



发行说明

2021.2.0 版本



此版本的 发行说明 指的是 Black Duck 的 2021.2.0 版本。

本文档在 2021年7月12日 创建或更新。

请将您的意见和建议发送至：

Synopsys  
800 District Avenue, Suite 201  
Burlington, MA 01803-5061 USA

版权所有 © 2021, 所有者：Synopsys。

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均为其各自所有者的独占财产。

<b>CH: 章节 1: 产品公告</b>	<b>1</b>
版本 2021.2.0 的公告	1
Azure 客户通知	1
对外部数据库弃用 PostgreSQL 版本 9.6	1
不再支持 Internet Explorer 11	1
已弃用的页面	1
日语	1
版本 2020.12.0 的公告	1
新容器和系统要求更改	1
终止对 Internet Explorer 11 的支持	2
日语	2
版本 2020.10.0 的公告	2
新容器和系统要求更改推迟到 2020.12.0 版本	2
日语	3
版本 2020.8.0 的公告	3
对外部数据库弃用 PostgreSQL 版本 9.6	3
2020.10.0 版本中的已弃用 API	3
日语	3
版本 2020.6.1 的公告	3
终止对 Internet Explorer 11 的支持	3
版本 2020.6.0 的公告	3
未来版本中的新容器和系统要求更改	3
弃用 Internet Explorer 11 支持	4
对外部数据库的 PostgreSQL 11 支持	4
版本 2020.2.0 的公告	5
单个文件匹配	5
Docker Compose 支持	5
版本 2019.12.0 的公告	5
升级 Black Duck	5
即将发布的 2020.2.0 版本中的单个文件匹配	6
Docker Compose 支持	7
<b>CH: 章节 2: 发布信息</b>	<b>8</b>
版本 2021.2.0	8

版本 2021.2.0 中的新增功能和更改功能 .....	8
修复了 2021.2.0 中的问题 .....	13
版本 2020.12.0 .....	14
版本 2020.12.0 中的新增功能和更改功能 .....	14
修复了 2020.12.0 中的问题 .....	18
版本 2020.10.1 .....	19
版本 2020.10.1 中的新增功能和更改功能 .....	19
修复了 2020.10.1 中的问题 .....	19
版本 2020.10.0 .....	19
版本 2020.10.0 中的新增功能和更改功能 .....	19
修复了 2020.10.0 中的问题 .....	24
版本 2020.8.2 .....	25
版本 2020.8.2 中的新增功能和更改功能 .....	25
修复了 2020.8.2 中的问题 .....	26
版本 2020.8.1 .....	26
版本 2020.8.1 中的新增功能和更改功能 .....	26
修复了 2020.8.1 中的问题 .....	26
版本 2020.8.0 .....	27
版本 2020.8.0 中的新增功能和更改功能 .....	27
修复了 2020.8.0 中的问题 .....	33
版本 2020.6.2 .....	34
版本 2020.6.2 中的新增功能和更改功能 .....	34
修复了 2020.6.2 中的问题 .....	34
版本 2020.6.1 .....	34
版本 2020.6.1 中的新增功能和更改功能 .....	34
修复了 2020.6.1 中的问题 .....	34
版本 2020.6.0 .....	34
版本 2020.6.0 中的新增功能和更改功能 .....	34
修复了 2020.6.0 中的问题 .....	39
版本 2020.4.2 .....	40
版本 2020.4.2 中的新增功能和更改功能 .....	40
修复了 2020.4.2 中的问题 .....	40
版本 2020.4.1 .....	40
版本 2020.4.1 中的新增功能和更改功能 .....	40
修复了 2020.4.1 中的问题 .....	40
版本 2020.4.0 .....	40
版本 2020.4.0 中的新增功能和更改功能 .....	40
修复了 2020.4.0 中的问题 .....	45
版本 2020.2.1 .....	46
版本 2020.2.1 中的新增功能和更改功能 .....	46
修复了 2020.2.1 中的问题 .....	46

版本 2020.2.0 .....	46
版本 2020.2.0 中的新增功能和更改功能 .....	46
修复了 2020.2.0 中的问题 .....	49
版本 2019.12.1 .....	50
版本 2019.12.1 中的新增功能和更改功能 .....	50
修复了 2019.12.1 中的问题 .....	50
版本 2019.12.0 .....	51
版本 2019.12.0 中的新增功能和更改功能 .....	51
修复了 2019.12.0 中的问题 .....	53
<b>CH: 章节 3: 已知问题和限制 .....</b>	<b>55</b>

## 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 and 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。

Black Duck 集成文档可在 [Confluence](#) 上找到。

## 客户支持

如果您在软件或文档方面遇到任何问题，请联系 Synopsys 客户支持。

您可以通过以下几种方式联系 Synopsys 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。

要打开支持案例，请登录 Synopsys Software Integrity 社区网站，网址为：<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](#)。

## Synopsys Software Integrity 社区

Synopsys Software Integrity 社区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 Synopsys 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](mailto:community.manager@synopsys.com)。

## 培训


Synopsys Software Integrity 的客户教育 (SIG Edu) 板块是满足您的所有 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 Synopsys Software Integrity 的客户教育 (SIG Edu) 板块，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>，或者从 Black Duck UI 的“帮助”

菜单 () 中选择 **Black Duck 教程** 获取 Black Duck 的帮助信息。

### 版本 2021.2.0 的公告

#### Azure 客户通知

Black Duck 版本 2021.2.0 在发布时存在一个已知问题, 该问题影响在 Azure Kubernetes Services (AKS) 上部署并将 Azure Database for PostgreSQL 用作外部数据库的客户。请注意, 这是针对 Azure 平台上的 Black Duck 客户推荐的标准配置。目前, 不建议在具有外部数据库的 Azure 平台上运行的客户升级到 2021.2.0。这样做将使系统无法运行, 并迫使您将安装恢复到先前的状态。

我们预计这一问题将在未来的 Black Duck 版本中得到解决, 并将在版本详细信息已知时发布公告。

如果您在 AKS 上运行并使用内部 PostgreSQL 数据库, 则不会出现问题, 系统将按预期工作。但是, 这将在 AKS 平台上的非典型安装。

如果您有任何疑虑和疑问, 请联系 Black Duck 支持部门寻求帮助。

#### 对外部数据库弃用 PostgreSQL 版本 9.6

从 Black Duck 2021.6.0 版本开始, Synopsys 不再支持将 PostgreSQL 版本 9.6 用于外部数据库。

从 Black Duck 2021.6.0 版本开始, Black Duck 只支持将 PostgreSQL 版本 11.x 用于外部数据库。

#### 不再支持 Internet Explorer 11

Synopsys 已终止对 Internet Explorer 11 的支持。

#### 已弃用的页面

“扫描 > 组件”页面从 2021.2.0 版本开始弃用, 并将在将来的版本中移除。

#### 日语

2020.12.0 版的 UI、联机帮助和发布说明已本地化为日语。

### 版本 2020.12.0 的公告

#### 新容器和系统要求更改

还有两个附加容器: 2020.12.0 版的 BOM 引擎和 RabbitMQ(现在是必需的容器)。

运行所有容器的单个实例的最低系统要求是:



- 6 个 CPU
- 26 GB RAM(最低 Redis 配置); 29 GB RAM(最佳配置), 可为 Redis 驱动的高速缓存提供更高的可用性
- 250 GB 可用磁盘空间, 用于数据库和其他 Black Duck 容器
- 数据库备份的相应空间

运行带有 Black Duck - 二进制分析 的 Black Duck 所需的最低硬件包括:

- 7 个 CPU
- 30 GB RAM(最低 Redis 配置); 33 GB RAM(最佳配置), 可为 Redis 驱动的高速缓存提供更高的可用性
- 350 GB 可用磁盘空间, 用于数据库和其他 Black Duck 容器
- 数据库备份的相应空间

**注意:** 每个附加的 binaryscanner 容器都需要一个额外的 CPU、2 GB RAM 和 100 GB 可用磁盘空间。

## 终止对 Internet Explorer 11 的支持

对 Internet Explorer 11 的支持已弃用, Synopsys 将从 Black Duck 2021.2.0 发布开始停止对 Internet Explorer 11 的支持。

## 日语

2020.10.0 版的 UI、联机帮助和发布说明已本地化为日语。

## 版本 2020.10.0 的公告

### 新容器和系统要求更改推迟到 2020.12.0 版本

Black Duck 此前曾宣布将增加两个容器: 2020.10.0 版的 BOM 引擎和 RabbitMQ(现在是必需的容器)。这一要求已推迟到 2020.12.0 版。

对于 2020.12.0 版, 运行所有容器的单个实例的最低系统要求是:

- 6 个 CPU
- 26 GB RAM(最低 Redis 配置); 29 GB RAM(最佳配置), 可为 Redis 驱动的高速缓存提供更高的可用性
- 250 GB 可用磁盘空间, 用于数据库和其他 Black Duck 容器
- 数据库备份的相应空间

对于 2020.12.0 版, 运行带有 Black Duck - 二进制分析 的 Black Duck 所需的最低硬件为:

- 7 个 CPU
- 30 GB RAM(最低 Redis 配置); 33 GB RAM(最佳配置), 可为 Redis 驱动的高速缓存提供更高的可用性
- 350 GB 可用磁盘空间, 用于数据库和其他 Black Duck 容器
- 数据库备份的相应空间

**注意:** 每个附加的 **binaryscanner** 容器都需要一个额外的 CPU、2 GB RAM 和 100 GB 可用磁盘空间。

## 日语

2020.8.0 版的 UI、联机帮助和发布说明已本地化为日语。

## 版本 2020.8.0 的公告

### 对外部数据库弃用 PostgreSQL 版本 9.6

从 Black Duck 2021.6.0 版本开始, Synopsys 不再支持将 PostgreSQL 版本 9.6 用于外部数据库。

从 Black Duck 2021.6.0 版本开始, Black Duck 只支持将 PostgreSQL 版本 11.x 用于外部数据库。

### 2020.10.0 版本中的已弃用 API

在 Black Duck 2020.10.0 版本中, `/api/catalog-risk-profile-dashboard` API 将返回 HTTP 410 (GONE), 从 Black Duck 2020.12.0 版本开始, 此 API 将不可用。

将在 2020.10.0 版本中公布一个新的 API 来取代 `/api/catalog-risk-profile-dashboard`。

## 日语

2020.6.0 版的 UI、联机帮助和发布说明已本地化为日语。

## 版本 2020.6.1 的公告

### 终止对 Internet Explorer 11 的支持

对 Internet Explorer 11 的支持已弃用, Synopsys 将从 Black Duck 2021.2.0 版本开始停止对 Internet Explorer 11 的支持。

## 版本 2020.6.0 的公告

### 未来版本中的新容器和系统要求更改

#### 2020.8.0 版本

在 **2020.8.0 版本**中, 将在 Black Duck 中添加新的 Redis 容器。此容器将在 Black Duck 中实现更一致的缓存功能, 并将用于提高应用程序性能。

以下是运行所有容器的单个实例所需的最低硬件:

- 5 个 CPU
- 21 GB RAM(最低 Redis 配置); 24 GB RAM(最佳配置), 可为 Redis 驱动的高速缓存提供更高的可用性
- 250 GB 可用磁盘空间, 用于数据库和其他 Black Duck 容器
- 数据库备份的相应空间

以下是运行带有 Black Duck - 二进制分析的 Black Duck 所需的最低硬件:

- 6 个 CPU
- 25 GB RAM(最低 Redis 配置); 28 GB RAM(最佳配置), 可为 Redis 驱动的高速缓存提供更高的可用性
- 350 GB 可用磁盘空间, 用于数据库和其他 Black Duck 容器
- 数据库备份的相应空间

**注意:** 每个附加的 binaryscanner 容器都需要一个额外的 CPU、2 GB RAM 和 100 GB 可用磁盘空间。

## 2020.10.0 版本

在 **2020.10.0** 版本中, Black Duck 将添加两个附加容器: BOM 引擎和 RabbitMQ(将是必需的容器)。这些容器将用于提高应用程序性能, 主要是提高项目版本 BOM 性能。

初始测试表明, 运行所有容器的单个实例的最低系统要求如下:

- 6 个 CPU
- 26 GB RAM(最低 Redis 配置); 29 GB RAM(最佳配置), 可为 Redis 驱动的高速缓存提供更高的可用性
- 250 GB 可用磁盘空间, 用于数据库和其他 Black Duck 容器
- 数据库备份的相应空间

初始测试表明, 运行带有 Black Duck - 二进制分析的 Black Duck 所需的最低硬件将是:

- 7 个 CPU
- 30 GB RAM(最低 Redis 配置); 33 GB RAM(最佳配置), 可为 Redis 驱动的高速缓存提供更高的可用性
- 350 GB 可用磁盘空间, 用于数据库和其他 Black Duck 容器
- 数据库备份的相应空间

**注意:** 每个附加的 binaryscanner 容器都需要一个额外的 CPU、2 GB RAM 和 100 GB 可用磁盘空间。

请注意, 这些系统要求基于初始测试结果。最终系统要求可能低于此处所示的要求, 但不会超过此处列出的要求。

## 弃用 Internet Explorer 11 支持

从 Black Duck 2021.2.0 版本开始, Synopsys 将不再支持 Internet Explorer 11。

## 对外部数据库的 PostgreSQL 11 支持

对于使用外部 PostgreSQL 的新安装, Black Duck 现在支持 PostgreSQL 11.7。尽管外部 PostgreSQL 实例仍然完全支持 PostgreSQL 9.6, 但 Synopsys 建议使用外部 PostgreSQL 的新安装使用 PostgreSQL 11.7。

对于内部 PostgreSQL 容器的用户, PostgreSQL 9.6 仍然是 Black Duck 2020.6.0 支持的版本。

## 版本 2020.2.0 的公告

### 单个文件匹配

如前所述, 为了减少由于不明确匹配而导致的误报, 作为特征扫描的一部分执行单个文件匹配不再是 **Black Duck CLI** 和 **Synopsys Detect** 扫描的默认行为。

单个文件匹配是纯粹基于单个文件的校验和信息来识别组件。在 **Black Duck** 中, 对于一小组文件扩展名 (.js、.apklib、.bin、.dll、.exe、.o 和 .so), 常规特征扫描根据与一个文件的校验和匹配将文件与组件匹配。不幸的是, 这种匹配并不总是准确的, 并且产生了相当多的误报。为了改善整个 **Synopsys** 客户群的整体开发人员体验, 单个文件匹配不再是默认行为, 现在它是可选功能。

升级到 **2020.2.0** 将关闭单个文件匹配, 并可能导致某些组件从 **BOM** 上丢失。要估计对 **BOM** 的影响, 请查找仅具有“精确文件”匹配类型的组件, 以查看可能从 **BOM** 中丢失的组件。请注意, 如果您正在扫描 **Docker** 映像, “精确文件”匹配不受此更改的影响。

特征扫描程序 具有一个新参数用于启用单个文件匹配。如果您使用 **Synopsys Detect** 进行扫描, **6.2** 版将有一个新参数, 支持打开/关闭单个文件匹配, 默认值为“关闭”。

### Docker Compose 支持

如前所述, **Docker Compose** 不再是 **2020.2.0** 版本支持的编排方法。

## 版本 2019.12.0 的公告

### 升级 Black Duck

在升级过程中, 作为对报告数据库所做更改的一部分, 迁移脚本将运行以清除 `audit_event` 表中不再使用的行。此迁移脚本可能需要一些时间来运行, 具体取决于 `audit_event` 表的大小。作为指南, `audit_event` 表大小为 **350 GB** 时, 迁移脚本运行大约 **20 分钟**。


要确定审核事件表的大小:

执行以下操作之一:

- 从 `bds_hub` 数据库中运行以下命令:

```
SELECT pg_size_pretty( pg_total_relation_size('st.audit_event') );
```

- 以“系统管理员”角色登录到 **Black Duck UI** 并执行以下操作:

1. 单击“展开菜单”图标  并选择**管理**。

此时将显示“管理”页面。

2. 选择**系统管理**以显示“系统信息”页面。
3. 在页面的左列中选择 **db**。
4. 滚动到**表大小**部分。查找 `audit_event` 表名称的 `total_tbl_size` 值。

对于本地 **Kubernetes** 和 **OpenShift** 用户, 在升级之前, 请禁用活跃度检查 (`--liveness-probes false`), 升级 **Black Duck**, 然后等待用户界面出现。出现用户界面后, 启用活跃度检查 (`--`

liveness-probes true)。

运行迁移脚本后, **Synopsys** 强烈建议在 `audit_event` 表上运行 `VACUUM` 命令以优化 **PostgreSQL** 性能。

- 根据您的系统使用情况, 运行 `VACUUM` 命令可以回收大量不再被 **Black Duck** 占用的磁盘空间。
- 通过运行此命令, 查询性能将得到提高。

**注意:** 如果不运行 `VACUUM` 命令, 可能会导致性能下降。

请注意, 此命令所需的磁盘空间量是 `audit_event` 表当前使用的磁盘空间量的两倍。

**重要提示:** 您必须确保有足够的空间运行 `VACUUM` 命令, 否则, 它将因磁盘空间不足而失败, 并可能损坏整个数据库。

要为具有容器化 **PostgreSQL** 数据库部署的 **Docker Compose** 和 **Docker Swarm** 用户运行 `VACUUM` 命令:

1. 如上所述确定 `audit_event` 表的大小。
2. 通过运行以下命令确定 **PostgreSQL** 容器的容器 ID:

```
docker ps
```

3. 运行以下命令以管理 **PostgreSQL** 容器:

```
docker exec -it <container_ID> psql bds_hub
```

4. 运行以下命令:

```
VACUUM FULL ANALYZE st.audit_event;
```

对于具有外部 **PostgreSQL** 数据库部署的 **Docker Compose** 和 **Docker Swarm** 用户: 确定 `audit_event` 表的大小, 执行 `VACUUM` 命令, 完成后重新启动部署。

对于本地 **Kubernetes** 和 **OpenShift** 用户, 有关详细信息, 请参阅 **Synopsys Operator** 升级说明。

## 即将发布的 2020.2.0 版本中的单个文件匹配

为了减少由于模糊匹配而导致的误报, 从 **Black Duck** 版本 2020.2 开始, 作为特征扫描的一部分执行单个文件匹配不再是 **Black Duck CLI** 和 **Synopsys Detect** 扫描的默认行为。

单个文件匹配是纯粹基于单个文件的校验和信息来识别组件。在 **Black Duck** 中, 对于一小组文件扩展名 (`.js`、`.apklib`、`.bin`、`.dll`、`.exe`、`.o` 和 `.so`), 常规特征扫描根据与一个文件的校验和匹配将文件与组件匹配。不幸的是, 这种匹配并不总是准确的, 并且产生了相当多的误报。这些误报要求您花费额外的精力审查和调整 **BOM**。尽管有些用户可能希望在 **BOM** 中达到这种精确度和精细度级别, 但大多数客户并不希望或不需要这种级别的匹配。因此, 根据客户和字段输入, 为了改善整个 **Synopsys** 客户群的整体开发人员体验, 单个文件匹配不再是默认行为, 而是可选功能。

这可能会导致某些组件从您的 **BOM** 中丢失, 这可能是需要的, 也可能是不需要的。因此, 在 **Black Duck 2020.2** 版本中, **Synopsys** 将提供一些机制, 以便您可以重新启用单个文件匹配, 包括通过 **CLI**、**Synopsys Detect** 和 **Synopsys Detect (Desktop)**。

## Docker Compose 支持

自 2019 年 12 月 31 日起, 不再支持 Docker Compose。

### 版本 2021.2.0

#### 版本 2021.2.0 中的新增功能和更改功能

##### 新的自定义漏洞仪表板

为了便于您轻松查看对您至关重要的漏洞, 在 2021.2.0 中, “安全”仪表板已根据您保存的漏洞搜索替换为自定义漏洞仪表板。Black Duck 现在允许您使用各种属性搜索您的项目和/或 Black Duck 知识库中使用的漏洞, 保存搜索, 然后使用“仪表板”页面从这些保存的搜索中查看仪表板。

对于每个漏洞, 自定义漏洞仪表板显示以下信息:

- BDSA 或 NVD 漏洞 ID。选择漏洞 ID 以显示有关漏洞的更多信息, 比如其他分数值。
- 受此漏洞影响的项目版本数, 带有可查看漏洞的**受影响的项目**选项卡的链接, 该选项卡列出了受此漏洞影响的项目版本。
- 总体风险评分。
- 解决方案、解决方法或漏洞利用是否可用。
- 首次检测、发布和最后修改漏洞的日期。
- 此安全漏洞的常见弱点枚举 (CWE) 编号。

##### 漏洞搜索增强

通过可用于搜索漏洞的属性以及搜索结果中显示的信息, 可以增强漏洞搜索功能。您可以选择是搜索项目中的漏洞还是 Black Duck 知识库中的漏洞。

搜索漏洞时, 可以使用以下属性:

- 影响项目
- 默认修复
- 可到达
- 漏洞利用
- 首次检测到
- 修复状态
- 解决方案
- 基本分数
- 可利用性分数
- 影响分数

- 总体得分
- 发布年份
- 严重性
- 来源(BDSA 或 NVD)
- 时间分数
- 解决方法

现在可以保存这些漏洞搜索结果并在“仪表板”页面中查看, 如上所述。

## 能够管理项目的许可证冲突

为了降低许可证侵权的风险, 您需要了解 BOM 中的组件拥有的许可证的条款与项目声明的许可证不兼容的情况。**Black Duck** 现在可以识别这些许可条款冲突, 并将它们显示在位于**法律**选项卡上的新的**许可证冲突**选项卡上。

您还可以设置在组件的许可证与项目版本的许可证冲突时触发的策略规则。

请注意, **Black Duck** 仅确定许可证风险较高的组件版本的许可证冲突。对于 **Black Duck** 许可证风险模型, “高风险”意味着此系列中的许可证在该业务场景(分发类型和组件用法组合)下往往存在许可证冲突, 从而导致许可证不兼容。中或低风险意味着, 如果业务场景发生变化(或定义不正确)或由于其他非许可证冲突因素, 它可能会存在风险。

## 依赖关系

在 **Synopsys Detect** 扫描中发现直接或过渡依赖关系时, **Black Duck** 现在会在项目版本的**安全**选项卡中列出每种依赖关系类型的匹配数。

对于过渡依赖关系, 依赖关系树显示引入此依赖关系的组件、按严重性级别列出的漏洞以及使用该依赖关系路径引入组件的次数的匹配计数。

## 报告数据库增强

已将忽略的组件的新表 (component\_ignored) 添加到报告数据库中。它包含以下列:

- id。ID
- project\_version\_id。项目版本 ID。
- component\_id。组件 ID。
- component\_version\_id。组件版本 ID。
- component\_name。组件名称。
- component\_version\_name。组件版本名称。
- version\_origin\_id。版本来源 ID。
- origin\_id。来源 ID。
- origin\_name。来源名称。
- ignored。布尔值, 指示是否忽略组件。
- policy\_approval\_status。策略审批状态。
- review\_status。查看组件的状态。
- reviewed\_by。审查组件的用户。



- reviewed\_on。审查组件的时间。
- security\_critical\_count。严重安全漏洞的数量。
- security\_high\_count。高风险安全漏洞的数量。
- security\_medium\_count。中等风险安全漏洞的数量。
- security\_low\_count。低风险安全漏洞的数量。
- security\_ok\_count。无风险安全漏洞的数量。
- license\_high\_count。高许可证风险的数量。
- license\_medium\_count。中等许可证风险的数量。
- license\_low\_count。低许可证风险的数量。
- license\_ok\_count。无许可证风险的数量。
- operational\_high\_count。高操作风险的数量。
- operational\_medium\_count。中等操作风险的数量。
- operational\_low\_count。低操作风险的数量。
- operational\_ok\_count。无操作风险的数量。

已将用户信息的新表 (user) 添加到报告数据库中。它包含以下列。

- id。ID。
- first\_name。用户的名字。
- last\_name。用户的姓氏。
- username。**Black Duck** 中用户的用户名。
- email。用户的电子邮件地址。
- active。表示此用户是否处于活动状态的布尔值。
- last\_login。用户上次登录到 **Black Duck** 的时间。

## 许可证编辑增强

在 **BOM** 中编辑许可证时进行了以下增强。

- 在编辑组件的许可证时, **Black Duck** 现在使您能够在根级别或与原始许可证相同的级别为 **BOM** 中的组件轻松创建新的或编辑现有的多许可证方案。
- 如果为组件选择了不同的许可证, 您现在可以将许可证恢复为 **Black Duck** 知识库 中定义的原始许可证。
- 组件名称版本“组件许可证”对话框中的一个新选项使您可以轻松地看到存在编辑模式。

## 报告增强

source\_date\_time.csv 项目版本报告的末尾添加了一个新列“存档上下文和路径”。此列将现有“路径”和“存档内容”列中显示的信息串联在一起, 以提供每个组件的完整路径。

## 通知文件报告

通知文件报告已得到改进, 版权数据不再包含单个组件来源的重复信息。

## 二进制扫描增强

现在, 二进制扫描除了返回完全匹配之外, 还返回部分匹配。


## 深度许可证数据增强

在审查文件中深度许可证数据的证据时, **Black Duck** 现在会突出显示触发许可证文本匹配的许可证文本。

## BOM 引擎

为了缩短 **Black Duck UI** 响应时间, 现在将由 **BOM** 引擎执行许可证更新。此过程可在“BOM 处理状态”对话框中显示为“许可证更新”或“许可条款履行更新”事件, 可从 **BOM** 访问该对话框。

## Black Duck 教程

要轻松查看 **Black Duck** 培训, 您现在可以从 **Black Duck UI** 的“帮助”菜单 () 中选择 **Black Duck 教程**。

## 修改密码配置

具有“系统管理员”角色的用户现在可以为本地 **Black Duck** 帐户设置密码要求。具有“超级用户”角色的用户无法再配置密码要求。

## 策略规则增强

策略管理现在提供了基于项目版本自定义字段创建策略规则的功能, 这些字段包括布尔值、日期、下拉列表、多选、单选和文本字段类型。




## Synopsys Detect 的托管位置

外部连接受限的 **Black Duck** 客户现在可以定义 **Synopsys Detect** 的内部托管位置。使用此信息, 这些用户可以利用 **Code Sight** 在其开发人员库中进行部署, 以运行按需软件组合分析 (SCA) 扫描。

## 保存的搜索仪表板增强

对于“仪表板”页面上显示的每个已保存搜索, **Black Duck** 现在会列出上次更新搜索的日期和时间。弹出窗口将显示保存的搜索过滤器以及一个链接, 使您可以打开“查找”页面以编辑和保存修订后的已保存搜索。

## 代码段分类增强

已将图标添加到**来源**选项卡, 以便更容易区分未确认 ()、已确认 () 和已忽略 () 代码段。

## 支持的浏览器版本

- Safari 版本 14.0.3( 156104.3.1.6、15610)
- Chrome 版本 88.0.4324.150( 正式版本) (x86\_64)
- Firefox 版本 85.0.2( 64 位)
- Microsoft Edge 版本 88.0.705.63( 正式版) ( 64 位)

## 容器版本

- blackducksoftware/blackduck-postgres:1.0.16
- blackducksoftware/blackduck-authentication:2021.2.0
- blackducksoftware/blackduck-webapp:2021.2.0
- blackducksoftware/blackduck-scan:2021.2.0
- blackducksoftware/blackduck-jobrunner:2021.2.0
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash:1.0.9
- blackducksoftware/blackduck-registration:2021.2.0
- blackducksoftware/blackduck-nginx:1.0.30
- blackducksoftware/blackduck-documentation:2021.2.0
- blackducksoftware/blackduck-upload-cache:1.0.15
- blackducksoftware/blackduck-redis:2021.2.0
- blackducksoftware/blackduck-bomengine:2021.2.0
- sigsynopsys/bdba-worker:2020.12-1
- blackducksoftware/rabbitmq:1.2.2

## 支持的 Docker 版本

Black Duck 安装支持 Docker 版本 18.09.x、19.03.x 和 20.10.x( CE 或 EE)。

## Docker webapp-volume

Docker webapp-volume 不再用于编排。(可选)用户可以备份和修整 Docker webapp-volume;其他情况下不需要执行任何操作。

## API 增强

- API 文档现在只能在 <https://<Black Duck server URL>/api-doc/public.html> 上获得。
- 增加了按创建日期过滤代码位置 (/api/codelocations) 的功能。
- 修复了用于下载 SAML 身份提供程序元数据 XML 文件 (api/sso/idp-metadata endpoint) 的 API, 该 API 在以前的版本中运行出错。
- 修复指导端点 (GET /api/components/{componentId}/versions/{componentVersionId}/remediating) 不再返回“410 GONE”响应。您必须切换到升级指导端点 (GET /api/components/{componentId}/versions/{componentVersionId}/upgrade-guidance), 该端点与已移除的修复指导端点不兼容。
- 添加了报告依赖关系路径端点以显示组件的依赖关系路径:  
  
`/api/project/{projectId}/version/{projectVersionId}/origin/{originId}/dependency-paths`
- 添加了 Synopsys Detect URI 端点, 仅用于设置或更新读取“系统设置”页面上的 Synopsys Detect URI:  
  
`/external-config/detect-uri`

## Ubuntu 操作系统

适合在 Docker 环境中安装 Black Duck 的首选 Ubuntu 操作系统现在为版本 18.04.x。

## 日语

2020.12.0 版的 UI、联机帮助和发布说明已本地化为日语。

## 修复了 2021.2.0 中的问题

在此发布中修复了客户报告的以下问题：

- (Hub-22103)。修复了 Black Duck 服务器在更新许可证状态时没有及时响应的问题。
- (Hub-22623)。修复了企业客户在 UI 中加载“摘要仪表板”时仪表板经常超时的的问题。
- (Hub-24332)。修复了扫描相同代码位置导致重复通知的问题。
- (Hub-25374)。修复了数据库 azure\_maintenance 的权限错误。
- (Hub-25580)。修复了 BOM 中显示的组件在第 9 页之后排序错误的问题。
- (Hub-25666)。修复了端点 /usergroups/<group #>/role 的分页问题。
- (Hub-26030)。修复了在执行操作后未按项目名称为仪表板保留排序选项的问题。
- (Hub-26324)。修复了上传扫描时出现以下错误“java.lang.IllegalStateException: [file:/C:/src/External/PackageManager/ProjectTemplates/com.unity.template.universal-10.1.0.tgz] 的父级不存在”的问题。
- (Hub-26343)。修复了无法注册 Black Duck 的问题，因为注册容器的堆空间不足。
- (Hub-26493)。修复了当用户移除自己项目成员身份时出现的混淆错误消息。
- (Hub-26501)。修复了无法在“编辑组件”对话框中选择 cordova-plugin-inappbrowser 组件的问题。
- (Hub-26536)。修复了关注的项目在页面标题中显示“未关注”图标 (  ) 的问题。
- (Hub-26540)。修复了除非重新启动 Black Duck，否则 SAML 的初始配置不会生效的问题。
- (Hub-26615)。修复了在项目 A 中具有“项目经理”角色和项目 B 中具有“项目经理”和“项目代码扫描者”角色的用户可以将扫描上传到项目 A 的问题。
- (Hub-26616)。修复了尝试忽略代码段失败并显示以下错误消息的问题：“无法更新现有代码段调整，因为不支持更改使用方、生产者、调整类型、起始行、结束行。”
- (Hub-26712、26962)。修复了在确认代码段匹配后，来源选项卡树视图中显示的代码段图标未清除的问题。
- (Hub-26726)。修复了创建策略规则时不能为自定义字段使用“不在内部”选项的问题。
- (Hub-26807)。修复了在尝试获取 BOM 组件版本的自定义字段时收到 HTML 状态代码 404 的问题。
- (Hub-26815)。修复了保存 SAML 集成设置导致页面重新加载并切换“身份提供程序元数据”设置的问题。
- (Hub-26904)。修复了设置选项卡上项目版本活动部分显示的匹配计数值与扫描名称页面上显示的值不同的问题。
- (Hub-26930)。修复了未触发组件通知的问题。
- (Hub-27002)。修复了创建克隆项目时发送错误通知的问题。
- (Hub-27049)。修复了在没有为用户分配“许可证经理”角色的情况下，无法在 Black Duck UI 中看

到项目版本报告的“许可条款”类别的问题。

- (Hub-27208)。修复了在配置 SAML 时, Synopsys Alert 无法加载的 blackduck-nginx 问题。
- (Hub-27227)。修复了代码段匹配需要很长时间才能完成的问题。
- (Hub-27264)。修复了审查组件会将其使用方式重置为默认值的问题。
- (Hub-27681)。修复了使用自定义安全上下文在 Kubernetes 上部署时 BOM 引擎必须由 root 用户启动的问题。

## 版本 2020.12.0

### 版本 2020.12.0 中的新增功能和更改功能

#### 新容器和系统要求更改

还有两个附加容器:2020.12.0 版的 BOM 引擎和 RabbitMQ(现在是必需的容器)。

运行所有容器的单个实例的最低系统要求是:

- 6 个 CPU
- 26 GB RAM(最低 Redis 配置);29 GB RAM(最佳配置),可为 Redis 驱动的高速缓存提供更高的可用性
- 250 GB 可用磁盘空间,用于数据库和其他 Black Duck 容器
- 数据库备份的相应空间

运行带有 Black Duck - 二进制分析的 Black Duck 所需的最低硬件包括:

- 7 个 CPU
- 30 GB RAM(最低 Redis 配置);33 GB RAM(最佳配置),可为 Redis 驱动的高速缓存提供更高的可用性
- 350 GB 可用磁盘空间,用于数据库和其他 Black Duck 容器
- 数据库备份的相应空间

**注意:**每个附加的 binaryscanner 容器都需要一个额外的 CPU、2 GB RAM 和 100 GB 可用磁盘空间。

#### 密码配置

具有“超级用户”角色的用户现在可以为本地 Black Duck 帐户设置密码要求。如果启用,Black Duck 将确保新密码符合您的要求,并拒绝被认为较弱的密码,比如“password”、“blackduck”或用户的用户名或电子邮件地址。

超级用户可以:

- 定义最小密码长度。
- 定义密码的最小字符类型数。可能的字符类型包括小写字母、大写字母、数字或特殊字符。
- 选择是否在当前用户登录 Black Duck 时对其强制执行密码要求。

默认情况下,将启用密码要求并具有以下设置:

- 密码的最小长度为八个字符。
- 只需要一种字符类型。
- 登录 **Black Duck** 时, 不对当前用户强制执行密码要求。

## 许可证增强

为了成功管理许可证风险, **Black Duck** 现在允许您为 **BOM** 中的组件创建新的或编辑现有的多许可证方案。

## 漏洞影响分析增强

- 已添加新的项目版本报告 `vulnerability_matches_date_time.csv`。列出漏洞可能接触的每个组件的组件、漏洞数据和漏洞影响分析数据。此报告包含以下列:
  - 组件名称
  - 组件 id
  - 正在使用
  - 组件版本名称
  - 版本 id
  - 渠道版本来源
  - 来源 id
  - 来源名称 id
  - 漏洞 id
  - 漏洞来源
  - CVSS 版本
  - 安全风险
  - 基本分数
  - 总体得分
  - 可用的解决方案
  - 可用的解决方法
  - 可用的漏洞利用
  - 调用的函数
  - 合格名称
  - 行号
- 报告数据库中添加了一个新表, 即漏洞方法匹配 (`vulnerability_method_matches`)。它包含以下列:
  - `id`。ID。
  - `project_version_id`。出现可访问漏洞的项目版本的 UUID。
  - `vuln_source`。漏洞的来源。对于漏洞影响分析, 值为 **BDSA**。
  - `vuln_id`。漏洞 ID, 比如 **BDSA-2020-1234**。
  - `qualified_name`。调用函数的类的名称。
  - `called_function`。代码中容易受到攻击的函数调用的名称, 该函数调用可使漏洞进入。

- `line_number`。代码中调用容易受到攻击的函数的行号。
- 漏洞报告(漏洞修复报告、漏洞状态报告和漏洞更新报告)现在在报告的末尾添加了一个新列“可访问”,以表示安全漏洞是可访问 (**true**) 还是不可访问 (**false**)。

## BOM 计算信息

Black Duck 现在提供了有关项目版本 BOM 计算状态的详细信息。

Black Duck UI 中项目版本标题中的新**状态**指示符(取代“组件”指示符)提供 BOM 的当前状态,并通知您 BOM 事件的处理状态。有关更多信息,新的“BOM 处理状态”对话框将列出待定、正在处理或已失败的事件。

Black Duck 还提供配置 BOM 事件清理作业 (`VersionBomEventCleanupJob`) 的频率的功能,该作业可清除那些由于处理错误或拓扑更改而可能卡滞的 BOM 事件。

## 策略增强

- 策略管理现在提供了基于以下自定义字段创建策略规则的功能:
  - 布尔值、日期、下拉列表、多选、单选和文本字段类型的组件自定义字段。
  - 布尔值、日期、下拉列表、多选、单选和文本字段类型的组件版本自定义字段。
- 现在,在为以下条件创建策略规则时,您可以区分已声明的许可证数据和深度(嵌入式)许可证数据:
  - 许可证
  - 许可证到期日期
  - 许可证系列

**注意:** 使用这些许可证条件的任何现有策略规则现在仅适用于已声明的许可证。您必须为这些许可证条件的深度(嵌入式)许可证创建单独的策略规则。

## 报告增强

以前仅在全局或项目级别提供的漏洞报告(漏洞修复报告、漏洞状态报告和漏洞更新报告)现在可用于项目版本。

## 配置代码段文件大小

现在,您可以修改为代码段扫描的默认最大文件大小,并选择 1MB 到 16MB 之间的值。

## 配置未映射代码位置的清除

Black Duck 每 365 天清除一次未映射的代码位置数据。您可以禁用此功能,以便不清除未映射的代码位置数据,或者,如果您定期扫描并希望经常丢弃数据,则将保留期设置为较低的天数。

## 访问令牌

现在,用户访问令牌范围的选项为“读取”或“读取和写入”。

## 支持的浏览器版本

- Safari 版本 14.0.1 (14610.2.11.51.10)
- Chrome 版本 87.0.4280.88( 正式版本) (x86\_64)



- Firefox 83.0( 64 位)
- Internet Explorer 11 11.630.19041.0

请注意, 对 Internet Explorer 11 的支持已弃用, Synopsys 将从 Black Duck 2021.2.0 发布开始停止对 Internet Explorer 11 的支持。

- Microsoft Edge 87.0.664.60( 正式版本) ( 64 位)

## 容器版本

- blackducksoftware/blackduck-postgres:1.0.16
- blackducksoftware/blackduck-authentication:2020.12.0
- blackducksoftware/blackduck-webapp:2020.12.0
- blackducksoftware/blackduck-scan:2020.12.0
- blackducksoftware/blackduck-jobrunner:2020.12.0
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash:1.0.8
- blackducksoftware/blackduck-registration:2020.12.0
- blackducksoftware/blackduck-nginx:1.0.26
- blackducksoftware/blackduck-documentation:2020.12.0
- blackducksoftware/blackduck-upload-cache:1.0.15
- blackducksoftware/blackduck-redis:2020.12.0
- blackducksoftware/blackduck-bomengine:2020.12.0
- sigsynopsys/bdba-worker:2020.09-1
- blackducksoftware/rabbitmq:1.2.2

## API 增强

- 增加了按 createdAt 字段对项目 (api/projects) 进行排序的功能。
- 增加了过滤在某个日期之前/之后创建的项目的 api/projects 端点的功能。
- 添加了用于显示漏洞匹配的 API, 作为漏洞影响分析功能的一部分。

GET /api/projects/{projectId}/versions/{projectVersionId}/vulnerabilities/{vulnerabilityId}/vulnerability-matches

- 添加了以下 BOM 端点:

- 获取 BOM 状态摘要:

GET /api/projects/{projectId}/versions/{projectVersionId}/bom-status

- 列举 BOM 的事件:

GET /api/projects/{projectId}/versions/{projectVersionId}/bom-events

- 删除失败的 BOM 事件:



DELETE /api/projects/{projectId}/versions/{projectVersionId}/bom-events/{bomEventId}

- 从 BOM 中删除所有失败的事件：

DELETE /api/projects/{projectId}/versions/{projectVersionId}/bom-events

#### ■ 新密码设置端点：

- 获取密码设置：

GET /api/password/security/settings

- 获取系统密码设置：

GET /api/password/management/settings

- 更新系统密码设置：

PUT /api/password/management/settings

- 验证密码：

POST /api/password/security/validate

- /api/catalog-risk-profile-dashboard API 现在返回“HTTP 404(未找到)”。

## 日语

2020.10.0 版的 UI、联机帮助和发布说明已本地化为日语。

## 修复了 2020.12.0 中的问题

在此发布中修复了客户报告的以下问题：

- (Hub-24839)。修复了无法从“添加/编辑组件”对话框中选择某些组件原始 ID 的问题。
- (Hub-24911)。修复了失败的 KBUUpdateJob 跳过组件更新的问题。
- (Hub-25230)。修复了用户尝试打开或编辑许可证文本时未显示许可证文本窗口的问题。
- (Hub-25452)。修复了一个问题，以便在**来源**选项卡中查看许可证搜索结果页面时，在选择许可证类型时自动添加**发现类型**过滤器。
- (Hub-25489)。修复了更改子文件夹时**来源**选项卡中的过滤器被重置的问题。
- (Hub-25603)。修复了一个问题，以便在选择替代路径时刷新**来源**选项卡上“代码段视图”对话框中**匹配的文件路径**字段中显示的路径。
- (Hub-25681)。修复了 Protex BOM 工具无法导入通用/未指定组件版本的许可证的问题。
- (Hub-25715)。修复了除非使用鼠标，否则无法修改“自定义字段管理”页面中的“活动”状态的问题。
- (Hub-25739)。修复了无法查看 BOM 组件的所有注释的问题。
- (Hub-25874)。修复了 bom\_component\_custom\_fields\_date\_time.csv 报告列出的数据与 components\_date\_time.csv 报告不同(即使数据位于同一列名称中)的问题。
- (Hub-26442)。修复了项目负责人无法在项目版本内删除扫描的问题。
- (Hub-26496)。修复了尽管在更改组件用法时许可证风险已发生变化，但仍触发了许可证风险的策略违反的问题。

## 版本 2020.10.1

### 版本 2020.10.1 中的新增功能和更改功能

#### 容器版本

- blackducksoftware/blackduck-postgres:1.0.13
- blackducksoftware/blackduck-authentication:2020.10.1
- blackducksoftware/blackduck-webapp:2020.10.1
- blackducksoftware/blackduck-scan:2020.10.1
- blackducksoftware/blackduck-jobrunner:2020.10.1
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash:1.0.8
- blackducksoftware/blackduck-registration:2020.10.1
- blackducksoftware/blackduck-nginx:1.0.26
- blackducksoftware/blackduck-documentation:2020.10.1
- blackducksoftware/blackduck-upload-cache:1.0.15
- blackducksoftware/blackduck-redis:2020.10.1
- sigsynopsys/bdba-worker:2020.09-1
- blackducksoftware/rabbitmq:1.2.2

### 修复了 2020.10.1 中的问题

在此发布中修复了客户报告的以下问题：

- (Hub-25489)。修复了在**来源**选项卡中选择的过滤器在选择其他文件夹时被重置的问题。
- (Hub-25515)。修复了主机实例运行 TLS 1.3 时特征扫描程序上传失败并显示以下错误消息的问题：“错误：无法保护与主机的连接”。
- (Hub-25791)。修复了从 2020.4.2 版升级到 2020.6.1/2020.6.2 版后扫描时间显著增加的问题。
- (Hub-26027)。修复了 Black Duck 显示以下错误消息的问题：“错误：应用程序遇到未知错误。(错误请求) error.{core.rest.common\_error}(尝试上传 Synopsys Detect 扫描时)。”
- (Hub-26085)。修复了二进制扫描添加第二个空扫描的问题。

## 版本 2020.10.0

### 版本 2020.10.0 中的新增功能和更改功能

#### 新的自定义组件仪表板

为了便于您轻松查看对您至关重要的组件版本，在 2020.10.0 中，组件仪表板已根据您保存的组件搜索替换为自定义组件仪表板。Black Duck 现在允许您使用各种属性搜索项目中使用的组件，保存搜索，然后使用“仪表板”页面从这些保存的搜索中查看仪表板。

对于每个组件版本，自定义组件仪表板显示以下信息：

- 使用此组件版本的项目版本数量以及每个项目版本的阶段、许可证、审查状态和安全风险
- 按风险类别划分的漏洞数量
- 许可证和操作风险
- 策略违反
- 审批状态
- 首次检测到组件版本的日期
- 根据 **Black Duck** 知识库发布组件的日期
- 新版本的数量
- 组件的漏洞上次更新的日期

### 组件和 **Black Duck** 知识库搜索增强

通过可用于搜索组件的属性以及搜索结果中显示的信息, 可以增强组件搜索功能。UI 也得到了增强, 因此您可以轻松区分对项目中的使用的组件的搜索以及对 **Black Duck** 知识库中的组件的搜索。

虽然 **Black Duck** 知识库搜索的搜索属性未更改, 但在搜索 **Black Duck** 项目中使用的组件版本时, 以下属性可用:

- 安全风险
- 许可证风险
- 操作风险
- 策略规则
- 策略违反严重性
- 审核状态
- 组件审批状态
- 首次检测到
- 许可证系列
- 缺少自定义字段数据
- 发布日期
- 许可证
- 漏洞 CWE
- 漏洞报告日期

对于与搜索条件匹配的每个组件版本, 将显示以下信息:

- 使用此组件版本的项目版本数量以及每个项目版本的阶段、许可证、审查状态和安全风险
- 按风险类别划分的漏洞数量
- 许可证和操作风险
- 策略违反
- 审批状态
- 首次检测到组件版本的日期
- 根据 **Black Duck** 知识库发布组件的日期

- 新版本的数量
- 组件的漏洞上次更新的日期

现在可以保存这些组件搜索结果并在“仪表板”页面中查看, 如上所述。

对于每个知识库组件搜索结果, 将显示以下信息:

- 使用此组件的项目版本数以及每个项目版本、其阶段、使用的组件版本以及相关安全风险的列表
- 提交活动趋势
- 最后提交日期
- 组件版本数量
- 此组件的标记

## 保存的搜索的增强

Black Duck 现在可以在“仪表板”页面上过滤和排序已保存的搜索。

## 许可证冲突

在 2020.10.0 版本中, Black Duck 现在可以为您指定不兼容的自定义许可条款。您可以为与 Black Duck 知识库条款或自定义许可条款冲突的禁止操作或必需操作定义自定义许可条款。

**注意:** 目前, 您无法在项目版本 BOM 中查看不兼容的许可条款。此功能将在将来的 Black Duck 发布中提供。

## 许可证管理增强

这三个新过滤器已添加到“许可证管理”中的**许可条款**选项卡中:

- 与许可证关联
- 有不兼容的条款
- 责任

## 新组件的用法

Black Duck 添加了一个“未指定”用法, 您可以使用该用法表明您需要调查组件的用法。您可能会发现使用此用法作为默认值来替代现有默认值(比如“动态链接”)会非常有用, 这样就可以消除混淆, 能够分辨组件被分配了实际用法值还是默认值。

## 新层级

Black Duck 添加了一个层级 0, 您可以使用它指定为最关键的层级。

由于此新层级, 这些默认策略规则已修改为包括层级 0:

- 没有具有 1 个以上高风险漏洞的外部层级 0、层级 1 或层级 2 项目
- 没有具有 3 个以上中等风险漏洞的外部层级 0、层级 1 或层级 2 项目

现有层级没有变化。

## 自定义字段的增强

自定义字段有以下增强

- **Black Duck** 现在提供了让您指定自定义字段是必填项的功能。
  - 查看自定义字段信息时, 会出现警告消息“\*附加字段为必填项”。但是, 如果没有为必填的自定义字段输入数据, 用户仍可以在页面上查看和保存非自定义字段信息和非必填自定义字段的信息。
  - **BOM** 中添加了一个新的过滤器“缺少自定义字段数据”, 以便您可以查看项目版本 **BOM** 中缺少信息的组件。
- 添加了在查看布尔字段类型和单选字段类型的自定义字段信息时清除选择的选项。

## 允许的特征列表

特征列表定义了 **Black Duck** 发送到 **Black Duck** 知识库 **Web** 服务的特征, 以识别扫描代码中包含的开源软件。特征扫描程序 现在有两个新参数, 您可以使用它们为二进制文件扩展名或源文件扩展名创建允许的特征列表。每个列表都是可选的, 并且与其他列表无关。

- **--BinaryAllowedList x, y, z**, 其中 **x**、**y**、**z** 是 **SHA-1**(二进制) 文件的批准文件扩展名。
- **--SourceAllowedList a, b, c**, 其中 **a**、**b**、**c** 是干净 **SHA-1**(源代码) 文件的批准扩展名。

## 漏洞影响分析的增强

对漏洞影响分析进行了以下增强:

- 在 `security_date_time.csv` 项目版本报告的末尾添加了一个新列“可访问”, 以表示安全漏洞是可访问 (**true**) 还是不可访问 (**false**)。
- 已将新的过滤器“可访问”添加到项目版本的**安全**选项卡中。

## 报告增强

以下报告得到了加强:

- 在 `components_date_time.csv` 项目版本报告的末尾添加了一个新列“注释”, 并列出了每个组件的注释。
- `vulnerability-status-report_date_time.csv` 报告末尾添加了一个新列“匹配类型”, 以标识匹配类型。

## 报告数据库的增强

以下列已添加到组件匹配表 (`component_matches`) 中:

- `match_confidence`。表示匹配的可信度, 不包括代码段、二进制或部分文件匹配。
- `match_archive_context`。相对于项目根目录的存档文件的本地路径。
- `snippet_confirmation_status`。审查代码段匹配的状态。

## HTTP/2 和 TLS 1.3

为了提高浏览器中 **Black Duck UI** 的安全性和渲染效果, **Black Duck** 现在在 **Black Duck NGINX Web** 服务器中支持 **HTTP/2** 和 **TLS 1.3**。请注意, **Black Duck NGINX Web** 服务器继续支持 **HTTP/1.1** 和 **TLS 1.2**。

## 对清除扫描的作业的更改

BomVulnerabilityNotificationJob 和 LicenseTermFulfillmentJob 现在也移除了旧的审核事件。

## API 增强

- 添加了一个端点以确定 Black Duck 的单点登录 (SSO) 状态。

GET /api/sso/status

- 添加了用于检索 SAML/LDAP 配置的端点(仅限管理员使用)。

- 读取 SSO 配置:

GET /api/sso/configuration

- 下载 IDP 元数据文件:

GET /api/sso/idp-metadata

- 还添加了以下 SSO 端点:

- 更新 SSO 配置:

POST /api/sso/configuration

- 上传 IDP 元数据文件:

POST /api/sso/idp-metadata

- 添加了以下 BOM 分层组件端点:

- 列出分层根组件:

GET /api/projects/{projectId}/versions/{projectVersionId}/hierarchical-components

- 列出分层子组件:

GET /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/hierarchical-components/{hierarchicalId}/children

- 列出分层子组件版本:

GET /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/hierarchical-components/{hierarchicalId}/children

- 在通知 API 中添加了新的漏洞字段, 以便进一步分类通知。这些通知涉及 BOM 中已更改的漏洞信息, 并包括以下字段:

- vulnerabilityNotificationCause

有关发生并触发通知的漏洞事件类型的信息, 比如漏洞已添加或删除、更改了注释、更改了修复详细信息、更改了漏洞严重性或状态已更改。

- eventSource

有关生成通知的来源的信息, 比如扫描、Black Duck KB 更新或用户操作(比如修复、优先级重新排序或调整)。

- The /api/catalog-risk-profile-dashboard API now returns HTTP 410 (GONE)。

## 支持的浏览器版本

- Safari 版本 13.1.2 (14609.3.5.1.5)
- Chrome 版本 86.0.4240.80
- Firefox 82( 64 位)
- Internet Explorer 11.572.19041.0

请注意, 对 Internet Explorer 11 的支持已弃用, Synopsys 将从 Black Duck 2021.2.0 发布开始停止对 Internet Explorer 11 的支持。

- Microsoft Edge 86.0.622.51( 正式版本)( 64 位)

## 容器版本

- blackducksoftware/blackduck-postgres:1.0.13
- blackducksoftware/blackduck-authentication:2020.10.0
- blackducksoftware/blackduck-webapp:2020.10.0
- blackducksoftware/blackduck-scan:2020.10.0
- blackducksoftware/blackduck-jobrunner:2020.10.0
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash:1.0.6
- blackducksoftware/blackduck-registration:2020.10.0
- blackducksoftware/blackduck-nginx:1.0.26
- blackducksoftware/blackduck-documentation:2020.10.0
- blackducksoftware/blackduck-upload-cache:1.0.15
- blackducksoftware/blackduck-redis:2020.10.0
- sigsynopsys/bdba-worker:2020.09
- blackducksoftware/rabbitmq:1.2.2

## 日语

2020.8.0 版的 UI、联机帮助和发布说明已本地化为日语。

## 修复了 2020.10.0 中的问题

在此发布中修复了客户报告的以下问题:

- (Hub-20559、22100)。修复了从不同根目录扫描相同代码位置或克隆项目版本时丢失代码段调整的问题。
- (Hub-21421)。修复了打印功能不适用于大型项目的问题。
- (Hub-23705、25560)。修复了用户无法删除其创建的报告的问题。
- (Hub-23709)。修复了扫描时出现以下 `scan.cli.sh` 警告消息的问题:“无法从所有清单中找到清



单。”

- (Hub-24330)。修复了在将 Protex 项目导入到 Black Duck 版本 2019.10.3 时出现错误消息(“重复密钥值违反了唯一限制”)的问题。
- (Hub-24673)。修复了在组件数超过 32,000 的情况下从“仪表板”页面导航失败的问题。
- (Hub-24675)。修复了 root\_bom\_consumer\_node\_id 设置不正确的问题
- (Hub-24871)。修复了自 2019.10.0 发布以来 PostgreSQL 数据库增长的问题。
- (Hub-24772)。修复了打印 BOM 时默认 .pdf 文件名不是项目名称和版本名称的问题。
- (Hub-24839)。修复了无法从“添加/编辑组件”对话框中选择某些组件原始 ID 的问题。
- (Hub-24947)。修复了将项目添加到 BOM 时搜索结果的列出不一致的问题。
- (Hub-25171)。修复了在使用 API 修复漏洞时漏洞计数在重新扫描后才更新的问题 (PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/origins/{originId}/vulnerabilities/{vulnerabilityId}/remediation)。
- (Hub-25219)。修复了通过 API 创建报告时的问题, 其中指定区域设置(比如“区域设置”:“ja\_JP”)被忽略。现在, 区域设置字段可以正确设置生成的报告的语言。
- (Hub-25234)。修复了打印 BOM 的打印按钮偶尔缺少条形图计数的问题。
- (Hub-25240)。修复了特定漏洞 (BDSA-2020-1674) 的浏览器或 API 调用失败的问题。
- (Hub-25241)。修复了 VersionBomComputationJob 扫描失败并显示以下错误消息的问题:“数据完整性违反(限制: not\_null, 详细信息: 在列 source\_start\_lines 上)”。
- (Hub-25244)。修复了在升级到 2020.4.2 版 Black Duck 后从 BOM 中删除手动添加的组件的问题。
- (Hub-25247)。修复了 Black Duck PostgreSQL 日志中出现以下错误消息的问题:“错误:重复密钥值违反了唯一限制 scan\_component\_scan\_id\_bdio\_node\_id\_key”。
- (Hub-25321)。修复了滚动 BOM 页面时, 文本出现在页面上不应显示文本的区域的问题。
- (Hub-25324)。修复了“扫描名称”页面没有换行的问题。
- (Hub-25478)。修复了“安全”页面上的安全风险过滤器变得不可见的问题。
- (Hub-25508)。修复了旧版媒体类型(v4 和 v5)并非始终适用于策略规则 API (GET /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/policy-rules) 的问题。
- (Hub-25522、25523)。修复了对于 Black Duck 版本 2020.8.0, 在 Chrome 的 BOM 打印预览窗口中出现格式错误的问题。
- (Hub-25548)。修复了在分层视图中选择新组件匹配时不更新“来源”视图中的组件匹配的问题。
- (Hub-25570)。修复了“安全仪表板”页面仅部分加载的问题。
- (Hub-25608)。修复了漏洞更新报告中“新漏洞”和“新修复漏洞”类别中漏洞计数两次的问题。
- (Hub-25649)。修复了“仪表板”页面上的策略违反弹出窗口无法关闭的问题。
- (Hub-25841)。修复了输入到“文本”类型的自定义字段中的数字转换为日期格式的问题。

## 版本 2020.8.2

### 版本 2020.8.2 中的新增功能和更改功能

Black Duck 版本 2020.8.2 是维护版本, 不包含新的或更改的功能。



## 修复了 2020.8.2 中的问题

在此发布中修复了客户报告的以下问题：

- (Hub-24871)。修复了自 2019.10.0 发布以来 PostgreSQL 数据库增长的问题。
- (Hub-25967)。修复了组件用法无法一致修改的问题。

## 版本 2020.8.1

### 版本 2020.8.1 中的新增功能和更改功能

#### 能够按时间清除未映射的代码位置

Black Duck 现在可以通过在 `blackduck-config.env` 文件中为 Docker Swarm 实施设置 `blackduck.scan.processor.scanpurge.cronstring` 变量来配置扫描清除 cron 作业。

#### 策略增强

Black Duck 现在允许您为漏洞的修复状态创建策略。

#### 容器版本

- `blackducksoftware/blackduck-postgres:1.0.13`
- `blackducksoftware/blackduck-authentication:2020.8.1`
- `blackducksoftware/blackduck-webapp:2020.8.1`
- `blackducksoftware/blackduck-scan:2020.8.1`
- `blackducksoftware/blackduck-jobrunner:2020.8.1`
- `blackducksoftware/blackduck-cfssl:1.0.1`
- `blackducksoftware/blackduck-logstash:1.0.6`
- `blackducksoftware/blackduck-registration:2020.8.1`
- `blackducksoftware/blackduck-nginx:1.0.25`
- `blackducksoftware/blackduck-documentation:2020.8.1`
- `blackducksoftware/blackduck-upload-cache:1.0.15`
- `blackducksoftware/blackduck-redis:2020.8.1`
- `sigsynopsys/bdba-worker:2020.06-2`
- `blackducksoftware/rabbitmq:1.2.1`

## 修复了 2020.8.1 中的问题

在此发布中修复了客户报告的以下问题：

- (Hub-24149)。修复了 Protex BOM 工具的问题，该工具显示“ERROR StatusLogger 无法识别...”错误消息，而不考虑执行的操作。
- (Hub-24480)。修复了从 Protex 导入的组件在 Black Duck 升级到 2020.4.1 版时丢失其忽略的状态的问题。
- (Hub-25254)。修复了在分发类型更改后错误触发策略违反的问题。
- (Hub-25269、25416)。修复了长时间运行的查询阻止扫描或导致 PostgreSQL 数据库死锁的问题。

题。

- (Hub-25387)。修复了 KbUpdateJob 间歇性失败的问题。
- (Hub-25509)。修复了 Black Duck 版本 2020.4.2 中数据库大小快速增长的问题。

## 版本 2020.8.0

### 版本 2020.8.0 中的新增功能和更改功能

#### 分析漏洞影响的能力

为了帮助您确定首先应解决的漏洞的优先级, **Black Duck** 现在可以确定 **Java** 应用程序调用的任何外部公共方法是否可能涉及到已知漏洞。**Black Duck** 可以识别源代码中被调用的完全限定公用函数名称, 并将它们与漏洞利用的已知函数名称相匹配。通过了解 **Java** 应用程序调用的任何外部公共方法是否可能涉及已知漏洞, 您可以确定需要关注的漏洞的优先级。

此功能在 **Synopsys Detect 6.5** 或更高版本(使用 **Synopsys Detect 6.5** 及更高版本的 **Synopsys Detect (Desktop)**) 中仅适用于 **Java** 应用程序。

请注意以下事项:

- **Synopsys Detect** 仅发现那些调用了可能易受攻击的函数的 **Java** 公共方法中的漏洞。
- 此功能仅显示 **BDSA** 的可访问函数。

#### 新的容器和系统要求

**Black Duck** 中添加了一个新的 **Redis** 容器。此容器在 **Black Duck** 中实现了更一致的缓存功能, 并将提高应用程序性能。

现在, 运行所有容器的单个实例所需的最低硬件是:

- 5 个 CPU
- 21 GB RAM(最低 **Redis** 配置); 24 GB RAM(最佳配置), 可为 **Redis** 驱动的高速缓存提供更高的可用性
- 250 GB 可用磁盘空间, 用于数据库和其他 **Black Duck** 容器
- 数据库备份的相应空间

现在, 运行带有 **Black Duck - 二进制分析** 的 **Black Duck** 所需的最低硬件是:

- 6 个 CPU
- 25 GB RAM(最低 **Redis** 配置); 28 GB RAM(最佳配置), 可为 **Redis** 驱动的高速缓存提供更高的可用性
- 350 GB 可用磁盘空间, 用于数据库和其他 **Black Duck** 容器
- 数据库备份的相应空间

**注意:** 每个附加的 **binaryscanner** 容器都需要一个额外的 CPU、2 GB RAM 和 100 GB 可用磁盘空间。

#### 自定义系统公告

系统管理员现在可以创建自定义登录和向您的 **Black Duck** 用户发布登录消息。

例如, 使用系统公告告诉用户即将发生的事件, 或者, 如果您需要显示一个免责声明, 以指明未经授权使用会发生什么情况, 也可以使用系统公告。

您可以创建四种类型的消息:

- 登录。用户登录 **Black Duck** 时向用户显示的消息。
- 横幅。出现在每页顶部的消息。
- 页脚。出现在每个页面的页脚中的消息。
- 欢迎。用户登录到 **Black Duck** 后出现的消息。

## 项目版本报告的增强

### 新的升级指导项目版本报告

新报告 `project_version_upgrade_guidance_date_time.csv` 已添加到项目版本报告中。

此报告包括:

- 组件版本详细信息, 包括来源信息和漏洞总数
- 组件(如有)的短期升级指导, 包括要升级到的版本/来源及其详细信息(比如漏洞总数)
- 组件(如有)的长期升级指导, 包括要升级到的版本/来源及其详细信息(比如漏洞总数)

此报告中的列包括:

- 组件 Id
- 组件版本 Id
- 组件来源 Id
- 组件名称
- 组件版本名称
- 组件来源名称
- 组件来源 Id
- 组件来源版本名称
- 已知漏洞总数
- 短期推荐版本 Id
- 短期推荐版本名称
- 短期推荐组件来源 Id
- 短期推荐来源名称
- 短期推荐来源 Id
- 短期推荐来源版本名称
- 短期严重漏洞
- 短期严重高风险漏洞
- 短期中等严重性漏洞
- 短期低严重性漏洞
- 长期推荐版本 Id

- 长期推荐版本名称
- 长期推荐组件来源 Id
- 长期推荐来源名称
- 长期推荐来源 Id
- 长期推荐来源版本名称
- 长期严重漏洞
- 长期高严重性漏洞
- 长期中等严重性漏洞
- 长期低严重性漏洞

新列已添加到 `security_date_time.csv` 报告中

这些新列已添加到 `security_date_time.csv` 项目版本报告的末尾:

- CVSS 版本。漏洞评分系统的版本: CVSS 2.0 或 CVSS 3.x。
- 匹配类型。

## 特征扫描程序的增强

向特征扫描程序添加了两个新属性,以控制如何将扫描数据从特征扫描程序串流(缓冲)到 Black Duck。在极少数情况下,您可能需要修改这些值以更好地适应您的网络,例如,如果您的网络出现问题,则降低这些值;如果您的网络高度稳定,则增加默认值。

- **--max-request-body-size**。上传扫描路径的扫描数据的主请求的大小。
- **--max-update-size** 可缓冲更新请求,以在特征扫描程序完成单个 URI(扫描路径)的数据上传时通知 Black Duck。

## API 增强

- 提供特定 Black Duck 用户的最后登录日期。

GET /api/users/{userId}/last-login

升级到 2020.8.0 后,所有用户的最后登录日期默认为升级日期,但之后使用实际登录数据。默认情况下,此端点将显示过去 30 天内未登录的所有用户,但您可以添加 `?sinceDays=` 查询参数以将回查期更改为所需的任何天数。这还将显示已创建但从未登录系统的用户。

- 查找休眠用户。

GET /api/dormant-users

- 为公告添加了以下端点:

- 创建登录公告。

POST /api/manage-announcement/login

- 创建欢迎公告。

POST /api/manage-announcement/welcome

- 创建横幅公告。  
POST /api/manage-announcement/banner
- 创建页脚公告。  
POST /api/manage-announcement/footer
- 编辑登录公告。  
PUT /api/manage-announcement/login/{announcementId}
- 编辑欢迎公告。  
PUT /api/manage-announcement/welcome/{announcementId}
- 编辑横幅公告。  
PUT /api/manage-announcement/banner/{announcementId}
- 编辑页脚公告。  
PUT /api/manage-announcement/footer/{announcementId}
- 删除登录公告。  
DELETE /api/manage-announcement/login/{announcementId}
- 删除欢迎公告。  
DELETE /api/manage-announcement/welcome/{announcementId}
- 删除横幅公告。  
DELETE /api/manage-announcement/banner/{announcementId}
- 删除页脚公告。  
DELETE /api/manage-announcement/footer/{announcementId}
- 获取登录公告。  
GET /api/manage-announcement/login
- 获取欢迎公告。  
GET /api/manage-announcement/welcome
- 获取横幅公告。  
GET /api/manage-announcement/banner
- 获取页脚公告。  
GET /api/manage-announcement/footer

- 按 ID 获取登录公告。

GET /api/manage-announcement/login/{announcementId}

- 按 ID 获取欢迎公告。

GET /api/manage-announcement/welcome/{announcementId}

- 按 ID 获取横幅公告。

GET /api/manage-announcement/banner/{announcementId}

- 按 ID 获取页脚公告。

- GET /api/manage-announcement/footer/{announcementId}

- 获取用户登录公告。

GET /api/announcement/login

- 获取用户欢迎公告。

GET /api/announcement/welcome

- 获取用户横幅公告。

GET /api/announcement/banner

- 获取用户页脚公告。

GET /api/announcement/footer

- 按 ID 获取用户登录公告。

GET /api/announcement/login/{announcementId}

- 按 ID 获取用户欢迎公告。

GET /api/announcement/welcome/{announcementId}

- 按 ID 获取用户横幅公告。

GET /api/announcement/banner/{announcementId}

- 按 ID 获取用户页脚公告。

GET /api/announcement/footer/{announcementId}

- 禁止欢迎公告。

POST /api/announcement/welcome/{announcementId}/suppress

- 为 API 来源响应添加了新的可选的 `originUrl` 字段。
- 为 `api/projects/id/versions/id/references` 添加了 BOM API (`api/projects/id/versions/id/components`) 引用。

- 在 `/api/codelocations/id/scan-summaries` 的响应中添加了 `createdByUsername`。
- 已将 `componentType` 字段添加到 `/api/projects/versions/hierarchical-components`, 如果项目的 `componentType` 为 `SUB_PROJECT`, 则其元数据中还将有 `project` 和 `projectVersion` 链接。
- 已将 `vulnerabilityWithRemediation` 块下的 `relatedVulnerability` 链接添加到 `/api/projects/{projectId}/versions/{projectVersionId}/vulnerable-bom-components`。
- 已向 `/api/projects/{projectId}/versions/{projectVersionId}/vulnerable-bom-components` 添加 `remediationCreatedBy` 和 `remediationUpdatedBy`
- 弃用的端点:
  - 列出修复选项: `GET /api/components/{componentId}/versions/{componentVersionId}/remediating`。

此端点已替换为 `GET /api/components/{componentId}/versions/{componentVersionId}/upgrade-guidance`。

## 支持的浏览器版本

- Safari 版本 13.1.2 (14609.3.5.1.5)
- Chrome 版本 84.0.4147.125( 正式版) ( 64 位)
- Firefox 79.0( 64 位)
- Internet Explorer 11.450.19041.0

请注意, 对 Internet Explorer 11 的支持已弃用, Synopsys 将从 Black Duck 2021.2.0 发布开始停止对 Internet Explorer 11 的支持。

- Microsoft Edge 44.19041.423.0
- Microsoft EdgeHTML 18.19041

## 容器版本

- `blackducksoftware/blackduck-postgres:1.0.13`
- `blackducksoftware/blackduck-authentication:2020.8.0`
- `blackducksoftware/blackduck-webapp:2020.8.0`
- `blackducksoftware/blackduck-scan:2020.8.0`
- `blackducksoftware/blackduck-jobrunner:2020.8.0`
- `blackducksoftware/blackduck-cfssl:1.0.1`
- `blackducksoftware/blackduck-logstash:1.0.6`
- `blackducksoftware/blackduck-registration:2020.8.0`
- `blackducksoftware/blackduck-nginx:1.0.25`
- `blackducksoftware/blackduck-documentation:2020.8.0`
- `blackducksoftware/blackduck-upload-cache:1.0.15`
- `blackducksoftware/blackduck-redis:2020.8.0`
- `sigsynopsys/bdba-worker:2020.03-1`
- `blackducksoftware/rabbitmq:1.2.1`

## 日语

2020.6.0 版的 UI、联机帮助和发布说明已本地化为日语。

## 修复了 2020.8.0 中的问题

在此发布中修复了客户报告的以下问题：

- (Hub-23467)。修复了超过 1,300 个匹配项时，“扫描”页面显示“服务器未及时响应”错误消息的问题。
- (Hub-23892)。修复了“扫描”页面上的**扫描大小**列为空的问题。
- (Hub-23937、24799)。修复了“许可证管理”页面加载失败的问题。
- (Hub-24009)。修复了 BOM 导入间歇性失败，且 Synopsys Detect 输出中显示 400 代码，并且 hub\_scan\_errors.log 列出“为空文档保存文档数据失败”的问题。
- (Hub-24112)。修复了一个问题，以便当不再在项目版本**来源**选项卡上选择节点时，用户现在可以返回到匹配计数过滤器视图。
- (Hub-24278)。修复了二进制扫描文件上传失败并显示以下错误消息的问题：上传二进制扫描时出现未知状态代码：0, null。
- (Hub-24291)。修复了 BOM 页面在尝试显示超过 32,767 个组件时显示“应用程序遇到未知错误”的问题。
- (Hub-24407)。修复了克隆代码段时出现错误消息“无法从字符串反序列化”的问题。
- (Hub-24432)。修复了尝试显示超过 32,000 个项目时无法加载“仪表板”页面的问题。
- (Hub-24451)。修复了在使用身份验证代理调用 Black Duck 知识库时忽略 HUB\_PROXY\_PASSWORD\_FILE docker 密钥的问题。
- (Hub-24480)。修复了将 Protex 导入 Black Duck 2020.4.1 时组件修改丢失的问题。
- (Hub-24529)。修复了对于具有修补状态(如 Black Duck 知识库所示)的组件错误触发策略违反的问题。
- (Hub-24583、25244)。修复了更新 Black Duck 知识库时手动添加的组件被删除的问题。
- (Hub-24646)。修复了升级 Black Duck 时出现的问题，即在“许可证管理”页面上更新了知识库许可证，但没有标识做出该更改的用户。
- (Hub-24673)。修复了在组件超过 32,000 个的情况下，从“仪表板”页面导航到“组件”页面失败时的的问题。
- (Hub-24716)。修复了出现已忽略组件的漏洞通知的问题。
- (Hub-24739)。修复了无法修改 LDAP 用户的电子邮件地址的问题。
- (Hub-24740)。修复了 bom\_component\_custom\_fields\_date\_time.csv 报告仅显示已忽略组件的问题。
- (Hub-24758)。修复了并排代码段视图未完全突出显示项目版本**来源**选项卡左侧的匹配代码的问题。
- (Hub-24845)。修复了**摘要**选项卡中的**统计**部分未更新的问题。
- (Hub-24866)。修复了特征扫描程序在尝试扫描磁盘上的整个根目录(同时排除了根目录的某些子目录)时报告“错误请求”错误的问题。
- (Hub-24885)。修复了尝试从分层视图查看项目版本**来源**选项卡中的匹配结果导致“应用程序遇到未知错误”消息的问题。



- (Hub-24968)。修复了尝试查看“安全仪表板”时出现以下错误消息“Black Duck 服务器未及时响应。”的问题。
- (Hub-25072)。修复了在为名称中包含波浪字符 (~) 的组件创建策略时出现“应用程序遇到未知错误。”错误消息的问题。
- (Hub-25115)。修复了在参数超过 32,767 个时扫描失败的问题。
- (HUP-25166) 修复了一个问题, 并添加了一个前后命令来修复 Istio 环境中的 postgres-init pod。

## 版本 2020.6.2

### 版本 2020.6.2 中的新增功能和更改功能

Black Duck 版本 2020.6.2 是维护版本, 不包含新的功能或更改的功能。

### 修复了 2020.6.2 中的问题

在此发布中修复了客户报告的以下问题:

- (Hub-24918)。修复了由于 BdioDataTransferJob 和 VersionBomComputation 作业无法正确读取扫描数据而导致扫描不一致返回结果的问题。

## 版本 2020.6.1

### 版本 2020.6.1 中的新增功能和更改功能

Black Duck 版本 2020.6.1 是维护版本, 不包含新增功能或更改的功能。

### 修复了 2020.6.1 中的问题

在此发布中修复了客户报告的以下问题:

- (Hub-23970)。修复了在选择版权选项时无法生成通知文件的问题。
- (Hub-24106)。修复了由于无法访问知识库服务而导致 KbUpdate 作业失败的问题。
- (Hub-24651)。修复了具有“项目经理”和“BOM 经理”角色的用户无法使用 /api/projects/ 页面上的发布阶段过滤器的问题。
- (Hub-24721)。修复了当 Black Duck 安全顾问 (BDSA) 不是许可模块时 BOM 组件报告失败的问题。
- (Hub-24739)。修复了无法修改 LDAP 用户电子邮件地址的问题。
- (Hub-24765)。修复了使用 SNIPPET\_MATCHING 选项扫描时不能始终识别代码段的问题。

## 版本 2020.6.0

### 版本 2020.6.0 中的新增功能和更改功能

#### 包含保存的搜索的新项目仪表板

Black Duck 提供了仪表板, 以便您可以查看与一个或多个项目版本中的组件相关的风险和策略违反的类型和严重程度。仪表板提供了所有项目和项目版本的整体视图。

为了便于您查看对您至关重要的项目和项目版本, 在 2020.6.0 中, 项目仪表板已被两个新的默认仪

表板取代, 并且您可以创建数量不限的自定义仪表板。

**Black Duck** 显示以下两个默认仪表板:

- **正在关注**。您关注的项目。
- **我的项目**。您的所有项目, 包括您没有关注的项目。

这些仪表板在项目级别的新“仪表板”页面上显示信息。此“仪表板”页面取代了“项目仪表板”页面。

此外, 您还可以创建自定义仪表板, 以便快速查看对您至关重要的项目版本。**Black Duck** 现在允许您使用各种属性搜索项目, 保存搜索, 然后使用此页面从这些保存的搜索中查看仪表板。基于已保存搜索的仪表板显示项目版本级别的信息。

为**正在关注**和**我的项目**仪表板显示的信息将实时更新。新作业 `SearchDashboardRefreshJob` 每五分钟刷新一次自定义仪表板。



单击 **Dashboard** 以显示仪表板。如果未显示, 请选择**仪表板**以显示这些仪表板。

## 项目搜索增强

通过可用于搜索项目的属性以及搜索结果中显示的信息, 可以增强项目搜索功能。

现在, 您可以使用以下属性在 **Black Duck** 中搜索项目:

- 正在关注。选择此项目是否为关注的项目。
- 安全风险。
- 许可证风险。
- 操作风险。
- 策略规则。从列表选择一个策略规则以查找违反此策略的项目。
- 策略违反。策略规则的严重性级别。
- 分发。
- 上次扫描日期。
- 发布阶段。
- 层级。

搜索结果显示符合搜索条件的项目版本。对于每个项目版本, 您可以查看以下项的数量:

- 找到的结果和数据库上次更新的时间。
- 具有最高安全风险、许可证风险或操作风险级别的组件。
- 每个风险类别的组件。
- 此项目版本具有最高策略严重性级别的组件。
- 按严重性级别列出策略违反的组件。

对于每个项目版本, 搜索结果还会显示:

- 此项目版本中的组件数。
- 上次扫描日期。

- 上次更新此项目版本的时间。
- 此项目版本的许可证。
- 此项目版本的阶段。
- 此项目版本的分发。

现在可以保存搜索结果并在仪表板中查看, 如上所述。

## 嵌入式版权声明检测

**Black Duck** 现在可以检测嵌入式版权声明的实例。通过在扫描代码时检测版权数据, 专注于许可证合规性的用户可以通过检测和管理开源软件和专有版权声明来降低许可证合规风险。

使用此功能, **Black Duck** 可搜索版权字符串文本并显示在**来源**选项卡中找到的文本。

(可选) 上传源文件, 以便审阅者可以从**来源**选项卡中查看文件中发现的版权文本。

## 克隆项目

**Black Duck** 现在为您提供克隆项目的能力。使用项目克隆将现有项目复刻到新项目。克隆将您在现有项目中定义的数据、分析和解决方案用作新项目的基准, 从而帮助减少您的工作量。

可以创建项目的用户就可以克隆项目。对于每个项目, 选择要克隆的版本和项目属性, 比如项目的设置或项目成员和组。

## 策略管理增强

- 策略管理现在提供了基于以下字段创建策略规则的功能:
  - 许可证到期日期
  - 布尔值、日期的 **BOM** 组件自定义字段。下拉列表、多选、单选和文本字段类型。
  - 项目过滤器现在包括布尔值、多选和文本字段类型的项目自定义字段。
- 评估具有多个许可证的组件的许可证策略条件的逻辑已被修改, 这可能导致新的策略违反或组件不再触发策略违反:

对于使用一个或多个许可证条件(许可证、许可证状态、许可证系列和/或许可证过期日期)创建的策略规则, 在评估具有多个许可证的组件时, 将评估每个许可证, 并且必须满足所有许可证条件, 才能构成策略违反。如果许可证风险包括在策略条件中, 则单独评估许可证风险: 评估组件的所有许可证, 而不仅仅是满足其他许可证策略条件的许可证。因此, 如果一个许可证满足多个条件的策略规则, 而该组件的另一个许可证满足许可证风险条件, 则会触发策略违反。

## 外部数据库支持 PostgreSQL 11.7

对于使用外部 PostgreSQL 的新安装, **Black Duck** 现在支持 PostgreSQL 11.7。尽管外部 PostgreSQL 实例仍然完全支持 PostgreSQL 9.6, 但 Synopsys 建议使用外部 PostgreSQL 的新安装使用 PostgreSQL 11.7。

对于内部 PostgreSQL 容器的用户, PostgreSQL 9.6 仍然是 **Black Duck 2020.6.0** 支持的版本。

## 外部 PostgreSQL 数据库支持的数字用户名

外部 PostgreSQL 实例现在支持仅由数字字符组成的用户名。

## 通知文件报告增强

未知许可证系列中的许可证现在从通知文件报告中排除。

## 现在可为各个项目提供的全局漏洞报告

现在可以为您有权访问的一个或多个项目运行漏洞修复报告、漏洞状态报告和漏洞更新报告, 为了区分报告是全局还是项目级别, 这些报告的文件名已修改为:

- `vulnerability-remediation-report_all_assigned_projects_YYYY-MM-DD_HHMMSS`(UTC 时间戳), 用于报告的全局版本
- `vulnerability-remediation-report_YYYY-MM-DD_HHMMSS`(UTC 时间戳), 用于一个或多个项目
- `vulnerability-status-report_all_assigned_projects_YYYY-MM-DD_HHMMSS`(UTC 时间戳), 用于报告的全局版本
- `vulnerability-status-report_YYYY-MM-DD_HHMMSS`(UTC 时间戳), 用于一个或多个项目
- `vulnerability-update-report_all_assigned_projects_YYYY-MM-DD_HHMMSS`(UTC 时间戳), 用于报告的全局版本
- `vulnerability-update-report_YYYY-MM-DD_HHMMSS`(UTC 时间戳), 用于一个或多个项目

## 添加到来源项目版本报告的附加信息

`source_date_time.csv` 报告通过以下信息进行增强:

- “扫描”列已添加到报告的末尾。由于项目版本 BOM 可以将多个扫描映射到项目版本, 因此该列列出找到了此匹配项的扫描。
- “路径”列现在显示依赖关系匹配的信息。对于直接依赖关系, 该列显示依赖关系的 ID 并显示匹配内容值。对于过渡依赖关系, 该列显示从顶层组件到声明组件的完全依赖关系路径。

## 支持 CVSS v3.1

Black Duck 现在支持 CVSS v3.1 分数。CVSS v3.1 是对评分标准的更新, 澄清了如何进行评分。虽然没有创建新的指标矢量或值, 但总体得分可能会因为该澄清而变化。

## 报告数据库增强

为了支持 CVSS 3.x, 在 `component_vulnerability` 表中添加了以下列:

- `severity_cvss3`
- `base_score_cvss3`
- `exploit_score_cvss3`
- `impact_score_cvss3`
- `temporal_score_cvss3`

## 重新扫描时保留部分代码段调整的选项


Black Duck 现在提供了一个设置, 以便您可以在重新扫描文件时应用来自部分代码段匹配的标识。这将最大程度减少您需要重新识别的代码段匹配的数量。

## 新审核事件

当用户出现以下行为时, 将发生审核事件:

- 创建策略, Black Duck 评估项目版本。
- 更新策略, Black Duck 评估项目版本。
- 启用策略, Black Duck 评估项目版本。
- 禁用策略, Black Duck 清除相应的策略违反。
- 删除策略, Black Duck 清除相应的策略违反。

## BOM 页面上的新信息图标

BOM 页面现在使用信息图标 () 来指示是否存在调整或自定义字段附加信息。

- 将鼠标悬停在图标上表示是否有调整或其他字段。
- 选择图标以打开“组件详细信息”对话框, 该对话框将显示附加信息。

## API 增强

- 添加了一个新端点, 以提供匹配操作期间发生的组件导入事件的列表。

`GET /api/bom-import/{graphId}/component-import-events`

- 添加了一个新端点, 以提供匹配操作期间发生的组件导入事件(按状态)的计数。

`GET /api/bom-import/{graphId}/component-import-events-count`

- 添加了一个 API, 以找出 BOM 所属的扫描, 该扫描提供了关联扫描发现的条目列表。

`GET /api/scan/{scanId}/bom-entries`

- 添加了对版权搜索的支持, 并为“来源”视图 API 的版权搜索添加了新的过滤器。
- 改进了最新扫描摘要 API

`GET /api/codelocations/{codeLocationId}/latest-scan-summary`

## 支持的浏览器版本

- Safari 版本 13.1.1 (14609.2.9.1.3)
- Chrome 版本 83.0.4103.97(正式版)(64 位)
- Firefox 77.0.1(64 位)
- Internet Explorer 11.836.18362.0
- Microsoft Edge 44.18362.449.0

## 容器版本

- blackducksoftware/blackduck-postgres:1.0.13
- blackducksoftware/blackduck-authentication:2020.6.0
- blackducksoftware/blackduck-webapp:2020.6.0
- blackducksoftware/blackduck-scan:2020.6.0

- blackducksoftware/blackduck-jobrunner:2020.6.0
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash:1.0.6
- blackducksoftware/blackduck-registration:2020.6.0
- blackducksoftware/blackduck-nginx:1.0.25
- blackducksoftware/blackduck-documentation:2020.6.0
- blackducksoftware/blackduck-upload-cache:1.0.14
- sigsynopsys/bdba-worker:2020.03-1
- blackducksoftware/rabbitmq:1.0.3

## 日语

2020.4.0 版的 UI、联机帮助和发布说明已本地化为日语。

## 修复了 2020.6.0 中的问题

在此发布中修复了客户报告的以下问题：

- (Hub-20003) 修复了一个问题，以便现在“添加组件”对话框可以识别自定义组件。
- (Hub-22599) 修复了克隆项目版本时 UI 超时的问题。
- (Hub-22695) 修复了克隆项目版本并重新扫描后手动识别的组件丢失的问题。
- (HUB-22812) 修复了打印 BOM 时忽略过滤器的问题。
- (HUB-23502) 修复了在 OpenShift 原生模式下部署的 Black Duck( 不带 --certificate-file-path 参数) 未在证书中生成“主题替代名称”的问题。
- (HUB-23601) 修复了一个问题，以便项目名称**设置**选项卡上的**所有者**下拉菜单显示所有可能的选择。
- (HUB-23736) 修复了 HierarchicalVersionBomJob 无法成功运行的问题。
- (HUB-23798) 修复了从“组件”仪表板将子项目作为组件编辑时出现 404 错误的问题。
- (HUB-23909, 23925) 修复了项目版本**安全**选项卡不提供查看漏洞( 无论其状态如何) 的功能的问题。
- (Hub-23984) 修复了对于没有分配角色的用户，为 GET /api/projects 端点返回所有项目的问题。
- (Hub-23985) 修复了选择匹配项或使用“在文件树中显示”选项无法滚动到来源树中的文件的问题。
- (Hub-23994) 修复了 Black Duck - 二进制分析 未清理上传的二进制文件的问题。
- (Hub-24011) 修复了在代码段扫描中出现“413 请求实体太大”错误消息的问题。
- (Hub-24040) 修复了 jobrunner 挂起且作业未完成的问题。
- (Hub-24097) 修复了更新组件版本后对用法所做的编辑未被保留的问题。
- (Hub-24107) 修复了选择版权选项时，通知文件报告因参数太多而失败的问题。
- (Hub-24239) 修复了 api/projects/<projectid>/versions/<versionid>/policy-status 显示 400 错误的问题。
- (Hub-24286) 修复了组件名称版本页面中仍显示软删除组件版本的问题。
- (Hub-24308) 修复了空的子项目在 BOM 页面上将“componentCount 组件”显示为来源的问题。

## 版本 2020.4.2

### 版本 2020.4.2 中的新增功能和更改功能

#### 容器版本

- sigsynopsys/bdba-worker:2020.03-1

### 修复了 2020.4.2 中的问题

在此发布中修复了客户报告的以下问题：

- (Hub-22837)。修复了项目版本 BOM 中并非所有组件都使用新的漏洞数据进行更新的问题。
- (Hub-23581)。修复了 webapp 容器不断重新启动的问题。
- (Hub-23869)。修复了除非还启用上传来源选项，否则启用代码段扫描时嵌入式许可证搜索结果不显示的问题。
- (Hub-24006)。修复了使用“许可证管理”页面更新包含大量组件的许可证导致 webapp 容器崩溃的问题。

## 版本 2020.4.1

### 版本 2020.4.1 中的新增功能和更改功能

Black Duck 2020.4.1 版包含了扫描改进功能。

### 修复了 2020.4.1 中的问题

在此发布中修复了客户报告的以下问题：

- (Hub-22188)。修复了扫描失败并显示错误消息“<path> 的父级不存在”的问题。
- (Hub-22251)。修复了由于 Black Duck 知识库通信问题导致的扫描失败问题。为了帮助防止通信问题，与 Black Duck 服务器之间的 Black Duck 知识库通信重试次数现在以增量间隔进行。
- (Hub-22559)。修复了扫描仍处于扫描后阶段，但结果已成功上传到 Black Duck 的问题。
- (Hub-23465)。修复了大型项目的 UPDATE scan\_composite\_leaf 查询速度慢的问题

## 版本 2020.4.0

### 版本 2020.4.0 中的新增功能和更改功能

#### 增强的版权声明管理

具有新的全局“版权编辑”角色的用户现在可以轻松管理其组织的开源版权声明，以便将版权所有者的完整列表包括在您的通知文件报告中。

具有“版权编辑”角色的用户可以：

- 查看组件版本的所有版权声明。
- 创建或编辑自定义版权声明。
- 编辑 Black Duck 知识库版权声明



- 将编辑过的 **Black Duck** 知识库版权声明恢复为其原始文本。
- 激活或停用版权声明。

**Black Duck** 按组件版本的来源名称/ID 管理版权声明。因此, 对组件版本的来源的版权声明所做的编辑适用于使用该组件版本来源的所有 **BOM**。这允许您在整个组织中重复使用数据并减少工作量。

## 全局修复状态

**Black Duck** 现在为具有新的“全局安全经理”角色的用户提供了为安全漏洞设置全局默认修复状态的功能。设置全局修复状态后, 当该漏洞出现在新 **BOM** 中时, 它将自动获得您定义的全局修复状态。

为了便于您轻松查找全局修复的漏洞, 安全仪表板上现在有一个**默认修复状态**过滤器。

## 策略类别

**Black Duck** 现在提供了您可以用于对策略进行分组的类别。使用“策略管理”页面和 **BOM** 页面上提供的新类别过滤器, 此功能使您可以轻松地按类别查找策略(在“策略管理”页面上)或策略违反(在 **BOM** 页面上)。

可能的类别包括组件、安全、许可证、操作和未分类(默认值)。

在 **2020.4.0** 版本之前创建的所有策略都被归入未分类类别。

## 报告数据库增强

报告数据库中的这些表中添加了新列:

- 组件表
  - review\_status
  - reviewed\_by
  - security\_critical\_count
  - security\_high\_count
  - security\_medium\_count
  - security\_low\_count
  - security\_ok\_count
  - license\_high\_count
  - license\_medium\_count
  - license\_low\_count
  - license\_ok\_count
  - operational\_high\_count
  - operational\_medium\_count
  - operational\_low\_count
  - operational\_ok\_count
- 组件策略表
  - overridden\_at
  - description



- severity
- 组件漏洞表
  - temporal\_score
  - attack\_vector
  - solution\_available
  - workaround\_available
  - published\_on
  - updated\_on
- 项目表
  - created\_at
- 项目版本表
  - created\_on
  - updated\_at
  - security\_critical\_component\_count
  - security\_high\_component\_count
  - security\_medium\_component\_count
  - security\_low\_component\_count
  - security\_ok\_component\_count
  - license\_high\_component\_count
  - license\_medium\_component\_count
  - license\_low\_component\_count
  - license\_ok\_component\_count
  - operational\_high\_component\_count
  - operational\_medium\_component\_count
  - operational\_low\_component\_count
  - operational\_ok\_component\_count

还为组件注释向 bds\_hub 的 reporting 架构添加了新视图。

报告数据库使用具体化视图。由于 Excel 不支持具体化视图, 因此不再支持将 Excel 与报告数据库一起使用。因此, 关于使用 Excel 的文档已从报告数据库指南中移除。

## 按来源进行批量修复

为了更轻松地对具有多个来源 ID 的单个组件的漏洞执行批量修复, BDSA 和 CVE 记录的受影响的 **项目** 选项卡已得到增强, 以显示每个项目版本中使用的来源。

## 修复指导

对于 BOM 中存在漏洞的组件, Black Duck 提供了有关可用的其他组件版本以及是否存在比 BOM 中使用的组件版本安全漏洞更少的版本的指导。您可以使用此信息指导您确定如何修复安全漏洞。

此功能不再是测试版功能, 现在可供所有客户使用。

## 能够在成功进行 LDAP 和 SAML 身份验证时禁止创建用户

Black Duck 现在提供了在成功进行 LDAP 或 SAML 身份验证时禁止自动创建用户的功能。

## 自定义字段的增强

Black Duck 现在提供了为下拉菜单、单选和多选自定义字段添加新选项或编辑现有选项的功能。

## 新作业

这些作业已添加到 Black Duck:

- JobMaintenanceJob, 用于管理现有作业的数据保留和清理。
- NotificationPurgeJob, 用于管理现有通知的数据保留。
- ReportPurgeJob, 用于管理现有报告的数据保留。
- SystemMaintenanceJob, 用于维护与系统相关的活动。

## API 增强

- 为自定义组件 API 添加了徽标或主要语言字段。
- 添加了严重风险优先级, 该优先级显示了使用 CVSS 3 评分时 /api/components 端点面临的严重风险。
- 为 /api/projects/:projectId/versions/:versionId/vulnerable-bom-components 添加了修复注释功能
- 当来源 ID 与从知识库返回的检索 ID 不同时, 在组件和版本响应的响应正文中添加了“已迁移”标志。
- 添加了最新扫描摘要的公共 API: /api/codelocations/:codeLocationId/latest-scan-summary
- 向以下端点添加了新字段: GET /api/projects/{projectId}/versions/{projectVersionId}/components 以显示每个条目的组件类型, 比如 KB\_COMPONENT、CUSTOM\_COMPONENT 或 SUB\_PROJECT。

## 移除 zookeeper 容器

zookeeper 容器已被移除。

- 升级到 2020.04.0 后, 您可以手动移除以下卷, 因为它们不再使用, 并且没有引用它们:
  - zookeeper-data-volume
  - zookeeper-datalog-volume
- 已弃用 jobrunner AP。

您不应该使用此 API 开发新查询, 因为它将在将来的版本中被移除和替换。

- 如果使用作业 API 的 terminateJob 函数终止作业, 则调用时它将始终返回 false。

当前无法取消作业。在将来的版本中, 将使用不同的机制重新实施此功能。

## 容器版本

- blackducksoftware/blackduck-postgres:1.0.13
- blackducksoftware/blackduck-authentication:2020.4.0
- blackducksoftware/blackduck-webapp:2020.4.0

- blackducksoftware/blackduck-scan:2020.4.0
- blackducksoftware/blackduck-jobrunner:2020.4.0
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash:1.0.6
- blackducksoftware/blackduck-registration:2020.4.0
- blackducksoftware/blackduck-nginx:1.0.23
- blackducksoftware/blackduck-documentation:2020.4.0
- blackducksoftware/blackduck-upload-cache:1.0.13
- sigsynopsys/bdba-worker:2020.03
- blackducksoftware/rabbitmq:1.0.3

请注意, 容器 sigsynopsys/appcheck-worker-<version> 已重命名为 sigsynopsys/bdba-worker-<version>。

## 移除 bdio 数据库

如 2019.10.0 发行说明中所述, bdio 数据库现已从 Black Duck 中完全移除。

## 对外部 PostgreSQL 的初始化文件 external-postgres-init.pgsql 的更改

external-postgres-init.pgsql 初始化文件经过修改, 使其与其他部署方法(比如 Kubernetes)更兼容。

配置外部 PostgreSQL 实例时, 必须编辑 docker-swarm 目录中的 external-postgres-init.pgsql 文件并执行以下操作:

- 将 POSTGRES\_USER 替换为 blackduck
- 将 HUB\_POSTGRES\_USER 替换为 blackduck\_user
- 将 BLACKDUCK\_USER\_PASSWORD 替换为您用于 blackduck\_user 的密码

## 使用 Kubernetes 或 OpenShift 通过 synopsysctl 安装或升级 Black Duck

从 2020.4.0 版本开始, synopsysctl 现在是使用 Kubernetes 或 OpenShift 安装或升级 Black Duck 的推荐方法。

此更改使 Synopsys 能够在未来的版本中包括更广泛的 Black Duck 产品增强, 同时保留管理集群中应用程序的完整功能。

单击[此处](#)了解有关 synopsysctl 的更多信息。

## 支持的浏览器版本

- Safari 版本 13.1 (14609.1.20.111.8)
- Chrome 版本 80.0.3987.162(正式版)(64 位)
- Firefox 版本 74.0(64 位)
- Internet Explorer 11.657.18362.0
- Microsoft Edge 44.18362.449.0
- Microsoft EdgeHTML 18.18363

## 日语

2020.2.0 版的 UI、联机帮助和发布说明已本地化为日语。

## 修复了 2020.4.0 中的问题

在此发布中修复了客户报告的以下问题：

- (Hub-15549)。修复了 BOM 中的策略规则过滤器显示已禁用策略的问题。
- (Hub-19745)。在 HTTP 标头中加入了内容安全协议 (CSP)。
- (Hub-21044)。修复了代码段匹配以忽略导入语句和包含语句的虚假匹配。
- (Hub-21299)。在项目版本 **设置** 选项卡中添加了一个新的 **上传扫描** 按钮，以便仅具有“项目代码扫描者”角色的用户可以在不查看用户无权查看的信息的情况下上传扫描。
- (Hub-21395)。修复了 bz2 文件的扫描大小计算不正确的问题。
- (Hub-22187)。修复了在“我的档案”页面上为用户显示非活动组角色的问题。
- (Hub-22609)。修复了使用 BDBA 扫描 OVA 文件时扫描失败的问题。
- (Hub-22657)。修复了特征扫描程序 CLI 显示“ERROR StatusLogger...”错误消息的问题。
- (Hub-22675)。修复了 crypto\_date\_time.csv 文件在“使用中”列中报告错误值的问题。
- (Hub-22692)。修复了扫描超出许可证限制时未收到通知的问题。
- (Hub-22753)。修复了通知未正确修整的问题。
- (Hub-22852)。修复了深度许可证数据搜索不显示特定文件类型的源代码的问题。
- (Hub-22937)。修复了相关漏洞的搜索结果不正确的问题。
- (Hub-22988)。修复了许可证管理中显示的许可证“使用位置”值为没有任何版本的组件显示的组件数量不正确的问题。
- (Hub-23097)。修复了策略覆盖信息在克隆项目版本后显示错误审核者的问题。
- (Hub-23139)。修复了用户无法以 HTML 格式打开漏洞更新报告的问题。
- (Hub-23175)。修复了在搜索结果中选择组件版本链接时从未加载页面的问题。
- (Hub-23217)。现在，BOM 页面上会出现一条消息，指示何时重建 BOM。
- (Hub-23237)。修复了访问项目版本时出现“错误：无法累积不同维度的数组”错误消息的问题。
- (Hub-23258)。修复了 audit\_event 导致被阻止的查询和超时的问题。
- (Hub-23296)。修复了启用深度许可证数据时不触发许可证策略违反的问题。
- (Hub-23306)。修复了端点 api/search/components 的分页损坏的问题。
- (Hub-23333)。修复了工具提示未显示过渡依赖关系的文件路径的问题。
- (Hub-23378)。修复了在启用特征扫描程序的情况下运行多个 Synopsys Detect 实例导致扫描失败并出现以下错误的问题：“错误：找不到 zip END 标头”。
- (Hub-23523)。修复了 ReportingDatabaseTransferJob 失败并显示密钥重复错误的问题。
- (Hub-23602)。修复了具有“项目经理”角色的用户在查看深度许可证数据时无权查看“参考文件”对话框中的来源 ID 信息的问题。
- (Hub-23845)。修复了 Internet Explorer 11 与 Black Duck 不兼容的问题。

## 版本 2020.2.1

### 版本 2020.2.1 中的新增功能和更改功能

#### 改进了嵌入式许可证搜索性能

**Black Duck** 在上传用于嵌入式许可证检测的源文件时提高了性能。

### 修复了 2020.2.1 中的问题

在此发布中修复了客户报告的以下问题：

- (Hub-22325)。修复了扫描空文件夹时 **Black Duck** 代码段扫描失败的问题。
- (HUB-22955)。修复了 **KBComponentUpdateJob** 失败并出现以下错误的问题：不存在具有该 ID 的对象。
- (Hub-22982)。修复了在 **BOM** 页面中，安全漏洞的组件计数与在以前版本的 **Black Duck** 中计算值的方式不一致的问题。

## 版本 2020.2.0

### 版本 2020.2.0 中的新增功能和更改功能

#### 单个文件匹配

作为特征扫描一部分的单个文件匹配不再是 **Black Duck CLI** 和 **Synopsys Detect** 扫描的默认行为。

此更改可能会导致某些组件从您的 **BOM** 中丢失，这可能是需要的，也可能是不需要的。因此，在 **Black Duck 2020.2.0** 版本中，您可以重新启用单个文件匹配。

特征扫描程序有一个新的参数 **--individualFileMatching**，它有三个选项，以便您可以启用单个文件匹配：

- **来源**。仅对具有此扩展名的文件执行单个文件匹配：**.js**。
- **二进制**。对具有以下扩展名的文件执行单个文件匹配：**.apklib**、**.bin**、**.dll**、**.exe**、**.o** 和 **.so**。
- **全部**。对具有以下扩展名的所有文件执行单个文件匹配：**.js**、**.apklib**、**.bin**、**.dll**、**.exe**、**.o** 和 **.so**。

如果您使用 **Synopsys Detect** 进行扫描，**6.2** 版将有一个新参数，支持打开/关闭单个文件匹配，默认值为“关闭”。

### Docker Compose

由于不再支持 **Docker Compose**，**Docker Compose** 目录已从发行版中移除，并且不再提供使用 **Docker Compose** 安装 **Black Duck** 指南。

### 嵌入式许可证检测

**Black Duck** 现在可以检测 **Black Duck** 知识库 未为组件声明的嵌入式开源许可证的实例。

通过在扫描代码时检测深度许可证数据，专注于许可证合规性的用户可以查看在其开源软件中检测到的许可证，以确保没有出现问题许可证，并确保所有许可证都在其 **BOM** 中得到统计。

使用此功能, **Black Duck** 可搜索许可证字符串文本并显示在**来源**选项卡中找到的许可证。

(可选) 上传源文件, 以便 **BOM** 审阅者可以从**来源**选项卡中查看发现的许可证文本。

特征扫描程序有一个新参数 **--license-search**, 用于启用嵌入式许可证的搜索。**Synopsys Detect 6.2** 版和更高版本中将提供启用深度许可证数据检测的属性。

## 向报告添加的深度许可证数据

组件项目版本报告 `components_date_#.csv` 和组件附加字段报告 `bom_component_custom_fields_date_#.csv` 已得到增强, 以包括深度许可证数据。

新列包括:

- 深度许可证 Id
- 深度许可证名称
- 深度许可证系列

这些字段添加到 `components_date_#.csv` 报告末尾以及 `bom_component_custom_fields_date_#.csv` 报告中的自定义字段列之前。

深度许可证数据也已添加到通知文件报告中。此信息可以在报告的**组件**部分所示的组件许可证列表中以及报告中所示的许可证文本中看到。

## 添加到安全项目版本报告的其他信息

`security_date_time.csv` 报告已得到改进, 报告末尾添加了以下字段:

- 总体得分
- CWE Id
- 可用的解决方案
- 可用的解决方法
- 可用的漏洞利用

## 改进了通知报告中版权报告的格式 - 测试版

对通知报告中版权报告的格式进行了其他改进。此功能是**可选的**, 目前是测试版功能。

## 新项目版本 BOM 过滤器

新的过滤器已添加到 **BOM** 页面, 以便您可以查看具有或不具有注释的组件。

## 项目版本“安全”选项卡

已发布列已添加到项目版本**安全**选项卡中显示的表中。

## 整合的作业

为了改进作业调度, 新作业 **KbUpdateJob** 将替换以下作业:

- **KbComponentUpdateJob**
- **KbVersionUpdateJob**

- KbVulnerabilityUpdateJob
- KbVulnerabilityBdsaUpdateJob

## 外部 PostgreSQL 数据库

对于使用外部 PostgreSQL 数据库的用户, Synopsys 建议升级到 9.6.16 版, 因为它包含与性能相关的修复。这是数据库容器中的版本。

此外, 如果第三方数据库提供商允许, Synopsys 建议外部 PostgreSQL 用户通过运行以下命令来调整其数据库:

```
alter system set autovacuum_max_workers = 8 ;
alter system set autovacuum_vacuum_cost_limit = 800 ;
```

然后重新启动 PostgreSQL。

如果第三方数据库提供商不允许调整, 则无需执行任何操作。

## 未映射的代码位置

Black Duck 现在可以让您计划清除未映射到项目版本的代码位置。在 `blackduckconfig.env` 文件中配置 `BLACKDUCK_HUB_UNMAPPED_CODE_LOCATION_CLEANUP` 和 `BLACKDUCK_HUB_UNMAPPED_CODE_LOCATION_RETENTION_DAYS` 属性。

## API 增强

- 新的匹配组件端点:  
`/api/projects/{projectId}/versions/{projectVersionId}/matched-components`
- 以下端点现在返回 `matchConfidencePercentage`:  
`/projects/{projectId}/versions/{projectVersionId}/matched-files`
- 用于显示所有创建的漏洞报告的状态的新漏洞报告端点:  
`/api/vulnerability-reports`
- 以下端点旨在替代现有的修复指导功能:  
`/api/components/{componentId}/versions/{componentVersionId}/upgrade-guidance`  
`/api/components/{componentId}/versions/{componentVersionId}/origins/{originId}/upgrade-guidance`
- 将忽略的字段添加到容易受到攻击的 BOM 组件端点, 从而启用基于忽略和未忽略组件的过滤:  
`GET /api/projects/{projectId}/versions/{projectVersionId}/vulnerable-bom-components`

## 支持的浏览器版本

- Safari 版本 13.0.4 (14608.4.9.1.4)
- Chrome 版本 80.0.3987.100( 正式版) ( 64 位)
- Firefox 版本 72.0.2( 64 位)



- Internet Explorer 11.657.18362.0
- Microsoft Edge 44.18362.449.0
- Microsoft EdgeHTML 18.18363

## 容器版本

- blackducksoftware/blackduck-postgres:1.0.11
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash:1.0.6
- blackducksoftware/blackduck-zookeeper:1.0.3
- blackducksoftware/blackduck-nginx:1.0.17
- blackducksoftware/blackduck-upload-cache:1.0.12
- blackducksoftware/blackduck-authentication:2020.2.0
- blackducksoftware/blackduck-webapp:2020.2.0
- blackducksoftware/blackduck-scan:2020.2.0
- blackducksoftware/blackduck-jobrunner:2020.2.0
- blackducksoftware/blackduck-registration:2020.2.0
- blackducksoftware/blackduck-documentation:2020.2.0
- sigsynopsys/appcheck-worker:2019.12
- blackducksoftware/rabbitmq:1.0.3

## 日语

2019.12.0 版的 UI、联机帮助和发布说明已本地化为日语。

## 修复了 2020.2.0 中的问题

在此发布中修复了客户报告的以下问题：

- (Hub-20742)。优化了用于检索“受影响的项目”页面数据的查询。
- (Hub-20821)。修复了添加组件或项目时出现错误消息(表明 **Black Duck** 搜索服务不可用)的问题。
- (Hub-21833)。修复了用户可以查看所有项目(而不仅仅是他们的项目)的组件的过滤器问题。
- (Hub-22181)。修复了来源选项卡上缺少组件名称和版本链接的问题。
- (Hub-22267)。修复了漏洞报告中**创建者**列为空的问题。
- (Hub-22310)。修复了 UI 中的漏洞基准分数与导出报告中的漏洞基准分数不同的问题。
- (Hub-22335)。修复了除非用户具有“全局项目查看者”角色,否则自定义字段不可见的问题。
- (Hub-22380)。修复了克隆项目版本后,尽管策略已被覆盖,但仍会触发策略违反通知的问题。
- (Hub-22466)。修复了在选择项目负责人时不隐藏非活动用户的问题。
- (Hub-22510)。修复了添加或编辑组件时无法找到自定义组件的问题。
- (Hub-22615)。修复了 KBReleaseupdatejob 持续失败的问题。
- (Hub-22626)。修复了扫描仍处于扫描后阶段,但结果已成功上传到 **Black Duck** 的问题。
- (Hub-22677)。修复了无法取消忽略组件的问题。



- (Hub-22681)。修复了添加包含代码段的子项目会扭曲子项目的组件计数的问题。
- (Hub-22709)。修复了创建策略时, 下拉项目自定义字段仅显示 10 个值的问题。
- (Hub-22805)。修复了 `source_date_time.csv` 报告为空的问题。
- (Hub-22811)。修复了尝试使用外部数据库安装 Black Duck 时出现的“角色‘blackduck\_user’不存在”的问题。
- (Hub-22850)。修复了 `license_term_fulfillment_date_time.csv` 报告为空的问题。

## 版本 2019.12.1

### 版本 2019.12.1 中的新增功能和更改功能

#### SSO 安全性增强

Black Duck 提高了 Black Duck 和单点登录 (SSO) 提供商之间通信的安全性。Black Duck 现在要求您在配置 SSO 身份验证提供商 (IdP) 时提供断言特征作为特征响应的一部分。虽然 Synopsys 不建议使用此特征, 但如果您的 IdP 无法提供此特征, 则可以禁用添加的此安全功能。有关详细信息, 请参阅安装指南。

#### API 增强

- 用于更新漏洞修复状态的新 API。BOM 组件版本漏洞修复使用户能够读取或更新漏洞修复状态并添加注释。

添加的没有来源的组件可通过以下方式访问:

```
https://.../api/projects/{projectId}/versions/{versionId}/components/{componentId}/versions/{componentVersionId}/vulnerabilities/{vulnerabilityId}/remediation
```

添加的带有来源的组件可通过以下方式访问:

```
https://.../api/projects/{projectId}/versions/{versionId}/components/{componentId}/versions/{componentVersionId}/origins/{originId}/vulnerabilities/{vulnerabilityId}/remediation
```

#### 容器信息

2019.12.0 发行说明列出了错误版本的 `blackducksoftware/blackduck-upload-cache` 容器。正确的版本是 `blackducksoftware/blackduck-upload-cache:1.0.12`。

### 修复了 2019.12.1 中的问题

在此发布中修复了客户报告的以下问题:

- (Hub-21861)。修复了升级后代码位置“损坏”的问题。
- (Hub-22091)。修复了升级到 2019.12.0 版后在 `scan.cli` 中扫描失败的问题。
- (Hub-22737、22851)。修复了作业失败并显示错误消息(指出参数太多)的问题。
- (Hub-22781)。修复了“编辑组件”对话框未加载组件或许可证信息的问题。

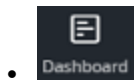
## 版本 2019.12.0

### 版本 2019.12.0 中的新增功能和更改功能

#### Black Duck UI 的增强

此版本改进了 Black Duck UI 的整体导航。增强包括：

- 新的固定导航系统将出现在页面的左侧部分。菜单选项包括：



- **Dashboard**。显示您上次查看的仪表板。



- **Find**。用于查看最近搜索结果的新菜单选项。



- **Scans**。显示“扫描”页面。




- **Reports**。显示“报告”页面。



- **Manage**。您可以从中选择的新菜单选项：组件管理、自定义字段管理、许可证管理或策略管理。



- **Admin**。显示“管理”页面。请注意，现在可以使用  选项管理自定义字段。

- 位于顶部导航栏上的新“帮助”菜单使您可以轻松访问 Black Duck 联机帮助、集成帮助和 API 文档。
- 管理用户访问令牌的功能已从“我的档案”页面移至顶部导航栏上的用户菜单中提供的单独页面。
- “工具”页面已更新。
- 新的过滤选项“匹配忽略”已添加到 BOM 页面。

#### 重新设计项目版本“安全”选项卡

项目版本 **安全** 选项卡经过重新设计，在漏洞表中添加了新布局、新过滤器和新列。

现在，您可以快速查看 **CWE ID** 以及漏洞的利用、解决办法或解决方案是否可用，无需向下钻取即可查看此信息。

#### 深度许可证数据

Black Duck 现在可以管理开源组件中可能存在的深度许可证（也称为子许可证或嵌入式许可证）。管理这些深度许可证数据可以降低许可证侵权的风险，并使您更容易了解和报告深度许可证及其在使用的开源组件中的风险。

默认情况下不启用深度许可证数据；您必须允许将深度许可证数据包括到 BOM 组件中。一旦启用，任何深度许可证（由 Black Duck 知识库 确定）将自动处于活动状态。

**注意:** 根据组件数量和深度许可证数量的不同, 允许查看深度许可证数据可能会影响 BOM 计算扫描时间。向 BOM 添加深度许可证数据会影响许可证风险并触发策略违反。

## 通知报告中包含的版权数据 - 测试版

现在可以选择将从 **Black Duck** 知识库获得的复制版权声明包含到通知报告中。这使得您可以轻松地将您使用的开源组件的版权所有者的完整列表包括在通知报告中。

此功能是 *可选的*, 目前是测试版功能, 结果可能包括格式不正确或缺失的版权。一个已知问题是截断包含特殊字符的版权声明。**Synopsys** 计划在未来的版本中添加有关版权发现和报告的附加功能。

请将任何有关错误或改进的反馈发送给您的 **Synopsys** 代表或我们的客户支持组织。

## 自定义许可证系列增强

- 为消除混淆, “限制性第三方专有”许可证系列已更名为“限制性第三方专有”。
- 知识库许可证现在与“限制性第三方专有”许可证系列相关联。这可能会影响您的许可证风险并触发策略违反。

## 策略管理增强

策略管理现在提供了基于以下漏洞条件创建策略规则的功能:

- CWE ID
- 可用的漏洞利用
- 总体得分
- 可用的解决方案
- 可用的解决方法

## 报告数据库的增强

对于项目、项目版本和 BOM 组件自定义字段, 新视图已添加到 bds\_hub 的 reporting 架构中。

## BOM 状态

项目版本 BOM 页面(也称为项目版本**组件**选项卡)中的标题现在包括组件的状态, 指示是否正在进行处理以更新 BOM。

## 自定义扫描特征

“自定义扫描特征”功能现在可供所有客户使用。

## 自定义字段增强

**Black Duck** 现在可以删除自定义字段。

## API 增强

- 如果自定义字段在策略中使用, 则阻止将其删除。  
如果在策略中使用自定义字段, 则自定义字段的 **DELETE** 端点将返回错误。

## 支持非 root 用户 ID/组 ID

此版本新增了一个功能,即支持在 Kubernetes 的 .yaml 配置文件中 使用非 root 用户 ID/组 ID 运行 Black Duck 映像。

## 支持的浏览器版本

- Safari 版本 13.0.3 (14608.3.10.10.1)
- Chrome 版本 78.0.3904.108(正式版)(64 位)
- Firefox 版本 71.0(64 位)
- Internet Explorer 11.476.18362.0
- Microsoft Edge 44.18362.449.0
- Microsoft EdgeHTML 18.18363

## 容器更改

- blackducksoftware/blackduck-postgres:1.0.10
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash:1.0.5
- blackducksoftware/blackduck-zookeeper:1.0.3
- blackducksoftware/blackduck-nginx:1.0.14
- blackducksoftware/blackduck-upload-cache:1.0.11
- sigsynopsys/appcheck-worker:2019.12
- blackducksoftware/rabbitmq:1.0.2

## 重命名的作业

KbReleaseUpdateJob 已重命名为 KbVersionUpdateJob,以更好地描述该作业的用途。

## 新审核事件

现在,当 Black Duck 知识库 弃用组件或组件版本时,将显示审核事件。

## 日语

2019.10.0 版的 UI、联机帮助和发布说明已本地化为日语。

## 修复了 2019.12.0 中的问题

在此发布中修复了客户报告的以下问题:

- (Hub-13468)。修复了 Black Duck UI 中显示的“已用计数”值不正确的问题。
- (Hub-16211、16713、17562)。修复了 BOM 似乎是最新,但处理仍在进行的问题。
- (Hub-16950)。已从 webapp 容器中移除外部映像。
- HUB-17685)。修复了在已审查组件的策略违反不再发生后,策略违反状态不会更新的问题。
- (Hub-17841)。修复了 scans.csv 项目版本报告在“扫描 ID”字段中显示代码位置 ID 的问题。
- (Hub-18257)。从 Black Duck 中移除了个人全球统一标识。
- (Hub-18978)。修复了无法从项目版本中删除组件的问题。

- (Hub-20997、21968)。修复了“扫描 > 组件”页面上未列出所有匹配组件的问题。
- (Hub-21205)。修复了尝试在**来源**选项卡上查看匹配结果时收到输入解析请求错误的问题。
- (Hub-21319)。修复了扫描历史记录显示匹配, 但“扫描 > 组件”页面没有显示结果的问题。
- (Hub-21353)。修复了组件版本的许可证无法修改的问题。
- (Hub-21369)。修复了按主要语言过滤组件搜索的功能不能正常运行的问题。
- (Hub-21538)。修复了使用 Edge 和 IE 11 浏览器时, **来源**选项卡上的“代码段视图”窗口未出现的问题。
- (Hub-21606)。修复了“本周创建的新项目”过滤器返回所有项目的问题。
- (Hub-21614)。修复了在**来源**选项卡的“代码段视图”窗口中未突出显示并排匹配代码的问题。
- (Hub-21664)。修复了在**来源**选项卡上选择替代匹配时, 源代码窗格中对应的匹配行未发生变化的问题。
- (Hub-21735)。修复了尝试更新**来源**选项卡上的空白依赖关系组件时出现“需要 createOrUpdateMany.arg1.compositePath”错误的问题。
- (Hub-21751)。修改了 SAML 注销页面上的文本。
- (Hub-21785)。修复了**来源**选项卡上的过滤器不显示所有现有文件和/或目录的问题。
- (Hub-21793)。修复了 Black Duck 2019.8.0 AMI 缺失图像的问题。
- (Hub-21796)。修复了对子目录所做的文件或目录匹配更改传播到**来源**选项卡上的父目录的问题。
- (Hub-21817)。修复了“工具”页面上缺少图标的问题。
- (Hub-21960)。修复了 VersionBomComputationJob 失败, 并显示以下错误消息的问题: 重复密钥值违反了唯一限制“uidx\_vuln\_remediation\_release\_vuln\_id”。
- (Hub-22042)。修复了指向已弃用集成的链接仍显示在“工具”页面上的问题。
- (Hub-22090)。修复了在组件版本**设置**选项卡上更新组件版本状态失败的问题。
- (Hub-22094、22477)。修复了升级到 2019.10.0 版后 LDAP 身份验证失败的问题。
- (Hub-22165)。修复了 API 端点 GET /api/vulnerabilities/{vulnerabilityId}/affected-projects 缺少访问控制的问题。
- (Hub-22167)。修复了从“许可证管理”表中选择空许可证时显示 404 错误的问题。
- (Hub-22175)。修复了将鼠标悬停在**来源**选项卡上匹配的文件上时文件路径不再出现的问题。

以下是 **Black Duck** 中已知问题和限制的列表：

- 如果使用 **LDAP** 目录服务器对用户进行身份验证，请考虑以下事项：
  - **Black Duck** 支持单个 **LDAP** 服务器。不支持多个服务器。
  - 如果从目录服务器中移除用户，**Black Duck** 用户帐户将继续显示为活动状态。但是，凭据不再有效，无法用于登录。
  - 如果从目录服务器中移除组，**Black Duck** 组不会移除。手动删除组。
- 标记只支持字母、数字以及加号 (+) 和下划线 (\_) 字符。
- 如果 **Black Duck** 正在对用户进行身份验证，则在登录期间用户名不区分大小写。如果启用了 **LDAP** 用户身份验证，则用户名区分大小写。
- 如果代码位置有大型材料清单，删除代码位置可能会失败，并出现用户界面超时错误。