思科 AMP Threat Grid 设备迁移说明

版本 2.2

最后更新日期： 2017 年 3 月 3 日

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标的列表，请访问此 URL：www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。

目录

简介

Threat Grid 设备采用的迁移过程在后台执行迁移，从而使设备能够在迁移期间保持活跃使用状态。

本文档介绍迁移期间的内容提要，并回答有关升级过程的常见问题。

如果您对于迁移有任何问题，请联系 Threat Grid 支持：
support@threatgrid.com

版本 2.2 迁移

要求

必须在安装 2.2 之前完成 2.1.5/2.1.6 中的 ElasticSearch 迁移。

内容提要

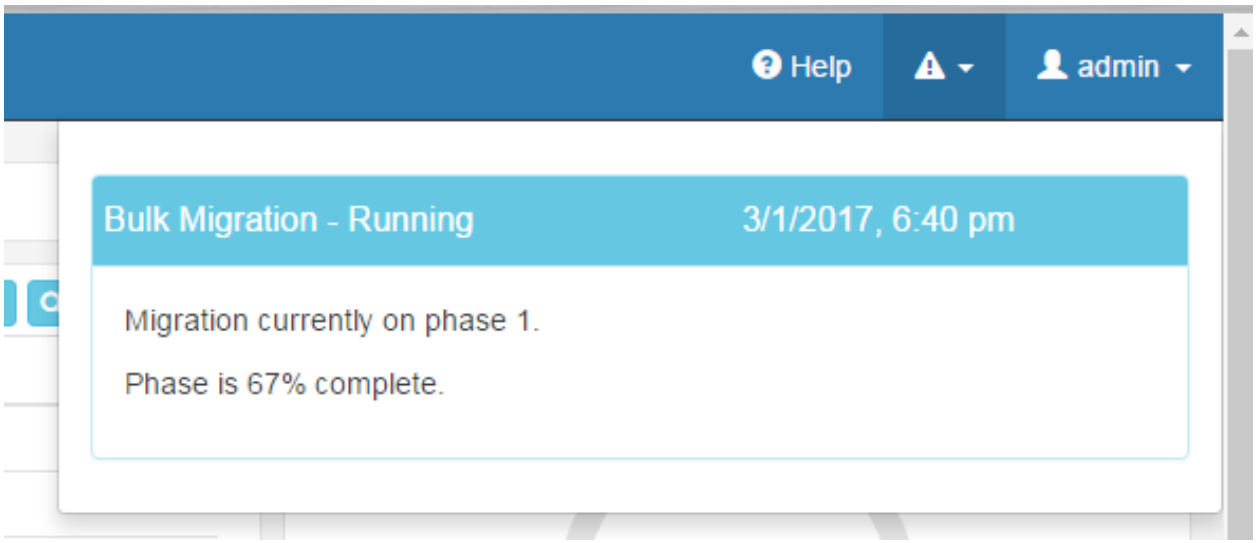
Threat Grid 设备版本 2.2 包含分四个阶段完成的重大数据迁移。

第 1 阶段迁移设备版本 1.x 中创建的低熵、非存档格式样本、工件和提取的 blob。

第 2 阶段迁移不符合上述某个条件的样本、工件和 blob。

第 3 阶段使第 1 阶段或第 2 阶段中迁移的样本再次可供下载；第 4 阶段将分析结果、报告和其他核心内容的存档格式存储转换为速度更快的随机访问格式。

系统通过服务通知传达迁移状态，包括每个阶段的完成百分比：



所需的时间

迁移将需要大量时间。所需时间量（特别是在第 1 阶段期间）完全取决于设备在 1.x 上的使用活跃程度。

每个设备会因设置、使用情况和存储而异，但是某些迁移需要 20 个小时或更长时间。某些迁移所需时间要少的多。

您可以在服务通知中跟踪迁移状态。

迁移期间的设备可用性

设备在迁移期间将保持可用。但是，在迁移运行期间可能无法从预更新提交内容中检索原始样本：第 1 阶段迁移了预更新样本后，该样本就将不可供下载，直至它在第 3 阶段中被重新处理为止。

元数据、状态、报告以及通常除原始样本本身以外的其他内容将保持持续可用。

完整功能在第 4 阶段期间再次可用。

数据问题

迁移将包含与 1.x 一致的 blob（磁盘工件）。其中包括根据样本的分析划分的内容，例如磁盘工件和网络工件等。

重要提示：

版本 2.2 会显著提高存储效率，使初始安装有版本 1.x 的系统上之前不可用的磁盘容量可用。这样将来可以再对旧内容实施修剪（删除）。

旧内容将在 2.2 中进行迁移。但是，较旧的内容（尤其是非常大量地产生但仅偶尔使用的分区磁盘和网络工件）***不再无限期保留***。

有关详细信息，请参阅相关文档 *Threat Grid 设备数据保留*:

http://www.cisco.com/c/dam/en/us/td/docs/security/amp_threatgrid/amp-threat-grid-appliance-data-retention.pdf。

版本 2.1.5 迁移

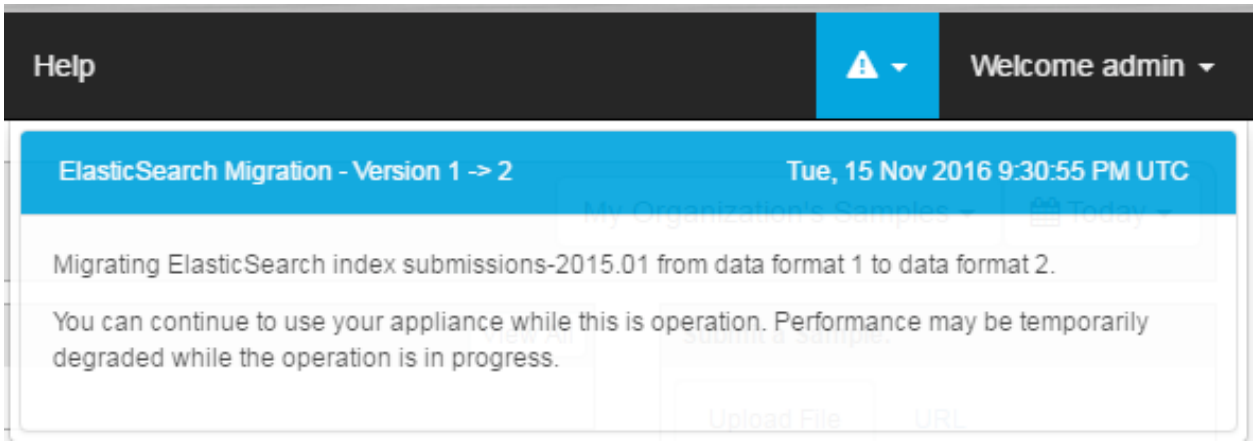
2.1.5 Threat Grid 设备版本更新了支持应用中各种搜索功能的 Datastore，尤其是支持设备与思科 ESA 和 WSA 设备集成的 API 调用。此 Datastore 在内容量大增时可能变得极其缓慢，导致 API 调用频繁失败或超时。新版本解决了这些问题，即使在高容量情况下也会保持高性能。但是，升级到新版本是一个耗时的过程，需要两次重建数据库索引。

内容提要

首先，将设备升级到版本 2.1.5。

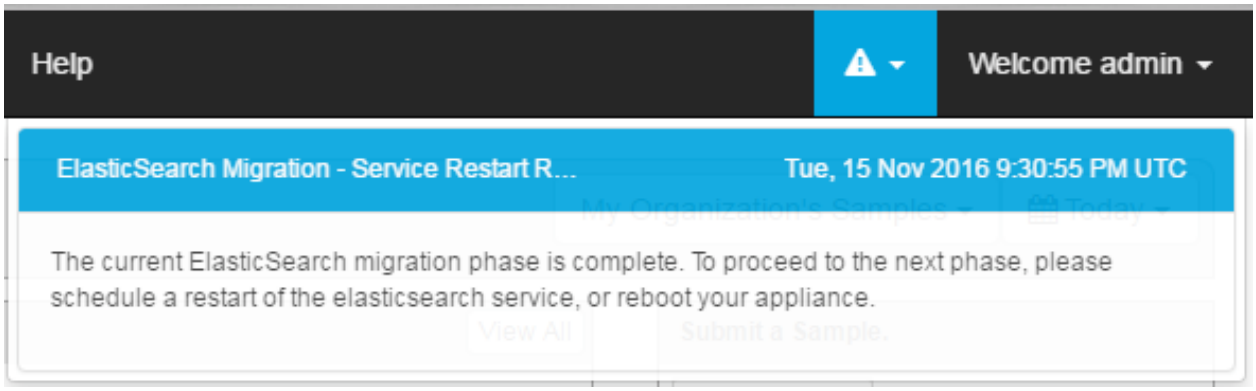
第 1 阶段

在升级设备后，CSA API 性能随即会达到与升级之前类似的水平。但是，在引导后的 10 分钟内，您应该会看到类似于下图的服务通知：



此通知将定期更新，以从不同月份迁移数据。

在所有 ElasticSearch 版本 1 内容都已升级到版本 2 之后，系统会提示请求重新启动：



第 2 阶段

在重新启动完成后，系统会将后台中的内容从版本 2 迁移到版本 5，并发出与用于从版本 1 迁移到版本 2 类似的通知。

此迁移完成后，通知将关闭，并且将来也不会生成服务通知。

常见问题解答

我需要安排什么样的停机时段?

安装版本 2.1.5 不会比升级任何其他典型设备需要的时间长，应该不到 30 分钟即可安装完毕。然后，系统应该马上就可以用了。一段时间后（所需时间因系统上的数据量而异。如需了解更多信息，请参阅下面的*这将需要多长时间？*），系统会宣布需要重新启动以开启第二阶段的迁移过程。这次重新启动只需要设备重新启动通常需要的时间量，一般不到 10 分钟。无需进一步停机。

这需要多长时间?

迁移的第 1 阶段在其他空闲情况下以大约 150,000 个样本/小时的速率运行，在重负载情况下以 75,000 个样本/小时的速率运行。

因此，为使 TG5500 设备持续使用 5000/天的完全采样率，在空载情况下每运行一个月的第 1 阶段，迁移时间预计为一小时；在迁移期间负载较重的情况下每运行一个月的第 1 阶段，迁移时间预计为两小时。

为了使 TG5000 设备持续使用 1500/天的完全采样率，第 1 阶段在空载情况下每运行一个月需要大约 20 分钟，在较重负载情况下每运行一个月需要 40 分钟。

第 2 阶段所需时间应略少于第 1 阶段；但是，由于性能在第 2 阶段开始时已改进（并且无需进一步重新启动或执行其他维护操作），因此对其完成时间的精准计时不太重要。

我何时会看到性能改进?

在第 1 阶段和第 2 阶段的间隔期间进行重新启动后，性能将比在先前版本中所见有显著改进，不过还未达到预计第 2 阶段完成后的速率。

在第 2 阶段完成后，CSA API 性能问题应完全彻底得到解决。

是否有任何功能警告?

在每个索引的迁移临近结束时有一个非常短暂的时期，在此时期在迁移过程中添加到该索引的数据库内容本身可能会在搜索结果中重复两次。

迁移过程是否会修改设备的存储要求?

允许加快搜索的存储格式更改确实会提高磁盘存储要求。但是，我们最近也已启用新近可用的选项来使用改进的压缩技术，从而基本上抵消此影响。

在我们的 QA 实验室中，我们看到最终结果通常是，数据/ElasticSearch 文件系统的存储要求提高 13%。

成功迁移需要多少可用磁盘空间?

应提供大约三倍于最大索引的磁盘空间，以将瞬态存储要求考虑在内。

实践中所见的最大索引大小往往大约为 15GB；因此，可用磁盘空间少于 45GB 的客户应在尝试此升级之前联系客户支持。

如何监控操作的进度?

如果为设备配置了邮件通知，则系统会将有关升级的状态发送到邮件中。无论是否配置了邮件通知，登录到 Threat Grid 应用并点击屏幕右上方带有惊叹号的三角形图标（如果显示）都将显示所有待处理的服务通知。

性能问题的原因是什么?

使用较低版本的 ElasticSearch 时，用来对 报告或列表、以及报告或最新 API 调用作出响应的数据库查询产生了过多的 I/O 负载。这也会导致引用同一存储区的其他 API 调用（例如处置查询）速度极大减缓，即使这些调用本会自行良好执行。

为什么此过程需要两个阶段?

ElasticSearch 5 无法直接加载或迁移 ElasticSearch 1 所使用的磁盘数据格式。因此，作为中间步骤，有必要将数据迁移到 ElasticSearch 2。

我首选尽可能缩短第 1 阶段和第 2 阶段之间的维护窗口；我是否可以避免重新启动?

可以在第 1 阶段和第 2 阶段之间仅重新启动 ElasticSearch 服务，而不重新启动整个系统。系统将显示一些警告：

- 如果使用 `tgsh` 界面自行重新启动此服务，则请注意，在升级后第一次尝试启动 ElasticSearch 时可能会报告故障。这是正常且意料之中的情况：在服务启动期间，关于系统上安装的可用服务的最新版本是否将能够成功操作此 Datastore，我们执行了一项检查；如果可以，我们会会关闭刚刚启动的服务版本并报告故障，这会导致稍后发生自动重新启动。让 ElasticSearch 服务第二次尝试启动应该会成功。

- 来自应用组件的 API 调用由于尝试使用为先前版本 Datastore 构建的 ElasticSearch 查询，可能会在最长 30 秒的时间内处于故障状态。在 30 秒超时到期后，应用将查询 Datastore 以获取其版本信息并开始使用适用于相应版本的查询，因此，这完全是瞬态错误。

我刚刚重新启动了设备，但是系统仍然显示消息，指示我需要重新启动设备。

设备在其重新启动后最长十分钟的时间内将会检查其迁移状态并启动任何所需或待处理操作，或者清除不再适用的迁移相关服务通知。在该时间之前，系统可能会显示该设备启动之前的消息。