



使用 Kubernetes 和 OpenShift 安装 Black Duck

Black Duck 2024.7.0

Black Duck 版权所有 ©2024。

保留所有权利。本文档的所有使用均受 Black Duck Software, Inc. 和被许可人之间的许可协议约束。未经 Black Duck Software, Inc. 事先书面许可，不得以任何形式或任何方式复制或传播本文档的任何内容。

Black Duck、Know Your Code 和 Black Duck 徽标是 Black Duck Software, Inc. 在美国和其他司法管辖区的注册商标。Black Duck Code Center、Black Duck Code Sight、Black Duck Hub、Black Duck Protex 和 Black Duck Suite 是 Black Duck Software, Inc. 的商标。所有其他商标或注册商标是其各自所有者的专有财产。

03-10-2024

内容

前言.....	5
Black Duck 文档.....	5
客户支持.....	5
Black Duck Software Integrity Community.....	6
培训.....	6
Black Duck 关于包容性和多样性的声明.....	6
Black Duck 安全承诺.....	7
1. 使用 Kubernetes 和 OpenShift 安装 Black Duck.....	8
2. 硬件要求.....	9
3. PostgreSQL 版本.....	10
常规迁移过程.....	10
4. 使用 Helm 安装 Black Duck.....	11
5. Artifactory 集成.....	12
6. 基本工作流.....	13
7. Artifactory 集成前提条件.....	14
8. 安装顺序.....	15
9. 安装 Artifactory 集成插件.....	16
配置 Artifactory 集成插件.....	16
测试连接.....	18
10. Artifactory 集成任务.....	19
11. 管理任务.....	21
在 Kubernetes 中配置密钥加密.....	21
在 Kubernetes 中生成种子.....	22
配置备份种子.....	22
在 Kubernetes 中管理密钥轮换.....	23
为 Blackduck 存储配置自定义卷.....	23

配置 jobrunner 线程池..... 26

配置就绪探针..... 27

配置 HUB_MAX_MEMORY 设置..... 27

使用 Helm 在 OpenShift 上进行迁移..... 27

前言

Black Duck 文档

Black Duck 的文档包括在线帮助和以下文档：

标题	文件	说明
发行说明	release_notes.pdf	包含与当前版本和先前版本中的新功能和改进功能、已解决问题和已知问题有关的信息。
使用 Docker Swarm 安装 Black Duck	install_swarm.pdf	包含有关使用 Docker Swarm 安装和升级 Black Duck 的信息。
使用 Kubernetes 安装 Black Duck	install_kubernetes.pdf	包含有关使用 Kubernetes 安装和升级 Black Duck 的信息。
使用 OpenShift 安装 Black Duck	install_openshift.pdf	包含有关使用 OpenShift 安装和升级 Black Duck 的信息。
入门	getting_started.pdf	为初次使用的用户提供了有关使用 Black Duck 的信息。
扫描最佳做法	scanning_best_practices.pdf	提供扫描的最佳做法。
SDK 入门	getting_started_sdk.pdf	包含概述信息和样本使用案例。
报告数据库	report_db.pdf	包含有关使用报告数据库的信息。
用户指南	user_guide.pdf	包含有关使用 Black Duck 的 UI 的信息。

在 Kubernetes 或 OpenShift 环境中安装 Black Duck 软件的安装方法是 Helm。单击以下链接查看文档。

- [Helm](#) 是 Kubernetes 的软件包管理器，可用于安装 Black Duck。Black Duck 支持 Helm3，Kubernetes 的最低版本为 1.13。

Black Duck 集成文档位置：

- <https://sig-product-docs.synopsys.com/bundle/integrations-detect/page/integrations/integrations.html>
- https://sig-product-docs.synopsys.com/category/cicd_integrations

客户支持

如果您在软件或文档方面遇到任何问题，请联系 Black Duck 客户支持。

您可以通过以下几种方式联系 Black Duck 支持：

- 在线：<https://www.synopsys.com/software-integrity/support.html>
- 电话：请参阅我们的[支持页面](#)底部的“联系我们”部分以查找您当地的电话号码。

要创建支持案例，请登录 Black Duck Software Integrity Community 网站：<https://community.synopsys.com/s/contactsupport>。

另一个可随时使用的方便资源是[在线客户门户](#)。

Black Duck Software Integrity Community

Black Duck Software Integrity Community 是我们提供客户支持、解决方案和信息的主要在线资源。该社区允许用户快速轻松地打开支持案例，监控进度，了解重要产品信息，搜索知识库，以及从其他 Software Integrity Group (SIG) 客户那里获得见解。社区中包含的许多功能侧重于以下协作操作：

- 连接 - 打开支持案例并监控其进度，以及监控需要工程或产品管理部门协助的问题
- 学习 - 其他 SIG 产品用户的见解和最佳做法，使您能够从各种行业领先的公司那里汲取宝贵的经验教训。此外，客户中心还允许您轻松访问 Black Duck 的所有最新产品新闻和动态，帮助您更好地利用我们的产品和服务，最大限度地提高开源组件在您的组织中的价值。
- 解决方案 - 通过访问 SIG 专家和我们的知识库提供的丰富内容和产品知识，快速轻松地获得您正在寻求的答案。
- 分享 - 与 Software Integrity Group 员工和其他客户协作并进行沟通，以众包解决方案，并分享您对产品方向的想法。

[访问客户成功社区](#)。如果您没有帐户或在访问系统时遇到问题，请单击[此处](#)开始，或发送电子邮件至 community.manager@synopsys.com。

培训


Black Duck Software Integrity Group (SIG) 客户教育是满足您所有 Black Duck 教育需求的一站式资源。它使您可以全天候访问在线培训课程和操作方法视频。

每月都会添加新视频和课程。

在 Black Duck Software Integrity Group (SIG) 客户教育中，您可以：

- 按照自己的节奏学习。
- 按照您希望的频率回顾课程。
- 进行评估以测试您的技能。
- 打印完成证书以展示您的成就。

要了解更多信息，请访问 <https://community.synopsys.com/s/education>，或者，要获取 Black Duck 的帮助

信息，请选择 Black Duck 教程（从“帮助”菜单（）（位于 Black Duck UI 中）选择）。

Black Duck 关于包容性和多样性的声明

Black Duck 致力于打造一个包容性的环境，让每位员工、客户和合作伙伴都感到宾至如归。我们正在审查并移除产品中的排他性语言以及支持面向客户的宣传材料。我们的举措还包括通过内部计划从我们的工程和工作环境中移除偏见语言（包括嵌入我们软件和 IP 中的术语）。同时，我们正在努力确保我们的 Web 内容和软件应用程序可供不同能力的人使用。由于我们的 IP 实施了行业标准规范，目前正在审查这些规范以移除排他性语言，因此您可能仍在我们的软件或文档中找到非包容性语言的示例。


Black Duck 安全承诺

作为一家致力于保护和保障客户应用程序安全的组织，Black Duck 同样致力于客户的数据安全和隐私。本声明旨在为 Black Duck 客户和潜在客户关于我们的系统、合规性认证、流程和其他安全相关活动的最新信息。

本声明可在以下位置获取：[安全承诺 | Black Duck](#)

1. 使用 Kubernetes 和 OpenShift 安装 Black Duck

Kubernetes 和 OpenShift™ 是用于通过容器管理云工作负载的编排工具。


 警告: 从 Black Duck 2023.7.0 版本开始, Black Duckctl 不再受支持, 也不会有更新。Black Duck 通过 Helm 图表支持部署, 请参阅 %install dir%/kubernetes/blackduck/ 中的文档以及 Helm 图表示例。

2. 硬件要求

Black Duck 硬件扩展指南

有关可扩展性调整指南，请参阅 [Black Duck 硬件扩展指南](#)。

Black Duck 数据库

 **危险：** 请勿删除 Black Duck 数据库 (bds_hub) 中的数据，除非 Black Duck 技术支持代表指示这样做。确保遵循适当的备份程序。删除数据会导致 UI 问题、Black Duck 完全无法启动等问题。Black Duck 技术支持无法重新创建已删除的数据。如果没有可用的备份，Black Duck 将尽力提供支持。

磁盘空间要求

所需的磁盘空间量取决于要管理的项目的数量，因此各个要求可能有所不同。考虑每个项目大约需要 200 MB。

Black Duck 软件建议监视 Black Duck 服务器上的磁盘利用率，以防止磁盘达到可能导致 Black Duck 出现问题的容量。

BDBA 扩展

调整 binaryscanner 副本的数量，以及根据每小时将执行的二进制扫描的预期数量增加 PostgreSQL 资源，从而完成 BDBA 扩展。对于每小时每 15 次二进制扫描，添加以下资源：

- 一个 binaryscanner 副本
- 一个用于 PostgreSQL 的 CPU
- 用于 PostgreSQL 的 4GB 内存

如果您的预期扫描速率不是 15 的倍数，则向上舍入。例如，每小时 24 次二进制扫描将需要以下资源：

- 两个 binaryscanner 副本、
- 两个用于 PostgreSQL 的额外 CPU，以及
- 用于 PostgreSQL 的 8GB 额外内存。

当二进制扫描为总扫描量（按扫描计数）的 20% 或更少时，此指南有效。


 **注：** 安装 Black Duck Alert 需要 1 GB 的额外内存。

3. PostgreSQL 版本


Black Duck 2023.10.0 支持新的 PostgreSQL 特性和功能，以提高 Black Duck 服务的性能和可靠性。从 Black Duck 2023.10.0 开始，PostgreSQL 14 是内部 PostgreSQL 容器支持的 PostgreSQL 版本。


从 Black Duck 2023.10.0 开始，PostgreSQL 设置将在使用 PostgreSQL 容器的部署中自动设置。使用外部 PostgreSQL 的客户仍需手动应用设置。

使用 PostgreSQL 容器并从 2022.2.0 至 2023.7.x (含) 之间的 Black Duck 版本升级的客户，将自动迁移到 PostgreSQL 14。从旧版本 Black Duck 升级的客户需要先升级到 2023.7.x，然后才能升级到 2024.7.0。

 注：有关 PostgreSQL 调整指南，请参阅 [Black Duck 硬件扩展指南](#)。

如果您选择运行自己的外部 PostgreSQL 实例，Black Duck 建议为新安装使用最新版本 PostgreSQL 16。

 注：Black Duck 2024.4.0 增加了对使用 PostgreSQL 16 作为外部数据库的初步支持，仅用于测试；从 Black Duck 2024.7.0 开始，PostgreSQL 16 完全支持生产使用。

 警告：不要在 PostgreSQL 数据目录上运行防病毒扫描。防病毒软件会打开大量文件，锁定文件，等等。这些操作会干扰 PostgreSQL 的运行。具体错误因产品而异，但通常会导致 PostgreSQL 无法访问其数据文件。一个例子是，PostgreSQL 失败，并显示“系统中打开的文件太多”。

常规迁移过程

此处的指南适用于从任何基于 PG 9.6 的 Hub (早于 2022.2.0 的版本) 升级到 2022.10.0 或更高版本。

1. 迁移由 blackduck-postgres-upgrader 容器执行。
2. 如果从基于 PostgreSQL 9.6 的 Black Duck 版本升级：
 - PostgreSQL 数据卷的文件夹布局经过重新排列，使未来的 PostgreSQL 版本升级更加简单。
 - 数据卷所有者的 UID 已更改。新的默认 UID 为 1001，但请参见特定于部署的说明。
3. 运行 pg_upgrade 脚本以将数据库迁移到 PostgreSQL 13。
4. 在 PostgreSQL 13 数据库上运行普通“分析”以初始化查询计划程序统计信息。
5. blackduck-postgres-upgrader 退出。

4. 使用 Helm 安装 Black Duck

Helm 图表说明了一组 Kubernetes 资源，Helm 部署 Black Duck 需要用到这些资源。Black Duck 支持 Helm 3.5.4，Kubernetes 最低版本为 1.17。

您可以在以下网址获取 Helm 图表：<https://sig-repo.synopsys.com/artifactory/sig-cloudnative>

单击[此处](#)了解有关使用 Helm 安装 Black Duck 的说明。Helm 图表引导在 Kubernetes 群集上使用 Helm 软件包管理器部署 Black Duck。

使用 Helm 在 Kubernetes 上进行迁移

如果您从基于 PostgreSQL 9.6 的 Black Duck 版本升级，此迁移将用 Black Duck 提供的容器替换 CentOS PostgreSQL 容器。此外，synopsys-init 容器将替换为 blackduck-postgres-waiter 容器。

在普通 Kubernetes 上，升级作业的容器将以 root 身份运行（除非覆盖）。但是，唯一的要求是作业与 PostgreSQL 数据卷的所有者以相同的 UID 运行（默认为 UID=26）。

在 OpenShift 上，升级作业假定它将使用与 PostgreSQL 数据卷所有者相同的 UID 运行。

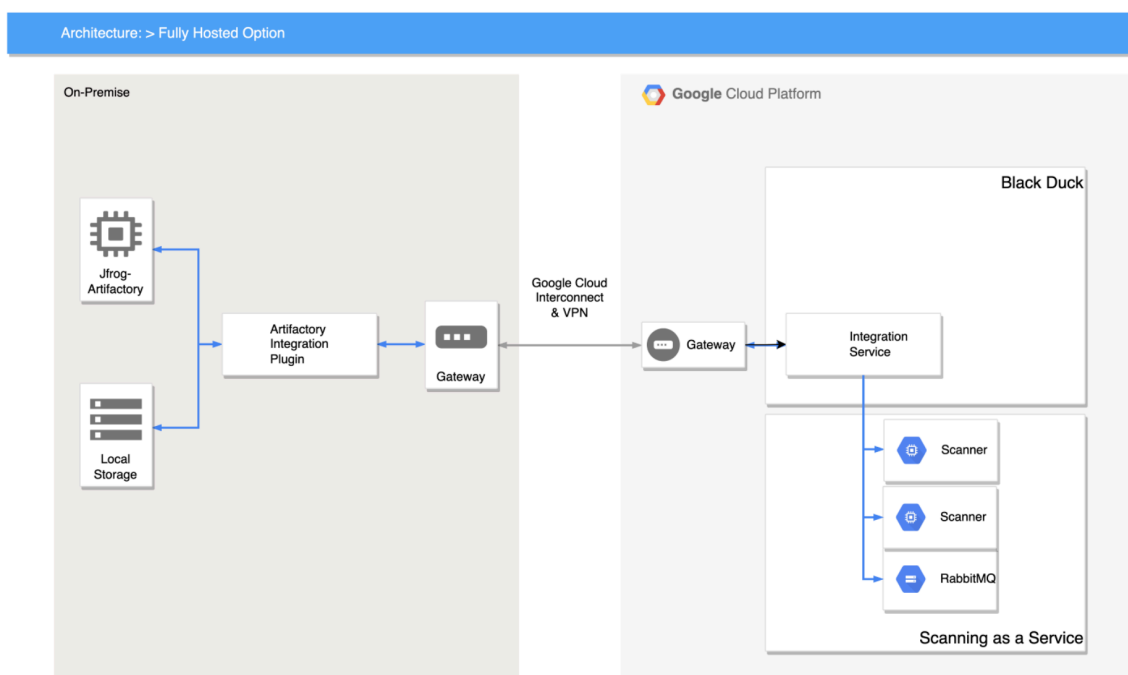
5. Artifactory 集成

概述

Artifactory 集成是保护软件供应链的 Black Duck 机制。由于 Artifactory 通常是该链的最终环节之一，因此扫描已配置的 Artifactory 存储库组中的每个工件可让客户控制其单个供应链。默认情况下，此版本的 Artifactory 集成会自动阻止从扫描的 Artifactory 存储库中进行违反 Black Duck 策略的下载。Black Duck 定义为“快速”或“两者”的策略将会应用于 Artifactory 集成。

架构

Black Duck 2023.10.0 中改进了 Artifactory 集成的架构方法，以支持重点关注完全托管的部署。这些变化反映在下面的架构图中。




操作

Artifactory 集成会定期检查配置的资源库中未扫描的工件、上次成功扫描后更新的工件或之前出现扫描错误的工件，并编译列表。

文件将发送到您的托管 Black Duck 实例，以根据 Black Duck 中定义的策略进行扫描和评估。Artifactory 集成会轮询您的 Black Duck 实例以获取结果，并在可用时使用结果注释工件，包括但不限于：

- 扫描结果（成功/失败）。
- Black Duck 实例扫描结果的 URL。
- 发现违反的任何策略的名称。

此外，可以为每个存储库配置阻止下载违反 Black Duck 策略的工件的功能。


 注：在 Artifactory 中使用 Artifactory 集成插件之前，必须安装和配置该插件，并拥有供该插件使用 Black Duck 的 API 密钥。

6. 基本工作流

使用以下工作流开始在 Artifactory 中使用 Black Duck 插件：

1. 确保满足要求。
2. 在 Black Duck 实例中的“集成”下配置 Artifactory 服务器。
3. 在 Black Duck 实例中创建用于 Artifactory 集成的 API 令牌，并将其复制到剪贴板。
4. 在 JFrog Artifactory 中安装 Black Duck Artifactory 集成插件。
5. 在 Artifactory 集成插件中配置以下内容：
 - a. Black Duck 要使用的服务器实例。
 - b. Black Duck 实例的 API 令牌。
 - c. Artifactory 服务器配置的名称。
6. 重新启动 Artifactory 实例或 HA 配置中的每个节点。
7. 扫描后，检查生成的工件属性，或点击链接（如果已配置）查看 Black Duck 实例上的结果。

7. Artifactory 集成前提条件

 注: 您必须在注册密钥上启用 Artifactory 集成, 才能使用此功能。启用后, 在 values.yaml 文件中添加以下内容:

```
enableIntegration: true
```

类别	要求
其他要求	<div>Artifactory 集成插件</div> <ul style="list-style-type: none">• JFrog Artifactory Pro 版本 7.43.x 或更高版本<ul style="list-style-type: none">• Black Duck Artifactory 集成插件安装在目标 JFrog Artifactory Pro 服务器中。• Artifactory 7.43.x 实例的 Java• Black Duck 版本 11。请参阅 Black Duck 版本兼容性, 了解 Black Duck 支持的版本。• Black Duck API 令牌, 用于插件访问 Black Duck 实例。• 该插件需要在 Black Duck 中拥有全局代码扫描者、项目创建者和全局项目查看者用户角色。<ul style="list-style-type: none">• 可以使用超级用户角色, 但不是插件所必需的。• 全局代码扫描程序和项目创建者角色仅允许您查看使用 Black Duck 用户帐户扫描的项目。• 需拥有全局项目查看者角色才能查看所有项目。

8. 安装顺序

下面提供了安装 Artifactory 集成的有序步骤的摘要：

1. 从您的 Black Duck 实例获取访问令牌并存储在安全位置。
2. 准备安装 Artifactory 集成插件：
 - a. 从 GitHub 下载插件。
 - b. 解压缩下载的文件。
 - c. 将插件文件移动到 Artifactory 安装中的相应目录。
3. 根据需要编辑 Artifactory 集成插件 `blackDuckPlugin.properties` 文件。
4. 重新启动 Artifactory 服务器。

9. 安装 Artifactory 集成插件

以下步骤描述了安装和配置 Artifactory 集成插件的过程。

下载并提取 Artifactory 插件

从 Black Duck Artifactory [Black Duck 外部 SIG 存储库](#) 下载 Black Duck Artifactory 集成插件存档 (.zip 或 .tgz) 发行版。

下载发行版后，提取存档文件。注意以下文件结构：

```
artifactory-integration-<version number>/
--blackDuckArtifactoryIntegration.groovy
- lib/
- -- artifactory-integration-common-<version number>.jar
- -- blackDuckArtifactoryIntegration.properties
- -- synopsysArtifactoryVersion.txt
```

发行版的组件如下：

- blackDuckArtifactoryIntegration.groovy：插件。
- lib：包含插件依赖关系的库文件夹。
- blackDuckArtifactoryIntegration.properties：插件的配置文件。

获取并配置 Black Duck 凭据

获取 [Black Duck API 令牌](#) 以用作 blackDuckArtifactoryIntegration.properties 文件中的凭据。

使用 blackDuckArtifactoryIntegration.properties 文件 [配置 Black Duck 凭据](#)，该文件位于 artifactory-integration-<version>/lib 文件夹中。

最后几步

将 artifactory-integration-<version>/blackDuckArtifactoryIntegration.groovy 文件和 artifactory-integration-<version>/lib 文件夹复制到 \${ARTIFACTORY_HOME}/var/etc/plugins/。

更改以下文件夹的用户：

- ```
chown -R 1030:1030 ${ARTIFACTORY_HOME}/var/etc/plugins/blackDuckArtifactoryIntegration.groovy
```
- ```
chown -R 1030:1030 ${ARTIFACTORY_HOME}/var/etc/plugins/lib
```

重新启动 Artifactory 服务器。

使用 Docker 安装的 Artifactory

执行 Docker cp 命令，将插件 groovy 文件和 lib 文件夹从提取的位置移至 \${ARTIFACTORY_HOME}/var/etc/plugins/。

配置 Artifactory 集成插件

必须先修改 blackDuckArtifactoryIntegration.properties 文件，插件才能正常运行，您可以使用任何文本编辑器手动编辑属性文件以配置该插件。

下文概述了 blackDuckArtifactoryIntegration.properties 文件的重要设置。

Black Duck 连接凭据

您需要连接到 Black Duck，可在属性文件中配置此连接。

您必须在属性中的 Black Duck 凭据下添加 Black Duck 令牌 blackduck.api.token=<BD API token> 和 Black Duck URL 文件。

```
# BlackDuck credentials
blackduck.url=
blackduck.api.token=
```

使用的是访问令牌，而不是 Black Duck 代理，那么这就是您在属性文件中的“凭据”部分需要提供的全部信息。

Artifactory 配置名称

您必须将配置名称设置为与 Black Duck 实例中 [Artifactory 集成配置](#) 的名称一致。Artifactory 集成初始化后，它将连接到上面配置的 Black Duck 实例，并根据以下配置检索集成设置：

```
blackduck.artifactory.config.name=
```

如果 Black Duck 实例中不存在给定 blackduck.artifactory.config.name 的配置，则会记录错误，Artifactory 集成将不会加载到您的 Artifactory 实例中。您需要修改名称并重新启动 Artifactory 实例。

常规属性

Artifactory 使用的日期时间模式可配置为显示扫描/检查时间戳。Artifactory 插件接受任何有效的 Java 8 ZoneId。有关更多信息，请参阅 <https://docs.oracle.com/javase/8/docs/api/java/time/ZoneId.html>。

```
# blackduck.artifactory.scan.cutoff.date must comply to this pattern
blackduck.date.time.pattern=yyyy-MM-dd'T'HH:mm:ss.SSS
blackduck.date.time.zone=
```

以下是短 ID 列表：

ID	值
EST	• 05:00
HST	• 10:00
MST	• 07:00
ACT	Australia/Darwin
AET	Australia/Sydney
AGT	America/Argentina/Buenos_Aires
ART	Africa/Cairo
AST	America/Anchorage
BET	America/Sao_Paulo
BST	Asia/Dhaka

CAT	Africa/Harare
CNT	America/St_Johns
CST	America/Chicago
CTT	Asia/Shanghai
EAT	Africa/Addis_Ababa
ECT	Europe/Paris
IET	America/Indiana/Indianapolis
IST	Asia/Kolkata
JST	Asia/Tokyo
MIT	Pacific/Apia
NET	Asia/Yerevan
NST	Pacific/Auckland
PLT	Asia/Karachi
PNT	America/Phoenix
PRT	America/Puerto_Rico
PST	America/Los_Angeles
SST	Pacific/Guadalcanal
VST	Asia/Ho_Chi_Minh

客户端扫描

未来的配置允许您使用客户端资源来扫描工件，从而无需跨防火墙传输到 Black Duck 进行扫描，而您的 Black Duck 实例上仍会进行匹配和策略评估。需要在防火墙内的客户硬件上设置客户端扫描和端点。

```
blackduck.client.scan.url=
blackduck.client.concurrent.scans=
```

如果没有为 blackduck.client.scan.url 提供 URL，Artifactory 集成会继续将工件传输到 Black Duck 进行扫描、映射和策略评估。

测试连接

当您安装和配置 Black Duck 插件时，Black Duck 建议您测试连接并确保插件工作正常。使用以下 curl 命令测试连接：

```
curl -X GET -u USERNAME:PASSWORD http://ARTIFACTORY_SERVER/artifactory/api/plugins/execute/blackDuckTestConfig
```

10. Artifactory 集成任务

升级 Artifactory 集成

1. 在升级到新版本之前，请运行以下命令以从图表博物馆中提取最新版本的图表：

```
$ helm repo update
$ helm pull synopsys/sca-as-a-service
```

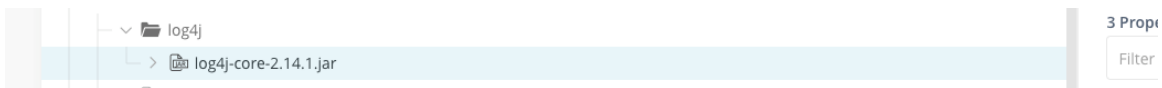
2. 升级 Artifactory 集成

```
$ helm upgrade ${SCAAAS_NAME} sca-as-a-service/ --namespace ${BD_NAME}
```

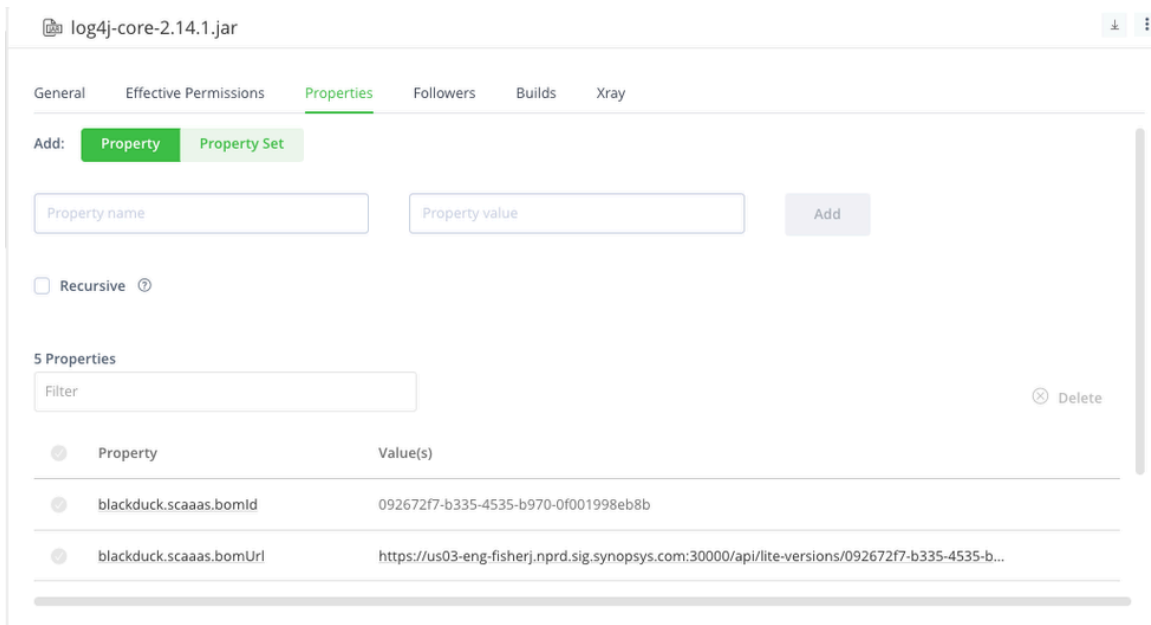
手动覆盖阻止的下载

如果 Artifactory 中的项目违反了您在 BlackDuck 中定义的策略，但您希望覆盖并允许下载该项目，请遵循以下说明：

1. 登录 Artifactory UI 并找到您要覆盖的违规项目。




2. 选择属性。



3. 在属性名称文本字段中输入 blackduck.allowDownload。
4. 在属性值文本字段中输入 true。

现在，无论 Artifactory 集成插件中设置的阻止策略如何，您都应该能够下载该项目。

 注：设置此属性仅影响此工件，不会影响可能包含此工件的其他工件。如果项目已更新（例如，上传新版本），它将被重新扫描，并且 blackduck.allowDownload 属性可能会被删除。您需要再次执行这些步骤以覆盖并允许下载文件。

禁用二进制和容器扫描

如果您的许可证不允许二进制和容器扫描，请在您的 values.yaml 文件中禁用 BDBA。这将导致 bdbaworker 容器不会加载，或被卸载（如果容器已加载）。仅支持签名扫描。

要禁用二进制和容器扫描，请编辑 values.yaml 文件的 “bdbaworker” 部分并设置：

```
enabled: false
```

11. 管理任务

在 Kubernetes 中配置密钥加密

Black Duck 支持对系统中的关键数据进行静态加密。此加密基于编排环境（Docker Swarm 或 Kubernetes）调配给 Black Duck 安装的密钥。创建和管理此密钥、创建备份密钥以及根据您所在组织的安全策略轮换密钥的过程如下所述。

要加密的关键数据如下：

- SCM 集成 OAuth 令牌
- SCM 集成提供商 OAuth 应用程序客户端密钥
- LDAP 凭据
- SAML 私有签名证书

 注：一旦启用了密钥加密，就永远不能禁用它。

什么是加密密钥？

加密密钥是一个随机序列，用于生成内部加密密钥以解锁系统内的资源。Black Duck 中的密钥加密由 3 个对称密钥（root 密钥、备份密钥和以前的密钥）控制。这三个密钥通过传递到 Black Duck 的种子，作为 Kubernetes 和 Docker Swarm 密钥生成。这三个密钥被命名：

- crypto-root-seed
- crypto-backup-seed
- crypto-prev-seed

在正常情况下，并非全部三个种子都会被激活使用。除非正在执行轮换操作，否则唯一活动的种子将是根种子。

保护根种子

必须保护根种子。拥有您的根种子以及系统数据副本的用户可以解锁并读取系统的受保护内容。某些 Docker Swarm 或 Kubernetes 系统默认情况下不静态加密密钥。强烈建议将这些编排系统配置为在内部加密，以便以后在系统中创建的密钥能够保持安全。

根种子是从备份重新创建系统状态（作为灾难恢复计划的一部分）所必需的。根种子文件的副本应存储在独立于编排系统的秘密位置，以便种子与备份的组合可以重新创建系统。不建议将根种子存储在与备份文件相同的位置。如果一组文件被泄露或被盗 – 两种情况都会出现，因此，建议为备份数据和种子备份设置单独的位置。

在 Kubernetes 中启用密钥加密

要在 Kubernetes 中启用密钥加密，必须在 values.yaml 编排文件中将 enableApplicationLevelEncryption 的值更改为 true：

```
# if true, enables application level encryption
enableApplicationLevelEncryption: true
```

密钥种子管理脚本

您可以在 Black Duck GitHub 公共存储库中找到示例管理脚本：

<https://github.com/blackducksoftware/secrets-encryption-scripts>

这些脚本不是用来管理 Black Duck 密钥加密，而是用来说明此处所述的低级 Docker 和 Kubernetes 命令的用法。有两组脚本，每组都在其自己的子目录中，对应于在 Kubernetes 和 Docker Swarm 平台上使用。对于 Kubernetes 和 Docker Swarm，各个脚本之间存在一对一对应关系（如果适用）。例如，两组脚本都包含一个具有如下名称的脚本：

createInitialSeeds.sh

在 Kubernetes 中生成种子

在 OpenSSL 中生成种子

可以使用任何机制（生成至少 1024 字节长度的安全随机内容）生成种子的内容。一旦创建种子并将其保存在密钥中，就应将其从文件系统中移除并保存在一个私密的安全位置。

OpenSSL 命令如下所示：

```
openssl rand -hex 1024 > root_seed
```

在 Kubernetes 中生成种子

有许多 Kubernetes 命令行将创建密钥。下面列出的命令可以更好地跟踪密钥及其是否更改，并确保能够使用联机系统操纵密钥。在 Black Duck 激活运行时，可以在 Kubernetes 中创建和删除密钥。

```
kubect1 create secret generic crypto-root-seed -n $NAMESPACE --save-config --dry-run=client --  
from-file=crypto-root-seed=./root_seed -o yaml | kubect1 apply -f -
```

要删除 Kubernetes 中之前的密钥：

```
kubect1 delete secret crypto-prev-seed -n $NAMESPACE
```

配置备份种子

建议备份根种子，以确保系统可以在灾难恢复场景中恢复。备份根种子是一个备用根种子，可用于恢复系统。因此，它必须以与根种子相同的方式安全地存储。

备份根种子具有一些特殊特性，即，一旦它与系统关联，即使在根种子轮换期间，它也仍然可行。一旦系统处理了备份种子，应将其从密钥中移除，以限制其受到攻击和泄漏的可能性。备份根种子可能有不同的（频率较低的）轮换计划，因为系统中的密钥不应在任何时候都处于“活动”状态。

当您需要或想要轮换根种子时，首先需要将当前根种子定义为上一个根种子。然后，您可以生成一个新的根种子并将其放置到位。

当系统处理这些种子时，以前的根密钥将用于轮换资源，以使用新的根种子。完成此处理后，应从密钥中移除之前的根种子，以完成轮换并清理旧资源。

创建备份根种子

初始创建后，备份种子/密钥将 TDEK（租户解密、加密密钥）低级密钥打包。示例脚本 createInitialSeeds.sh 将创建根种子和备份种子。一旦 Black Duck 运行，它使用两个密钥来打包 TDEK。

该操作完成并且根种子和备份种子都安全地存储在其他位置后，应删除备份种子密钥；请参阅[示例脚本 cleanupBackupSeed.sh](#)。

如果根密钥丢失或泄漏，备份密钥可用于替换根密钥；请参阅[示例脚本 useRootSeed.sh](#)。

轮换备份种子

与根密钥类似，备份种子应定期轮换。与根种子不同（旧的根种子存储为以前的种子密钥，而新的根种子密钥提供给系统），备份种子只是通过创建新的备份种子来进行轮换。请参阅[示例脚本 rotateBackupSeed.sh](#)。

轮换完成后，新的备份种子应安全存储并从 Black Duck 主机文件系统中移除。

在 Kubernetes 中管理密钥轮换

根据组织的安全策略定期轮换正在使用的根种子是一种好做法。要执行此操作，还需要一个额外的密钥来执行轮换。要轮换根种子，将当前根种子配置为“上一个根种子”，并生成新生成的根种子并将其配置为根种子。一旦系统处理此配置（具体细节如下），密钥将被轮换。

此时，新旧种子都能够解锁系统内容。默认情况下，将使用新的根种子，允许您测试并确保系统按预期工作。一旦所有内容都得到验证，您就可以通过移除“以前的根种子”来完成轮换。

从系统中移除之前的根种子后，就不能再将其用于解锁系统内容，并且可以将其丢弃。新的根种子现在是正确的根种子，应适当地备份和保护。

根密钥用于打包实际加密和解密 Black Duck 密钥的低级 TDEK（租户解密、加密密钥）。应该在方便 Black Duck 管理员并符合用户组织规则时，定期轮换根密钥。

轮换根密钥的过程是使用当前根种子的内容创建以前的种子密钥。然后，应创建一个新的根种子并将其存储在根种子密钥中。

Kubernetes 中的密钥轮换

对于 Kubernetes 来说，这三个操作都可以在运行 Black Duck 的情况下完成。Kubernetes 示例脚本 `rotateRootSeed.sh` 将把根种子提取到 `prev_root` 中，创建一个新的根种子，然后重新创建以前的种子和根种子。

轮换完成后，应移除上一个种子密钥；请参阅[示例脚本 cleanupPreviousSeed.sh](#)。同样，可以对正在运行的 Kubernetes Black Duck 实例执行此清理。

在用户界面中，转到“管理” > “系统信息” > “加密”，查看“加密诊断”选项卡即可跟踪轮换状态。

为 Blackduck 存储配置自定义卷

存储容器可配置为最多使用三 (3) 个卷来存储基于文件的对象。此外，可以将配置设置为将对象从一个卷迁移到另一个卷。

为什么使用多个卷？

默认情况下，存储容器使用单个卷来存储所有对象。此卷的大小取决于存储对象的典型客户使用情况。由于每个客户都不同，因此可能需要拥有比卷所能提供的空间更多的可用空间。由于并非所有卷都是可扩展的，因此可能需要添加不同的、更大的卷并将数据迁移到新卷。

可能需要多个卷的另一个原因是：卷托管在远程系统（NAS 或 SAN）上，并且该远程系统将被停用。需要创建托管在新系统上的第二个卷，并将内容移至该卷。

配置多个卷

要在 Kubernetes 中配置自定义存储提供商，请创建包含以下内容的覆盖文件：

```
storage:
  providers:
    - name: "file-1"
      enabled: true
      index: 1
      type: "file"
      preference: 20
      readonly: false
      migrationMode: "none"
      existingPersistentVolumeClaimName: ""
      pvc:
        size: "100Gi"
        storageClass: ""
        existingPersistentVolumeName: ""
      mountPath: "/opt/blackduck/hub/uploads"
    - name: "file-2"
      enabled: true
      index: 2
      type: "file"
      preference: 10
      readonly: false
      migrationMode: "none"
      existingPersistentVolumeClaimName: ""
      pvc:
        size: "200Gi"
        storageClass: ""
        existingPersistentVolumeName: ""
      mountPath: "/opt/blackduck/hub/uploads2"
    - name: "file-3"
      enabled: false
      index: 3
      type: "file"
      preference: 30
      readonly: false
      migrationMode: "none"
      existingPersistentVolumeClaimName: ""
      pvc:
        size: "100Gi"
        storageClass: ""
        existingPersistentVolumeName: ""
      mountPath: "/opt/blackduck/hub/uploads3"
```

在上述覆盖文件中，提供商 1 和 提供商 2 均已启用，而提供商 2 具有较高的优先级（较低的偏好程度编号），因此所有新内容都将定向到该位置。

每个提供商的可能设置如下所示：

设置	详细信息
name	默认值：无。 有效值：任意。 备注：这是一个识别标签，用于帮助管理这些提供商。
enabled	默认值：true用于提供商 1，false 用于其他。 有效值：true 或 false。 备注：指示是否启用提供商。
index	默认值：无。 有效值：1、2、3。 备注：指示提供商编号。配置文件中的顺序并不重要。
type	默认值：file。

设置	详细信息
	有效值：file。 备注：“file”是唯一受支持的提供商类型。
preference	默认值：index乘以 10。 有效值：0-999。 备注：设置提供商的偏好程度。有最高优先级（最低偏好程度编号）的提供商将具有向其添加的新内容。 注意：所有提供商偏好程度必须唯一，两个提供商不能共享相同的值。
readonly	默认值：false。 有效值：true 或 false。 备注：表示提供商为只读。最高优先级（最低偏好程度编号）的提供商不能为只读状态，否则系统无法正常工作。 处于“只读”状态的提供商不会因添加数据或移除数据而更改存储卷，但数据库中的元数据将被处理，以记录对象删除和其他更改。
migrationMode	默认值：none。 有效值：none、drain、delete、duplicate。 备注：配置提供商的迁移模式。本文档的迁移章节详细介绍了此模式以及使用它的方法。
existingPersistentVolumeClaimName	默认值：“”。 有效值：任何有效的 k8s 标识符。 备注：允许您为该卷指定特定的持久性卷声明名称。
pvc.size	默认值：none。 有效值：任何有效大小。 备注：允许您指定该卷的可用空间量。
pvc.storageClass	默认值：“”。 有效值：任何有效的 k8s 标识符。 备注：允许您为该卷指定特定的存储类。
pvc.existingPersistentVolumeName	默认值：“”。 有效值：任何有效的 k8s 标识符。 备注：允许您为该卷指定特定的持久性卷名称。
mountPath	默认值：特定于索引 - 请参阅注释。 有效值： /opt/blackduck/hub/uploads /opt/blackduck/hub/uploads2 /opt/blackduck/hub/uploads3 备注： 设置特定提供商的挂载点。索引为一 (1) 的提供商必须指定挂载点 /opt/blackduck/hub/uploads。索引为二 (2) 的提供商必须指定挂载点 /opt/blackduck/hub/uploads2。索引为三 (3) 的提供商必须指定挂载点 /opt/blackduck/hub/uploads3

在卷之间迁移

配置多个卷后，可以将内容从一个或多个提供商卷迁移到新的提供商卷。这只能对不是最高优先级（最低偏好程度）的提供商执行。为此，请使用以下迁移模式之一配置卷。配置完成后，需要重新启动 Black Duck 才能启动迁移，迁移由后台作业执行，直至完成。

迁移模式	详细信息
none	目的：表示没有正在进行的迁移。 备注：默认迁移模式。
drain	目的：此模式将内容从配置的提供商移动到最高优先级（最低偏好程度编号）的提供商。移动内容后，将立即从源提供商中移除该内容。 备注：这是一个直接的移动操作 - 将其添加到目标提供商并从来源中移除。
delete	目的：此模式将内容从配置的提供商复制到最高优先级（最低偏好程度编号）的提供商。复制内容后，该内容将在源提供商中标记为删除。应用标准删除保留期 - 在该期限之后，内容将被移除。 备注：此移动允许系统在保留窗口期内从备份中恢复，以便源提供商中的内容仍然保持可行。默认保留期为 6 小时。
duplicate	目的：此模式将内容从配置的提供商复制到最高优先级（最低偏好程度编号）的提供商。复制内容后，来源（包括元数据）将保持不变。 备注：重复迁移后，数据库中将有多个卷，其中包含所有内容和元数据。如果您在“复制和转储”过程中执行下一步骤并取消配置原始卷，则文件将被删除，但元数据将保留在数据库中 - 引用未知卷，并在删减程序作业中生成警告（作业错误）。要解决此错误，请使用以下属性启用孤立元数据记录的删减： <code>storage.pruner.orphaned.data.pruning.enable=true</code>

配置 jobrunner 线程池

在 Black Duck 中，有两个作业池，一个运行计划作业（称为定期池），另一个运行从某些事件（包括 API 或用户交互）启动的作业（称为按需池）。

每个池都有两个设置：最大线程数和预取。

最大线程数是 jobrunner 容器可以同时运行的最大作业数。将定期和按需最大线程数相加，总和不应大于 32，因为大多数作业使用数据库，并且最多有 32 个连接。Jobrunner 内存很容易饱和，因此默认的线程数设置得非常低。

预取是每个 jobrunner 容器在每次往返数据库的过程中将抓取的作业数。该值设置得越高，效率越高，但该值设置得越低，将使负载更均匀地分布在多个 jobrunner 中（但通常情况下，均匀的负载不是 jobrunner 的设计目标）。

在 Kubernetes 中，可以使用以下覆盖文件覆盖线程计数设置：

```
jobrunner:
  maxPeriodicThreads: 2
  maxPeriodicPrefetch#1
  maxOndemandThreads#4
```

```
maxOndemandPrefetch#2
```

配置就绪探针

通过编辑以下 values.yaml 中的布尔值标志，您可以启用或禁用就绪探针：

```
enableLivenessProbe: true
enableReadinessProbe: true
enableStartupProbe: true
```

配置 HUB_MAX_MEMORY 设置

在基于 Kubernetes 的部署中，会自动为相关容器设置配置参数 HUB_MAX_MEMORY。该值按内存限制的百分比计算，默认值为 90%。

在 gen04 部署调整中，maxRamPercentage 控制使用的百分比；选择此设置的值，以使 HUB_MAX_MEMORY 具有与之前相同的值。

使用 Helm 在 OpenShift 上进行迁移

如果您从基于 PostgreSQL 9.6 的 Black Duck 版本升级，此迁移将用 Black Duck 提供的容器替换 CentOS PostgreSQL 容器。此外，synopsys-init 容器将替换为 blackduck-postgres-waiter 容器。

在普通 Kubernetes 上，升级作业的容器将以 root 身份运行（除非覆盖）。但是，唯一的要求是作业与 PostgreSQL 数据卷的所有者以相同的 UID 运行（默认为 UID=26）。

在 OpenShift 上，升级作业假定它将使用与 PostgreSQL 数据卷所有者相同的 UID 运行。