安全加社区

公益译文项目

2017

TAXII 服务规范

V1.1

Mark Davidson，Charles Schmidt

2014 年 1 月 13 日

MITRE

《指标信息的可信自动化交换》（TAXII™）定义了有关各方通过网络交换结构化网络威胁信息的机制。本文描述了 TAXII 的功能、服务、消息及消息交换。

文档信息			
原文名称	The TAXII Services Specification		
原文作者	Mark Davidson, Charles Schmidt	原文发布日期	2014 年 1 月 13 日
作者简介			
原文发布单位	MITRE 公司		
原文出处			
译者	小蜜蜂公益翻译组	校对者	小蜜蜂公益翻译组

“安全加”社区　　小蜜蜂公益翻译组

目录

商标信息

反馈

欢迎在社区注册页面（http://taxii.mitre.org/community/registration.html）注册后，就本文及其他 TAXII 规范提供反馈并将反馈发至 taxii-discussion-list@lists.mitre.org。您也可以直接将反馈发至 MITRE 邮箱 taxii@mitre.org。
若有任何意见、问题、建议，敬请反馈。

1 引言

本文规范了 TAXII 服务、消息及消息交换，提出的要求适用于所有的 TAXII 消息绑定及协议绑定。建议读者先阅读《TAXII 概述》[1]，了解各 TAXII 规范之间的关系。

1.1 TAXII 服务规范

本规范为 TAXII 服务、消息及消息交换提供了标准化文本。TAXII 消息的传输方法在《协议绑定规范》中进行了规定，这里并未详述。同样，TAXII 消息的格式在《消息绑定规范》中进行了规定，本文仅就其内容做了描述。

1.1.1 TAXII 服务版本 ID

就本文所述 TAXII 版本，对应的 TAXII 服务版本 ID 为：

urn:taxii.mitre.org:services:1.1

此版本 ID 及其他 TAXII 版本 ID 字符串的具体含义见 4.1.7 节。

1.2 文档约定

本文档中的关键用词“必须（或“须”）”、“不可以”、“要求”、“应”、“不得”、“应该”、“不应”、“建议”、“可以（或“可能”、“可”）”及“可选”的含义与国际互联网工程任务组（IETF）的 RFC 2119 的规定一致 [2]。

1.3 术语及定义

本节定义了 TAXII 规范中具有特定含义的术语。

1.3.1 TAXII 概念

下列术语在各 TAXII 规范中反复出现，本文围绕 TAXII 定义对这些术语进行了阐释：

网络威胁信息（Cyber Threat Information） – 指对于分析或响应网络威胁的人来说有意义的任何信息，包括但不限于恶意软件信息、威胁源起方、攻击行动、网络安全事件、威胁对应的可观察物以及与网络威胁细节相关的其他信息。

TAXII 数据集合（TAXII Data Collection） – 指可通过 TAXII 进行交换的结构化网络威胁信息集合。每个 TAXII 数据集合被分配一个唯一标识名称，以和来自相同网络威胁信息源的其他集合区分开来。有关 TAXII 数据集合名的更多信息，详见 4.1.2 节。存在两种 TAXII 数据集合： TAXII 数据 Feed 与 TAXII 数据集（TAXII Data Set）。

TAXII 数据 Feed– 指有序 TAXII 集合。在 TAXII 数据 Feed 中，为每个内容分配一个时间戳标签，对记录进行排序。TAXII 数据 Feed 经过组织后，用户可请求其部分内容（如，“提供上次请求完成后产生的所有内容”）。

TAXII 数据集 – 指无序 TAXII 集合。

TAXII 内容 – 指结构化网络威胁信息。TAXII 内容被视为最小颗粒，因为 TAXII 不支持将一个内容拆分发送（但是，若不允许接收方查看某一内容的部分内容，这些内容在传送前可删除）。

时间戳标签 – 指分配给 TAXII 数据 Feed 中每个内容、以时间戳形式存在的标签。有关时间戳标签的更多内容，详见 4.1.4 节。

TAXII 消息 – 指通过网络在实体之间传递的不连续信息块。

TAXII 消息交换（TAXII Message Exchange） – 指双方按规定顺序交换的信息，一般以请求和响应的形式存在。

TAXII 服务 – 指通过一次或多次 TAXII 消息交换所访问或调用的功能。TAXII 服务支持通过一次或多次消息交换提供功能。

TAXII 功能（TAXII Capability） – 指 TAXII 通过一项或多项 TAXII 服务所支持的抽象活动。

1.3.2 TAXII 角色

TAXII 角色指根据使用 TAXII 服务的总体目标所定义的 TAXII 参与者。

生产者 – 提供结构化网络威胁信息的实体（包括个人、组织、机构等）。

消费者 – 接收结构化网络威胁信息的实体。

注意，这些角色并非互斥，一个实体可以同时是结构化网络威胁信息的消费者和生产者。

1.3.3 TAXII 网络组件

使用典型客户端 / 服务器模型的 TAXII 实现所包含的组件定义如下：

TAXII 实现 – 指 TAXII 架构的具体实现。

TAXII 后台 –TAXII 实现中提供一项或多项 TAXII 服务的部分。要支持这个功能，TAXII 后台应通过网络持续监听是否发起了新的 TAXII 请求。

TAXII 客户端 –TAXII 实现中请求同远程 TAXII 后台进行交换的部分。TAXII 客户端无需维持网络长连接，当需要同 TAXII 后台交互时打开连接，交互结束时断开网络连接。

注意，TAXII 网络组件并不直接对应之前定义的 TAXII 角色。例如，某实体既可以运行 TAXII 后台，又可以作为 TAXII 消费者使用 TAXII 客户端。这里定义的网络组件是以网络为中心的 TAXII 参与者，而之前的角色是以活动为中心定义的。

1.4 与 TAXII 1.0 的不同之处

与 TAXII 1.0 相比，TAXII 1.1 做了如下改动：

- 在轮询请求与订阅请求中新增了基于内容的查询指令；
- 在之前有序的数据 Feed 基础上新增了无序数据集的概念；之前文档中使用的“数据 Feed”若同时适用于数据集和数据 Feed，在现有 TAXII 规范中统一称为“数据集合”；
- 收件箱消息（Inbox Message）可以请求将所含内容添加至接收方的一个或多个数据集合中；
- 可暂停与恢复当前订阅业务；
- 可请求记录计数、而不是接收完整记录列表；
- 对单个内容可提供普通文本消息；
- 生产者可描述与单个数据集合相关的内容数量；
- 扩展了消息 ID 的格式，新版本中可为任何 URI 格式字符串；
- 解决了混合使用时间戳标签包含与不包含范围的问题；
- 修复了几个问题，澄清了一些描述。

2 TAXII 服务

TAXII 服务指用以支持一个或多个 TAXII 功能的一整套机制。一个 TAXII 实现可支持多个或所有定义的 TAXII 服务，也可以不支持任何此类服务。（后一种情况下，用户无需运行 TAXII 后台用以支持 TAXII 服务，而仍可使用 TAXII 的某些功能。）

2.1 服务定义

本节定义了如下服务：

- 发现服务 – 提供现有 TAXII 服务的相关信息；
- 集合管理服务（Collection Management Service）– 支持对于 TAXII 数据集合订阅的管理；
- 收件服务（Inbox Service）– 支持生产者发起的网络威胁信息推送（也就是推送消息服务）；
- 轮询服务（Poll Service）– 支持消费者发起的网络威胁信息获取（也就是获取消息服务）。

下文就这些服务进行了详细讨论。

2.1.1 发现服务

发现服务机制提供 TAXII 服务是否可用及其使用情况等信息。发现服务为请求者提供一个 TAXII 服务清单以及这些服务的调用方法（即实现相关服务的 TAXII 后台的地址以及该后台所支持的绑定）。单个发现服务可从多个端点或甚至跨组织上报 TAXII 后台运行的 TAXII 服务，具体范围由发现服务所有者根据需要设置，但此种设置须符合法律规定、道德规范及其他相关要求。发现服务不需要提供其所检测到的所有服务信息，可基于多个因素决定向请求者（包括但不限于请求者的身份）提供哪些服务的信息。为了便于自动化，每个《TAXII 协议绑定规范》就发现服务推荐了默认地址。

发现服务实现必须支持 3.3 节定义的发现交换。

2.1.2 集合管理服务

集合管理服务作为一种机制，允许消费者请求获取 TAXII 数据集合信息、订阅 TAXII 数据集合、获取订阅状态信息或终止现有 TAXII 数据集合订阅。集合管理服务不发送 TAXII 数据集合内容（即生产者发布的与指定 TAXII 数据集合相关的威胁信息）。TAXII 数据集合内容可以通过生产者发起的交换流程发送给消费者的 TAXII 后台，通过后台实现收件服务，或者在消费者向生产者的轮询服务发送请求后直接发送给消费者。

订阅中可以包含查询，对推送和主动获取的数据集合内容进行限制，只传送符合条件的内容。

集合管理服务实现必须支持 3.4 和 3.5 节中定义的集合信息交换或订阅管理交换。

集合管理服务实现可以同时支持集合信息交换和订阅管理交换。

2.1.3 收件服务

收件服务机制允许消费者在生产者发起的交换流程中接收生产者的消息。消费者欲通过生产者发起的交换流程接收 TAXII 数据集合内容时可使用这项服务，这里所说的内容可以是消费者向生产者订阅的数据或生产者推送的数据。

收件服务实现必须支持 3.2 节定义的收件交换。

2.1.4 轮询服务

轮询服务机制中，生产者允许消费者发起请求，主动获取 TAXII 数据集合。消费者联系轮询服务，明确告知所需要的 TAXII 数据集合内容，这种请求可在消费者方便时随时发起。注意，在提供 TAXII 数据集合内容时，生产者可将其发起的推送到消费者收件服务的内容与消费者向生产者轮询服务请求的内容结合起来。

消费者在联系轮询服务时可设置查询条件，只接收符合条件的集合内容。

轮询服务实现必须支持 3.6 节定义的轮询交换。

轮询服务实现可支持 3.6.1 节定义的拆分轮询机制。所有的 TAXII 1.1 客户端在与轮询服务通信时必须支持拆分轮询机制。

2.2 服务实例

本规范频繁提及“服务实例”，一个服务实例指单个网络地址获取的由某个协议绑定承载的某一类 TAXII 服务。注意，这是对服务实例的书面定义，而并不是对于 TAXII 架构实现的要求。例如，某 TAXII 架构允许单个网络地址接收多种 TAXII 服务的消息，然而，TAXII 规范将此视为多个服务实例（每个实例指所支持的一种 TAXII 服务），尽管只有一个网络后台监听连接。重要的是记住 TAXII 消息使用类型 - 绑定 - 地址三元组记录服务，而实际的 TAXII 服务实现要灵活得多。

3 TAXII 消息交换

本章介绍了需要支持上文定义的 TAXII 服务的 TAXII 消息交换。这些交换仅考虑 TAXII 消息，不关注用以传输消息的网络协议，因为这些网络协议在传输 TAXII 消息之前可能会要求额外的网络交换（如 SSL/TLS 握手），或者将一个 TAXII 消息分割成多个部分单独传输。下文中的示意图表示的是 TAXII 消息传输与响应的概念性顺序。

交换中的方框与支持特定 TAXII 服务的 TAXII 后台（见“服务”一节中的描述）或 TAXII 客户端对应。注意，一个 TAXII 后台可能会实现多个 TAXII 服务。就此点而言，为了简化表达，我们将支持 ABC 服务的某 TAXII 后台称为“ABC 后台”，如，支持收件服务的 TAXII 后台就称为“收件后台”。

3.1 消息概述

TAXII 消息交换仅包含本规范所定义的 TAXII 消息（TAXII 消息的详细描述，见第 4 章）。本规范定义的 TAXII 消息归纳如下：

- TAXII 状态消息 – 用于指示错误状况，在某些交换中，是对收到消息的确认。
- TAXII 发现请求 – 请求获取所支持的 TAXII 服务的信息。
- TAXII 发现响应 – 对 TAXII 发现请求所回复的响应，其中包含所支持的 TAXII 服务信息。
- TAXII 集合信息请求 – 请求获取所支持的 TAXII 数据集合的信息。
- TAXII 集合信息响应 – 对 TAXII 集合信息请求所回复的响应，其中包含所支持的 TAXII 数据集合信息。
- TAXII 集合订阅管理请求 – 请求新建订阅或管理现有订阅。
- TAXII 集合订阅管理响应 – 对 TAXII 集合订阅管理请求所回复的响应，其中包含指定 TAXII 数据集合的新的订阅状态。
- TAXII 轮询请求 – 请求获取与 TAXII 数据集合相关的内容。
- TAXII 轮询响应 – 对 TAXII 轮询请求所回复的响应，其中包含 TAXII 数据集合相关内容。
- TAXII 收件箱消息 – 用以将内容推送至接收方。
- TAXII 轮询实现请求 – 请求获取延后提供的结果（如标为“待处理”状态的消息）或拆分结果的其他部分。

3.2 收件交换

在这个交换中，收件箱消息由 TAXII 客户端传输到处于监听状态的收件后台。收件箱消息可以是请求（如订阅服务在注册后发送消息给接收方）或非请求（如主动为接收方提供内容）的消息。收件后台可能有能力基于发送方身份认证结果过滤消息。

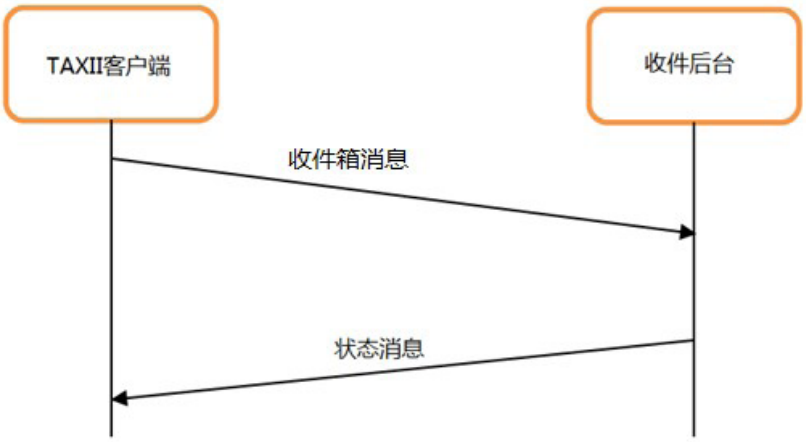

图 1 收件交换

在这个交换中，TAXII 客户端向收件后台发送收件箱消息。若检测到有错误使消息无法处理（如格式不正确的消息），收件后台必须回复相应的状态消息，说明交换失败。否则，收件后台会将收件箱消息及其相关信息传递给它的 TAXII 后端。TAXII 后台必须发送一条状态消息，作为对收件箱消息的回复，说明消息交换是否成功。注意，“成功”状态消息仅表示收件后台成功收到并解析了消息，且消息符合 TAXII 级要求（例如，包含内容绑定 ID、关联了正确权限等等）。接收方的 TAXII 后端可能仍会因各种原因丢弃内容，这种情况不会通知发送方。非“成功”状态消息提供接收消息和 / 或内容的错误信息。若返回了此类消息，收件箱消息接收方必须丢弃接收到的收件箱消息中的内容（也就是说，若 TAXII 客户端接收到非“成功”消息，会知道收件箱消息未成功接收）。有关状态消息支持的状态类型及其表示的条件，详见 4.4.1 节。

3.2.1 推送内容给 TAXII 数据集合

有时，推送内容的目的是需要接收方（作为 TAXII 生产者）将内容添加至一个或多个 TAXII 数据集合。例如，在辐射型架构中，交换参与者会将内容推送给交换中心的特定数据集合，交换中心然后自动将内容公开，供其他参与者使用。

TAXII 支持两种方法的自动化路由： 隐式与显式。隐式路由是指接收方配置自己的收件服务自动将收到的内容添加至一个或多个数据集合。发送方可通过收件服务描述及相关数据集合描述知晓这种配置，然后仅需将内容定向至相关的收件服务，不需要进行其他操作。采取显式路由的情况下，收件交换中的收件箱消息可指定一个或多个 TAXII 数据集合，这些集合由消息接收方操作，发送方可将内容添加至这些数据集合中。

应注意 TAXII 不会要求收件箱消息接收方将任何内容添加至数据集合中。在任何情况下，TAXII 总是允许接收方丢弃而不是添加内容。相关各方签订的具体共享协议可能会对操作有具体要求，但是 TAXII 并没有此类强制要求。

将内容推送至一个或多个数据集合的交换过程与上述收件交换过程一致。发送方的 TAXII 客户端发送收件箱消息至接收方的收件后台，收件后台会回复相应的状态消息。不过，无论使用的是隐式还是显式模式，推送内容给数据集合适用下述规则：

1. 若接收方的收件后台返回了非“成功”状态消息，收件箱消息中的所有内容必须丢弃。
2. 若返回了“成功”状态消息，仅表示接收方确认收到了内容。无论何时，接收方均可以视具体情况自主决定丢弃内容而不可以添加内容至数据集合。若所有内容均被丢弃，接收方可选择回复错误状态消息，说明丢弃原因，还可以回复“成功”状态消息，说明内容被接收并处理（此种处理的最终结果是内容被丢弃）。后一

种情况很重要，因为最终决定是添加内容至数据集合中，这只有在对所提供内容进行人工评审后才可以实现，而这时网络交换早已完成了。

3. 为了尽可能避免误解，推荐共享协议规定：在提供了目标集合名后只会将内容添加至这些指定集合中。这样，发送者就可以更好地控制如何使用显式方法推送内容。不过，TAXII 对此行为不做强制要求。

有关推送内容至指定数据集合的更多信息，详见 5.2.3 节。

3.3 发现交换

在这个交换中，TAXII 客户端请求获取特定方所提供 TAXII 服务的信息。发现后台收到请求后，回复 TAXII 服务清单。注意，发现后台不必将其检测到的所有 TAXII 服务提供给所有 TAXII 客户端。

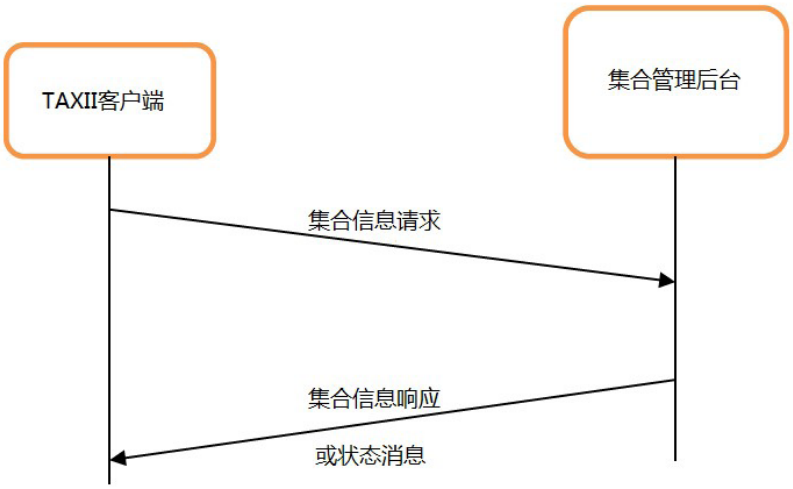

图 2 发现交换

在这个交换中，TAXII 客户端向发现后台发送发现请求。若检测到有错误使消息无法处理，发现后台必须回复相应的状态消息，说明交换失败。否则，发现后台会将相关信息传递给自己的 TAXII 后端。TAXII 后端基于这个信息以及自己的访问控制策略新建一个 TAXII 服务清单并返回，也可以决定不实现这个请求（例如，请求可能因为缺乏对请求方的验证而被拒绝）。若决定实现请求，则将 TAXII 服务清单打包至发现响应中，回复给 TAXII 客户端。（注意，若请求方没有查看服务的权限，则该清单可能为 0 字节。）TAXII 客户端收到消息，将信息传递给自己的 TAXII 后端处理。若因为某种原因没有回复发现响应，发现后台必须回复状态消息，说明原因。TAXII 状态消息的内容必须且只能是说明有错误发生或明示拒绝请求。

3.4 集合信息交换

在这个交换中，TAXII 客户端请求集合管理后台提供所支持的 TAXII 数据集合信息，集合管理后台随后回复 TAXII 数据集合清单。集合后台的响应由其 TAXII 后端控制，后者可能会考虑在响应中进行相应的访问控制。注意，集合管理后台不必将检测到的所有 TAXII 数据集合提供给所有的 TAXII 客户端。

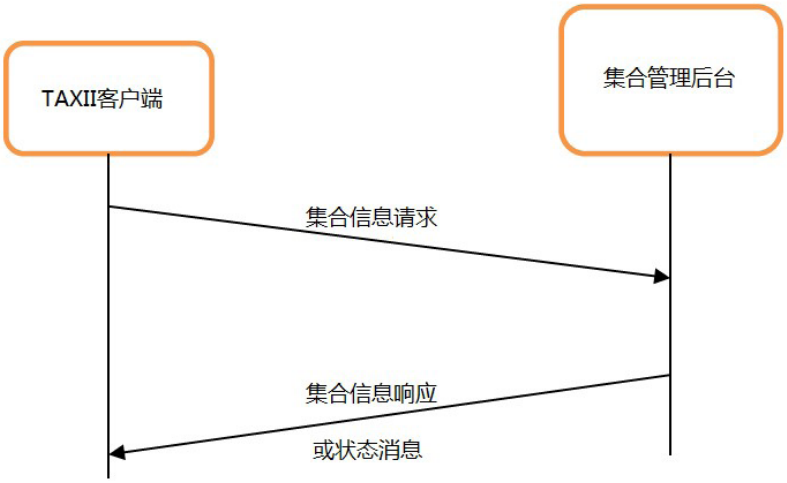

图 3 Feed 信息交换

在这个交换中，TAXII 客户端向集合管理后台发送集合信息请求。若检测到有错误使消息无法处理，集合管理后台必须回复相应的状态消息，说明交换失败。否则，集合管理后台会将相关信息传递给自己的 TAXII 后端。TAXII 后端基于这个信息以及自己的访问控制策略新建一个数据集合清单（长度可能为 0）并返回，也可以决定不实现这个请求。若决定实现请求，则将数据集合清单打包至集合信息响应中，回复给 TAXII 客户端。TAXII 客户端收到消息，将 TAXII 数据集合内容传递给自己的 TAXII 后端处理。若因为某种原因没有实现请求（如，未返回集合信息响应），集合管理后台必须回复状态消息，说明原因。TAXII 状态消息的内容必须且只能是说明有错误发生或明示拒绝请求。

3.5 订阅管理交换

在这个交换中，客户端发送集合订阅管理请求给集合管理后台，以新建订阅或更改现有订阅的状态。集合管理后台将请求传递给自己的 TAXII 后端，由其确定响应内容，最后响应返回给 TAXII 客户端。

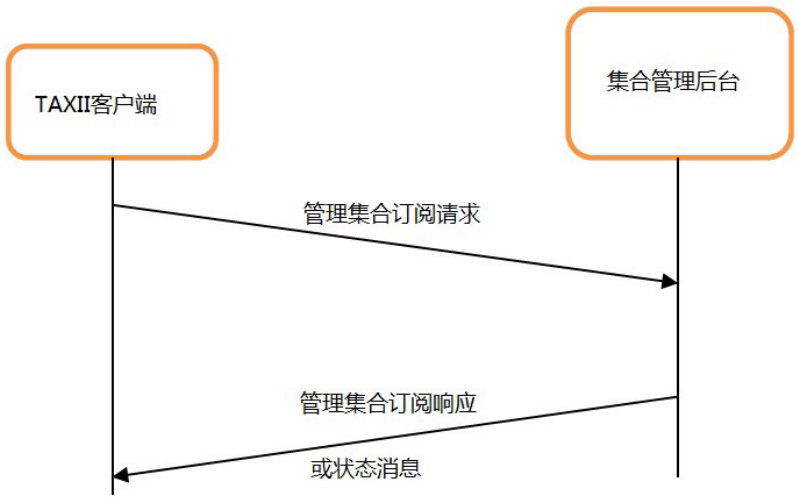

图 4 订阅管理交换

在这个交换中，TAXII 客户端向集合管理后台发送集合订阅管理请求。若检测到有错误使消息无法处理，集合管理后台必须回复相应的状态消息，说明交换失败。否则，集合后台会将相关信息传递给自己的 TAXII 后端。TAXII 后端基于这个信息以及自己的访问控制策略，确定是否允许订阅管理操作。若允许该请求，集合管理后台必须回复集合订阅管

理响应（即使这种行为并未改变订阅状态）。若拒绝该请求，集合管理后台必须回复状态消息，说明拒绝理由。TAXII 状态消息的内容必须且只能是说明有错误发生或明示拒绝请求。若返回了状态消息而非集合订阅管理响应，则最初的请求不可以更改订阅状态或增加订阅内容。

3.6 轮询交换

通过这个交换，消费者请求获得生产者的 TAXII 数据集合内容。轮询后台将请求传递给自己的 TAXII 后端，由其确定响应内容，最后响应返回给 TAXII 客户端。注意，轮询后台不必全盘提供所有请求的内容，可根据自己的策略剔除或修改任何内容。

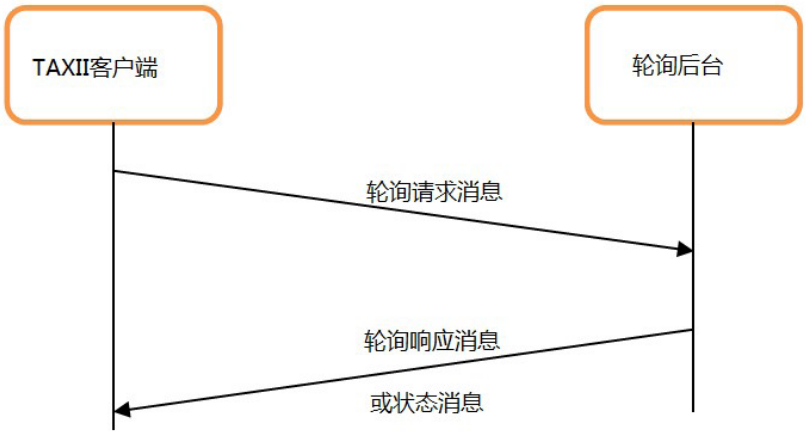

图 5 轮询交换

消费者的 TAXII 客户端向生产者的轮询后台发送轮询请求消息，发起交换。若检测到有错误使消息无法处理，轮询后台必须回复相应的状态消息，说明交换失败。否则，轮询后台会将相关信息传递给自己的 TAXII 后端。TAXII 后端评估这些信息，确定响应内容。若决定实现请求，则立刻作出相应回应，新建包含内容的轮询响应消息，将其返回给 TAXII 客户端。否则，轮询后台必须发送 TAXII 状态消息给客户端，说明拒绝理由，或者以异步形式提供结果（关于异步轮询，详见 3.6.2 节）。不管是哪种情况，TAXII 客户端收到消息，都会将信息传递给自己的 TAXII 后端处理，轮询后台不可以回复“成功”状态消息。

3.6.1 拆分轮询交换

有时，轮询请求获取到的内容太多，无法通过一条 TAXII 消息发送。数据生产者无论何时均可以拒绝发送这种内容，同时发送一条相应的 TAXII 错误状态信息。不过，有时生产者可能想要满足这种请求。这种情况下，就要用到拆分轮询交换，这种交换允许消费者通过多条消息接收轮询响应结果集。

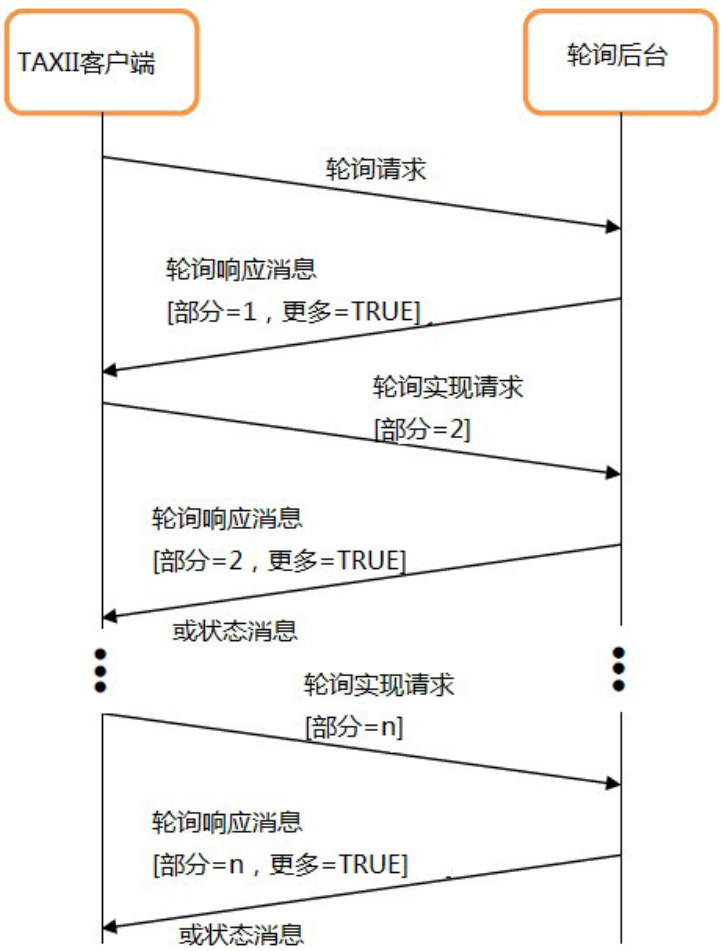

图 6 拆分轮询交换

和常规轮询交换一样，拆分轮询交换的第一步是消费者的 TAXII 客户端向生产者的轮询后台发送轮询请求（实际上，一开始，TAXII 客户端可能并不知道会进行拆分轮询交换）。这种情况下，不会返回错误消息（否则就是单纯的轮询交换了，这个交换中轮询后台会立即回复状态消息），轮询后台的 TAXII 后端开始收集要返回的内容。之后，轮询后台（或其后端）确定结果集太大，无法通过一条 TAXII 响应回复。随后，结果集被拆分成几部分，每部分可以单独通过轮询响应消息发送。拆分结果集时，记录必须保持完整（也就是说，拆分不应发生在记录中，而应发生在记录边界）。每部分分配一个序号，序号从 1 开始。接下来，新建结果集第一部分的轮询响应并返回至 TAXII 客户端。注意，轮询响应中，“更多”标志的值为“真”（TRUE），通知 TAXII 客户端还有更多结果要发送。此外，轮询响应消息中还包含结果 ID，以便消费者识别后续几部分结果。

TAXII 客户端发送包含结果 ID 和下一部分序号的轮询实现请求，以获取下一条结果。若轮询实现请求出错，轮询后台必须回复错误状态消息。否则，轮询后台必须回复轮询响应消息，其中含有轮询实现请求中指定的部分结果。一般情况下，TAXII 客户端会按序请求结果（2、3、4、5 等等），但也可以不按顺序请求任何一个有效结果（多数情况下，这是因为之前请求的这部分内容在传输中被损坏或没有成功发送，因而要求重新发送）。这个过程反复进行，直到 TAXII 客户端收到轮询响应消息，其中的“更多”标志被置为“假”（FALSE），表示没有更大序号的结果了。

注意，若 TAXII 后台针对某一特定轮询实现请求回复了错误状态消息，这并不一定意味着 TAXII 客户端就无法成功发送其他的轮询实现请求了。一般说来，若 TAXII 客户端造成轮询实现请求格式出错，不会要求全部请求重头来过，生产者应允许 TAXII 客户端更正错误，从断点继续请求结果。生产者可根据情况确定结果集的哪些部分已无法收集。

在所有这些交互中，TAXII 客户端从轮询后台收到相应的响应消息后，都会将信息传递给自己的 TAXII 后端处理。

3.6.2 异步轮询

除了直接响应或不响应，TAXII 支持“异步轮询”特性。当轮询请求接收方准备满足请求但无法或不会立即行动时，就需要进行异步轮询。例如，若汇编结果集需要花费数小时来查找未索引记录，生产者可选择利用异步轮询实现请求。

与常规轮询交换一样，异步轮询的第一步是 TAXII 客户端发送轮询请求。TAXII 客户端在轮询请求消息中设置“允许异步”属性，表示支持异步轮询（TAXII 客户端可能并不知道自己的轮询请求会要求异步处理，但是通过设置这一属性，表示愿意接受这种交换方式）。轮询后台收到并处理消息，这与常规轮询请求一样。之后，它判断自己无法立刻提供结果集，但是生产者希望提供结果集（若不想提供结果集，生产者会回复错误状态消息，交换终止，这就是一个常规轮询交换）。若条件满足，轮询后台回应“待处理”状态消息。这种消息应说明生产者预期何时提供结果、特定结果集 ID 以及如何将结果集提供给请求方。结果集可通过两种方式提供给请求方： 消费者可主动获取结果或生产者推送结果。下面分别介绍这两种方法。

3.6.2.1 主动获取异步轮询结果

收到“待处理”状态消息后，TAXII 客户端可随时发送轮询实现请求消息给轮询后台。轮询实现请求中包含“待处理”状态消息提供的 ID，用以标识所请求的结果集。

- 若轮询实现请求本身有错误，轮询后台必须回复相应的 TAXII 状态消息。若 TAXII 客户端更正了错误，重新发送了轮询实现请求，识别出的结果集还会提供给客户端。
- 若识别出的结果集已经不存在（例如，生成结果集时意外出错、没有对应 ID 的结果集等等），轮询后台必须回复“异步轮询错误”状态消息。
- 若没有出错，但是结果集未准备就绪，轮询后台必须回复“待处理”状态消息。这个状态消息中包含最新的预测结果到位时间以及上述其他信息。
- 若结果集准备就绪可以收集，轮询后台回复含有结果集的轮询响应消息。

  注意，若结果集极大，轮询响应消息会将“更多”字段置为“真”，这样，就进入到 3.6.1 节所述的拆分轮询交换，区别是 TAXII 客户端发送的第一条消息是轮询实现请求而不是轮询请求。

结果集收集完毕后，生产者根据情况确定保留多长时间。生产者可能限制结果集的访问权限，仅允许发出请求的消费者访问，但是也可以选择将结果集提供给任何人，只要知道对应的结果集 ID。（例如，若特定结果集对一个群体广泛使用，原始请求方可能会将结果集 ID 发布给其他人，允许这些人立即下载，而不是让每个人浪费大量时间发起相同的轮询请求，让生产者为每个人单独生成相同的结果集。）TAXII 两种情况均适用，不对任何一种情况做强制要求。

3.6.2.2 推送异步轮询结果

异步轮询结果集在准备就绪后也可以推送给请求方，这种形式需要消费者和生产者搭建更为复杂的架构。因此，不要求生产者和消费者支持这种方法，这个方法只有在双方明确同意情况下才会使用。

消费者若愿意接收推送结果，须在轮询请求消息中提供具体的收件服务信息以及联系方式。这种信息只在异步轮询场景下使用。消费者在发送轮询请求时可能并不知道请求需要通过异步方式实现，因此，在轮询请求中提供这个信息只是为了以防万一。（消费者可以这么表示：“若请求将以异步方式实现，请将结果推送到如下收件服务。”）

收到轮询请求后，轮询后台若确定该请求需要以异步方式实现，只会检查请求中用以识别收件服务的字段。只有满足了下列条件，生产者才会同意在结果集准备就绪之后，将其推送给指定收件服务：

1. 生产者愿意推送该异步结果集（生产者可因为任何原因拒绝推送）；
2. 轮询请求包含收件服务识别字段，以接收异步轮询结果（也就是说，消费者已表示愿意接收推送结果）；
3. 生产者有能力通过指定的协议和消息绑定将收件箱消息发送给指定收件服务。

若上述要求均已满足，生产者通过“待处理”状态消息（发送给 TAXII 客户端）中的一个参数表示愿意在结果集准备就绪后将其以异步方式推送。针对识别出的结果集，TAXII 客户端可能还会将轮询实现请求发送给轮询服务，通常这么做是为了更新自己预期的结果集准备时间。结果集准备完毕后，生产者使用常规收件交换将其发送给消费者指定的收件服务。若结果集太大，无法通过一个收件箱消息发送，则会拆分成多个部分（有关拆分轮询交换的详细内容，见 3.6.1 节），通过多个收件交换发送，每个收件箱消息包含结果集的一个部分（注意，这种情况下，不必为各部分分配序号）。

生产者可能会要求指定的收件服务用与原始轮询请求一样的身份进行认证，以防止恶意用户发送会产生超大结果集的轮询请求，之后再将结果集定向至其他人的收件服务，使其瘫痪。

4 TAXII 消息

本章对各种 TAXII 消息进行了定义，描述了其内容及用途。有些消息（如 TAXII 状态消息）用于多种消息交换中，而有些仅用在单一消息交换中。此处定义的消息仅指那些允许在 TAXII 消息交换中发送的消息。实现 TAXII 时，用户可自定义部分字段值，但不可以新建消息类型。

4.1 消息概念

本节对各种 TAXII 消息进行了定义，并介绍了相关信息。

4.1.1 消息 ID

每一个 TAXII 消息都有个“Message ID”字段，用以将请求与响应关联起来。具体说，若 TAXII 消息 B 为 TAXII 消息 A 的响应消息，则消息 B 必须包含“In Response To”字段，它的值为消息 A 的 ID。这样，消息 B 的接收者就知道接收到的消息是对哪个请求的回复。

若还未收到某请求消息的响应消息，消息发送方不可以复用该请求消息的 ID，以避免引起混乱，无法知晓响应消息对应的请求。

消息 ID 必须符合 URI 格式规范 [3]。

4.1.2 数据集合名

每个 TAXII 数据集合都有一个 ID，作为唯一标识，与生产者的其他 TAXII 数据集合区分开来。不同的生产者只要不共享集合管理或轮询服务，便可以使用相同的集合名。

消费者在自己的请求消息中用集合名作为句柄，指向生产者的 TAXII 数据集合。注意，集合名的唯一性只针对单个生产者，而并非全局唯一，因此，一个消费者可与多个生产者交互，在这种交互过程中，可能会见到两个不同 TAXII 数据集合具有相同的名称。所以，消费者需要同时跟踪集合名和相关生产者身份，两者结合则是全局唯一。

数据集合名必须符合 URI 格式规范 [3]。

4.1.3 订阅与结果 ID

TAXII 消费者可向 TAXII 生产者订阅 TAXII 数据集合。为了方便管理现有订阅，TAXII 定义了订阅 ID。消费者向生产者成功订阅后，生产者为该订阅分配 ID。接下来，消费者和生产者在消息中使用这个 ID 指代该订阅。若一个消费者两次订阅了同一 TAXII 数据集合，这两个订阅不可以使用相同的 ID。

同样，在某些情况下，轮询请求产生的结果集不会在轮询响应中返回（或不会完全返回）（详细信息，参见 3.6.1 和 3.6.2 节的“拆分轮询交换”和“异步轮询”）。这种情况下，生产者需要提供结果 ID 以识别后续交换中的结果集。注意，结果 ID 只在拆分轮询交换和异步轮询中需要，其他情况下，不必为结果集分配 ID。相同 TAXII 数据集合的两个不同结果集不可以使用相同的 ID。

订阅和结果 ID 必须符合 URI 格式规范 [3]。

4.1.4 时间戳标签

时间戳标签用于为 TAXII 数据 Feed 排序。时间戳标签为 TAXII 数据 Feed 提供索引，这样，就可以请求获得某一特定时间戳标签之前及 / 或之后的 TAXII 数据 Feed 内容。

TAXII 数据 Feed 中的每个内容都有一个时间戳标签。不同的内容不可以使用相同时间

戳标签，除非将其添加至相关 TAXII 数据 Feed 中且此种添加为最小粒度行为（这会防止出现如下竞争条件：请求方收到与某一时间戳标签相关的部分内容，但是漏掉了其他内容，因为在添加内容集时请求并未完全收到）。时间戳标签采用的是时间戳的形式。需要注意的是，时间戳标签不必与事件在时间上对应起来，也不必与 TAXII 数据 Feed 内容中出现的时间戳一致。时间戳标签仅仅是一个标签，而并不具有真正的时间含义。

时间戳标签必须符合下列规则：

1. 时间戳标签必须符合 IETF RFC 3339 定义的日期 - 时间构造 [4]。
2. TAXII 数据 Feed 中的每个内容都必须有一个时间戳标签。
3. 当有内容（或内容集）新增至 TAXII 数据 Feed 时，必须为该内容分配一个比这个 Feed 中其他内容要晚的时间戳标签。注意，必须坚持如下原则，即使生产者分配了其他时区的时间戳标签： 新的时间戳标签必须比 TAXII 数据 Feed 中已存在的其他时间戳标签要晚（换句话说，时间戳标签可以为一个 TAXII 数据 Feed 中的内容进行排序）。
4. 时间戳标签的小数秒可以精确到 0 到 6 位，不可以超过 6 位。TAXII 目前禁止时间戳标签含有超过 6 位的小数秒，但后端处理不应依赖这个规定，因为 TAXII 的后续版本可能会删除这个要求。

4.1.5 扩展头和详细状态名

所有的 TAXII 消息都支持使用扩展头，对 TAXII 消息进行扩展。

扩展头由成对的名称和值构成，扩展头的名称必须符合 URI 格式规范 [3]。为避免意外的名称冲突，扩展头名称应包含“Authority”，用于标识管理该扩展头含义的实体。

同样，TAXII 状态消息可以包含“详细状态”（Status Detail）字段，提供与指定的状态类型相关的机器可解析信息。“详细状态”字段由成对的名称和值构成，以清晰传达信息。扩展头的名称必须符合 URI 格式规范，应包含“Authority”，以避免名称冲突。

对扩展头的值与“详细状态”的值不做限制，可以包含任何字符，甚至是结构化内容。注意，《TAXII 消息绑定》可能会禁止包含某些字符或要求在 TAXII 消息中对值进行编码前将某些字符转义。具体的《TAXII 消息绑定》会有此等具体要求。

4.1.6 查询格式 ID

一些 TAXII 消息会包含查询表达，消费者可利用这样的查询表达设置条件，评估数据集合中的记录，符合条件的记录被视为“匹配”查询。TAXII 提供默认查询格式，但也允许第三方使用自己的查询格式。关于 TAXII 中的查询表达，详见 5.5 节。

TAXII 的每个查询格式均有一个识别 ID，这些 ID 必须全局唯一。为 TAXII 定义具体查询格式的人负责分配全局唯一 ID。所有的查询格式 ID 必须符合 URI 格式规范 [3]。所有诸如此类的 URI 必须包含“Authority”（即域名），表示对 ID 含义进行管理的实体。

4.1.7 版本 ID、内容绑定 ID 及内容绑定子类型 ID

本文所提到的 TAXII 版本 ID 具体指 TAXII 服务版本 ID、TAXII 协议绑定版本 ID、TAXII 查询格式 ID 及 TAXII 消息绑定版本 ID。

TAXII 版本 ID 用于某些 TAXII 消息中，表示特定版本的 TAXII 规范。每个 TAXII 规范有自己的版本 ID，标识不同的版本。版本 ID 可在 TAXII 消息中引用，以识别特定版本的 TAXII 及其绑定。

同样，内容绑定 ID 标识 TAXII 消息中各内容的格式及版本，可能会与内容绑定子类型 ID 同时出现。《TAXII 内容绑定参考》[5] 定义了标准的内容绑定 ID，并为所支持的核心内容类型定义了适用子类型 ID。内容绑定 ID 与内容绑定子类型 ID 可在 TAXII 消息中引用，标识 TAXII 消息所使用的特定内容类型。

除了 TAXII 规范中定义的版本 ID 与《TAXII 内容绑定参考》中定义的内容绑定 ID 与子类型 ID，第三方可定义自己的消息绑定版本 ID、协议绑定版本 ID 及内容绑定 ID 和子类型 ID，标识自定义消息绑定、自定义协议绑定以及《TAXII 内容绑定参考》中不包含的内容类型。第三方不可以定义其他 TAXII 服务版本 ID。

所有的版本 ID、内容绑定 ID 和内容绑定子类型 ID 必须符合 URI 格式规范 [3]。所有这些 ID 必须全局唯一，所有的 ID URI 必须包含 "Authority"（即域名），表示对 ID 含义进行管理的实体。

4.2 TAXII 消息表达规范

本节介绍了用以传达 TAXII 消息的数据模型，但并未对这种数据模型规定任何具体绑定，相关内容见《TAXII 内容绑定规范》。这里描述的是 TAXII 消息所传达的信息，而《TAXII 消息绑定规范》则规定了如何表达此种信息。因此，数据模型中的字段与数据绑定中的字段并不总是一一对应。例如，有些绑定可能要求用多个字段结构（如 XML[6] 绑定中的元素和属性）表达本文所述的单一字段的含义。一定要牢记，本节描述的是数据模型中的概念性字段，消息绑定遵循这些概念，但是考虑到特定绑定的局限性或功能，在结构上可能会有差异。实施 TAXII 时，需要查阅相应《TAXII 消息绑定规范》，了解具体的绑定要求与细节。

TAXII 消息包含两部分： 消息头与消息体。头部包含的信息与消息体类型相关，消息体包含的信息与特定消息类型相关。下文介绍了消息头与消息体类型的用途及其所包含的字段，每个字段均提供如下信息：

- 名称 –TAXII 规范用以指称该字段的句柄。这可能与出现在《TAXII 消息绑定规范》中的结构化字段名不完全一致（如 XML 元素或属性名）。由于功能的变化，TAXII 1.1 对 TAXII 1.0 中的部分字段进行了重新命名。这种情况下，TAXII 1.0 中的名称在 TAXII 1.1 中会放到括号里（如: “集合名【Feed 名】”意思是“集合名”在 TAXII 1.0 中被称为“Feed 名”）。在比较两种版本时，应同等对待这些不同名称。
- 是否必选 – 字段是否必须出现在消息中。多数情况下，缺失非必选字段表示没有对应值或字段与特定场景无关。不过，可选字段的缺失有时会有特定含义（即具有默认值），这会在字段描述中提及。
- 是否多个 – 字段具有唯一值还是多个值。
- 描述 – 描述字段对于消息发送方和接收方所表达的含义。

字段所属数据类型、字段使用的受控词汇定义等详细信息不在本文讨论之列，详见具体的《TAXII 消息绑定规范》。有些字段被记为具有“子字段”，仅为了方便表述，对其在特定绑定中的表达并无要求。针对特定子字段，“是否必选”与“是否多个”的值仅反映了其在父字段中的用途。例如，某个子字段可能不允许多个值，但是在父子段的每个实例中仍会出现，并具有唯一值。

4.3 TAXII 消息头

本节为 TAXII 消息头字段定义了概念模型。

表 1 TAXII 头字段

名称	是否必选	是否多个	描述
消息 ID（Message ID）	是	否	用以标识消息。
消息体类型（Message Body Type）	是	否	TAXII 消息的类型。本字段仅允许使用 4.4 节中定义的 TAXII 消息标识符（也就是说，第三方不可以自定义 TAXII 消息体类型）。
响应给（In Response To）	若为回复消息，则必选	否	提供本回复消息所对应请求消息的 ID（若适用）。
扩展头（Extended-Header）	否	是	第三方可以自定义其他的头字段。接收方未确认的“扩展头”字段应该忽略。有关“扩展头”字段的要求见 4.1.5 节。
签名（Signature）	否	否	提供 TAXII 消息的加密签名。签名范围为全部 TAXII 消息（即本字段所含签名可指示 TAXII 消息的全部或任意部分内容）。有关签名的表达方法，详见各具体《TAXII 消息绑定规范》。

4.4 TAXII 消息体

TAXII 消息体用于支持特定的 TAXII 消息交换。下文详述了各种 TAXII 消息体类型。

4.4.1 TAXII 状态消息

TAXII 状态消息用以指示是否成功或出错。状态消息总是由 TAXII 后台发送给 TAXII 客户端，作为对某 TAXII 消息的响应。TAXII 状态消息可表示在处理收到的 TAXII 消息时出现错误。错误出现的原因包括请求本身无效或接收方不愿或无法满足请求。状态消息也用于收件交换（见 3.2 节）中，表示成功收到收件箱消息，或出现在异步轮询（见 3.6.2 节）中，表示轮询请求会在稍后实现。

表 2 TAXII 状态消息字段

名称	是否必选	是否多个	描述
状态类型（Status Type）	是	否	指表 3 定义的某种状态类型或第三方定义的状态类型。
详细状态（Status Detail）	视状态类型而定	No	用机器可读格式提供的补充状态信息。本字段内容包括 0 或多个名称 / 值对（这些名称 / 值对在特定消息绑定中的构造方法详见相应的《TAXII 消息绑定规范》）。用状态类型表示子字段（若有）的标准名称和对应值，值可包括结构化内容。第三方可以自定义“详细状态”子字段。
消息（Message）	否	否	状态的补充信息。这些信息面向人类操作者，不一定是机器可读的。

报告错误的 TAXII 后台应在“消息”字段提供尽可能多的细节。表 3 列举了 TAXII 状态消息的状态类型。针对每种状态类型，明示了是否为其定义了“详细状态”名称 / 值对。

对于提供了“详细状态”名称 / 值对的状态类型，该类型的状态消息应提供“详细状态”字段及其所有已命名子字段。在少数实例中，必须提供规范的名称 / 值对，这在对应的状态类型描述中会特别说明。对任一种状态类型（包括第三方定义的类型），都可以提供补充的第三方名称 / 值对。每个《TAXII 消息绑定规范》对建议的对应“详细状态”名称 / 值的表达详细规定了构造方法。

表 3 TAXII 状态类型

状态类型	描述
成功（Success）	TAXII 后台解析了发送的消息，请求动作成功完成。注意，有些请求消息有对应的响应消息表示成功完成请求。这种情况下，必须使用该响应消息，而不能发送“成功”状态消息。 **详细状态名称** / **详细状态值** 无
异步轮询错误（Asynchronous Poll Error）	生产者在新建异步轮询结果集时发生意外错误（见 3.6.2 节）。因此，该结果集无法提供给消费者。 **详细状态名称** / **详细状态值** 无
错误消息（Bad Message）	TAXII 后台无法解析消息（如因为格式错误而无法解析）。 **详细状态名称** / **详细状态值** 无
拒绝（Denied）	TAXII 客户端动作因其他原因被拒绝，而并不是由于无法提供相应认证凭证。例如，集合管理服务可能会限制特定消费者新建订阅的数量。这样的话，若消费者试图创建过多订阅，TAXII 后台可能会发送“拒绝”状态消息。 **详细状态名称** / **详细状态值** 无
目标集合错误（Destination Collection Error）	收件箱消息里使用的“目标集合名”字段出现问题，原因如下： 收件箱消息接收方要求发送方提供目标集合名称，但收件箱消息不含此信息； 收件箱消息接收方禁止发送方规定目标集合名称，但是收件箱消息内含一个或多个“目标集合名”字段。 关于推送内容至数据集合的更多信息，详见 3.2.1 节。 **详细状态名称** / **详细状态值** 可接受目标 / 数据集合名称列表，允许发送者将内容发送给这些数据集合（其中有些数据集合可能因为其他原因拒绝特定内容）。若收件箱消息中禁止指定目标集合名称，则该字段为空。
失败（Failure）	轮询实现请求若要求特定“拆分结果编号”，而结果实际拆分的数量小于该编号，则会发送该状态。 “详细状态”字段必须包含下表所列名称 / 值对。 **详细状态名称** / **详细状态值** 最大拆分结果编号 / 拆分结果中的最大编号。
网络错误（Network Error）	TAXII 消息交换在网络层出错。多数情况下，网络层错误在消息传递到 TAXII 组件前出现，因此，可能会通过协议的本地错误消息通知发送者（如 HTTP 错误消息）。TAXII 消息发送方需能够正确处理此类本地协议错误，不应假设一定会使用这里的状态类型。当需要用 TAXII 方式描述网络错误时，可以使用这个状态类型。 **详细状态名称** / **详细状态值** 无
不存在（Not Found）	请求指定的目标（如 TAXII 数据集合名称）在 TAXII 后台不存在。 **详细状态名称** / **详细状态值** 项目 / TAXII 后台没有定位到的目标。
待处理（Pending）	轮询请求结果会稍后提供（而不是直接在轮询响应中提供）。主要用在如下情况：轮询请求所需处理时间超过了基础协议允许的范围，但是生产者仍想建立结果集提供给消费者。 “详细状态”字段必须包含下表所列名称 / 值对。 **详细状态名称** / **详细状态值** 预计等待时长 / 预期产生结果所需的时长（单位：秒），值为正整数。 结果 ID / 可用结果的 ID。 是否推送 / 若消费者提供了发送参数，生产者在结果准备就绪后将其推送至指定收件服务，则值为“真”；否则，值为“假”。
不支持轮询（Polling Not Supported）	请求方试图新建订阅，以轮询内容，但是相关 TAXII 数据集合无法通过轮询方式提供给请求方。 **详细状态名称** / **详细状态值** 无
重试（Retry）	当前无法实现请求，但可能稍后可以。所请求的操作只有在重新发送请求后才会进行。 **详细状态名称** / **详细状态值** 预计等待时长 / 预期成功进行请求重试所需的时长（单位：秒），值为正整数。

状态类型	描述
未授权（Unauthorized）	所请求的活动要求认证，但是 TAXII 客户端并未提供认证或认证身份并不具有相应访问权限（注意：认证凭证需在协议层而非 TAXII 消息中提供）。 **详细状态名称**：预计等待时长 **详细状态值**：预期成功进行请求重试所需的时长（单位：秒），值为正整数。
不支持的消息绑定（Unsupported Message Binding）	请求方指定了一系列消息绑定用于实现请求，但是所请求的操作并不支持这些绑定。 **详细状态名称**：支持的绑定 **详细状态值**：可接受的内容绑定 ID 列表，包括内容绑定子类型 ID（若适用）。
不支持的协议绑定（Unsupported Protocol Binding）	请求方指定了一系列协议绑定用于实现请求，但是所请求的操作并不支持这些绑定。 **详细状态名称**：支持的绑定 **详细状态值**：可接受的协议绑定 ID 列表
不支持的查询格式（Unsupported Query Format）	请求中包含查询表达，但是使用的是不支持的表达格式（或接收服务不支持查询）。 **详细状态名称**：支持的查询格式 **详细状态值**：可接受的查询格式 ID 列表。若服务不支持查询，则该字段为空。

4.4.1.1 第三方状态类型

第三方可定义其他状态类型表示错误状态，而不利用表 3 中的状态类型。第三方状态类型可用于表示某个特定的 TAXII 实现或用户组的错误状态。若接收方无法识别第三方状态类型，该状态类型应视为“失败”（Failure）。出于这个原因，第三方不可以定义其他状态类型表示非错误状态。

第三方定义的状态类型应符合 URI 格式规范 [3]。为避免意外名称冲突，第三方定义的状态类型应包含“authority”，指定管理该状态类型含义的实体。第三方不可以对表 3 中的标准状态类型作其他解释。

第三方定义的状态类型可利用“详细状态”字段，提供特定状态条件的机器可读信息。自定义状态类型者负责确定相应的“详细状态”的特性。

4.4.2 TAXII 发现请求

该消息发送至发现服务，请求所提供的 TAXII 服务的相关信息，包括提供怎样的 TAXII 服务、如何访问支持这些服务的 TAXII 后台以及所支持的协议和消息绑定。消息体为空。

4.4.3 TAXII 发现响应

若 TAXII 发现请求成功，发现服务将返回 TAXII 发现响应消息。若出错，则发送 TAXII 状态消息说明错误的原因。

表 4 TAXII 发现响应消息包含的字段

名称		是否必选	是否多个	描述
支持的查询		否	是	该字段表示服务支持特定格式的查询表达。该字段仅对集合管理服务或轮询服务有效。因此，对于其他服务类型，接收方应忽略该字段。“查询格式”子字段表示所支持的查询格式的类型。可能也会包含其他子字段并提供指定的查询格式相关的其他支持信息，这些参数将在指定的查询格式的定义中设定。有关“查询格式”的定义，请参见 5.5 节。该字段可存在多个实例，但每个实例须包含不同的“查询格式”值。若不包含该字段，表示指定的服务不支持查询表达。
	查询格式 ID	是	否	该字段指定具体的查询格式，表示“支持的查询”的格式。
	收件箱服务接受内容	否	是	该字段仅对收件服务有效。若为其他服务类型，接收方应忽略该字段。该字段指定收件服务所接受的内容绑定。每个收件服务接受内容必须为《TAXII 内容绑定参考》或第三方定义的内容绑定 ID。当服务类型为收件服务时，若不包含此字段，表示收件服务接受所有内容绑定。
	子类型	否	是	该字段表示指定内容绑定的内容绑定子类型。每个子类型都必须为《TAXII 内容绑定参考》或第三方定义的内容绑定子类型 ID。若不包含此字段，表示收件服务接受指定的内容绑定的所有子类型。
	可用	否	否	该字段表示是否允许请求方（已认证或未认证的）访问该 TAXII 服务。该字段的选项包括：请求方具备访问权限、不具备访问权限和访问权限未知。若不包含该字段，表明请求方的访问权限未知。
	消息	否	否	该字段包含该服务实例相关消息。该消息一般面向人类操作员，不要求机器可读。

每个服务实例记录表示特定 TAXII 后台运行的一个 TAXII 服务实例。2.2 节中提到，TAXII 规范中，一个服务实例对应一个服务类型，该服务类型包含一个协议绑定及该绑定的网络地址。根据这个定义，每个“服务实例”字段指定一个服务实例。一个服务实例可指定多个《TAXII 消息绑定规范》和多个内容绑定（若 TAXII 服务为收件服务）。

在一个服务实例记录中，每个消息绑定和内容绑定的组合都是应该可接受的。例如，若一个收件服务记录列出两个可接受的消息绑定（1 和 2）和三个可接受的内容绑定（A、B 和 C），则这两种绑定的六个组合（1A、1B、1C、2A、2B 和 2C）也被视为是可接受的。若一特定收件服务仅支持消息绑定和内容绑定的某些组合，则可为此服务创建多个服务实例记录，以避免错误地指定本不支持的组合。例如，若某个收件服务支持两个消息绑定（1 和 2）和三个内容绑定（A、B 和 C），但仅支持二者的某些组合，如 1A、1B、2B 和 2C，则该服务需由多个服务实例记录表示，即一个记录用于表示对消息绑定 1 和内容绑定 A 和 B 的支持，另一个记录用于表示对消息绑定 2 和内容绑定 B 和 C 的支持。这种情况仅在以下场景出现：收件服务的一个实例支持多个消息绑定和内容绑定，但仅支持这两种绑定的部分组合。

发现服务无需列出发现的全部现有 TAXII 服务。例如，某些 TAXII 服务可能仅发布给已认证的特定对象。因此，向发现服务发送发现请求后，不同请求方可能会收到不同响应。

4.4.4 TAXII 集合信息请求

此类请求消息发送给集合管理服务，用于请求有关可用的 TAXII 数据集合的信息。消息体为空。

4.4.5 TAXII 集合信息响应

此类响应消息是对 TAXII 集合信息请求成功后的响应。若出错，则发送 TAXII 状态消息说明错误原因。请注意，生产者无义务列出所有集合，可出于各种原因，在响应消息中剔除任何或全部集合。例如，生产者可能希望在集合列表中剔除为特定消费者创建的集合。这样，不同请求方向集合管理服务发送请求后可能收到不同的集合列表。

表 5 TAXII 集合信息响应包含的字段

名称	是否必选	是否多个	描述
集合信息 [Feed 信息]	否	是	该字段可能出现任意次（也可能省略），每次出现均表示一个不同的 TAXII 数据集合。该字段具有数个子字段。
集合名 [Feed 名称]	是	否	该字段指定 TAXII 数据集合的名称。
集合类型	否	否	该字段指定数据集合是数据 Feed（有序集合）还是数据集（无序集合）。若不包含该字段，表明该集合是一个数据 Feed。
集合描述 [Feed 描述]	是	否	该字段对 TAXII 数据集合进行平实的描述。并且，该字段说明了若需带外操作（如要求提供购买合同或人工审批），如何获取 TAXII 数据集合的访问权限。
集合数量	否	否	该字段表示通常每天向数据集合中添加的记录数量。该字段指定了一个常用值，生产者无义务确保数据集合的记录数量保持这一水平。
支持的内容	否	是	该字段指定内容绑定 ID，表明该 TAXII 数据集合中可包含哪些内容类型。每个支持的内容值必须为《TAXII 内容绑定参考》或第三方定义的内容绑定 ID。若不包含此字段，表示数据集合支持全部内容类型。
子类型	否	是	该字段表示所指定的支持内容绑定的内容绑定子类型。每个子类型均应为《TAXII 内容绑定参考》或第三方定义的内容绑定子类型 ID。若不包含此字段，表示数据集合支持特定的支持内容绑定的全部子类型。
可用	否	否	该字段表示是否允许请求方（已认证或未认证的）访问该集合（访问指可订阅和 / 或发送轮询请求）。该字段的选项包括：请求方具备访问权限、不具备访问权限和访问权限未知。若不包含该字段，表明请求方的访问权限未知。
推送方法	否	是	该字段指定采用何种协议推送订阅的数据集合内容和 / 或推送异步轮询结果。若 TAXII 数据集合中的内容可通过多个协议推送，该字段可能会出现多次。该字段有多个子字段。若不包含此字段，表示无法通过 TAXII 向消费者推送该数据集合中的内容。
订阅协议	是	否	该字段指定集合管理服务实例支持的协议绑定。该协议绑定必须为《TAXII 协议绑定规范》或第三方定义的 TAXII 协议绑定版本 ID。
订阅地址	是	否	该字段指定与运行集合管理服务实例的 TAXII 后台进行通信的地址。该字段应使用与订阅协议字段的值匹配的格式。
订购消息绑定	是	是	该字段指定集合管理服务实例支持的消息绑定。每个消息绑定必须为《TAXII 协议绑定规范》或第三方定义的 TAXII 消息绑定版本 ID。
接收收件服务	否	是	该字段指定收件服务的绑定和地址，内容推送至该收件服务后将被添加至指定数据集合。若多个收件服务可接收内容添加至 TAXII 数据集合，该字段可能出现多次。若不包含此字段，消费者无法通过 TAXII 消息请求只添加至特定数据集合中的内容。注意：接收方可能出于任何理由拒绝接受向该收件服务发送的内容，而不将其添加至特定数据集合。
收件协议	是	否	该字段指定收件服务实例支持的协议绑定。该协议绑定必须为《TAXII 协议绑定规范》或第三方定义的 TAXII 协议绑定版本 ID。
收件地址	是	否	该字段指定与运行收件服务实例的 TAXII 后台进行通信的地址。该字段的格式须与“收件协议”字段的值相匹配。
收件消息绑定	是	是	该字段指定收件服务实例支持的消息绑定。每个消息绑定均必须为《TAXII 协议绑定规范》或第三方定义的 TAXII 消息绑定版本 ID。
内容	否	是	该字段指定内容绑定 ID，表示指定的收件服务仅接受采用特定内容绑定的内容。每个支持的内容值必须为《TAXII 协议绑定规范》或第三方定义的内容绑定 ID。若不包含该字段，表示收件服务接受数据集合支持的所有内容绑定。
子类型	否	是	该字段表示指定的支持内容绑定的内容绑定子类型。每个子类型必须为《TAXII 协议绑定规范》或第三方定义的内容绑定子类型 ID。若不包含该字段，表示收件服务接受数据集合支持的特定的支持内容绑定的所有子类型。

4.4.6 TAXII 集合订阅管理请求

此类消息用于新建订阅或管理现有订阅。若请求成功且可实现，集合管理服务返回 TAXII 集合订阅管理响应；若请求被拒绝或出错，将返回 TAXII 状态消息。

表 6 TAXII 集合订阅管理请求包含的字段。

名称	是否必选	是否多个	描述
集合名 [Feed 名称]	是	否	该字段指定动作所针对的 TAXII 数据集合的名称。
动作	是	否	该字段指定采取的动作， 包括： • 订阅（SUBSCRIBE）：请求订阅指定的 TAXII 数据集合。 • 取消订阅（UNSUBSCRIBE）：请求取消订阅指定的 TAXII 数据集合。 • 暂停（PAUSE）：暂停指定订阅涉及内容的交付。 • 恢复（RESUME）：恢复指定订阅涉及内容的交付。 • 状态（STATUS）：请求提供请求方与指定的 TAXII 数据集合相关的订阅信息。对此动作响应时，订阅状态不变。
订阅 ID	视“动作”字段的值而定	否	该字段指定先前创建的订阅。若“动作”字段设置为“取消订阅”、“暂停”或“恢复”，此字段必选；若设置为“订阅”，该字段须忽略；若设置为“状态”，该字段可选。
订阅参数	仅在“动作”字段设置为“订阅”时必选。	否	该字段包含多个子字段，提供所请求订阅的各方面信息。只有在消息中的“动作”字段设置为“订阅”，该字段必选；若设置为其他值，该字段应被忽略。
响应类型	否	否	该字段表示订阅中的请求的响应类型， 包括： • 完整响应（FULL）：请求方要求响应消息包含完整内容。 • 仅计数（COUNT ONLY）：请求方要求订阅响应消息只包含计数信息（即不包含内容）。 若不包含此字段，表示请求返回完整响应。
内容绑定	否	是	该字段指定内容绑定 ID，表示消费者欲订阅的内容类型。可指定多个内容绑定 ID。该字段必须为《TAXII 内容绑定规范》或第三方定义的内容绑定 ID。若数据集合不支持列出的内容绑定值，应返回“不支持的内容绑定”（Unsupported Content Binding）状态消息。若不包含此字段，表示接受所有的内容绑定。
子类型	否	是	该字段表示指定内容绑定的内容绑定子类型。每个子类型必须为《TAXII 内容绑定规范》或第三方定义的内容绑定子类型 ID。若不包含此字段，表示接受指定的内容绑定的所有子类型。
查询	否	否	该字段指定订阅请求相关的查询表达。若订阅请求成功，订阅响应只包含查询表达匹配的内容。查询表达可以是结构化的，“查询格式”字段指定查询表达采用的特定结构。
查询格式	是	否	该字段指定具体的查询格式，用于标识“查询”字段指定的查询表达格式。
交付参数	否	否	该字段包含的参数适用于按订阅要求推送内容给消费者的情况。该字段仅在“行动”字段设置为“订阅”时有效。若设置为其他值，应忽略该字段。若“行动”字段为“订阅”时不包含此字段，表示请求方不请求推送内容，而是通过轮询服务查询订阅内容。在这种情况下，若 TAXII 数据集合不支持轮询，应返回“不支持轮询”（Polling Not Supported）状态消息。
收件协议	是	否	该字段指定具体协议，用于将 TAXII 数据集合内容推送至消费者的 TAXII 收件服务实现。若数据集合不支持指定的收件协议，应返回“不支持的协议绑定”（Unsupported Protocol Binding）状态消息。收件协议必须为《TAXII 协议绑定规范》或第三方定义的 TAXII 协议绑定版本 ID。
收件地址	是	否	该字段指定与运行邮箱服务的 TAXII 后台进行通信的地址，用于接收消费者所请求的 TAXII 数据集合的内容。该地址应为“收件协议”字段指定的网络协议所支持的类型。
交付消息绑定	是	否	该字段指定用于推送订阅内容的消息绑定。若 TAXII 数据集合不支持该字段，应返回“不支持的消息绑定”（Unsupported Message Binding）状态消息。该字段的值必须为《TAXII 消息绑定规范》或第三方定义的 TAXII 消息绑定版本 ID。

对于集合订阅管理请求，应依次按如下规范处理：

1. 管理需认证的订阅时，若请求方未进行合理认证，应返回相应的 TAXII 状态消息（一般是“未授权”（Unauthorized）），而不更改现有订阅。认证是订阅管理的首要限制条件。
2. 管理集合时，若请求的集合名与现有集合名不匹配，应返回相应的 TAXII 状态消息（一般为“不存在”），而不更改现有订阅。

3. 取消订阅时（“取消订阅”动作），若订阅 ID 与消费者指定的 TAXII 数据集合的现有订阅不匹配，则该请求应视为失败，返回 TAXII 集合订阅管理响应，而不更改现有订阅。换言之，通知请求方没有与此订阅 ID（尽管根本不存在该订阅 ID）匹配的订阅。
4. 新建订阅时（“订阅”动作），若不支持所请求的“收件协议”、“交付参数绑定”、“查询格式”或“内容绑定”（以及“子类型”，若有的话），应返回相应的 TAXII 状态消息（一般为“不支持的协议绑定”、“不支持的消息绑定”、“不支持的查询格式”或“不支持的内容绑定”），而不更改现有订阅。
5. 新建订阅时（“订阅”动作），若新订阅与现有订阅相同（如“集合名”、“订阅参数”和“交付参数”相同），应返回 TAXII 集合订阅管理响应，提供现有订阅的订阅 ID，而不更改现有订阅。换言之，集合管理服务不应重复创建相同订阅，但需告知消费者其所请求的订阅已存在。
6. 暂停订阅时，若该订阅之前已中止（“暂停”动作），应返回 TAXII 集合订阅管理响应（表明成功），而不更改现有订阅状态。同样，恢复订阅时（“恢复”动作），若该订阅当前并未处于中止状态，应返回 TAXII 集合订阅管理响应，而不更改现有订阅状态。换言之，用户暂停或恢复目前处于暂停或可用状态的订阅时，应让其感觉请求成功实现。
7. 暂停（“暂停”动作）或恢复（“恢复”动作）订阅或查看（即订阅 ID 值与请求方所指定的数据集合的现有订阅不匹配）订阅状态时，若订阅不存在，应返回“不存在”TAXII 状态信息。

4.4.6.1 “状态”动作

“状态”动作允许订阅用户检索其对某个数据集合的现有订阅的相关信息。若订阅用户因其记录已丢失不清楚目前有哪些订阅、订阅状态如何和 / 或配置如何，“状态”动作就显得非常有必要。

“状态”动作不会对集合管理服务管理的订阅进行修改。若包含“状态”动作的集合订阅管理请求未指定订阅 ID 值，表示查询集合管理服务管理的全部订阅（包括暂停和当前有效的订阅）的信息。若此类集合订阅管理请求包含订阅 ID 值，表示只查询该特定订阅的信息。对于以上两种状态请求，集合订阅管理响应消息均包含每个订阅的信息及其状态（通常原样列出包含“订阅”动作（新建了该订阅）的集合订阅管理请求的相关字段）。

4.4.7 TAXII 集合订阅管理响应

TAXII 集合管理请求消息中所请求的动作成功完成后，会返回 TAXII 集合订阅管理响应消息。

表 7 TAXII 集合订阅管理响应包含的字段

名称	是否必选	是否多个	描述
集合名 [Feed 名称]	是	否	该字段指定动作所针对的 TAXII 数据集合的名称。
消息	否	否	该字段指定订阅响应相关消息。该消息一般面向人类操作员，不要求机器可读。
订阅实例	视集合订阅管理请求中的“动作”字段的值而定	是	该字段列出请求方所请求的特定 TAXII 数据集合的现有订阅信息。针对“状态”动作的响应，该字段会出现多次（也可能不出现）；针对其他动作的响应，该字段只出现一次。
订阅 ID	是	否	该字段指定具体的订阅，用于在后续交换中引用特定订阅。
状态	否	否	该字段指定订阅状态。订阅状态包括： • 可用（Active）：订阅已创建且处于可用状态。 • 暂停（Paused）：订阅已创建但目前处于暂停状态。 • 取消订阅（Unsubscribed）：订阅已被移除（仅在针对“取消订阅”动作的响应中出现）。 若不包含此字段，则订阅状态为“可用”。
订阅参数	视集合订阅管理请求中“动作”字段的值而定	否	该字段与创建了该订阅的集合订阅管理请求消息中的订阅参数相同。针对“状态”动作的响应，该字段必选。针对其他动作的响应，该字段可选。
响应类型	否	否	这些字段与用于创建该订阅的集合订阅管理请求消息中的相关字段对应。这些字段只有在请求消息中存在时，才会出现在相应的响应消息中。
内容绑定	否	否	
子类型	否	否	
查询	否	否	
查询格式	否	否	
交付参数	否	否	该字段与用于创建该订阅的集合订阅管理请求消息中的交付参数（若有的话）相同。只有生产者为履行已创建的订阅而将内容推送至特定邮箱服务时，该字段才存在（跟当前订阅状态是否为“暂停”无关）。
收件协议	是	否	这些字段与用于创建该订阅的集合订阅管理请求消息中的相关字段对应。
收件地址	是	否	
交付消息绑定	是	否	
轮询实例	否	是	每个轮询实例均表示一个轮询服务的实例，用于检索特定订阅的相关内容。该字段的子字段表示特定订阅的轮询请求消息的目的地址。若存在多个轮询服务提供订阅内容，该字段可能会出现多次，即存在多个轮询实例。若不包含该字段，表示 TAXII 不支持通过轮询检索订阅内容。
轮询协议	是	否	该字段指定轮询服务实例支持的协议绑定。该字段的值必须为《TAXII 协议绑定规范》或第三方定义的 TAXII 协议绑定版本 ID。
轮询地址	是	否	该字段指定与运行轮询服务的 TAXII 后台进行通信的地址。该字段必须使用与“轮询协议”字段的值相匹配的格式。
轮询消息绑定	是	是	该字段指定与轮询服务实例交互时使用的一个或多个消息绑定。每个消息绑定必须为《TAXII 协议绑定规范》或第三方定义的 TAXII 消息绑定版本 ID。

4.4.8 TAXII 轮询请求

消费者向 TAXII 轮询服务发送此类消息，请求获得 TAXII 数据集合中的数据。轮询请求一般针对特定 TAXII 数据集合。至于消费者是否需创建订阅接收 TAXII 数据集合的内容，取决于生产者且因数据集合的不同而异。

表 8 TAXII 轮询请求包含的字段

名称	是否必选	是否多个	描述
集合名 [Feed 名称]	是	否	该字段指定轮询的 TAXII 数据集合的名称。
开始时间戳标签（不含）	否	否	该字段指定时间戳标签，表示请求方希望获取 TAXII 数据 Feed（即有序的 TAXII 数据集合）内容的起始时间。若指定的 TAXII 数据集合为数据集（即无序的 TAXII 数据集合），负责接收内容的 TAXII 轮询服务必须忽略该字段。时间戳范围不包含该字段的值，即请求方请求的是本字段表示的时间之后的内容。若不包含该字段，表示请求方对轮询的数据 Feed 不做开始时间限制。
结束时间戳标签（含）	否	否	该字段指定时间戳标签，表示请求方希望获取 TAXII 数据 Feed 内容的结束时间。若指定的 TAXII 数据集合为数据集，负责接收内容的 TAXII 轮询服务必须忽略该字段。时间戳范围包含该字段的值，即请求方请求的截至本字段表示的时间的内容。若不包含该字段，表示请求方不对轮询的数据 Feed 进行截止时间的限制。
订阅 ID	订阅 ID 和轮询参数，二者必选其一。	否	该字段指定消费者希望轮询的现有订阅。若轮询服务要求创建订阅进行轮询，但又不包含该字段，轮询服务应返回“拒绝”（Denied）TAXII 状态消息。
轮询参数		否	该字段包含多个子字段，指定通过轮询响应返回的内容。若提供订阅 ID，则不可以包含该字段；若提供订阅 ID，则利用订阅中的相应信息。
响应类型	否	否	该字段表示所请求的响应类型， 包括： • 完整响应（Full）：请求方要求响应消息包含完整内容。 • 仅计数（COUNT ONLY）：请求方要求订阅响应消息只包含计数信息（即不包含内容）。 若不包含此字段，表示请求返回完整响应。
内容绑定	否	是	该字段指定内容绑定 ID，表示消费者请求接收哪些类型的内容。可指定多个内容绑定 ID。该字段的值须为《TAXII 内容绑定参考》或第三方定义的内容绑定 ID。若数据集合不支持列出的内容绑定值，应返回“不支持的内容绑定”状态消息。若不包含此字段，表示接受所有内容绑定。
子类型	否	否	该字段表示指定内容绑定的内容绑定子类型。每个子类型均须为《TAXII 内容绑定参考》或第三方定义的内容绑定子类型 ID。若不包含此字段，表示接受指定的内容绑定的所有子类型。
查询	否	否	该字段指定查询表达。只有与指定的查询表达匹配的内容才通过响应消息发送。查询表达可能是结构化的，查询格式字段指定了查询表达采用的特定结构。
查询格式	是	否	该字段指定具体的查询格式，用于标识“查询”字段指定的查询表达格式。
允许异步	否	否	该字段表示消费者是否支持异步轮询。若该字段设置为“否”（FALSE），不可以返回状态类型为“待处理”（Pending）的状态消息。若不包含该字段，视为该字段的值为“否”。有关异步轮询的更多信息，请参见 3.6.2 节。
交付参数	否	否	该字段指定如何将异步轮询结果推送至轮询请求方指定的收件服务，前提是请求方希望提供此等推送服务。若“允许待处理”（Allow Pending）不存在或值为“否”（False），则请求中不可以包含此字段。若该参数不存在且“允许待处理”的值为“是”（TRUE），表示消费者将主动获取所有异步轮询结果，而不是被动接收所推送的此类结果。若轮询响应消息包含轮询结果，轮询服务会忽略此字段。（若忽略交付参数，不被支持的子字段的值不应导致错误状态消息。） 若轮询服务将异步轮询结果推送给消费者，也会忽略此字段。
收件协议	是	否	该字段指定具体协议，异步轮询结果推送至消费者的 TAXII 收件服务实现。该字段的值须为《TAXII 协议绑定规范》或第三方定义的 TAXII 协议绑定版本 ID。
收件地址	是	否	该字段指定可与运行收件服务的 TAXII 后台进行通信的地址，用于接收异步轮询结果。该地址应为“收件协议”字段指定的网络协议所支持的类型。
交付消息绑定	是	否	该字段指定用于推送异步轮询结果的消息绑定。该字段的值须为《TAXII 消息绑定规范》或第三方定义的 TAXII 消息绑定版本 ID。

轮询请求中可包含“交付参数”字段及其子字段以支持通过推送的消息实现异步轮询（详情参见 3.6.2.2 节）。鉴于此，轮询请求消息可包含“交付参数”，明确如何将准备好的异步轮询结果推送至请求方指定的收件服务。“交付参数”仅在以下条件均满足时使用:

1. 轮询服务支持异步轮询。
2. 轮询请求需要花费很长时间处理，有必要采取异步轮询方式。
3. 轮询服务愿意推送异步轮询结果。

只有在以上条件全部满足时，轮询服务才会根据这些字段的值进行操作；否则，忽略这些字段。需注意的是，即使不支持某些发送参数值也不应触发错误状态消息，除非以上三个条件均满足。

4.4.9 TAXII 轮询响应

TAXII 轮询响应是轮询服务针对 TAXII 轮询请求发送的响应。需注意的是，对于生产者提供的任何内容，响应中包含的内容在发送前可能会经生产者出于任何原因编辑或删除。因此，若两个消费者利用相同参数发起同一轮询服务，可能会收到不同的 TAXII 数据集合内容。

若指定的 TAXII 数据集合为 TAXII 数据 Feed，则请求执行时，TAXII 轮询响应指定 TAXII 数据 Feed 内容的时间范围。如上所述，可能会对某些消费者屏蔽内容，这样，轮询响应中的开始时间戳和结束时间戳字段指定生产者所考虑的时间戳范围，但该时间段的内容并不一定全部均包含在轮询响应消息中。一般，轮询响应中的时间戳范围与轮询请求中的一致，只是“无上限”（No Upper Bound）字段由生产者提供内容的最新时间戳替换。某些情况下，生产者提供的内容所处的时间段可能与请求中的不同，例如生成响应内容时，生产者仅考关注消费者所请求的时间段内的某段时间。

表 9 TAXII 轮询响应包含的字段

名称	是否必选	是否多个	描述
集合名 [Feed 名称]	是	否	该字段指定轮询的 TAXII 数据集合的名称。
订阅 ID	否	否	该字段指定具体订阅，为其提供内容。若不包含此字段，表示提供内容与现有 TAXII 数据集合订阅无关。
订阅 ID	视“动作”字段的值而定	否	该字段指定先前创建的订阅。若“动作”字段设置为“取消订阅”、“暂停”或“恢复”，此字段必选；若设置为“订阅”，该字段须忽略；若设置为“状态”，该字段可选。
开始时间戳标签（不含）	否。最多出现其中一个字段。	否	这两个字段的作用是相同的。保留“开始时间戳标签（不含）”字段是为了与 TAXII 1.0 兼容。因此，不建议使用此字段。这两个字段不可以在同一消息中同时出现。 这两个字段均指定时间戳标签，表示轮询响应消息覆盖的时间范围的开始时间，唯一区别为是否包含字段的值。若不包含这两个字段，表示轮询响应覆盖时间最早的 TAXII 数据 Feed。若指定的 TAXII 数据集合为数据集，则不可以包含这两个字段。
开始时间戳标签（含）		否	
结束时间戳标签（含）	仅在数据集合为 Feed 时必选，而在其他情况下不使用。	否	该字段指定一个时间戳标签，表示轮询响应覆盖的最晚时间。时间范围包含该字段的值。若指定的数据集合为数据 Feed，该字段必选；若指定的数据集合为数据集，不可以包含该字段。
更多	否	否	该字段指定一个布尔值。若该字段的值为“真”（TRUE），表示结果很大，后续还会提供其他部分。若该字段的值为“假”（FALSE），表示结果集中不存在更多的拆分结果。若不包含该字段，按照该字段为“假”时处理。
结果 ID	否	否	该字段指定具体结果，用于在轮询请求中标识结果集中的其他部分。若“更多”字段设置为“真”（TRUE），该字段必选。
拆分结果编号	否	否	该字段为一个整数，指定具体的拆分结果。对于拆分结果响应，会为每个部分分配一个序号，从 1 开始。因此，对于首个轮询请求的响应，该字段的值为 1。若不包含此字段，按照该字段的值为 1 时处理。
记录数量	否	否	该字段表示特定轮询请求的相关记录数量。该字段的值必须大于等于该请求消息的内容块中返回的内容记录数量。所有轮询响应消息均应包含该字段。

名称	是否必选	是否多个	描述
部分计数	否	否	该字段表示所提供的“记录数量”是相关记录的确切数量还是数量下限（实际可能存在更多记录）。该字段的值为布尔类型。值为“真”（TRUE）时表示实际的相关记录数量可能要高于“记录数量”字段的值。值为“假”（FALSE）表示“记录数量”的值为确切的记录数量。若不包含此字段，按照该字段的值为“假”时处理。
消息	否	否	该字段为消息接收方提供补充信息。这些信息面向人类读者，不要求机器可读。
内容块	否	是	该字段提供内容及其补充信息。该字段可能会被省略，也可能出现多次。有关内容块的定义，请参见 4.5 节。

需注意的是，TAXII 1.1 提供两个字段，用于指定时间戳标签的开始时间。这两个字段仅在内容源自数据 Feed 时都适用，内容若源自数据集，则不可以使用。若在内容源自数据 Feed 时不包含这两个字段，表示轮询响应包含指定的数据 Feed 的最早记录。若 TAXII 轮询响应消息提供 TAXII 数据 Feed 的开始时间戳标签，则必须采用这两个字段的其中一个表示响应消息中内容的开始时间。不建议使用此字段，之所以保留“开始时间戳标签（含）”字段是为了向后兼容， 若消息中包含这两个字段的其中一个，应确保所有 TAXII 1.1 轮询服务实现能正常运行。所有 TAXII 1.1 实现应在其发送的 TAXII 轮询响应消息中包含“开始时间戳标签（不含）”字段，除非请求方明确表示不接受包含该字段的响应（详情参见所支持的消息绑定版本）。

4.4.10 TAXII 收件消息

TAXII 收件消息用于将内容从一个实体推送至另一个实体的 TAXII 收件服务。

表 10 TAXII 收件消息中包含的字段

名称	是否必选	是否多个	描述
目的集合名	否	是	该字段指定消息内容的目的 TAXII 数据集合。
消息	否	否	该字段对消息接收方进行平实的描述。该消息一般面向人类操作员，不要求机器可读。
结果 ID	否	否	该字段指定包含该消息内容的具体结果集。该字段一般在生产者推送异步轮询结果（参见 3.6.2.2 节）时使用。
订阅信息	否	否	若是为了实现现有订阅而发送内容，消息中可包含此字段。若不包含此字段，表示并非为实现现有订阅而发送该消息。
集合名 [Feed 名称]	是	否	该字段指定提供内容的具体 TAXII 数据集合。
订阅 ID	是	否	该字段指定发送内容所针对的具体订阅。
开始时间戳标签（不含）	否。最多出现其中一个字段。	否	这两个字段的作用是相同的。不建议使用此字段，之所以保留“开始时间戳标签（含）”字段是为了与 TAXII 1.0 兼容。这两个字段不可以在同一消息中同时出现。 这两个字段均指定时间戳标签，表示收件消息覆盖的时间范围的开始时间，唯一区别为时间范围是否包含字段的值。若不包含这两个字段，表示收件消息覆盖时间最早的 TAXII 数据 Feed。若指定的 TAXII 数据集合为数据集，则不可以包含这两个字段。
开始时间戳标签（含）		否	
结束时间戳标签（含）	仅在数据集合为 Feed 时必选。在其他情况下不应使用。	否	该字段均指定时间戳标签，表示收件消息覆盖的时间范围的结束时间，所覆盖的时间范围包含该字段的值。若指定的数据集合为数据 Feed，则该字段必选。若指定的数据集合为数据集，则不可以包含该字段。
记录数量	否	否	该字段表示特定响应的相关记录数量。该字段的值应大于或等于该消息的内容块中返回的内容记录数量。所有轮询响应消息均应包含该字段。
部分计数	否	否	该字段表示所提供的“记录数量”是相关记录的确切数量还是数量下限（实际可能存在更多记录）。该字段的值为布尔类型。值为“真”（TRUE）时表示实际的相关记录数量可能要高于“记录数量”字段的值。值为“假”（FALSE）表示“记录数量”的值为实际的相关记录数量。若不包含此字段，按照该字段的值为“假”时处理。
内容块	否	是	该字段提供内容及其补充信息。该字段可能会被省略，也可能出现多次。有关内容块的定义，请参见 4.5 节。

通过“目的集合名”，收件消息的发送方可指定添加所附内容的一个或多个数据集合。

该字段可用于各种共享模型。消息接收方自行决定是否要将这些内容添加至指定的数据集合中。有关“目的集合名”的使用，请参见 3.2.1 节。

与轮询响应消息一样，收件消息也可以使用两个字段，指定时间戳标签的开始时间：“开始时间戳标签（不含）”（推荐）和“开始时间戳标签（含）”（不推荐）。TAXII 1.1 实现应采用开始时间戳标签（不含）”字段（如果可能），但考虑到向后兼容，应同时支持这两个字段。这两个字段在收件消息中的用法与在轮询响应消息中的用法相同。

4.4.11 TAXII 轮询实现请求

TAXII 轮询实现请求用于从创建了结果集的轮询服务收集结果。一般来说，此类请求通过异步轮询（参见 3.6.2 节）收集结果或通过拆分轮询交换（参见 3.6.1 节）收集大型结果集的多个拆分部分。

名称	是否必选	是否多个	描述
集合名	是	否	该字段指定所请求的具体 TAXII 数据集合。
结果 ID	是	否	该字段指定所请求的具体结果集。
拆分结果编号	是	否	若该字段出现，表示所收集的具体拆分结果。

4.5 TAXII 内容块

TAXII 内容块包含由结构化的网络威胁信息组成的内容。

表 11 TAXII 内容块

名称	是否必选	是否多个	描述
内容绑定	是	否	该字段指定具体内容绑定 ID（定义参见 4.1.7 节）或嵌套表达（定义参见 5.3 节），表示该内容块中的“内容”字段指定内容的类型。
子类型	否	否	该字段表示指定内容绑定的内容绑定子类型。每个子类型均必须为《TAXII 内容绑定参考》或第三方定义的内容绑定子类型 ID。若不包含该字段，表示内容不一定属于任何特定子类型。
内容	否	否	该字段指定订阅请求相关的查询表达。若订阅请求成功，订阅响应只包含查询表达匹配的内容。查询表达可以是结构化的，“查询格式”字段指定查询表达采用的特定结构。
	是	否	该字段为“内容绑定”字段指定类型的内容。
时间戳标签	否	否	该字段指定内容块相关的时间戳标签。该字段仅在内容来自 TAXII 数据 Feed 时有效。内容发送方决定是否包含该字段。
消息	否	否	该字段为消息接收方提供平实的描述。该消息一般面向人类操作员，并不要求机器可读。
填充	否	否	该字段指定内容块的任意大小的填充内容。该字段用于在内容加密时对内容块的大小进行模糊处理。处理内容块时，必须忽略该字段。
签名	否	否	该字段指定内容块的相关签名。该字段的使用仅限于内容块包含该字段的情况。

5 TAXII 处理

本章介绍了对 TAXII 生产者架构内的 TAXII 内容的预期处理。

尽管 TAXII 规范并未明确内容处理的诸多方面，例如内容存储方法和访问控制机制，但 TAXII 规定了一些内容处理要求，方便生产者架构之间进行兼容。

5.1 访问控制

很多网络威胁信息被信息传输方视为敏感信息。鉴于此，可能需对 TAXII 传播的内容进行访问控制防护。TAXII 未明确应利用何种访问控制措施或如何实现这些措施，而将这些问题留给了各生产者解决， 但 TAXII 针对访问控制策略对内容传播的总体影响进行了推测。

5.1.1 生产者对信息共享拥有完全控制权

生产者对其与 TAXII 消费者共享的信息具有完全控制权，包括编写或修改 TAXII 内容或出于任何原因不向 TAXII 消费者提供某些内容。此外，生产者有权不在 TAXII 发现响应中透露 TAXII 服务，且不在 TAXII 集合信息响应中提及 TAXII 数据集合。此外，生产者无需向消费者说明屏蔽了某些信息或进行了修改。甚至在提供 TAXII 状态消息说明错误情况时，TAXII 生产者也有权决定提供何种程度的细节。总之，若生产者不愿提供某些信息，TAXII 不强制要求其提供。

5.1.2 访问级别变化

若消费者的数据集合的访问级别发生了变化，他们或可接触到之前被屏蔽的信息。例如，请求某一特定时间段的 TAXII 数据 Feed 时，不同时间发出的 TAXII 轮询请求可能获得不同的结果（信息数量不同）。

TAXII 未明确消费者的访问权限变化后，是否要对其之前的请求进行更新或如何更新。TAXII 未规定消费者访问权限发生变化后向其发送消息，通知其权限变化。

当前的 TAXII 订阅应仍有效，并随消费者的权限级别变化而改变。也就是说，消费者的访问权限变化后，其当前订阅应仍有效，且下次按其新访问权限接收内容。

5.2 数据集合及内容

TAXII 数据集合反映了生产者在 TAXII 架构中展示内容的方法。生产者可采取任何方式将内容分配给数据集合。这些集合与用户群体、网络威胁信息类别或生产者期望采用的任何其他分组对应。本节围绕 TAXII 内容和 TAXII 数据集合之间的关系提出了一些设想和需求。

5.2.1 TAXII 不关注内容

TAXII 规范未详细介绍 TAXII 中记录的基本内容格式。就 TAXII 而言，所有内容格式均是“黑盒子”。针对 TAXII 的消息级别的处理行为均无需对存储在消息内容中的任何信息进行检测。尽管 TAXII 后端对不同类型的信息存在不同的处理路径和要求，但对于所传送的信息，并未明确 TAXII 服务、消息和交换。这就使得 TAXII 可适用于各种共享场景。

5.2.2 数据 Feed 与数据集

TAXII 支持两类数据集合：有序集合（数据 Feed）和无序集合（数据集）。数据生产者可根据需要使用这两类数据集合。下文将描述这两类数据集合对 TAXII 活动的影响。

5.2.2.1 订阅

数据 Feed 和数据集的订阅基本相同，但有一项重要区别。对于数据 Feed 和数据集的内容，内容添加至数据集合时应考虑交付。从首批内容开始，去除以下记录：与任何提供的表达式不匹配的记录、使用订阅用户不支持的内容绑定表示的记录，或者或访问控制策略对订阅用户屏蔽的记录。其余的记录将按照订阅请求中的机制交付至订阅用户。

此外，此外，之前添加至数据集中的记录的任何变更也应考虑。TAXII 消息未明确说明某项记录是对旧记录的修订还是添加至数据集合中的新记录。内容可能还包含用于检测修订的标识符，但这不属于 TAXII 范畴。

5.2.2.2 轮询范围

对于轮询请求，可能会限制数据 Feed 的请求范围。这一点，可通过提供时间戳标签指定时间范围来实现。由于数据集是无序的，不可实行同等限制，并且数据集的轮询请求应考虑覆盖所有记录。（出于这个原因，消费者在发送针对于数据集合的轮询请求时，可能希望查询表达来限制返回信息的数量。）

对于数据 Feed 的轮询请求，时间戳标签在请求限制方面发挥着重要作用。如 4.4.8 节“TAXII 轮询请求消息”中所述，针对数据 Feed 的轮询请求可包括时间戳标签的上限和下限，指定消费者的内容轮询范围。其目的是确保该范围可覆盖生产者在创建响应时所“考虑”到的内容。生产者在做出响应时应尊重消费者请求的时间戳标签范围。

生产者考虑数据 Feed 的范围指，将访问控制策略和类似策略允许，且时间戳标签在特定范围内的那些内容纳入响应中。需指出的是，生产者在结果集中添加的内容需同时满足以下条件：1. 生产者愿与消费者分享的内容。2. 内容与任何一条提供的查询表达匹配。3. 内容的时间戳标签在生产者的响应中设定的时间戳标签范围之内。也就是说，生产者提供的响应需包含生产者在响应中设定的范围内的内容。

在确定生产者响应的时间戳标签范围时，生产者应使用考虑到范围而非返回内容的实际范围。例如，消费者发送了下限为 X 的轮询请求，在轮询的数据 Feed 中，不存在时间戳为 X 的内容，但其时间戳为 Y（第二大时间戳）的内容匹配轮询请求。生产者返回响应时以 X 作为时间戳下限，这是因为生产者从 X 开始查询 Feed 内容，尽管到达 Y 后才找到内容。如果生产者使用 Y 作为下限，消费者无从知道是否能接收到时间戳标签介于 X 和 Y 之间的内容。

生产者发送的轮询响应中包含的时间戳标签范围可与消费者所请求的时间戳范围不同。例如，用户所请求的时间范围内的内容要比生产者在一个轮询响应中所返回的内容要多。

如 4.4.9 节所述，即使消费者针对于数据 Feed 的请求中未设定时间戳上限，但生产者返回的响应中应包含上限。如果生产者的响应中包含具有数据 Feed 中的最新时间戳标签的内容，生产者提供的上限必须大于或等于最新一条内容的时间戳标签，并且必须小于生产者将分配给下一条加入到数据 Feed 中的内容的下一条时间戳标签。

5.2.2.3 数据 Feed 与拆分结果

如 3.6.1 节所述，大型结果集可分解为多个部分进行交付。如结果集中的内容源自数据集，还应遵循以下规则： 结果集的每部分必须表示数据 Feed 的一个连续范围，并且必须包含该范围内的结果集的所有记录。这需要明确是结果由消费者推送的（见 3.6.1 节），还是推送给消费者的。因为这两种情况对于异步轮询产生的大型结果集均存在（见 3.6.2.2 节）。还要求看在创建结果集时是否使用了查询表达。换言之，每个包含结果集部分内容的消息都需要遵守轮询范围规则（见 5.2.2 节）。实际上，需对数据 Feed 的整个结果集按照时间标签进行分类并拆分为多个部分，每个部分表示结果集的一个时间段。

由于数据集是无序的，它没有此项要求，可发送任意部分的记录。

5.2.2.4 数据 Feed 内的内容不可变

如上所述，数据 Feed 内的每条内容添加至 TAXII 数据 Feed 时会分配一个时间戳标签。这样做的目的是提供一个句柄，可将特定内容纳入数据 Feed 的内容排序范围。这样，消费者可以了解，对特定范围的轮询请求返回的是看似在这个范围内的所有内容（因访问控制的原因，可能会对某些内容屏蔽）。因此（除非消费者的访问级别发生改变），没必要在给定的数据 Feed 的既定范围内进行重新轮询。

正因如此，内容在添加到数据 Feed 后不可以修改。这意味着不可执行修改、更正和撤销操作，而是要在数据 Feed 中添加新记录（为其分配最新时间戳标签）来实现此等操作。TAXII 消息没有可以表明新内容是对旧内容的修改、更正或撤销；在可能和适当的情况下，此类迹象需由新内容自身体现。

生产者可从数据 Feed 中删除一条内容，使消费者无法进一步以轮询方式请求特定范围的内容。然而，删除内容并不是表示修改、更正或撤销内容的好办法，因为消费者之前轮询过包含该条内容的范围，未必会对此范围重新轮询来了解该条内容已删除。

相比之下，并不要求数据集内容不可变。数据集中的记录可任意修改或删除。值得注意的是，虽然订阅数据集合的消费者将接收的已修改的记录作为订阅的一部分，但消费者可自行决定是否要替换某条记录及何时替换（见 5.2.2.1 节）。

5.2.3 将收件箱内容添加至数据集合

如 3.2.1 节所述，TAXII 支持通过收件交换将推送内容添加至一个或多个数据集合中。如果轮辐可代表轮轴重新发送所提交的内容，一些辐射型架构可利用此功能。3.2.1 节中描述了可实现该操作的收件交换。以下为关于该功能的其他说明：

- 接收方有权决定是否将提交的内容添加至特定的数据集合中。接收方可以任何理由拒绝内容。
- 还需要注意的是，由于 TAXII 表示将内容“自动”添加至数据集合，因此不要求立即添加内容。内容接收方可能希望内容在添加至数据集合之前由人类操作员进行审核。
- 收件箱消息中的内容块可能包含与任何提交内容相关的时间戳标签。尽管内容发送至数据 Feed，接收方可在将内容添加至数据 Feed 时为其分配时间戳标签。该时间戳标签可与内容发送时的时间戳标签相同或不同。

多数情况下，共享参与者之间的协议应规定是否应处理发送至数据集合的内容及如何处理。如下问题不收 TAXII 约束，但需在协议中做出回答：

- 接收方可否将内容添加至除发送人指定的数据集合之外的数据集合？
- 接收方可否将内容添加至数据集合前对其修改？
  - 或者，接收方是否应在将内容添加至数据集合前进行修改（如，内容再分享前进行匿名化处理）？
- 只将内容添加至数据集合，还是整个内容块添加至数据集合？ （有时会需要添加整个内容块，因为这样会保留内容来源及相关消息。）
- 如果内容被再次共享，是否采用某些访问限制或其他保护（如加密）。

5.2.4 只负责接收内容的数据集合

本文几乎通篇介绍消费者通过数据集合从生产者那里收集信息。然而，需要注意的是，

创建数据集合并不要求所有消费者都可以访问数据集合的内容。例如，创建的数据集合可能用于接收其他各方发送的内容的“投件箱”。可以配置收件箱，将提交的内容添加至特定数据集合，但这些数据集合可能仅限接收方内部使用，不得提供给任何外部消费者使用。因此，可能会出现这种情况：集合信息响应消息中的某条记录可能源自既不存在内容轮询方法，也无订阅方法的数据集合。

5.3 内容嵌套与加密

将 TAXII 内容从生产者传递给消费者时，内容块中的“Content Binding”字段表示内容块中内容的类型。例如，如果内容使用假设的威胁信息结构，一旦从内容块中提取出来，威胁信息内容可直接由威胁信息兼容工具处理。然而，在其他情况下，某类内容在使用前需要从另一类内容中提取。例如，如果威胁信息内容在“Content”字段中已被加密、压缩或编码，“Content”字段中的内容需要加以处理，以提取威胁信息内容。TAXII 支持通过多种方法利用内容块的“Content Binding”字段嵌入一种内容。

在下面的讨论中，假设有一个“加密结构”，并为其分配内容绑定 ID，Encstr。对于威胁信息内容，假设内容绑定 ID 为“ThreatInfo”。（真正的内容绑定 ID 可能包括版本和格式信息，但出于通用性考虑，下例中使用简化 ID。）加密结构中包含一个字段，可设置为一个二进制大对象（BLOB），表示某些内容的加密形式。下面几节分别介绍使用加密结构传输加密内容的三种方法。请注意，下文为加密示例，但其他内容嵌套形式，例如用于支持压缩，也可使用这些方法。

5.3.1 盲式嵌套

在内容嵌套中，“Content Binding”字段只规定了内容荣的最外层格式。对于这一假设的加密架构，该字段如下：

内容绑定 = EncStr

收到包含该“Content Binding”字段的内容块后，接收方知道其为加密结构。然而，“Content Binding”字段中并不提供加密架构中内容的相关信息。收件人需要通过其他方法确定所含信息的性质。

5.3.2 Explicit Nesting 显式嵌套

在显式嵌套中，“Content Binding”字段可表示每级嵌套的内容类型。“Content Binding”字段按照从最外层到最内层的顺序列出每个内容绑定 ID，并用竖线（|）隔开。例如，对于包含威胁信息内容的加密架构，“Content Binding”字段如下所示：

内容绑定 = EncStr|ThreatInfo

有了显式嵌套，接收方最终收到的内容类型清晰明了，尽管接收方在使用内容前需要从一个或多个嵌套中提取内容。通过“Content Binding”字段值的内容，我们可确定结构中内容的特性，无需再猜测。另一方面，外部观察者即使无法理解加密结构中的内容含义，也能了解内容特性。可见，一般认为，显式嵌套优于盲式嵌套，建议尽可能地使用显示嵌套。

“Content Bindings Subtype”不可以用于显式嵌套表达中。

5.3.3 内容块嵌套

外层内容类型不直接包含另一个内容类型，而是可以包含另一个 TAXII 内容块。每个 TAXII 消息绑定规范均定义了自己的内容绑定 ID，表示嵌套内容具有内容模块结构。例如，对于使用“ContentBlock”字符串的 TAXII 消息绑定，内容块嵌套形式如下：

内容绑定 = EncStr|ContentBlock

下图中展示使用内容块嵌套的加密。

```
A = Payload Block {
        Payload Binding = ThreatInfo
        Payload = ThreatInfo payload
        Signature = Digital signature scoped to A
        Padding = ASDFGHJKL...
}
A’  = A, encrypted and represented in the fictional "Encryption Struct" format

B = Payload Block {
        Payload Binding = EncStr|PayloadBlock
        Payload = A’
        Signature = Digital signature scoped to B
}
```

图 7 威胁信息内容的内容块嵌套

在上例中，A 代表包含威胁信息内容的内容块。“Signature”为可选字段，表示该内容块中的数字签名。“Padding”字段表示扩展内容块大小的任意数据。

B 代表另外一个内容块。在该内容块内，内容使用加密结构表达。在此例中，加密对象是内容块 A 的加密版本。B 的“Content Binding”字段表明“Content”字段为加密结构格式，并且加密结构格式包括另一个内容块。在 B 中，数字签名属于内容块 B。请注意，因为现在 A 已被加密，其“Padding”字段模糊化了 A 的“Content”字段的大小。

内容块嵌套可以把盲式嵌套和显式嵌套各自的优点结合起来：一旦接收方从内容块 B 中提取和解密“Content”字段，内部内容的类型就会提供给接收方，因为内容块 A 的“Content Binding”字段中明确给出了这些信息。然而，同时外部观察者无从了解传输的内容类型。另外，您可以了解如何在内部内容块中使用“Padding”字段模糊化传输内容的实际大小。

基于以上原因，相对于盲式嵌套和显式嵌套，内容块嵌套是内容加密处理的最佳方法。

5.3.4 内容嵌套仅用于内容块

内容绑定 ID 用于内容块之外的字段中，表示在特定上下文（如数据集合、订阅或服务）中可接受的内容格式。与内容块中的“Content Binding”字段不同的是，这些字段可指定多个内容绑定 ID。嵌套表达（如竖线（|）分隔的内容绑定 ID）不不可以用于这些字段。相反，当提供了支持的内容绑定列表时，表示支持这些内容绑定的任何有效嵌套组合。内容嵌套适用于内容块，无需列出。

例如，如果 TAXII 轮询请求消息表明消费者支持格式 W（该格式可包含其他内容类型包含其他内容类型）及格式 A 和 B，这表明对这些格式的任何有效嵌套组合都是支持的。例如，A、B、W、W|A、W|B、W|ContentBlock、W|W|A 和 W|W|B 等都是请求接受的绑定格式。

5.4 发送请求的内容

TAXII 的最终目标是将网络威胁信息从生产者传送至消费者。如上文所述，生产者可拥有共享内容的终极控制权。然后，生产者有义务以某种方式提供其愿意共享的信息内容，以方便消费者使用。

5.4.1 针对内容请求

消费者可通过订阅或发送轮询请求表达其希望接收到的内容绑定。内容绑定列表表明消费者希望接收的格式。生产者不应发送使用了消费者不支持的内容绑定的内容。同样地，如果消费者已表明支持特定内容绑定的内容绑定子类型，生产者不应发送使用了不支持的内容绑定子类型的内容。

类似地，订阅或轮询请求中可包括查询表达。生产者不应发送与查询表达不匹配的记录。也就是说，若某些内容由消费者不支持的内容绑定表达，即使允许消费者接收这些内容，生产者也不会发送这些内容。

请注意，生产者可能并不了解内容的特性。例如，内容可通过生产者提供的密钥之外的密钥加密。（如果生产者直接转发其他各方发送的内容时会出现这种情况。） 如果不是生产者的请求，生产者应只发送确定匹配的记录。如果生产者无法访问评估查询所需的信息，将不会产生匹配记录。

另一方面，如果没有查询表达，生产者应根据消费者支持的内容类型发送其接受的任何内容。例如，消费者接受格式为 W 的内容。如果生产者有 W 格式的内容，但并不知道其中包含的信息，生产者应发送该内容，因为生产者并不知道消费者无法解读包含的内容。这意味着，消费者最终将会收到其无法解析的内容。消费者不可以将此视为错误情况。（例如，如果收件箱服务收到格式不支持的内容，不会返回“不支持的内容绑定”状态消息。）

5.4.2 暂停订阅

数据集合的订阅用户可以请求为履行订阅目的进行的内容交付，稍后再恢复订阅。订阅暂停时，在为履行订阅而发送内容一方不可以将收件箱消息发送给订阅用户。当订阅者恢复内容交付时，为履行订阅而发送内容的一方应正常提供订阅暂停期间本应发送的所有内容。即使订阅处于暂停状态，轮询服务器仍可处理订阅相关的轮询请求。

5.5 查询

通过查询表达，消费者可描述内容记录中自己关注的内容特征，并对从生产者那里收集到的信息进行筛选，只关心那些具有这些特征的记录。查询表达可添加到轮询请求或订阅管理请求（即“动作”值为 SUBSCRIBE 的集合管理请求）中。在前种情况下，消费者只接受特定轮询请求返回的结果。在后种情况下，只有所提供的内容与指定的查询表达匹配才被视为履行了订阅。

消费者和生产者可自行决定是否需 TAXII 支持查询。并且，TAXII 查询能力是可扩展的，允许生产者和消费者支持各种的查询表达格式。生产者在发现响应消息中列出特定 TAXII 服务支持的格式，表明其支持的查询格式（若有）。轮询服务须支持其接收到的轮询请求中包含的一种或多种查询表达格式的查询格式。同样地，集合管理服务必须支持其接收到的订阅管理请求中包含的一种或多种查询表达的查询格式。生产者可选择仅在某些服务中支持查询表达，还可以选择在不同服务中支持不同的查询格式。

TAXII 在《缺省 TAXII 查询规范》中定义了一种缺省查询格式。而且，第三方可自定义查询格式，用于 TAXII 查询表达。本节介绍如何定义用于 TAXII 的查询格式，以及 TAXII 如何使用查询表达来指定消费者所关注的内容。

5.5.1 查询格式规范要求

《查询格式规范》定义在 TAXII 中使用特定查询格式的规则。每种查询规范必须定义一个查询格式 ID，以识别 TAXII 信息中的查询格式。查询格式 ID 必须全局唯一。关于查询格式 ID 的更多信息，详见 4.1.6 节。

轮询请求和集合订阅管理请求中的查询字段仅指定包含查询格式 ID 的单个子字段。查询字段中的其他信息（包括任何子字段和需要包含的信息类型）是由查询格式规范定义的。《查询格式规范》需定义所有子字段，描述这些字段的语法（如，必选或可选等），如何表达数据及类似信息。并且，《查询格式规范》还需要介绍如何利用这些字段描述内容比较标准。特别是，《查询格式规范》应描述如何使用字段及其内容来判断某个记录是否与特定的查询表达相匹配。

一些查询格式本身有一些可选的特征，并非所有实现都支持这些特征。在这种情况下，《查询格式规范》需要定义一个或多个支持的查询子字段。支持的查询子字段在发现响应信息中支持的查询字段的子字段。（支持的查询字段已包括用于识别查询格式的查询格式 ID 子字段。然而，像查询字段一样，其他子字段也是许可的。）《查询格式规范》可定义支持的查询子字段，各项参数表示某项 TAXII 服务所支持的查询格式。《查询格式规范》中定义相关的子字段，描述子字段的可能值，以及消费者对子字段的理解，从而提供必要的信息构成 TAXII 服务理解的查询表达。

由于 TAXII 消息中的查询表达和支持的查询子字段通过一些 TAXII 消息绑定来定义，非常有必要对这些用于表达信息的消息绑定进行定义。这些消息绑定可能是《查询格式规范》或某些单独文档的一部分。

5.5.2 通用查询处理

《查询格式规范》中介绍了处理查询表达（即，如何判断记录是否匹配指定的查询表达）最重要的几个方面。然而，大致说来，所有查询格式的查询表达处理没有什么差别。

当收到包含查询表达的消息时，TAXII 服务应检查查询格式 ID，以判断是否是可识别的查询格式。对于不支持的查询格式，TAXII 后台应发一条状态类型为 “不支持的查询格式” 的状态信息。对于支持的查询格式，TAXII 执行所请求的动作。对于轮询请求消息，将会生成包含查询表达匹配的记录的结果集。通常，对于为履行订阅目的而发送的任何记录，均需检查其是否与查询表达相匹配，只有匹配的记录才能发送给订阅用户，以履行该订阅。

6 参考书目

[1] The MITRE Corp., "TAXII Overview 1.0," The MITRE Corp., 2013.

[2] S. Bradner, "RFC 2119 - Key words for use in RFCs to Indicate Requirement Levels," The Internet Engineering Task Force, 1997.

[3] T. Berners-Lee, R. Fielding and L. Masinter, "RFC 3986 - Uniform Resource Identifier (URI): Generic Syntax," The Internet Engineering Task Force, 2005.

[4] G. Klyne and C. Newman, "RFC 3339 - Date and Time on the Internet: Timestamps," The Internet Engineering Task Force, 2002.

[5] The MITRE Corp., "The TAXII Content Binding Reference," The MITRE Corp., 2013.

[6] T. Bray, J. Paoli, C. M. Sperberg-McQueen, E. Maler and F. Yergeau, "Extensible Markup Language (XML) 1.0 (Fifth Edition)," W3C, 2008.

[7] The MITRE Corp., "The Default TAXII Query Specification 1.0," The MITRE Corp., 2014.

TAXII 服务规范

安全加社区

公益译文项目

2017

网络安全公益译文项目旨在分享国外先进网络安全理念，将网络安全战略性文档翻译为中文，促进国内安全组织在相关方面的思考和交流。该项目由安全加社区发起，安全加社区是国内的网络安全社区，社区欢迎网络安全人士的加入，并致力于交付网络安全问题的解决能力。