了解涉及多个组织的总体策略选择

目录

简介

本文档介绍在某些情况下考虑的多个Umbrella组织的策略。

概述

在某些情况下，可以考虑多个Umbrella组织的策略。例如，一个组织的漫游客户端或移动设备连接到另一个组织的网络。本文详细介绍当前在这种情况下如何选择策略，以及Umbrella打算进行哪些更改以改进此行为。

单个组织的策略选择

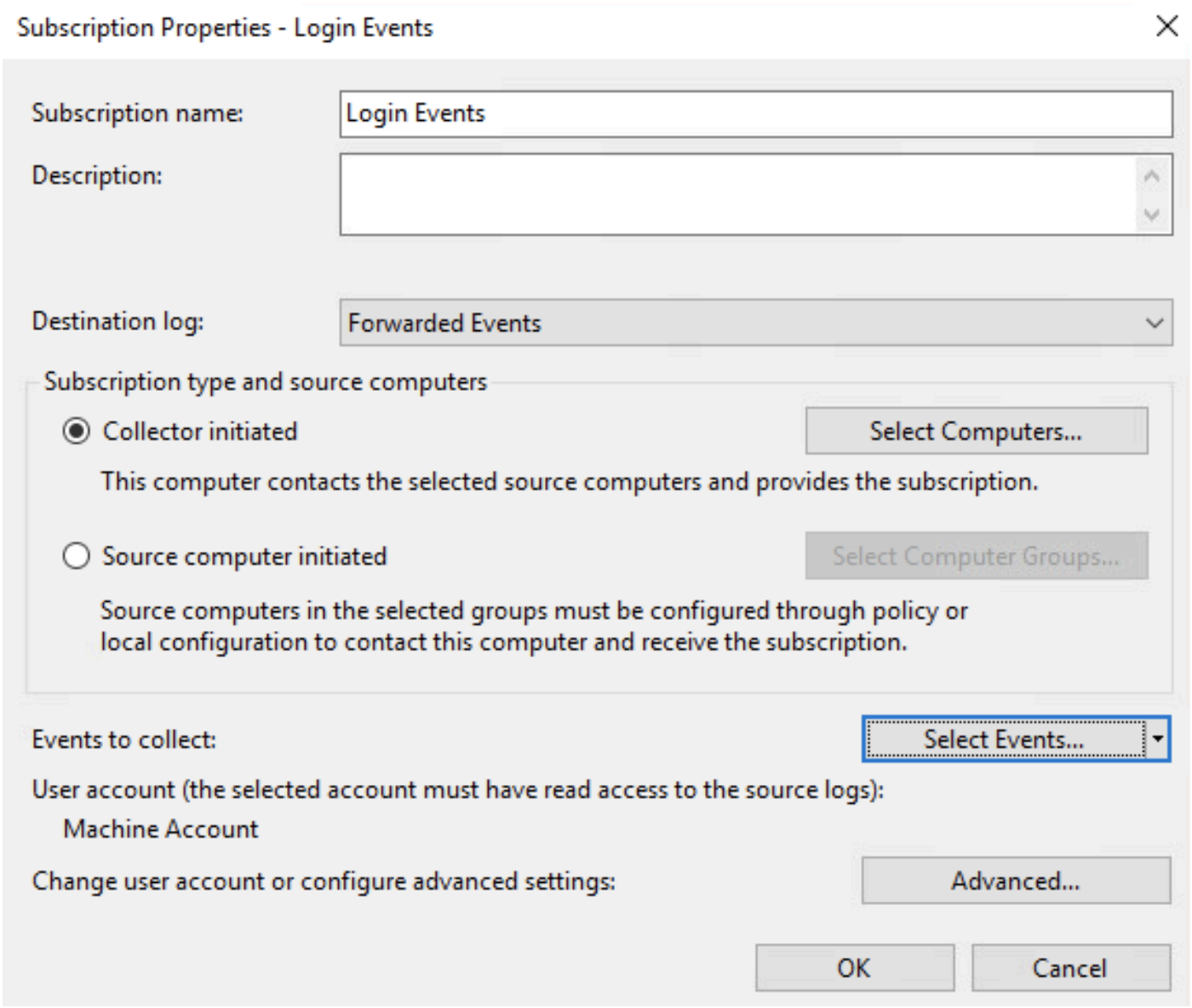
当DNS查询发送到Umbrella时，可能会有多个身份与该查询关联。例如，来自受保护的网络后面的漫游客户端(RC)的查询将包括RC的设备ID以及网络的IP地址。同样，来自虚拟设备的查询包括站点ID、内部网络、AD用户和AD组。

通常，查询中包含的标识都与单个组织相关联。在本例中，实施的策略使用文档中详述的策略优先规则：

https://docs.umbrella.com/deployment-umbrella/docs/policy-precedence

简而言之，Umbrella根据控制面板中的顺序为每个策略分配一个优先级，最顶层的策略具有最高优先级。Umbrella解析器选择适用于查询中存在的至少一个身份的最高优先级策略。

例如，组织A可以定义以下策略：



mceclip0.png

漫游计算机的策略的优先级为2，而网络的策略的优先级为1。因此，如果查询来自已加入外部网络的漫游计算机，则应用策略2。但是，如果漫游计算机已加入组织A的一个网络，则策略1将适用，因为网络的策略具有更高的优先级。

多个组织的策略选择

当查询中包含来自多个组织的标识时，也会应用相同的逻辑。但是，由于涉及多个组织，因此要考虑每个组织的策略列表的相对优先级。

一个例子最能说明这一点。组织A和组织B各自在各自的伞状控制面板中定义了以下策略：

- Minimize Latency
  - Makes sure that events are delivered by having minimal delay.
  - The appropriate choice if you collect alerts or critical events.
  - Uses push delivery mode, and sets a batch time-out of 30 seconds.

mceclip2.png

然后，来自组织A的漫游计算机加入属于组织B的网络。因此，发送到Umbrella的DNS查询包含组织A的RC设备ID和组织B的网络的IP地址。

使用单个组织的逻辑，我们可以获得每个身份策略的优先级。来自组织A的RC获取优先级为2的策略A2，而来自组织B的网络获取优先级为1的策略B1。因此，将应用用于组织B网络的策略（策略B1）。

与多个组织进行报告

当查询包含来自多个组织的标识时，查询仅出现在其策略被选定的组织的报告中。该组织的报告仅显示属于该组织的身份。组织永远无法查看查询中属于其他组织的其他身份。

对当前策略选择行为的影响

由于所描述的策略选择行为，属于一个组织的身份可能会被另一个组织的策略覆盖。这包括所有策略功能，包括安全和内容阻止、目标列表、阻止页面设计和日志记录设置（注意报告的限制），但阻止页面重定向除外。

涉及多个组织的方案的专用阻止页面

截至2021年7月16日，当Umbrella解析器检测到查询包含来自多个组织的标识时，它将所有被阻止的查询重定向到专用块页面。此阻止页面通知用户检测到多个组织，因此查询可能由于其他组织的策略而被阻止。

涉及多个组织的策略选择计划更改

当涉及多个组织时，改变策略选择行为的总括计划。未来的变更包括：

策略选择行为

Umbrella修改策略选择行为，以便为每个组织选择并实施最高优先级的策略。然后，如果其中任何策略将阻止查询，则阻止查询。这样，所有参与的组织都可以确保其策略不被绕过。我们可以用类比来解释此行为：

爱丽丝的父母说，她个人的规矩比家庭规矩更重要。Alice不允许在任何时间、任何地点吃冰淇淋。

Bob的父母说，家庭规则比个人规则更重要。他们从来不允许在家里吃披萨。

当前型号:

爱丽丝去鲍勃家。Bob's house rules适用，而不是Alice's individual rules。爱丽丝可以吃冰淇淋，但是不能吃比萨。Bob的父母收到一份报告说，有人在他们家里吃了冰淇淋，但是没说是Alice的名字。

推荐的模型：

爱丽丝去鲍勃家。Bob的房屋规则适用，Alice的个体规则适用。爱丽丝没有冰淇淋和披萨。Bob的父母收到一份报告称，有人被拒吃披萨和冰淇淋，但并没有说是Alice的名字。

为所有相关组织提供报告

当策略选择行为到位时，Umbrella还确保涉及多个组织的身份的任何查询都包括在所有相关组织的报告中。报告仅包含属于该组织的标识 — 给定组织从不查看其他组织的标识。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。