续对请求作出响应。

注释 可以使用 Base 许可证启用思科 pxGrid，但必须使用 Plus 许可证才能启用思科 pxGrid 角色。此外，如果您最近安装了 的升级许可证，则某些扩展的思科 pxGrid 服务可能在基本安装中可用。

注释 应定义思科 pxGrid，以便使用被动 ID 工作中心。有关详细信息， 请参阅被动 ID 工作中心。

思科 pxGrid 客户端和功能管理

使用 Cisco pxGrid 服务之前，连接到思科 ISE 的客户端必须注册并获得帐户审批。Cisco pxGrid 客户端使用 Cisco pxGrid SDK 中提供的 Cisco pxGrid 客户端库成为客户端。思科 ISE 同时支持自动和手动批准。客户端可以使用唯一名称和基于证书的相互身份验证登录 Cisco pxGrid。类似于交换机上的 AAA 设置，客户端可以连接已配置的 Cisco pxGrid 服务器主机名或 IP 地址。

Cisco pxGrid 功能是指 Cisco pxGrid 上供客户端发布和订用的信息主题或信道。在思科 ISE 中，仅支持身份、自适应网络控制 (ANC) 和安全组访问 (SGA) 等功能。当客户端创建新功能时，它显示于**按功能查看 (View by Capabilities)** 窗口中。此窗口的导航路径为**管理 (Administration)** > **pxGrid 服务 (pxGrid Services)** > **按功能查看 (View by Capabilities)** 。您可以启用或禁用单个功能。可通过发布、定向查询或批量下载查询，从发布方获取功能信息。

当 Web 客户端发布者使用 REST API 或 WebSocket 协议时，Web 客户端发布者中添加的主题不会立即列在思科 ISE 的**管理 (Administration)** > **pxGrid 服务 (pxGrid Services)** > **Web 客户端 (Web Clients)** 选项卡中。此类 Web 客户端主题仅在它的第一个实例发布后才显示在 **Web 客户端 (Web Clients)** 选项卡中。

注释 分配到终端保护服务 (EPS) 用户组的用户可以在会话组中执行操作，因为思科 pxGrid 会话组是 EPS 组的一部分。如果用户被分配到 EPS 组，该用户将能够订阅 Cisco pxGrid 客户端上的会话组。

相关主题

生成思科 pxGrid 证书

启用 pxGrid 服务

开始之前

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

步骤 1 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 **Refresh** 查看最新的状态。

启用 pxGrid 功能

开始之前

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

步骤 1 选择**管理 (Administration)** > **pxGrid 服务 (pxGrid Services)**。

步骤 2 点击右上角的**根据功能查看 (View by Capabilities)** 。

步骤 3 选择要启用的功能，并点击**启用 (Enable)**。

步骤 4 点击 **Refresh** 查看最新的状态。

部署思科 pxGrid 节点

在独立节点和分布式部署节点上都可以启用思科 pxGrid 角色。

开始之前

- 可以使用 Base 许可证启用 pxGrid，但必须使用 Plus 许可证才能启用 pxGrid 角色。此外，如果最近安装了升级许可证 ，则某些扩展的 pxGrid 服务可能会在基本安装中可用。
- 所有节点都将 CA 证书用于思科 pxGrid 服务用途。如果在升级之前对思科 pxGrid 服务使用默认证书，则升级时会将该证书替换为内部 CA 证书。
- 必须为 Websocket (pxGrid 2.0) 打开端口 8910，并为 XMPP (pxGrid V1.0) 打开端口 5222。如果在节点上禁用思科 pxGrid 服务，则端口 5222 将关闭，但是端口 8910 仍正常工作，并继续响应请求。

步骤 1 选择**管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 2 在**部署节点 (Deployment Nodes)** 窗口中，选中要为其启用思科 pxGrid 服务的节点旁的复选框，然后点击**编辑 (Edit)**。

步骤 3 点击**常规设置 (General Settings)** 选项卡， 选中 **pxGrid** 复选框。

步骤 4 点击 **Save**。

当从以前的版本升级时，系统可能会禁用**保存 (Save)** 选项。当浏览器缓存引用以前版本的思科 ISE 中的旧文件时，就会发生这种情况。清除浏览器缓存以启用**保存 (Save)** 选项。

配置思科 pxGrid 设置

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择**管理 (Administration)** > **pxGrid 服务 (pxGrid Services)** > **设置 (Settings)**。

步骤 2 根据您的要求选中以下复选框之一：

- **自动审批新的基于证书的帐户 (Automatically approve new certificate-based accounts)**：选中此复选框可自动批准来自新思科 pxGrid 客户端的连接请求。
- **允许创建基于密码的帐户 (Allow password-based account creation)**：选中此复选框可为思科 pxGrid 客户端启用基于用户名或密码的身份验证。如果启用了此选项，则无法自动批准思科 pxGrid 客户端。

步骤 3 点击**保存**。

使用思科 pxGrid 的**设置 (Settings)** 窗口中的**测试 (Test)** 选项来对思科 pxGrid 节点执行运行状况检查。在 pxgrid 或 pxgrid-test.log 文件中查看详细信息。

生成思科 pxGrid 证书

开始之前

- 某些版本的思科 ISE 具有使用 NetscapeCertType 的思科 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 生成思科 pxGrid 证书。
- 如果思科 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思科 pxGrid 证书。

步骤 1 选择**管理 (Administration)** > **pxGrid 服务 (pxGrid Services)** > **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）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思科 pxGrid 客户端的 IP 地址。
- **FQDN**：输入 pxGrid 客户端的 FQDN。

注释　如果选择**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 单击**创建**。

您创建的证书在思科 ISE 的**已颁发证书 (Issued Certificates)** 窗口中可见。

步骤 11 此页面的导航路径为：**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书颁发机构 (Certificate Authority)** > **已颁发的证书 (Issued Certificates)**

步骤 12 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)** > **已颁发的证书 (Issued Certificates)**

注释　从思科 ISE 2.4 补丁 13 开始，pxGrid 服务的证书要求变得更加严格。如果您使用思科 ISE 默认自签名证书作为 pxGrid 证书，则思科 ISE 可能会在应用思科 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思科 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**密钥用法 (Key Usage)** 扩展名必须包含**数字签名 (Digital Signature)** 和**密钥加密 (Key Encipherment)** 字段。
- 证书中的**扩展密钥用法 (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**密钥用法 (Key Usage)** 扩展必须包含**密钥证书签名 (Key Cert Sign)** 字段。

. 证书也会下载到浏览器的“下载”目录中。

控制思科 pxGrid 客户端的权限

您可以创建 Cisco pxGrid 授权规则来控制 Cisco pxGrid 客户端的权限。使用这些规则可控制提供给 Cisco pxGrid 客户端的服务。

您可以创建不同类型的组，并将提供给 Cisco pxGrid 客户端的服务映射到这些组。使用**权限 (Permissions)** 窗口中的**管理组 (Manage Groups)** 选项可添加新组。您可以在“权限 (Permissions)”窗口中查看使用预定义组（如EPS和ANC）的预定义授权规则。请注意，只能更新预定义规则的**操作 (Operations)** 字段。

要为 pxGrid 客户端创建授权规则，请执行以下操作：

步骤 1 选择**管理 (Administration)** > **pxGrid 服务 (pxGrid Services)** > **权限 (Permissions)**。

步骤 2 从**服务 (Service)** 下拉列表中，选择以下选项之一：

- **com.cisco.ise.pubsub**
- **com.cisco.ise.config.anc**
- **com.cisco.ise.config.profiler**
- **com.cisco.ise.config.trustsec**
- **com.cisco.ise.service**
- **com.cisco.ise.system**
- **com.cisco.ise.radius**
- **com.cisco.ise.sxp**
- **com.cisco.ise.trustsec**

- **com.cisco.ise.mdm**

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>**

  注释 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（如 EPS 和 ANC）和手动添加的组列在此下拉列表中。

思科 pxGrid 实时日志

“实时日志”(Live Logs) 窗口会显示所有 pxGrid 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。

此窗口的导航路径为**管理 (Administration)** > **pxGrid 服务 (pxGrid Services)** > **实时日志 (Live Log)**。您还可以清除日志并重新同步或刷新列表。