SYNOPSYS®

リリースノート

Black Duck 2022.10.0

目次

まえがき

Black Duck ドキュメント

Black Duckのドキュメントは、オンラインヘルプと次のドキュメントで構成されています。

タイトル	ファイル	説明
リリースノート	release_notes.pdf	新機能と改善された機能、解決された問題、現在のリリースおよび以前のリリースの既知の問題に関する情報が記載されています。
Docker Swarmを使用したBlack Duckのインストール	install_swarm.pdf	Docker Swarmを使用したBlack Duckのインストールとアップグレードに関する情報が記載されています。
使用する前に	getting_started.pdf	初めて使用するユーザーにBlack Duckの使用法に関する情報を提供します。
スキャンベストプラクティス	scanning_best_practices.pdf	スキャンのベストプラクティスについて説明します。
SDKを使用する前に	getting_started_sdk.pdf	概要およびサンプルのユースケースが記載されています。
レポートデータベース	report_db.pdf	レポートデータベースの使用に関する情報が含まれています。
ユーザーガイド	user_guide.pdf	Black DuckのUI使用に関する情報が含まれています。

KubernetesまたはOpenShift環境にBlack Duckソフトウェアをインストールするためのインストール方法は、SynopsysctlとHelmです。次のリンクをクリックすると、マニュアルが表示されます。

- Helmは、Black Duckのインストールに使用できるKubernetesのパッケージマネージャです。
- Synopsysctlは、KubernetesおよびRed Hat OpenShiftにBlack Duckソフトウェアを展開するためのクラウドネイティブの管理コマンドラインツールです。

Black Duck 統合に関するドキュメントはConfluenceで入手できます。

カスタマサポート

ソフトウェアまたはドキュメントについて問題がある場合は、Synopsysカスタマサポートに問い合わせてください。

Synopsysサポートには、複数の方法で問い合わせできます。

- オンライン：https://www.synopsys.com/software-integrity/support.html
- 電話：お住まいの地域の電話番号については、サポートページの下段にあるお問い合わせのセクションを参照してください。

サポートケースを開くには、Synopsys Software Integrityコミュニティサイト（https://community.synopsys.com/s/contactsupport）にログインしてください。

常時対応している便利なリソースとして、オンラインカスタマポータルを利用できます。

Synopsys Software Integrityコミュニティ

Synopsys Software Integrityコミュニティは、カスタマサポート、ソリューション、および情報を提供する主要なオンラインリソースです。コミュニティでは、サポートケースをすばやく簡単に開いて進捗状況を監視したり、重要な製品情報を確認したり、ナレッジベースを検索したり、他のSoftware Integrityグループ(SIG)のお客様から情報を得ることができます。コミュニティセンターには、共同作業に関する次の機能があります。

- つながる – サポートケースを開いて進行状況を監視するとともに、エンジニアリング担当や製品管理担当の支援が必要になる問題を監視します。
- 学ぶ – 他のSIG製品ユーザーの知見とベストプラクティスを通じて、業界をリードするさまざまな企業から貴重な教訓を学ぶことができます。さらにCustomer Hubでは、最新の製品ニュースやSynopsysの最新情報をすべて指先の操作で確認できます。これは、オープンソースの価値を組織内で最大限に高めるように当社の製品やサービスをより上手に活用するのに役立ちます。
- 解決する – SIGの専門家やナレッジベースが提供する豊富なコンテンツや製品知識にアクセスして、探している回答をすばやく簡単に得ることができます。
- 共有する – Software Integrityグループのスタッフや他のお客様とのコラボレーションを通じて、クラウドソースソリューションに接続し、製品の方向性について考えを共有できます。

Customer Successコミュニティにアクセスしましょう。アカウントをお持ちでない場合や、システムへのアクセスに問題がある場合は、こちらをクリックして開始するか、community.manager@synopsys.comにメールを送信してください。

トレーニング

Synopsys Software Integrity, Customer Education(SIG Edu)は、すべてのBlack Duck教育ニーズに対応するワンストップリソースです。ここでは、オンライントレーニングコースやハウツービデオへの24時間365日のアクセスを利用できます。

新しいビデオやコースが毎月追加されます。

Synopsys Software Integrity, Customer Education(SIG Edu)では、次のことができます。

- 自分のペースで学習する。
- 希望する頻度でコースを復習する。
- 試験を受けて自分のスキルをテストする。
- 終了証明書を印刷して、成績を示す。

詳細については、https://community.synopsys.com/s/educationを参照してください。また、Black Duckのヘルプについては、Black Duck UIの[ヘルプ]メニュー()から、[Black Duckチュートリアル]を選択します。

包括性と多様性に関するSynopsysの声明

Synopsysは、すべての従業員、お客様、パートナーが歓迎されていると感じられる包括的な環境の構築に取り組んでいます。当社では、製品およびお客様向けのサポート資料から排他的な言葉を確認して削除しています。また、当社の取り組みには、設計および作業環境から偏見のある言葉を取り除く社内イニシアチブも含まれ、これはソフトウェアやIPに組み込まれている言葉も対象になっています。同時に、当社は、能力の異なるさまざまな人々が当社のWebコンテンツおよびソフトウェアアプリケーションを利用できるように取り組んでいます。なお、当社のIPは、排他

的な言葉を削除するための現在検討中である業界標準仕様を実装しているため、当社のソフトウェアまたはドキュメントには、非包括的な言葉の例がまだ見つかる場合があります。

1. Black Duckバージョン2022.10.x

2022.10.0の発表

PostgreSQL 11の廃止

PostgreSQL 11でBlack Duckを実行することに関するサポートは、2022.10.0リリースで終了しています。このリリース以降、PostgreSQL 11でBlack Duckを実行しようとするとエラーが発生し、Black Duckは起動しません。

PostgreSQL 13コンテナの移行

Black Duck 2022.10.0はPostgreSQLイメージをバージョン11からバージョン13に移行しており、PostgreSQL 9.6コンテナ（バージョン4.2から2021.10.xまで）またはPostgreSQL 11コンテナ（バージョン2022.2.0から2022.7.xまで）を使用したバージョンからのアップグレードをサポートしています。インストール中に、blackduck-postgres-upgraderコンテナは既存のデータベースをPostgreSQL 13に移行し、完了すると終了します。

コア以外のPG拡張機能を使用しているお客様の場合は、移行前にそれらをアンインストールし、移行が正常に完了した後に再インストールすることを強くお勧めします。そうしないと、移行が失敗する可能性があります。

レプリケーションを設定しているお客様は、移行前に、pg_upgradeのドキュメントの手順に従う必要があります。そこで説明されている準備が行われていない場合、移行はおそらく成功しますが、レプリケーションの設定が壊れます。

SynopsysのPostgreSQLイメージを使用していないお客様には影響はありません。

重要：移行を開始する前に：

- システムカタログのデータコピーによるディスクの使用に起因する予期しない問題を回避するため、10%ほどの余裕をディスク容量に確保してください。
- ディスク容量が不足するとLinuxシステムが中断する可能性があるため、ルートディレクトリの容量とボリュームマウントを確認してください。

KubernetesおよびOpenShiftユーザーの場合：

- プレーンなKubernetesでは、アップグレードジョブのコンテナはルートとして実行されます。ただし、唯一の要件は、ジョブがPostgreSQLデータボリュームの所有者と同じUIDで実行されることです。
- OpenShiftでは、アップグレードジョブは、PostgreSQLデータボリュームの所有者と同じUIDで実行されることを前提としています。

Swarmユーザーの場合：

- 移行は完全に自動化されているため、Black Duckの標準アップグレードの操作以外に追加の操作は必要ありません。
- 上記のレイアウトとUIDの変更を行うには、blackduck-postgres-upgraderコンテナをルートとして実行する必要があります。
- その後のBlack Duckの再起動時に、blackduck-postgres-upgraderは移行が不要であると判断し、すぐに終了します。

データベースbds_hub_reportの廃止

Black Duck 2021.10.0のリリースノートに記載されているように、Black Duckの新規インストールではbds_hub_reportデータベースは作成されません。2022.10.0では、bds_hub_reportデータベースが削除されます。

bds_hub_reportデータベースを保存したいユーザーは、hub_create_data_dump.shスクリプトを使用してbds_hub_reportデータベースをダンプできます（ある場合）。

2022年11月のBlack Duckナレッジベース IPアドレス変更に関する通知

2022年11月14日の週に、Black Duckナレッジベース（https://kb.blackducksoftware.com）のIPアドレスが変更されます。この14日の週の間は、DNSを更新して新しいIPアドレスにトラフィックが転送されるようにします。ほとんどのお客様は何もする必要はありません。

IP許可リストを使用してKBと通信するオンプレミスのお客様は、ファイアウォールを更新し、許可リストにこれらの新しいIPアドレスを含める必要があります。トラフィックまたはIP許可リストを制限するためにファイアウォールルールを使用しないお客様は影響を受けません。

IPアドレスを使用しているお客様の場合、リストを許可するために次のIPアドレスを追加する必要があります。

NAM（北米）

kb-na.blackducksoftware.com：34160126173

EMEA（ヨーロッパ、中東、アフリカ）

kb-emea.blackducksoftware.com： 34.149.112.69

APAC（アジア太平洋、アジア、中国）

kb-apac.blackducksoftware.com：34.111.46.24

この変更は、IPアドレスの更新を自動的に処理するため、DNS解決を使用する大部分のお客様には影響しません。IPアドレス許可リストを使用しているお客様は、次の3つの新しいIPアドレスを許可リストに追加する必要があります。34.160.126.173、34.149.112.69、34.111.46.24。

現在のIPアドレス（参照用）は次のとおりです。

NAM：35.224.73.200

EMEA：35.242.234.51

APAC：35220236106

この変更は、可用性の高い安全なKBを提供するための継続的な取り組みの一環として行われています。

サーバー移行後に質問がある場合や問題が発生した場合は、サポートケースを提出してください。

オブジェクトストレージサービスの今後のシステムリソース要件

Black Duck 2023.1.0では、オブジェクトストレージサービスを展開するための最小システムリソース要件が増加します。オブジェクトストレージサービスには、さらにCPUを1つ、1 GBメモリ、および10 GBのディスク領域を追加する必要があります。これらの要件は今後のリリースで随時変更されることに注意してください。

ドキュメントのローカライゼーション

UI、オンラインヘルプ、およびリリースノートのバージョン2022.7.0が日本語と簡体字中国語にローカライズされました。

2022.10.0の新機能および変更された機能

GitリポジトリSCM統合 – フェーズ2

Black Duck 2022.10.0では、プロジェクトとバージョンの作成時にユーザーがリポジトリ/ブランチフィールドを追加できるようになりました。承認されたSCMプロバイダ（GitHub StandardおよびGitHub Enterpriseのみ）を追加できるよう

になりました。この機能は、新しいプロジェクトを作成するときに選択できます。これを実行すると、新しいプロジェクトの[プロジェクト設定]ページにリポジトリURLとブランチバージョンが自動的に入力されます。

この機能はDetect 8.x以降と互換性があり、新しいパッケージマネージャスキャンで有効になります。

SCM統合はBlack Duckではデフォルトでは有効になっておらず、環境に以下を追加して有効にする必要があります。

Swarmユーザーの場合は、blackduck-config.envファイルに以下を追加します。

```
blackduck.scan.scm.enableIntegration=true
```

Kubernetesユーザーの場合は、environsセクションでvalues.yamlファイルに以下を追加します。

```
environs:
    blackduck.scan.scm.enableIntegration: "true"
```

プロジェクトバージョンコンポーネントの新しい一括アクション

一括更新機能では、プロジェクトバージョンページのコンポーネントで次のアクションがサポートされるようになりました。

1. コンポーネントを無視/無視解除する
2. コンポーネントの使用法の種類を設定する
3. レビュー済み/未レビューとしてマークする
4. 通知ファイルに包含/除外を設定する

構成表にUTF8を使用したレポートの作成

この機能はBlack Duck 2022.7.0で追加されましたが、同バージョンのリリースノートから誤って省略されていることに注意してください。

Black Duck 2022.7.0では、アルファベット以外の文字を使用しているお客様向けのレポートで、構成表の文字エンコードにUTF8のサポートが導入されました。この機能を有効にするには、blackduck-config.envファイルに以下を追加します。

```
USE_CSV_BOM=true
```

新しいヒートマップデータのダウンロード

ヒートマップを圧縮CSVとしてダウンロードして端末スキャンの傾向を確認および分析し、スプレッドシートプログラムのピボットとしてヒートマップを作成することができるようになりました。このデータをダウンロードするには、[管理者] > [診断] > [システム情報]の順に移動します。

新しいSBOMレポートフィールド

プロジェクトに新しいSBOMフィールドを追加して、ソフトウェア構成表（SBOM）レポートに詳細を含めることができるようになりました。SBOMフィールドには、次の新しいフィールドがあります。

構成表コンポーネントレベルでの設定：

- パッケージURL：SPDXレポートのreferenceCategory: PACKAGE_MANAGER要素のreferenceType: purlとしてexternalRefsセクションにリストされ、CycloneDXレポートのpurlとしてcomponentsセクションの下にリストされます。
- パッケージサプライヤ：両方のレポートタイプに対して、（supplier）としてリストされます。

- CPE：SPDXレポートのreferenceCategory: SECURITY要素のreferenceLocatorとしてexternalRefsセクションにリストされ、CycloneDXレポートのcpeとしてcomponentsセクションの下にリストされます。

コンポーネントレベルでの設定：

- 説明：両方のレポートタイプに対して、（description）としてリストされます。
- 発信者：SPDXレポートのpackagesセクションの下にoriginatorとしてリストされ、components CycloneDXレポートの下にauthorとしてリストされます。

新しいグローバル通知ビューアの役割

すべてのプロジェクトへの読み取り専用アクセス権を持ち、ユーザー設定に関係なくすべてのシステム通知を受信できる新しい役割が作成されました。

新しい通知サブスクリプション管理

ユーザーが受信する通知を有効または無効にすることができるようになりました。これらの設定を管理するには、[管理] > [システム設定] > [通知]の順に選択します。グローバル通知ビューアの役割を持つユーザーは、システム上のすべての通知を引き続き受信します。

更新されたウォッチするプロジェクトの通知管理

[マイ設定]ページで、通知を受信するウォッチするプロジェクトを管理できるようになりました。これを実行するには、右上のメニューでユーザー名をクリックし、[ウォッチするプロジェクト]をクリックして、[ウォッチするプロジェクト]タブを選択します。

更新された通知保持期間

通知保持のデフォルト設定値は、30日間から14日間に短縮されました。これは、blackduck-config.envでBLACKDUCK_HUB_NOTIFICATIONS_DELETE_DAYS環境変数を設定することによって実行できます。

ポリシーの新しい脆弱性条件

新しい脆弱性タグのカテゴリがリモートコード実行（RCE）の脆弱性を置換して含めるポリシーの脆弱性条件に追加されました。このカテゴリには、ポリシーの作成時または編集時に次のフィルタオプションが含まれます。

- ゼロクリックリモートコード実行：システム上でコードが実行される可能性がある脆弱性。第三者のアクションを必要とせずに、リモートの攻撃者によってトリガーされます。
- 特定された悪意のあるコード：悪意のあるコードを含むソフトウェアで、システ内で実行された場合、有害または破壊的な結果をもたらすように設計されています。
- 開示禁止脆弱性の詳細：現在、技術的詳細が開示禁止中であり、現時点ではベンダーから詳細が公開されていない脆弱性。
- 未確認の脆弱性：ベンダーが、コンポーネントの動作が意図したものであり、脆弱性が存在しないと判断したために、コードベースの修正が行われていない脆弱性。

脆弱性更新レポートに新しい脆弱性タグが追加されました

脆弱性更新レポートに脆弱性タグが表示されるようになりました（該当する場合）。これらのレポートには、上記の脆弱性タグが含まれます。

リストと表の新しいエクスポート機能

次のページでリストと表をCSVにエクスポートできるようになりました。

- [ダッシュボード]ページ：ダッシュボードの[結果の概要]セクションにあります。

- [検索]ページ:[検索]ページの左側にある検索フィールドの上にあります。
- [スキャン]ページ:[スキャン]ページの左上にある[削除]ボタンの横にあります。
- [ユーザーとグループ]ページ:[ユーザーとグループ]ページの左上にある[ユーザーの作成]ボタンの横にあります。

バイナリスキャンおよびProtex構成表インポート用にBDIOをインポートする際に強化されたソースビュー

現在、[スキャン]ページには、構成表インポートログに見つからないコンポーネントがリストされます。2022.10.0リリースでは、マッチしないコンポーネントも[ソースビュー]タブに表示されます。マッチしないコンポーネントは、新規スキャンの場合にのみソースビューに表示されることに注意してください。既存のスキャンは変更されません。

レポートスキーマの機能強化

reporting.componentビューに、次の3つのフィールドが追加されました。

- reporting.component.created_at: コンポーネントの作成時に、構成表からコピーされました。コンポーネントが初めて構成表に追加されたことを表します。
- reporting.component.updated_at: コンポーネントの更新時に、構成表からコピーされました。コンポーネントが構成表で更新された最新の時刻を表します。
- reporting.user_group_project_mapping: どのユーザーがどのグループ(複数の場合あり)にマッピングされ、どのユーザーがどのプロジェクト(複数の場合あり)にマッピングされているかを追加します。

新しい短期署名スキャン -お客様の使用の制限

短期署名スキャンは、Black Duck内に永続的なストレージを作成または使用しない新しいスキャンモードです。このため、構成表(BOM)は保存されません。これは、指定されたスキャンターゲット内のポリシー違反をすばやく検出するために使用されます。一時署名スキャンを使用するには、次を実行している必要があります。

- Synopsys Detect 8.2.0以降
- Black Duck 2022.10.0以降
- ホストされたナレッジベース
- Match as a Serviceの有効化

この機能には使用制限があるため、Black Duck 2022.10.0では一般的には利用できません。

Synopsysctlの更新

Synopsysctlは新しいPostgreSQL 13コンテナで動作するよう更新されました。

コンテナバージョン

- blackducksoftware/blackduck-postgres:13-2.13
- blackducksoftware/blackduck-authentication:2022.10.0
- blackducksoftware/blackduck-webapp:2022.10.0
- blackducksoftware/blackduck-scan:2022.10.0
- blackducksoftware/blackduck-jobrunner:2022.10.0
- blackducksoftware/blackduck-cfssl:1.0.10
- blackducksoftware/blackduck-logstash:1.0.21
- blackducksoftware/blackduck-registration:2022.10.0

- blackducksoftware/blackduck-nginx:2.0.28
- blackducksoftware/blackduck-documentation:2022.10.0
- blackducksoftware/blackduck-upload-cache:1.0.29
- blackducksoftware/blackduck-redis:2022.10.0
- blackducksoftware/blackduck-bomengine:2022.10.0
- blackducksoftware/blackduck-matchengine:2022.10.0
- blackducksoftware/blackduck-webui:2022.10.0
- sigsynopsys/bdba-worker:2022.9.1
- blackducksoftware/rabbitmq:1.2.14

APIの機能強化

APIリクエストの詳細については、Black Duckで入手可能なREST API開発者ガイドを参照してください。

新しいスキャン監視APIエンドポイント

新しいREST APIエンドポイントが追加されました。このエンドポイントを使用してスキャンのエラー率を分析し、指定された時間内にシステムの端末スキャンからスキャン監視情報を取得できます（デフォルトは過去1時間に設定されています）。

- GET /api/scan-monitor

リクエストパラメータは次のとおりです。

- level （必須）。数値1または2（デフォルトは1）。
  リクエストの例: GET /api/scan-monitor?level=1

  障害発生率が設定された最大しきい値（デフォルトは30%）を超えた場合、レベル1は単純なバイナリ応答OKまたはNOT OKです。

  レベル2は、ステータスに応じて16進数のカラーコード（緑、黄、赤）を返します。緑色（#00FF00）は、監視対象時間（デフォルトでは過去1時間）の障害発生率が、設定されている最小しきい値（デフォルトは10%）を下回っていることを示します。黄色（#FFFF00）は、障害発生率が最小しきい値と最大しきい値（10%～30%）の間にあることを示します。赤色（#FF0000）は、障害発生率が最大しきい値（30%）を超えていることを示します。

カスタムフィールドのnull値の処理の向上

次のパブリックAPIリクエストは、カスタムフィールド値がnullの場合にエラーメッセージを返すよう更新されました。

- PUT /api/projects/{projectId}/custom-fields/{customFieldId}
- PUT /api/projects/{projectId}/versions/{projectVersionId}/custom-fields/{customFieldId}
- PUT /api/components/{componentId}/custom-fields/{customFieldId}
- PUT /api/components/{componentId}/versions/{componentVersionId}/customfields/{customFieldId}
- PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/custom-fields
- PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/custom-fields/{customFieldId}
- PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/custom-fields
- PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/custom-fields/{customFieldId}

通知エンドポイントの更新

次のREST APIパブリックエンドポイントが更新され、ユーザーがサブスクリプションの通知を受信する必要があるかどうかに基づいてnotifyUserフィールドが返されます。

- GET /api/users/{userId}/notification-subscriptions/{subscriptionId}
- GET /api/users/{userId}/notification-subscriptions

新しい構成表ステータスのエンドポイント

特定のスキャンに対して構成表が更新されたタイミングを判断するために、新しいREST APIエンドポイントが作成されました。

- GET /api/projects/{projectId}/versions/{versionId}/bom-status/{scanId}

ステータス値には、NOT_INCLUDED、BUILDING、SUCCESS、FAILUREがあります。

PUT /api/settings/auto-remediate-unmappedの廃止

Black Duck 2022.4.1では、パブリックエンドポイントPUT /api/settings/auto-remediate-unmappedはPATCH /api/settings/auto-remediate-unmappedに変更されましたが、PUTエンドポイントは廃止されており、下位互換性を維持するために保持されています。現時点でのリリースでは、PUT /api/settings/auto-remediate-unmappedエンドポイントが削除されました。

ライセンスAPIリクエストの廃止と削除

次のAPIリクエストは削除されました。

- GET /api/licenses/{licenseId}/obligations
- GET /api/licenses/{licenseId}/obligations-filters

GET api/licenses/{licenseId}/obligationsが削除されたため、必須のAPIはどのAPIからも返されなくなります。代わりに、ライセンス条項API（/api/licenses/{licenseId}/license-terms）が返されます。

また、次のAPIリクエストは廃止予定です。

- GET /api/licenses
- POST /api/licenses
- GET /api/licenses-filters
- GET /api/licenses/{licenseId}
- PUT /api/licenses/{licenseId}
- GET /api/licenses/{licenseId}/text
- PUT /api/licenses/{licenseId}/text

新たに強化されたコンポーネントエンドポイント

コンポーネントレベルでSBOMフィールド値を取得/変更するための新しいREST APIエンドポイントが追加されました。

- GET /api/components/{componentId}/sbom-fields
- PUT /api/components/{componentId}/sbom-fields

次のREST APIエンドポイントは、メタ/リンクセクションにsbom-fieldエンドポイントを含むコンポーネントのSBOMフィールド値を取得するように拡張されました。

- GET /api/components/{componentId}

バイナリスキャナ情報

バイナリスキャナがバージョン2022.9.0に更新されました。バイナリスキャナは、パッケージマネージャサポートを通じてNPMをサポートするようになりました。

2022.10.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (HUB-29825)。[システム設定]([プロジェクトマネージャの役割設定]>[セキュリティマネージャ])が無効になっている場合、個人の役割とグループ全体の役割の両方にグローバルセキュリティマネージャを割り当てても修復が許可されない(グレー表示になる)問題が修正されました。
- (HUB-30488)。階層型の構成表ツリーに子コンポーネントが断続的に表示されない問題を修正しました(ツリーがトリクルダウンしない)。
- (HUB-33274)。「構成表コンポーネント表現」に「componentVersionName」と「componentVersion」が含まれるようにREST APIドキュメントを更新しました。
- (HUB-33407)。一部のユーザーが無制限のコードベースサイズを持っているときに「スキャンできるコードの最大量を超えました」という通知を受信する問題を修正しました。
- (HUB-33693)。スニペットビューにアップロードされたソースウィンドウがすぐに表示されない問題を修正しました。
- (HUB-33847)。プロジェクト作成リクエストの本文にクローンカテゴリフィールドcloneCategoriesが表示されない場合、すべてのクローンカテゴリが選択され、有効になる問題を修正しました。また、APIを使用してプロジェクトを作成する際に、フィールドprojectLevelAdjustmentsは、それが存在しない場合、デフォルトで「true」になります。
- (HUB-33922)。30日分のジョブ履歴がある場合でも、[管理] > [診断] > [ジョブ]に7日分のジョブ履歴だけが表示されていた問題を修正しました。
- (HUB-33945、HUB-34938)。プロジェクトのBlack Duckで大規模なHTML脆弱性レポートを生成する際に、アプリケーションがクラッシュしたり、予想以上に時間がかかったりする問題を修正しました。修正の一環として、HTMLレポートのダウンロードを管理するために、設定可能なHUB_MAX_HTML_REPORT_SIZE_KBプロパティが追加されました。このプロパティはHTMLレポートの表示にのみ影響し、他のレポートの生成やダウンロードには影響しません。
- (HUB-33972)。OnPrem KB Marchデータで文字列検索/著作権検索が機能しない問題を修正しました。
- (HUB-34085)。コンポーネント管理ページで名前順に並べ替えると大文字/小文字が区別される問題を修正しました。
- (HUB-34246)。[プロジェクトバージョン比較]ビューに関連するブラウザ表示の問題を修正しました。
- (HUB-34511)。依存関係スキャンのプロジェクト名が中国語を使用すると読み取り不能な文字になる問題を修正しました。
- (HUB-34676)。無効なカスタムフィールドを更新すると、すべてのプロジェクトバージョンで構成表の計算がトリガーされる問題を修正しました。

- (HUB-34712)。BDBAコンテナのヘルスチェックのタイムアウト設定がDocker SwarmおよびKubernetesと同期していないために(30秒)、バイナリスキャンポッドがCrashLoopBackOff状態になる可能性がある問題を修正しました。また、ヘルスチェックのタイムアウト値がカスタマイズできるようになりました。
  - Kubernetesの場合は、次の引数を使用します。この場合、###は秒単位です:
    --set binaryscanner.timeout=###
  - Docker Swarmの場合は、dockerスタック展開コマンドでタイムアウト値を指定します。この場合、###は秒単位です:

    ```
    BDBA_HEALTH_CHECK_TIMEOUT=### docker stack deploy -c docker-compose.yml -c sizes-gen03/10sph.yaml -c docker-compose.bdba.yml hub
    ```

- (HUB-34839)。postgres-upgraderセクションをdocker-compose.local-overrides.ymlに追加しました。
- (HUB-34887)。自動呼出しが長時間ハングし、登録サービスが応答しない場合にシステムが誤動作する原因となるエアギャップ環境の問題を修正しました。
- (HUB-35110)。マップされていないコードの場所のデフォルトの保持期間について、blackduck-config.env内部のドキュメントを修正しました。
- (HUB-35140)。脆弱性コメントを共有しているコンポーネントのコメントが取得元固有ではない問題を修正しました。
- (HUB-35184)。Black Duck 2022.4.2で見つかった脆弱性を修正するため、Zulu Javaバージョンを11.0.16+8にアップグレードしました。
- (HUB-35196)。コンポーネント/コンポーネントバージョンフィルタを使用してもコンポーネント名の結果が表示されない問題を修正しました。
- (HUB-35222)。[影響を受けるプロジェクト]タブで、特定の脆弱性(CVE-2016-1000027)のページをナビゲートするときにページをロードできない問題を修正しました。
- (HUB-35366)。[コンポーネントの詳細]画面にカスタムフィールド値が表示されない問題を修正しました。
- (HUB-35369)。Black Duck BOM pdfを印刷する場合、レポートがページの端で重なるため、すべてのコンポーネントが正しくリストされない問題を修正しました。
- (HUB-35407)。null値を持つカスタムフィールドが原因でKbUpdateWorkflowJob-Component Version Updateジョブが失敗する問題を修正しました。
- (HUB-35524)。/api/projects/<project_id>/versions/<version_id>/policy-rulesパブリックエンドポイントの使用時に発生するユーザー権限の問題を修正しました。
- (HUB-35660)。スキャンクライアントでエントリIDが重複しているため、終了コード70「java.util.ConcurrentModificationException」エラーが発生する可能性がある問題を修正しました。

2. Black Duckバージョン2022.7.x

バージョン2022.7.2の発表

Black Duck 2022.7.2に関する新たな発表はありません。

バージョン2022.7.2の新機能および変更された機能

Black Duck 2022.7.2には、新規のまたは変更された機能はありません。

コンテナバージョン

- blackducksoftware/blackduck-postgres:11-2.15
- blackducksoftware/blackduck-authentication:2022.7.2
- blackducksoftware/blackduck-webapp:2022.7.2
- blackducksoftware/blackduck-scan:2022.7.2
- blackducksoftware/blackduck-jobrunner:2022.7.2
- blackducksoftware/blackduck-cfssl:1.0.9
- blackducksoftware/blackduck-logstash：1.0.20
- blackducksoftware/blackduck-registration:2022.7.2
- blackducksoftware/blackduck-nginx：2.0.25
- blackducksoftware/blackduck-documentation:2022.7.2
- blackducksoftware/blackduck-upload-cache：1.0.27
- blackducksoftware/blackduck-redis:2022.7.2
- blackducksoftware/blackduck-bomengine:2022.7.2
- blackducksoftware/blackduck-matchengine:2022.7.2
- blackducksoftware/blackduck-webui:2022.7.2
- sigsynopsys/bdba-worker:2022.6.0
- blackducksoftware/rabbitmq：1.2.10

APIの機能強化

Black Duck 2022.7.2には、新規のまたは変更されたAPIリクエストはありません。APIリクエストの詳細については、Black Duckで入手可能なREST API開発者ガイドを参照してください。

2022.7.2で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- （HUB-35687）。CVEとBDSAの脆弱性が関連しており、関連する脆弱性が脆弱性修正に誤って追加される可能性がある問題を修正しました。この問題が発生する場合、vulnerable-bom-components APIは、この問題のあるコンポーネントに適用されるとHTTP Response 400 / Bad Requestエラーを返します。

バージョン2022.7.1の発表

Black Duck 2022.7.1に関する新たな発表はありません。

バージョン2022.7.1の新機能および変更された機能

GitリポジトリSCM統合 - フェーズ2

Black Duck 2022.7.1では、プロジェクトとバージョンの作成時にユーザーがリポジトリ/ブランチフィールドを追加できるようになりました。承認されたSCMプロバイダ（GitHub StandardおよびGitHub Enterpriseのみ）を追加できるようになりました。この機能は、新しいプロジェクトを作成するときに選択できます。これを実行すると、新しいプロジェクトの[プロジェクト設定]ページにリポジトリURLとブランチバージョンが自動的に入力されます。

この機能はDetect 8.x以降と互換性があり、新しいスキャンで有効になります。

SCM統合はBlack Duckではデフォルトでは有効になっておらず、環境に以下を追加して有効にする必要があります。

Swarmユーザーの場合は、blackduck-config.envファイルに以下を追加します。

```
blackduck.scan.scm.enableIntegration=true
```

Kubernetesユーザーの場合は、environsセクションでvalues.yamlファイルに以下を追加します。

```
environs:
  blackduck.scan.scm.enableIntegration: "true"
```

新しいヒートマップデータのダウンロード

システム内の端末スキャンの情報を保持するヒートマップデータをダウンロードできるようになりました。この情報をダウンロードするには、[管理] > [診断] > [システム情報]の順に移動します。移動先で、[ヒートマップのダウンロード（.zip）]ボタンをクリックします。出力は.csvファイルです。

構成表にUTF8を使用したレポートの作成

この機能はBlack Duck 2022.7.0で追加されましたが、同バージョンのリリースノートから誤って省略されていることに注意してください。

Black Duck 2022.7.0では、アルファベット以外の文字を使用しているお客様向けのレポートで、構成表の文字エンコードにUTF8のサポートが導入されました。この機能を有効にするには、blackduck-config.envファイルに以下を追加します。

```
USE_CSV_BOM=true
```

プロジェクトバージョンコンポーネントの新しい一括アクション

一括更新機能では、プロジェクトバージョンページのコンポーネントで次のアクションがサポートされるようになりました。

- コンポーネントを無視/無視解除する
- コンポーネントの使用法の種類を設定する

- 通知ファイルに包含/除外を設定する

コンテナバージョン

- blackducksoftware/blackduck-postgres:11-2.16
- blackducksoftware/blackduck-authentication:2022.7.1
- blackducksoftware/blackduck-webapp:2022.7.1
- blackducksoftware/blackduck-scan:2022.7.1
- blackducksoftware/blackduck-jobrunner:2022.7.1
- blackducksoftware/blackduck-cfssl:1.0.9
- blackducksoftware/blackduck-logstash：1.0.20
- blackducksoftware/blackduck-registration:2022.7.1
- blackducksoftware/blackduck-nginx：2.0.27
- blackducksoftware/blackduck-documentation:2022.7.1
- blackducksoftware/blackduck-upload-cache：1.0.28
- blackducksoftware/blackduck-redis:2022.7.1
- blackducksoftware/blackduck-bomengine:2022.7.1
- blackducksoftware/blackduck-matchengine:2022.7.1
- blackducksoftware/blackduck-webui:2022.7.1
- sigsynopsys/bdba-worker:2022.6.0
- blackducksoftware/rabbitmq：1.2.13

APIの機能強化

新規または変更されたAPIリクエストの詳細については、Black Duckで入手可能なAPIドキュメントを参照してください。

新しいスキャン監視APIエンドポイント

新しいREST APIエンドポイントが追加されました。このエンドポイントを使用してスキャンのエラー率を分析し、指定された時間内にシステムの端末スキャンからスキャン監視情報を取得できます（デフォルトは過去1時間に設定されています）。

- GET /api/scan-monitor

リクエストパラメータは次のとおりです。

- level （必須）。数値は1または2または3です（デフォルトは「1」）。
  リクエストの例： GET /api/scan-monitor?level=1

  失敗率が設定された最大しきい値を超えた場合（デフォルトは30%）、レベル1はOKまたはNOT OKの単純なバイナリ応答です。

  レベル2は、ステータスに応じて16進数のカラーコード（緑、黄、赤）を返します。緑色（#00FF00）は、監視対象の時間内（デフォルトは過去1時間）の障害発生率が、設定されている最小しきい値（デフォルトは10%）を下回って

いることを示します。黄色(#FFFF00)は、障害率が最小しきい値と最大しきい値の間(10%～30%)であることを示します。赤色(#FF0000)は、障害率が最大しきい値(30%)を超えていることを示します。

レベル3は、スキャンの状態に基づいて集計されたスキャン数を返します。

監視対象期限、最小、および最大しきい値は次で設定できます:

カスタムフィールドのnull値の処理の向上

次のパブリックAPIリクエストは、カスタムフィールド値がnullの場合にエラーメッセージを返すよう更新されました。

- PUT /api/projects/{projectId}/custom-fields/{customFieldId}
- PUT /api/projects/{projectId}/versions/{projectVersionId}/custom-fields/{customFieldId}
- PUT /api/components/{componentId}/custom-fields/{customFieldId}
- PUT /api/components/{componentId}/versions/{componentVersionId}/custom-fields/{customFieldId}
- PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/custom-fields
- PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/custom-fields/{customFieldId}
- PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/custom-fields
- PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/custom-fields/{customFieldId}

2022.7.1で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (HUB-33693)。パネルがクリックされない限り、スニペットを含むファイルのスキャンされたファイルビューが読み込まれない問題を修正しました。
- (HUB-34246)。[プロジェクトバージョン比較]ビューの印刷時に発生するブラウザ表示の問題を修正しました。
- (HUB-34472、HUB-34781、HUB-34682)。コンポーネントバージョンページでライセンスを削除しても構成表レポートに反映されない問題を修正しました。
- (HUB-34511)。プロジェクト名とバージョン名がBDIOヘッダーではなくHTTPヘッダーからプルされることで、ラテン文字以外の文字を使用すると、読み取り不能な文字が表示される問題を修正しました。
- (HUB-34618)。KBオンプレミス環境でバージョン詳細レポートを生成する場合のパフォーマンスが改善されました。
- (HUB-35110)。マップされていないコードの場所のデフォルトの保持期間について、blackduck-config.env内部のドキュメントを修正しました。
- (HUB-35196)。コンポーネント/コンポーネントバージョンフィルタを使用してもコンポーネント名の結果が表示されない問題を修正しました。
- (HUB-35222)。[影響を受けるプロジェクト]タブで、特定の脆弱性(CVE-2016-1000027)のページをナビゲートするときにページをロードできない問題を修正しました。
- (HUB-35304)。2022.7.0へのアップグレード時に、ユーザーグループに割り当てられたスーパーユーザーの役割が2022.7.0で導入された新しい役割に移行されない問題を修正しました。
- (HUB-35349)。マッチングプロセスの完了後にメッセージが送信されるため、Black Duck 2022.7.0にアップグレードすると高速スキャンが失敗する問題を修正しました。この問題は、環境で複数のマッチコンテナが実行されている場合に発生する可能性が高くなっていました。

- （HUB-35407）。null値を持つカスタムフィールドが原因でKbUpdateWorkflowJob-Component Version Updateジョブが失敗する問題を修正しました。

バージョン2022.7.0の発表

PostgreSQL 9.6の廃止

以前の発表のように、PostgreSQL 9.6でのBlack Duckの実行のサポートは、Black Duckの2021.6.0リリースで終了しました。Black Duckの2022.7.0リリース以降、PostgreSQL 9.6でBlack Duckを実行しようとするとエラーが発生し、Black Duckは起動しません。

今後のPostgreSQL 11の廃止

PostgreSQL 11でBlack Duckを実行することに関するサポートは、2022.10.0リリースで終了します。そのリリース以降、PostgreSQL 11でBlack Duckを実行しようとするとエラーが発生し、Black Duckは起動しません。

PostgreSQLコンテナの11から13への移行

Black Duckは、2022.10.0リリースでPostgreSQLイメージをバージョン11からバージョン13に移行します。SynopsysのPostgreSQLイメージを使用していないお客様には影響はありません。

今後のカスタムフィールドAPIの変更

Black Duckの2023.1.0リリースでは、無効になっているカスタムフィールドを読み取りまたは変更しようとすると、次のAPIがエラーを返すように変更されます。フィールドにアクセスするには、フィールドを再度有効にする必要があります。

. `GET api/components/{componentId}/custom-fields/{custom-field-id}`
. `PUT api/components/{componentId}/custom-fields/{custom-field-id}`
. `GET api/components/{componentId}/versions/{componentVersionId}/custom-fields/{custom-field-id}`
. `PUT api/components/{componentId}/versions/{componentVersionId}/custom-fields/{custom-field-id}`

従来の署名スキャンと従来のパッケージマネージャスキャンのサポートの廃止

この機能は、Black Duck 2023.7.0リリースで正式に廃止されます。

互換性を確保するためには、Detect 8.xにアップグレードする必要があります。Detect 8.xは、2022年5月または6月のリリースを予定していて、これはBlack Duck 2022.7.0のリリースおよびこの廃止に関するリリースノートと一致します。これにより、将来の廃止日までにDetectをアップグレードする期間として1年間の猶予が与えられます。

今後のHelm2のサポート終了

2023.1.0リリース以降、Black DuckはKubernetes導入用のHelm2をサポートしなくなります。サポートされるKubernetesの最小バージョンは1.13（Helm3でサポートされる最も古いバージョン）に引き上げられます。

訂正：GitリポジトリSCM統合 - フェーズ1

2022.4.0リリースノートに記載されている、Swarmユーザー向けのBlack DuckでのGitリポジトリSCM統合の有効化に関する手順が正しくありませんでした。正しい変数の設定は次のとおりです。

docker-compose.yaml環境の場合：

```
webapp:
```

```
  environment:
    blackduck.scan.scm.enableIntegration: 'true'
```

また、blackduck-config.envファイルに以下を追加します。

```
blackduck.scan.scm.enableIntegration=true
```

PostgreSQLサポートスケジュールの更新

将来の2022.10.0リリース以降、Black Duckは外部PostgreSQL 11のサポートを終了します。今後のPostgreSQLバージョンに関しては、サポートの開始日と終了日を以下の表で確認してください。

PGバージョン	最初のリリース	最終リリース	BD外部サポートの追加	BD外部サポートの終了
16.x	2023年後半	2028年後半	2024.7.0	2026.10.0
15.x	2022年後半	2027年後半	2023.7.0	2025.10.0
14.x	2021年9月	2026年11月	2022.7.0	2024.10.0
13.x	2020年9月	2025年11月	2021.8.0	2023.10.0
12.x	2019年10月	2024年11月	X	X
11.x	2018年10月	2023年11月	2020.6.0	2022.10.0

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2022.4.0が日本語にローカライズされました。

簡体字中国語

UI、オンラインヘルプ、およびリリースノートのバージョン2022.4.0が簡体字中国語にローカライズされました。

バージョン2022.7.0の新機能および変更された機能

PostgreSQL 14の外部データベースのサポート

Black Duckは、外部PostgreSQLを使用する新規インストール用にPostgreSQL 14をサポートおよび推奨するようになりました。Black Duck 2022.7.xへの移行では、PostgreSQL 14への移行は必要ありません。

内部PostgreSQLコンテナのユーザーは、アクションは必要ありません。

注： PostgreSQL 14.0から14.3には、インデックスが破損するというバグがあるため、サポートされているPostgreSQL 14の最小バージョンは14.4です。

スーパーユーザーの役割を管理ドメインの役割に分割

現在、スーパーユーザーの役割を持つすべてのBlack Duckユーザーは、すべてのユーザーの権限を作成/修正でき、自分のユーザーを含む任意のユーザーにシステム管理者の役割を割り当てることができます。これにより、すべてのスーパーユーザーが、SysAdmin役割を含む、Black Duckインスタンスへの完全なアクセスと制御を取得できるようになります。これは特権昇格の欠陥として表示されますが、役割は意図したとおりに機能しています。

このシナリオを回避するために、スーパーユーザーの役割が削除され、以前にその役割に関連付けられていたさまざまな責任を担当する次の新しい役割が作成されました：グローバルプロジェクト管理者、グローバルプロジェクトグループ管理者、ユーザー管理者、カスタムフィールド管理者。これらの新しい役割の詳細については、Black Duckヘルプを参照してください。

新しいInfrastructure as Code（IaC）の問題の表示

アプリケーションは単なるアプリケーションコードではありません。インフラストラクチャと導入方法は、アプリケーションのセキュリティを確保するための重要なコンポーネントです。そのため、IaCは、さまざまなクラウドおよびオンプレミス環境でアプリケーションの導入とセットアップを自動化するために使用されています。これらの構成オプションは、アプリケーションのセキュリティを確保する上で重要な役割を果たし、コンテナ化されたアプリケーションやサービスベースのアプリケーションでは特に重要です。

Black Duck 2022.7.0では、スキャンにIaCが含まれている場合、プロジェクトのバージョンページの構成表を表示するときにIaCの問題が表示されるようになりました。表示される情報は、コードで見つかった潜在的な問題に対処するのに必要な情報を提供します。

IaCスキャンを実行するには、次のオペレーティングシステム要件を満たし、Detect 7.14以降を使用している必要があります。

Infrastructure as Codeスキャンの詳細については、コミュニティページを参照してください。

スキャンCLIの堅牢性の向上

再試行メカニズムの導入により、スキャンCLIがサーバー上で完了したときにハングしないようになりました。これは、Hub、scan、またはnginxサービスの再起動後でも、スキャンが完了し、通常どおりアップロードされることを意味します。

プロジェクトバージョンコンポーネントの一括コメントの新しいサポート

この新機能では、一括コメントを追加して、構成表のユーザーレビューとキュレーションを容易にすることができます。たとえば、コンポーネントに個別にコメントを適用する代わりに、プロジェクトバージョンページで任意の数のコンポーネントを選択し、選択したアイテムに同時にコメントを追加できます。

新しいAPIアクセストークン自動パージ機能

この新機能により、Black Duckシステムのユーザー管理者は、非アクティブなアクセストークンを自動的にパージするスケジュールを設定することで、アクセストークンを介したBlack Duckへのアクセスをより適切に維持および制御できるようになります。この機能は、新しい[管理] > [アクセストークン]ページにあります。このページから、既存のすべてのアクセストークンを手動でキュレートすることもできます。

バイナリスキャンコンテナのメモリ割り当ての増加

バイナリスキャンが失敗しないように、バイナリスキャンコンテナのメモリを2 GBから4 GBに増やしました。

ポリシールールのユーザーエクスペリエンスの強化

ポリシーを作成または編集するときに、「in」または「not in」演算子が使用されている場合、コンポーネントバージョンをポリシーに追加または除外する方法を明確に示す指示が[コンポーネントの条件]に表示されるようになりました。

Black Duckナレッジベース検索の更新

[検索] > [Black Duckナレッジベース]ページの外観と、検索実行後の結果の表示方法が若干変更されました。

以前のリリースでは、Black Duckナレッジベース検索では、結果セットにBlack Duckプロジェクトとカスタムコンポーネントがナレッジベースコンポーネントとともに表示されました。2022.7.0以降、Black Duckナレッジベース検索では、ナレッジベースコンポーネントデータのみが返されます。カスタムコンポーネントを検索するには、[コンポーネント検索]タブを使用する必要があります。Black Duckプロジェクトを検索するには、[プロジェクト]検索タブを使用する必要があります。

また、[Black Duckナレッジベース]ページの[コンポーネントソース]フィルタ（カスタムコンポーネントおよびBlack Duckプロジェクト）が削除されました。

ナレッジベース更新ジョブのタスクの強化

以前は、ナレッジベース更新ジョブを構成するタスク(コンポーネント、コンポーネントバージョン、ライセンス、NVD脆弱性、およびBDSA脆弱性)は、事前に設定された順序で実行されていました。コンポーネントタスクが失敗した場合、後続のタスクは実行されませんでした。2022.7.0の新機能として、失敗したタスクを管理する継続メカニズムが導入されました。これにより、後続のタスクの実行がブロックされなくなります。

また、特定のタスクが失敗した理由に関する詳細情報が存在する場合は、ジョブページでより詳細に確認できます。

高速スキャンに追加された新しいプロパティ

高速スキャンの出力に、次のプロパティが追加されました。

- cweIds: このセキュリティ脆弱性の共通脆弱性タイプ一覧(CWE)IDのリスト。
- shortTermUpgradeGuidance: この脆弱性に対処するための短期的な処置として推奨されるアップグレード先のコンポーネントバージョン。これは、使用中のものと同じメジャーバージョンであるためです。
- longTermUpgradeGuidance: 長期的な処置として推奨されるアップグレード先のコンポーネントバージョン。この処置を実行するには、メジャーバージョン番号のアップグレードが必要になる場合があり、より慎重に計画する必要があります。

Detectエンドポイントに対する新しいアップグレードガイダンス情報

Detectコンポーネントのスキャン結果に次のものが追加されました。

- shortTermUpgradeGuidance: この脆弱性に対処するための短期的な処置として推奨されるアップグレード先のコンポーネントバージョン。これは、使用中のものと同じメジャーバージョンであるためです。
- longTermUpgradeGuidance: 長期的な処置として推奨されるアップグレード先のコンポーネントバージョン。この処置を実行するには、メジャーバージョン番号のアップグレードが必要になる場合があり、より慎重に計画する必要があります。

プロジェクトバージョンの更新されたデータ保持管理

プロジェクトバージョンのデータ保持ポリシーをより適切に管理できるようになりました。お使いの環境で自動データ削除が有効になっている場合、削除から保護する特定のプロジェクトバージョンを選択できるようになりました。これは、新規プロジェクトを作成するとき、または既存のプロジェクトバージョンを編集するときに有効にできます。プロジェクトを表示すると、自動データ削除から保護されているプロジェクトバージョンの行の末尾にロックアイコンが表示されます。

更新されたソフトウェア構成表(SBOM)レポートタイプとエクスポート形式

プロジェクトのソフトウェア構成表レポートをCycloneDX v1.4形式でエクスポートできるようになりました。CycloneDX v1.4形式には、セキュリティ脆弱性情報が含まれています。BDSAレコードがNVDレコードとともに含まれるようになりました。

CycloneDX v1.4の詳細については、CycloneDX v1.4リファレンスページを参照してください。

レポートの生成後に使用されたタイプをより適切に識別できるように、レポートタイプ(SPDX、CycloneDX v1.3、またはCycloneDX v1.4)もレポート名に含まれます。

また、SBOMレポートを生成するときに、新しいレポート形式を使用できます。レポートの出力として、JSON、YAML、RDF、またはtag:valueを選択できるようになりました。

新しいデータベースパーティションジョブ

ジャーナルテーブルは月別にパーティション分割されるようになりました。最初のパーティションは特別なパーティションで、既存のすべてのジャーナルイベントが含まれています。JournalPartitionMaintenanceJobジョブは、プロジェ

クトの監査記録用の新しいデータベースパーティションを作成し、5年以上前の古いパーティションとジャーナルイベントを削除します。

スキャン状態/ステータスのリファクタリング

以前、スキャンステータスは、スキャン状態とスキャン進行状況の設計上の組み合わせであり、現在のキューベースのスキャンアーキテクチャではうまく機能しませんでした。新しいアプローチは、状態を提供してから、スキャンがシステム内で進行するにつれてスキャンの進行状況を追跡する方法を提供します。このアプローチは、従来のスキャンアーキテクチャを組み込んで1つのアプローチを使用できるように、十分な柔軟性を備えている必要があります。状態はデータベースに残る必要がありますが、一時的で頻繁に更新される進行状況はキャッシュに移動する必要があります。

レポートデータベースの機能強化

reporting.component_vulnerabilityマテリアライズドビューにexposed_onフィールドが追加されました。

レポートスキーマの若干の変更

2023.1.0では、255文字を超えるパスに対応できるように、reporting.scan_viewのbasedir列のタイプがcharacter varyingからtextに変更されます。

サポートされるブラウザのバージョン

- Safariバージョン15.5（17613.2.7.1.8）
  - Safariバージョン13.0以前はサポートされなくなりました
- Chromeバージョン103.0.5060.114（公式ビルド）（x86_64）
  - Chromeバージョン71以前はサポートされなくなりました
- Firefoxバージョン102.0（64ビット）
  - Firefoxバージョン71以前はサポートされなくなりました
- Microsoft Edgeバージョン103.0.1264.44（公式ビルド）（64ビット）
  - Microsoft Edgeバージョン78以前はサポートされなくなりました

コンテナバージョン

- blackducksoftware/blackduck-postgres:11-2.15
- blackducksoftware/blackduck-authentication:2022.7.0
- blackducksoftware/blackduck-webapp:2022.7.0
- blackducksoftware/blackduck-scan:2022.7.0
- blackducksoftware/blackduck-jobrunner:2022.7.0
- blackducksoftware/blackduck-cfssl:1.0.9
- blackducksoftware/blackduck-logstash：1.0.20
- blackducksoftware/blackduck-registration:2022.7.0
- blackducksoftware/blackduck-nginx：2.0.25
- blackducksoftware/blackduck-documentation:2022.7.0
- blackducksoftware/blackduck-upload-cache：1.0.27
- blackducksoftware/blackduck-redis:2022.7.0

- blackducksoftware/blackduck-bomengine:2022.7.0
- blackducksoftware/blackduck-matchengine:2022.7.0
- blackducksoftware/blackduck-webui:2022.7.0
- sigsynopsys/bdba-worker:2022.6.0
- blackducksoftware/rabbitmq：1.2.10

APIの機能強化

新規または変更されたAPIリクエストの詳細については、Black Duckで入手可能なAPIドキュメントを参照してください。

Sigma Scannerをダウンロードするための新しいAPI

Sigmaバイナリをアップロードキャッシュから直接ダウンロードするための新しいエンドポイントが作成されました。APIリクエストには、目的のアーキテクチャを示すのに必要なパス変数archと、versionという名前のオプションのヘッダーパラメータがあります。

. `GET /api/tools/sigma?arch={arch}`

2022.7.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- （HUB-33231）。スキャンページでスキャンサイズによってスキャンをソートしても、リストが正しい順序で表示されない問題が修正されました。
- （HUB-33974）。脆弱性の影響を受けるプロジェクトの数が誤解を招く可能性がある問題を修正しました。コンポーネントを無視すると、[概要]ページで、特定のリスクがあるコンポーネントの数が変わります。脆弱性検索では、無視されたコンポーネントはカウントされませんが、コンポーネント検索ではカウントされます。
- （HUB-32773）。コンポーネントがローカルで変更された場合に、システムがそれをナレッジベースからのコンポーネントではなく、ローカルコンポーネントと見なす問題を修正しました。構成表の計算は、コンポーネントの新しい情報を取得するときに、ナレッジベースを照会しませんでした。
- （HUB-34468）。実行時間の長い他のスキャンタイプのマッチングが完了するまでの間、キューで待機しているときに、高速スキャンがタイムアウトする問題を修正しました。
- （HUB-34459）。--matchConfidenceThresholdパラメータを従来のscan.cliで使用した場合に機能しなかった問題を修正しました。
- （HUB-33477）。SAMLが無効になっている場合に、Black DuckメタデータURLダウンロードボタンが使用可能になっていた問題を修正しました。
- （HUB-33549）。[ポリシー管理] > [ポリシールールの作成] > [コンポーネントの条件]の[マッチタイプ]選択リストに[直接的な依存関係バイナリ]オプションと[推移的な依存関係バイナリ]オプションがない問題が修正されました。
- （HUB-34215）。4つの高の脆弱性の発見に対応して、jackson-databindおよびgsonコンポーネントを更新しました。
- （HUB-33551）。コードの場所がnullのBDIOファイルをアップロードすると、ステータスコード400で失敗する問題を修正しました。
- （HUB-32919）。Hubから集約モードのBDIOを使用してスキャンをダウンロードしようとすると、0バイトの破損した/空のBDIOが生成される問題を修正しました。
- （HUB-29445）。プロジェクトのREST APIフィルタリングがカンマを含むプロジェクト名をサポートしていなかった問題を修正しました。

- （HUB-33164）。システムログのサイズが大きすぎる場合に、それをBlackduck UIからダウンロードできない問題を修正しました。
- （HUB-34282）。メモリの制限と予約がJavaヒープサイズよりも512 MBを超えて大きく設定されている場合に、system_check.shスクリプトが誤警告を生成する可能性がある問題を修正しました。小さなコンテナをドキュメントに従ってセットアップした場合に誤警告が発生しないように、オーバーヘッドが20%超でメモリが1024 MB超の場合にフラグが付けられるようにスクリプトが更新されました。
- （HUB-33923）。[管理] > [診断] > [システム情報] > [ジョブページ]を更新した場合に、ジョブ履歴の統計情報に大幅に異なる数が表示される可能性がある問題を修正しました。
- （HUB-34195）。REST APIドキュメントを更新し、[バージョンレポートの作成]セクション（または/api/versions/{projectVersionId}/reportsリクエスト）から、reportTypeからの値としてのSBOMを削除しました。
- （HUB-34296）。正しくないi18n文字が原因で、日本語設定でポリシー上書き日付情報を表示できないという問題を修正しました。
- （HUB-32008）。QuartzVersionBomEventCleanupJobジョブによって「Up-to-date with error」イベントが自動クリーンアップされないことが原因で、[セキュリティリスクランキング]ページが処理中にスタックするという問題を修正しました。
- （HUB-33727）。脆弱性の修正ステータスまたはコメントを更新する際のUIのバグを修正しました（[プロジェクトバージョン]の[セキュリティ]タブ内）。
- （HUB-33691）。既知の弱点がある暗号化アルゴリズムの[暗号文]タブに警告アイコンが表示されないというUIのバグを修正しました。
- （HUB-34240）。/api/projects/{projectId}/custom-fields/{customFieldId}リクエストがnull値を送信するときに400エラーを生成する可能性がある問題を修正しました。
- （HUB-34246）。[プロジェクトバージョン比較]ビューでのブラウザ表示の問題を修正しました。
- （HUB-33246）。REST APIドキュメントを明確にしました。https://<server-url>/api/のhttps://.../への参照を置き換えました。
- （HUB-33481）。2021.8.x以降のバージョンの間で/api/projects/{pid}/versions/{vid}/matched-files?offset={larger than totalCount}の応答が一貫していないという問題を修正しました。matched-filesエンドポイントは、offset>totalCountの場合でも、空のアイテムで一貫して200 OK応答を返すようになりました。
- （HUB-34468）。高速スキャンが次のエラーで失敗する問題を修正しました：「開発者スキャン結果の取得中にエラーが発生しましたタイムアウトが発生した可能性があります。」または、マッチエンジンの遅延により発生するHTTP 404 Not Found応答を修正しました。
- （HUB-33512）。[管理] > [設定] > [ユーザー認証]の下にある[テスト接続、ユーザー認証およびフィールドマッピング]のテキストを更新しました。「テストユーザーのメタデータのマッピング結果を表示します」という記述を削除しました。
- （HUB-34836）。BLACKDUCK_HUB_SHOW_UNMATCHEDフラグが有効になっているときに、マッチしなかったコンポーネントをプロジェクト自体として編集できた問題を修正しました。
- （HUB-34380）。非常に多くの調整が行われたプロジェクトで新しいバージョンをスキャンしようとしたときに、「例外が発生しました。パラメータが多すぎます」というメッセージを伴ってサーバーで新しいバージョンのBOMスキャンが失敗するという問題を修正しました。
- （HUB-33793）。セキュリティリスクランキングの変更で「Black Duckセキュリティアドバイザリ」でライセンスされていない登録キーを使用した場合に、プロジェクトバージョン詳細レポートが失敗する問題を修正しました。
- （HUB-33375）。どのフィールドでソートするかを決定するループの外側にORDER_BYがあったクエリ構築コードの不適切なSQL文法を修正しました。ソートフィールドがない場合、ORDER_BYはnullになります。
- （HUB-34780）。500を超えるプロジェクト/バージョンが作成または削除された場合に、[管理] > [診断] >[使用方法：プロジェクト] > [Project_created/Version_Created/Version_Deleted]の統計が500に制限される問題を修正しました。

- （HUB-34592）。マッチしたコンポーネントがゼロであるが、テストで空のコンポーネントと既存のコンポーネントの両方が失敗する場合の、CodeLocationBomMatchCacheEntryエラーの逆シリアル化を修正しました。
- （HUB-34588）。リンクのエンコードされていないハッシュ文字が原因で、conanパッケージの著作権リンクが機能しない問題を修正しました。
- （HUB-24664）。BDSBackgroundUpdateWorkerが、HTTPSではなくHTTPを介して登録サーバーと通信しようとしていた問題を修正しました。
- （HUB-33679）。複合要素の抽出時に、MaaS対応スキャンが失敗することがある問題を修正しました。
- （HUB-34218）。「構成表コンポーネント表現」に「componentVersionName」と「componentVersion」が含まれるようにREST APIドキュメントを更新しました。

3. Black Duckバージョン2022.4.x

バージョン2022.4.2の新機能および変更された機能

データベース移行スクリプトのパフォーマンスの向上

Black Duckのバージョンをアップグレードする際に使用されるデータベース移行スクリプトのパフォーマンスが向上し、インストール時間が短縮されました。

コンテナバージョン

- blackducksoftware/blackduck-postgres:11-2.11
- blackducksoftware/blackduck-authentication:2022.4.2
- blackducksoftware/blackduck-webapp:2022.4.2
- blackducksoftware/blackduck-scan:2022.4.2
- blackducksoftware/blackduck-jobrunner:2022.4.2
- blackducksoftware/blackduck-cfssl:1.0.7
- blackducksoftware/blackduck-logstash：1.0.18
- blackducksoftware/blackduck-registration:2022.4.2
- blackducksoftware/blackduck-nginx：2.0.20
- blackducksoftware/blackduck-documentation:2022.4.2
- blackducksoftware/blackduck-upload-cache：1.0.27
- blackducksoftware/blackduck-redis:2022.4.2
- blackducksoftware/blackduck-bomengine:2022.4.2
- blackducksoftware/blackduck-matchengine:2022.4.2
- blackducksoftware/blackduck-webui:2022.4.2
- sigsynopsys/bdba-worker:2022.3.0
- blackducksoftware/rabbitmq：1.2.7

APIの機能強化

新規または変更されたAPIリクエストの詳細については、Black Duckで入手可能なAPIドキュメントを参照してください。

2022.4.2で修正された問題

Black Duck 2022.4.2には、お客様から報告された修正済みの問題は含まれていません。

バージョン2022.4.1の新機能および変更された機能

関連するマッチしなかったBDSAレコードを含むCVEを自動的に無視する新しいBDSA自動修正設定

この設定を有効にすると、修正ステータスがIGNOREDに設定され、脆弱性が修正された理由を説明するメッセージが追加されて、関連するマップされていないBDSAを含む新しいCVE脆弱性が自動的に修正されます。

この新しい設定は、関連するBDSAの脆弱性を含むCVE脆弱性にのみ適用されます。CVEはコンポーネントバージョンにマッピングされているが、関連するBDSAがそのコンポーネントバージョンにマッピングされていない場合、システムはシステム設定に基づいてCVE脆弱性を自動的に修正する可能性があります。

BDSA自動修正機能は、[管理者] > [システム設定] > [BDSA自動修正]ページで有効にできます。

高速スキャンに追加された新しいプロパティ

高速スキャンの出力に、次のプロパティが追加されました。

- cweIds: このセキュリティ脆弱性の共通脆弱性タイプ一覧(CWE)IDのリスト。
- shortTermUpgradeGuidance: この脆弱性に対処するための短期的な処置として推奨されるアップグレード先のコンポーネントバージョン。これは、使用中のものと同じメジャーバージョンであるためです。
- longTermUpgradeGuidance: 長期的な処置として推奨されるアップグレード先のコンポーネントバージョン。この処置を実行するには、メジャーバージョン番号のアップグレードが必要になる場合があり、より慎重に計画する必要があります。

ユーザー権限評価のパフォーマンスの向上

ほとんどのAPIリクエストに対するユーザー権限評価が改善されました。これにより、ユーザーの役割や権限に関係なく、構成表の読み込みを含む、読み込み時の整合性が向上します。

Synopsysctlの更新

Black Duck 2022.4.0インストールのsizes-gen03導入サイズのサポートが追加されるように、Synopsysctlが3.0.1に更新されました。

コンテナバージョン

- blackducksoftware/blackduck-postgres:11-2.11
- blackducksoftware/blackduck-authentication:2022.4.1
- blackducksoftware/blackduck-webapp:2022.4.1
- blackducksoftware/blackduck-scan:2022.4.1
- blackducksoftware/blackduck-jobrunner:2022.4.1
- blackducksoftware/blackduck-cfssl:1.0.7
- blackducksoftware/blackduck-logstash:1.0.18
- blackducksoftware/blackduck-registration:2022.4.1
- blackducksoftware/blackduck-nginx:2.0.16
- blackducksoftware/blackduck-documentation:2022.4.1
- blackducksoftware/blackduck-upload-cache:1.0.23
- blackducksoftware/blackduck-redis:2022.4.1

- blackducksoftware/blackduck-bomengine:2022.4.1
- blackducksoftware/blackduck-matchengine:2022.4.1
- blackducksoftware/blackduck-webui:2022.4.1
- sigsynopsys/bdba-worker:2022.3.0
- blackducksoftware/rabbitmq：1.2.7

APIの機能強化

新規または変更されたAPIリクエストの詳細については、Black Duckで入手可能なAPIドキュメントを参照してください。

プロジェクトエンドポイントのパフォーマンスの向上

次のAPIプロジェクトエンドポイントはパフォーマンスが低下しており、最適化されました。

. `/api/projects/{ID}/versions/{ID}/compare/projects/{ID}/versions/{ID}/components`
. `/api/projects/{ID}/versions/{ID}/components`

2022.4.1で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- （HUB-32395、HUB-33033）。マッチしたコンポーネントに対する変更済みの宣言されたライセンスがSPDXレポートに表示されないことがある問題を修正しました。
- （HUB-29532）。ディストロイメージのrootfsパスがルートディレクトリではなくサブディレクトリで開始される場合に、Linuxディストロパッケージの一致が崩れる問題が修正されました。
- （HUB-33947）。[影響を受けるプロジェクト]ページから[修正ステータス]を更新したときにセキュリティリスクが更新されなかった問題を修正しました。
- （HUB-33551）。コードの場所の名前がnullのbdioファイルをアップロードすると、リクエストがステータスコード400で失敗し、バックグラウンドで例外がスローされる問題を修正しました。
- （HUB-34065）。SPDX検証ツールで次のエラーの原因となっていたSPDX 2.2レポート形式を修正しました。

  ```
  The following warning(s) were raised: [object instance has properties which are not
   allowed by the schema: ["packageSupplier"] for {"pointer":"/packages/0"}
  ```

- （HUB-33616）。スキャンクライアントが誤ったIDでBDIOを生成することがあり（スキャンされたアーカイブ内にアーカイブエントリが重複している場合）、これによりbdioファイルがデータベースに保存されるときにエラーが発生する問題を修正しました。
- （HUB-33915、HUB-33865）。スキャンアップロードAPIがスキャンデータ全体をチャンクせずに1つのメッセージとしてRabbitMQに送信し、メッセージサイズエラーが発生する問題を修正しました。
- （HUB-24664）。登録コンテナのログにHTTP経由の通信の試行が表示されていた問題を修正しました。
- （HUB-33579）。--matchConfidenceThresholdパラメータを従来のscan.cliで使用した場合に機能しなかった問題を修正しました。
- （HUB-33311）。署名スキャナがエラーコード74で失敗する可能性がある問題を修正しました。このエラーを軽減するために、再試行機能が導入されました。

バージョン2022.4.0の発表

Spring Frameworkのセキュリティアドバイザリ（CVE-2022-22965）

Synopsysは、2022年3月30日に発表されたSpring Frameworkオープンソースソフトウェア CVE-2022-22965（Black Duck KnowledgeBase™でBDSA-2022-0858として追跡）に関連して公開されたセキュリティ上の問題を認識しています。この脆弱性の詳細については、CVEの公式エントリを参照してください。https://tanzu.vmware.com/security/cve-2022-22965

2022年3月31日、SpringはSpring Frameworkバージョン5.3.18および5.2.20をリリースし、CVE-2022-22965で説明されている脆弱性に対処しました。

現在、Synopsysは、Synopsys SIGの製品、サービス、システムへの露出が制限されていると考えています。露出された範囲で、悪用を防止する緩和策を適用しています。すべての社内調査が完了し、その調査結果は、コミュニティアドバイザリページの「製品ステータス」セクションに記載されています。

最後に、前述の調査はCVE-2022-22965（Spring Framework）のみに焦点を当てており、CVE-2022-22963（Spring Cloud Function）と混同しないようにしてください。

公開時に、SynopsysはSIG製品でCVE-2022-22963（Black Duck Hub KnowledgeBase™でBDSA-2022-0850として追跡）への暴露を特定していません。この評価を変更する新しい詳細情報が入手可能になった場合は、CVE-2022-22963の別の勧告が公開されます。

Black Duck 2022.4.0へのアップグレード

Black Duck 2022.4.0へのアップグレードには、このバージョンで導入された移行スクリプトやその他の新しいプロセスの実行により、予想よりも時間がかかる場合があります。詳細については、以下の新機能と変更機能のセクションを参照してください。

リソースガイダンスの変更

デフォルトのリソース設定が更新され、すべてのスキャンボリュームの推奨設定が増加しました。以前のリソース設定は引き続き使用可能であり、以下に説明するように新しいディレクトリに移動しましたが、使用は推奨されません。

正確な推定スキャンスループットは、スキャンサイズ、タイプ、コンポジションによって異なることに注意してください。しかしながら、この内訳を社内テストで使用して、以下の表に情報を収集しました。

- 50%フル署名スキャン
- 40%フルパッケージマネージャスキャン
- 10%開発者パッケージマネージャスキャン

コンテナリソースの制限

Black Duck 2022.4.0以降では、すべてのコンテナにリソース制限が設定されていますが、以前は一部のコンテナには設定されていませんでした。たとえば、以前のリソース割り当てでは、BomEngineコンテナのCPU制限が設定されていなかったため、制限のあるコンテナとは不釣り合いにCPUが使用される可能性がありました。以下の新しいサイズでは制限のないCPU使用が許可されないため、古い制限に近い新しいサイズを選択すると、スキャンスループットが低下することがあります。

ファイル編成の変更

上記の変更に加え、リソース上書きYAMLファイルの編成が変更されました。

Kubernetesの場合、Helmチャート内のリソース上書きYAMLファイルの編成が変更されました。

- valuesフォルダの名前がsizes-gen01に変更されました。
- 以前の4つのサイズ（S、M、L、XL）のファイル（small.yamlなど）は、新しいsizes-gen02ディレクトリに移動しました。
- 新しいディレクトリ（sizes-gen03）には、次の表に示す各構成のリソース上書きファイルが含まれます。これらのファイルには、10sph.yaml、120sph.yamlなどの名前が付けられています。

Swarmの場合、Black Duckはコンテナリソースを直接docker-compose.ymlに割り当てなくなります。代わりに、リソースは別の上書きファイルで指定されます。以前のリソース割り当ては（Black Duckバージョン2022.2.0以前）、sizes-gen02/resources.yamlに移動しました。Black Duck 2022.4.0以降では、sizes-gen03 folderで複数の割り当てが可能になります。

KubernetesとSwarmのどちらの場合も、1時間あたりの平均スキャン数で測定された負荷に基づいて、7つの割り当てがあります。予想される負荷が事前定義された割り当てのいずれにも一致しない場合は切り上げます。たとえば、1時間に100スキャンと予想される場合、sizes-gen03/120sph.yamlを選択します。

リソースガイダンスとコンテナの拡張性

これらの設定は、KubernetesとSwarmの両方のインストールに適用されます。

名前	スキャン/時間	Black Duckサービス	PostgreSQL	合計
10sph	10	CPU：12コア メモリ：30 GB	CPU：2コア メモリ：8 GB	CPU：14コア メモリ：38 GB
120sph	120	CPU：13コア メモリ：46 GB	CPU：4コア メモリ：16 GB	CPU：17コア メモリ：62 GB
250sph	250	CPU：17コア メモリ：118 GB	CPU：6コア メモリ：24 GB	CPU：23コア メモリ：142 GB
500sph	500	CPU：28コア メモリ：210 GB	CPU：10コア メモリ：40 GB	CPU：38コア メモリ：250 GB
1000sph	1000	CPU：47コア メモリ：411 GB	CPU：18コア メモリ：72 GB	CPU：65コア メモリ：483 GB
1500sph	1500	CPU：66コア メモリ：597 GB	CPU：26コア メモリ：104 GB	CPU：92コア メモリ：701 GB
2000sph	2000	CPU：66コア メモリ：597 GB	CPU：34コア メモリ：136 GB	CPU：100コア メモリ：733 GB

PostgreSQLの設定

PostgreSQLコンテナを使用しているお客様は、ALTER SYSTEMを使用して手動で値を設定する必要があり、shared_buffersへの変更は、次回PostgreSQLを再起動するまで有効になりません。これらの設定は、KubernetesとSwarmの両方のインストールに適用されます。

名前	スキャン/時間	PostgreSQL CPU/メモリ	shared_buffers（MB）	effective_cache_size（MB）
10sph	10	CPU：2コア メモリ：8 GB	2654	3185
120sph	120	CPU：4コア メモリ：16 GB	5338	6406
250sph	250	CPU：6コア	8018	9622

		メモリ:24 GB		
500sph	500	CPU:10コア メモリ:40 GB	13377	16053
1000sph	1000	CPU:18コア メモリ:72 GB	24129	28955
1500sph	1500	CPU:26コア メモリ:104 GB	34880	41857
2000sph	2000	CPU:34コア メモリ:136 GB	45600	54720

今後のPostgreSQL 9.6の廃止

以前の発表のように、PostgreSQL 9.6でのBlack Duckの実行のサポートは、Black Duckの2021.6.0リリースで終了しました。Black Duckの2022.7.0リリース以降、PostgreSQL 9.6でBlack Duckを実行しようとするとエラーが発生し、Black Duckは起動しません。

RHEL 7およびCentOS 7でのDesktop Scannerのサポート終了

2022.4.0以降、Black DuckはRed Hat Enterprise Linux 7およびCentOS 7用のDesktop Scannerの新しいバージョンを構築しなくなります。また、次期2022.7.0リリースでは、バイナリはすべて削除される予定です。

PostgreSQLサポートスケジュールの更新

将来の2022.10.0リリース以降、Black Duckは外部PostgreSQL 11のサポートを終了します。今後のPostgreSQLバージョンに関しては、サポートの開始日と終了日を以下の表で確認してください。

PGバージョン	最初のリリース	最終リリース	BD外部サポートの追加	BD外部サポートの終了
16.x	2023年後半	2028年後半	2024.7.0	2026.10.0
15.x	2022年後半	2027年後半	2023.7.0	2025.10.0
14.x	2021年9月	2026年11月	2022.7.0	2024.10.0
13.x	2020年9月	2025年11月	2021.8.0	2023.10.0
12.x	2019年10月	2024年11月	X	X
11.x	2018年10月	2023年11月	2020.6.0	2022.10.0

Azure PostgreSQL 13 Flexサーバー構成

Black Duckをインストールすると、initスクリプトexternal-postgres-init.pgsqlの実行時に、Azureユーザーに次のエラーメッセージが表示されることがあります。

```
psql:/dev/fd/63:25: ERROR: extension "pgcrypto" is not allow-listed for "azure_pg_admin" users in Azure Database for PostgreSQL
```

このエラーを回避するには、Azure PG 13 Flexサーバーの使用時に、サーバーパラメーターazure.extensionsに値PGCRYPTOがあることを確認してください。

非推奨API

次のレガシーAPI Solrエンドポイントは非推奨となり、Black Duck 2022.7.0リリースでは削除されます。

- GET /api/search/components
- GET /api/autocomplete/component

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2022.2.0が日本語にローカライズされました。

簡体字中国語

UI、オンラインヘルプ、およびリリースノートのバージョン2022.2.0が簡体字中国語にローカライズされました。

バージョン2022.4.0の新機能および変更された機能

Spring Frameworkの更新

Spring Frameworkは、重要なCVE-2022-22965の脆弱性に対処するために5.3.18に更新されました。

新しい脆弱性のメトリックの比較

この新機能により、脆弱性の概要ページが変更され、必要に応じてメトリックを並べて表示できるようになりました。BDSAとNVDの両方のレコードがある脆弱性を表示すると、[スコアとメトリック]セクションに、BDSAとNVDの両方の脆弱性タイプを比較したグラフが表示されます。CVSS v2とCVSS v3.xを交互に使用して、詳細を把握してください。

GitリポジトリSCM統合 - フェーズ1

Black Duck 2022.4.0では、リポジトリ、ブランチ、ビルド、リリースの管理に統合を活用することで、顧客の新規プロジェクトのオンボーディングを簡素化する方法が導入されます。フェーズ1から、プロジェクト作成モーダルおよびプロジェクト設定ページに新しいSCM URLフィールドが、プロジェクトバージョン設定ページにSCMブランチフィールドが追加されます。

このフェーズでは、これらのフィールドに手動で情報を入力します。ただし、次回のDetectリリースでは、gitリポジトリのスキャン後に自動的に情報が入力されます。Detectは、関連付けられているgitリポジトリのURLとブランチを自動的に識別し、その情報をBlack Duckに送信します。

この機能はBlack Duckではデフォルトでは有効になっておらず、環境に以下を追加して有効にする必要があります。

Swarmユーザーの場合は、以下をdocker-compose.yml webapp環境に追加します。

```
webapp:
    environment: {blackduck.scan.scm.enableIntegration: true}
```

Kubernetesユーザーの場合は、以下をwebappコンテナ環境に追加します。

```
containers:
- env:
  - name: blackduck.scan.scm.enableIntegration
    value: true
```

BDSA脆弱性の新しい[コンポーネント]タブ

新しい[コンポーネント]タブが、BDSA脆弱性レコードに追加されました。このタブでは、特定のBDSA脆弱性の影響を受ける既知のすべてのコンポーネントバージョンを確認できます。

コンポーネントダッシュボードの拡張によってクエリ表示を実現

SearchDashboardRefreshJobに関連するすべてのクエリは、パフォーマンスを向上させるために最適化されました。LicenseDashboardRefreshJobの使用が可能になり、それに関連するビューがSearchDashboardRefreshJobの下で更新されます。つまり、[ライセンス管理]ページに表示されるカウントが、SearchDashboardRefreshJobの終了時に更新されます。

注:これらの変更の結果、Black Duck 2022.4.0へのアップグレードには、移行スクリプトの実行のために通常より時間がかかる場合があります。

PostgreSQL 11コンテナの移行

Synopsys提供のPostgreSQLコンテナを使用したKubernetesとOpenShiftの導入において、2022.2.0で追加された次の永続ボリューム要求は不要になりました。このボリューム要求とそれに関連付けられている永続ボリュームは安全に削除できます。

```
{{ .Release.Name }}-blackduck-postgres-tmp
```

Javaヒープサイズの割り当てと新しい環境変数を更新

以前のリリースでは、JavaはヒープサイズをHUB_MAX_MEMORYにまで徐々に増加させることが許可されていました。Black Duck 2022.4.0以降では、効率性と予測可能性を活用するために、起動時にHUB_MAX_MEMORY全体が事前に割り当てられます。

この更新の一環として、次の新しい環境変数が追加されました。HUB_MIN_MEMORY.この変数を使用すると、Javaヒープサイズの下限を設定できます。

デフォルトでは最適な設定として、HUB_MIN_MEMORYはHUB_MAX_MEMORYに等しく設定されますが、512mなどの少ない量に明示的に設定し、HUB_MIN_MEMORYからHUB_MAX_MEMORYまで徐々にJavaにメモリを取得させることができます。

高速スキャンポリシーの上書きを特定の脆弱性に制限

以前のBlack Duckバージョンでは、高速スキャンポリシー違反がポリシーとコンポーネントによって上書きされる可能性がありました。ただし、新しい脆弱性が見つかった場合、既存の上書きによって違反が抑制され、偽陰性になる可能性があります。

Black Duck 2022.4.0では、既存のYAMLアップロードメカニズムを使用して、高速スキャンの特定の脆弱性を上書きできるようになりました。

脆弱性IDでは、予想される形式への一致が検証されます。

```
---
version: 1.0
policy:
  overrides:
  - policyName: policyA
    components:
    -  name: component1
       version: version1
       vulnerabilities:
       - vulnerabilityId1
       - vulnerabilityId2
    - name: component2
  - policyName: policyB
    components:
    - name: component3
```

新しい高速スキャンの脆弱性プロパティの追加

高速スキャンの出力の脆弱性には、次のプロパティが追加されました。

- publishedDate（日付値）
- vendorFixDate（日付値）
- workaround（文字列値）
- solution（文字列値）

新しいBDSA自動修正設定（ベータ版）

Black Duckセキュリティアドバイザリ（BDSA）チームは、CVE脆弱性を分析するとき、脆弱性の影響を受けるコンポーネントバージョンを確認します。場合によっては、この脆弱性がさまざまなバージョンに適用されることがわかります。この新機能を使用すると、脆弱性がそのコンポーネントバージョンに適用されないことをBDSAチームが発見した場合に、CVE脆弱性を自動的に無視することができます。これは、ステータスがNEWの脆弱性にのみ影響します。

BDSA自動修正はベータ機能であり、デフォルトでは有効になっていません。この機能を有効にするには、次の環境変数を設定する必要があります。

```
BDSA_AUTO_REMEDIATION=true
```

BDSA自動修正設定は、[管理者] > [システム設定] > [BDSA自動修正]ページで変更できます。

注： ユーザーが設定を保存するたびに、システムによってチェックが行われ、すべてのプロジェクトの脆弱性が更新される可能性があります。大規模なシステムではこれに時間がかかり、Black Duckのパフォーマンスに影響する可能性があります。

ユーザーとグループの管理表示を更新

[管理者] > [ユーザーとグループ]の[ユーザー]タブと[グループ]タブの外観が更新され、さまざまなセクション（ユーザー/グループの詳細、全体的な役割、プロジェクトグループ、プロジェクト、ユーザー/ユーザーグループ）がそれぞれのページに分かれて明確に表示され、ユーザーとグループの管理が容易になりました。

ポリシーの新しいコンポーネント条件ルール

未確認スニペットの新しいコンポーネント条件が追加されました。新しいポリシー条件では、ポリシーを作成または編集して、レビューされていないスニペットにポリシー違反をトリガーできます。

新しいソフトウェア構成表（SBOM）レポートのCycloneDX v1.3エクスポート形式

プロジェクトのソフトウェア構成表レポートをCycloneDX v1.3形式でエクスポートできるようになりました。これを行うには、プロジェクトバージョンを表示し、[レポート]タブをクリックし、[レポートの作成]ボタンをクリックして、CycloneDX v1.3 – JSONを選択します。CycloneDX v1.3の詳細については、CycloneDX v1.3リファレンスページを参照してください。

新しいコンポーネント依存関係の重複感度システムプロパティ

新しいシステムプロパティがBlack Duckに追加され、パッケージマネージャスキャンで結果の依存関係ツリーに追加するコンポーネントごとにノード（マッチ）の最大数を制御できるようになりました。

```
blackduck.match.limit.per.component
```

このシステムプロパティのデフォルト値は10であるため、ツリー内で重複するコンポーネントの数は、blackduck.match.limit.per.componentの値（コンポーネントごとのマッチ制限）を超えることはできません。

サポートされるブラウザのバージョン

- Safariバージョン15.4（16613.1.17.1.13、16613）
  - Safariバージョン13.0以前はサポートされなくなりました

- Chromeバージョン100.0.4896.75（公式ビルド）（x86_64）
  - Chromeバージョン71以前はサポートされなくなりました
- Firefoxバージョン99.0（64ビット）
  - Firefoxバージョン71以前はサポートされなくなりました
- Microsoft Edgeバージョン100.0.1185.36（公式ビルド）（64ビット）
  - Microsoft Edgeバージョン78以前はサポートされなくなりました

コンテナバージョン

- blackducksoftware/blackduck-postgres:11-2.11
- blackducksoftware/blackduck-authentication:2022.4.0
- blackducksoftware/blackduck-webapp:2022.4.0
- blackducksoftware/blackduck-scan:2022.4.0
- blackducksoftware/blackduck-jobrunner:2022.4.0
- blackducksoftware/blackduck-cfssl:1.0.7
- blackducksoftware/blackduck-logstash：1.0.18
- blackducksoftware/blackduck-registration:2022.4.0
- blackducksoftware/blackduck-nginx：2.0.14
- blackducksoftware/blackduck-documentation:2022.4.0
- blackducksoftware/blackduck-upload-cache：1.0.23
- blackducksoftware/blackduck-redis:2022.4.0
- blackducksoftware/blackduck-bomengine:2022.4.0
- blackducksoftware/blackduck-matchengine:2022.4.0
- blackducksoftware/blackduck-webui:2022.4.0
- sigsynopsys/bdba-worker:2021.12.2
- blackducksoftware/rabbitmq：1.2.7

APIの機能強化

新規または変更されたAPIリクエストの詳細については、Black Duckで入手可能なAPIドキュメントを参照してください。

プロジェクトエンドポイントのパフォーマンスの向上

次のAPIプロジェクトエンドポイントはパフォーマンスが低下しており、最適化されました。

. `/api/projects/{ID}/versions/{ID}/compare/projects/{ID}/versions/{ID}/components`
. `/api/projects/{ID}/versions/{ID}/components`

2022.4.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- （HUB-33047）。KbUpdateJobプロセス中にNULLポインタ例外エラーが発生した場合、ジョブの進行が非常に遅くなったり、スタックしているように見えたりする問題が修正されました。
- （HUB-32336）。BOMページのコンポーネントフィルタの名前は、実際の機能に合わせてコンポーネントバージョンに変更されました。
- （HUB-32316）。JVMの最大メモリ割り当てプールを定義するHUB_MAX_MEMORY環境変数がDocker登録コンテナ展開で設定解除されたままになる問題が修正されました。
- （HUB-32492）。MITライセンスがBlack Duckで承認済みに設定されているが、MITライセンスを持つコンポーネントが高速スキャンで「ライセンス未承認」および「ライセンス未確認」のポリシー違反をトリガーする可能性がある問題が修正されました。
- （HUB-31839）。BDIOアップロードエンドポイントプロジェクトとバージョン値がURLデコードされない問題が修正されました。
- （HUB-32692、HUB-32672）。コンポーネントに複数の脆弱性があり、それぞれの脆弱性ステータスが異なる場合、コンポーネントのすべての脆弱性が選択したポリシールールに一致しない限り、ポリシールールがポリシー違反をトリガーしない問題が修正されました。
- （HUB-31872）。高速スキャンでユーザー権限が検証されない問題が修正されました。一致するプロジェクトバージョンBOMがスキャンで検出されたが、ユーザーに権限がない場合、スキャンはプロジェクトバージョンまたはBOMコンポーネントデータなしで実行されます。
- （HUB-33231）。スキャンページでスキャンサイズによってスキャンをソートしても、リストが正しい順序で表示されない問題が修正されました。
- （HUB-33096）。ライセンスファミリによってフィルタリングしても、修正されたナレッジベースライセンスが正しく表示されない問題が修正されました。
- （HUB-30463）。golang.org/x/sysコンポーネントがHub UIナレッジベース検索に表示されない問題が修正されました。
- （HUB-31891）。Apache HTTPサーバーコンポーネントを検索すると、Debianコンポーネントページにリンクする問題が修正されました。
- （HUB-28406）。一部のOSSコンポーネントおよびバージョンの[セキュリティ]タブと[詳細情報]タブに表示される脆弱性の数が異なることがある問題が修正されました。
- （HUB-32883）。accessTokenValiditySeconds設定のMax-AgeおよびExpiresフィールドがJSON Webトークン（JWT）の有効期限値と一致しない問題が修正されました。
- （HUB-32313）。パッケージマネージャのスキャンデータの高負荷を処理する際のREST API /api/projects/<id>/versions/<id>/componentsエンドポイントのパフォーマンスの問題が修正されました。
- （HUB-32571）。コンポーネントバージョンの著作権タブおよびBlack Duck通知レポート（およびBOMセキュリティタブ）で、元の名前空間の表示が一貫しない問題が修正されました。
- （HUB-32949）。ユーザーをプロジェクトグループに直接割り当て、プロジェクトグループにも割り当てられているユーザーグループに同じユーザーを割り当てると、複数のプロジェクトグループがAPIによって返されてDetectが失敗する問題が修正されました。
- （HUB-33132）。依存関係パスAPIが大量のサービスメモリを消費し、ディスクにページングしていた問題を修正しました。
- （HUB-33155）。ハブ登録の更新が停止し、JobRunnerがロックを保持する時間が長引いて、クエリがブロックされる問題が修正されました。
- （HUB-32010）。プロジェクトグループ階層を移動するときに、サブグループ内のプロジェクトをクリックすると、ユーザーがルートプロジェクトグループに戻る可能性がある問題が修正されました。
- （HUB-32977）。大文字と小文字が混在したタグがポリシールールを期待どおりにトリガーしない問題が修正されました。

- （HUB-33305）。docker-compose.local-overrides.ymlファイル内のインデントの問題が修正されました。
- （HUB-27940）。最小CPUリソースが指定されていない状態でEKSに展開するとき、ポッドに0.25（250m）のCPUコアが割り当てられ、bomengine/rabbitmqが動作しない問題が修正されました。
- （HUB-33455）。CVE-2022-23395の脆弱性の詳細ページへのリンクが404 Not Foundエラーページに移動する問題が修正されました。
- （HUB-32256）。カスタム署名レベルに空の値を送信すると、誤ったエラーメッセージが生成される問題が修正されました。
- （HUB-32800）。依存関係ツリー内のコンポーネントごとに大量のマッチがあるため、bitbake/yoctoスキャン中にJobRunnerでmatchengineが再起動するかジョブがハングし、OutOfMemory例外が発生することがある問題が修正されました。詳細については、上記の新機能および変更された機能に関するセクションの「新しいコンポーネント依存関係の重複感度システムプロパティ」を参照してください。
- （HUB-33349）。webappコンテナがデフォルトで{{ .Release.Name }}-blackduck-webappという名前の永続ボリューム（Release.Nameは一般的にhubまたは展開時に選択した別のラベル）を必要とする問題が修正されました。また、webapp values.yamlのオーバーライドでpersistentVolumeClaimNameを設定することで、カスタム永続ボリューム名を設定しているお客様もいます。これらの設定、永続ボリューム、永続ボリューム要求は不要になり、安全に削除できます。
- （HUB-32678）。デフォルトのIPスキャンで、一致するコンポーネントをフィルタリングするためのscan.cli引数--matchConfidenceThresholdがサポートされない問題が修正されました。
- （HUB-29532）。ディストロイメージのrootfsパスがルートディレクトリではなくサブディレクトリで開始される場合に、Linuxディストロパッケージの一致が崩れる問題が修正されました。

4. Black Duckバージョン2022.2.x

バージョン2022.2.2の新機能および変更された機能

Black Duck バージョン2022.2.2はメンテナンスリリースであり、新機能や変更された機能はありません。セキュリティ脆弱性を回避するために、オンラインヘルプを修正しました。

コンテナバージョン

- blackducksoftware/blackduck-postgres:11-2.8
- blackducksoftware/blackduck-authentication:2022.2.2
- blackducksoftware/blackduck-webapp:2022.2.2
- blackducksoftware/blackduck-scan:2022.2.2
- blackducksoftware/blackduck-jobrunner:2022.2.2
- blackducksoftware/blackduck-cfssl:1.0.6
- blackducksoftware/blackduck-logstash：1.0.16
- blackducksoftware/blackduck-registration:2022.2.2
- blackducksoftware/blackduck-nginx：2.0.12
- blackducksoftware/blackduck-documentation:2022.2.2
- blackducksoftware/blackduck-upload-cache：1.0.21
- blackducksoftware/blackduck-redis:2022.2.2
- blackducksoftware/blackduck-bomengine:2022.2.2
- blackducksoftware/blackduck-matchengine:2022.2.2
- blackducksoftware/blackduck-webui:2022.2.2
- sigsynopsys/bdba-worker:2021.12.2
- blackducksoftware/rabbitmq：1.2.7

APIの機能強化

新規または変更されたAPIリクエストの詳細については、Black Duckで入手可能なAPIドキュメントを参照してください。

2022.2.2で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- （HUB-34065）。SPDX検証ツールで次のエラーの原因となっていたSPDX 2.2レポート形式を修正しました。

```
The following warning(s) were raised: [object instance has properties which are not
 allowed by the schema: ["packageSupplier"] for {"pointer":"/packages/0"}
```

バージョン2022.2.1の新機能および変更された機能

更新されたデータ削除機能（ベータ版）

データ削除機能を使用すると、定義した条件に従ってプロジェクトバージョンを自動的に削除する方法を検討できます。バージョン制限、ディスク容量の制約、またはデータベースのボトルネックがあるユーザーの場合、古いバージョンの増加は、プロセスまたはシステムパフォーマンスのいずれかで問題となる可能性があります。この機能は、時間の経過とともに複数のプロジェクトバージョンを生成し、時間の経過とともに廃版になる場合に役立ちます。

Black Duck 2022.2.0には新しい環境変数が追加されました。

- BLACKDUCK_AUTOMATIC_VERSION_REMOVAL_RELEASE_PHASES
  - データ削除プロセスに適用できるプロジェクトバージョンフェーズを定義します。
  - リリースフェーズの値は、Planning（計画）、Development（開発）、Released（リリース）、Deprecated（廃止）、Archived（アーカイブ）、Prerelease（プレリリース）です。
  - 設定しない場合、デフォルト値はDevelopmentです。
  - 値では大文字と小文字が区別されません。
  - 複数のリリースフェーズは、カンマで区切って追加できます。

プロジェクトおよびプロジェクトグループの役割割り当てを更新

プロジェクトおよびプロジェクトグループにプロジェクトビューアとしてユーザーを追加できるようになりました。プロジェクトまたはプロジェクトグループにユーザーを追加すると、プロジェクトビューアの役割が自動的に選択され、デフォルトの役割として機能します。その後、必要に応じてユーザーに役割を追加できます。

最小スキャン間隔の設定を更新

Detect 7.13以降から、Black Duck Hubスキャン設定の最小スキャン間隔は無効になります。最小スキャン間隔は、次のようにDetectを使用してコマンド引数として設定する必要があります。

```
--detect.blackduck.signature.scanner.arguments='--min-scan-interval=##'
```

ここで、##は時間単位の時間です。

コンテナバージョン

- blackducksoftware/blackduck-postgres:11-2.8
- blackducksoftware/blackduck-authentication:2022.2.1
- blackducksoftware/blackduck-webapp:2022.2.1
- blackducksoftware/blackduck-scan:2022.2.1
- blackducksoftware/blackduck-jobrunner:2022.2.1
- blackducksoftware/blackduck-cfssl:1.0.6
- blackducksoftware/blackduck-logstash：1.0.16
- blackducksoftware/blackduck-registration:2022.2.1
- blackducksoftware/blackduck-nginx：2.0.12
- blackducksoftware/blackduck-documentation:2022.2.1
- blackducksoftware/blackduck-upload-cache：1.0.21

- blackducksoftware/blackduck-redis:2022.2.1
- blackducksoftware/blackduck-bomengine:2022.2.1
- blackducksoftware/blackduck-matchengine:2022.2.1
- blackducksoftware/blackduck-webui:2022.2.1
- sigsynopsys/bdba-worker:2021.12.2
- blackducksoftware/rabbitmq：1.2.7

APIの機能強化

新規または変更されたAPIリクエストの詳細については、Black Duckで入手可能なAPIドキュメントを参照してください。

2022.2.1で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- （HUB-32540）。重複した値を挿入すると、ジョブの速度が低下したり、ジョブが失敗したりする可能性があるという、KbUpdateJobのまれな問題を修正しました。
- （HUB-32544）。スキャンによってすでに挿入されたversion_bom_componentをKbUpdateJobが挿入しようとする競合状態の問題を修正しました。
- （HUB-33045）。高速スキャン専用のポリシールールを作成すると、すべてのプロジェクトバージョンが再計算状態になり、BOMのステータスが「処理中」に変わる問題が修正されました。
- （HUB-32363およびHUB-33027）。次のシナリオでコードの場所をマッピング解除している間の競合状態を修正しました（--detect.project.codelocation.unmap=trueを使用しない）。
  - コードの場所を再スキャンし、他のプロジェクトバージョンにマッピングする。
  - コードの場所をUIから手動でマッピング解除する。
  - コードの場所をUIから手動で削除する。
  - コードの場所をScanPurgeJobによって削除する。
- （HUB-33155）。ハブ登録の更新が停止し、JobRunnerがロックを保持する時間が長引いて、クエリがブロックされる問題が修正されました。
- （HUB-33132）。依存関係パスAPIが大量のサービスメモリを消費し、ディスクにページングしていた問題を修正しました。
- （HUB-31212）。1つのサブプロジェクトグループのメンバーがすべてのプロジェクトグループとそのツリーにアクセスできる問題を修正しました。
- （HUB-33162）。最高優先度のセキュリティリスクランキングセットが脆弱性タイプ（BDSAとNVD）およびCVSSプリファレンスと一致しない場合に、高速スキャンで不正な情報が表示される問題を修正しました。
- （HUB-31756）。プロジェクトビューアおよびプロジェクトグループビューアの役割が、プロジェクトおよびプロジェクトグループに追加されたユーザーに割り当てられない問題を修正しました。
- （HUB-33047）。KbUpdateJobプロセス中にNULLポインタ例外エラーが発生した場合、ジョブの進行が非常に遅くなったり、スタックしているように見えたりする問題が修正されました。

バージョン2022.2.0の発表

強化された署名生成

Black Duck 2022.2.0以降、署名スキャナはデフォルトでは、サーバーではなくクライアント上で署名を生成するようになります。

Black Duckでホストされるサービスを使用している場合、またはこのリリースに含まれているHelmチャートまたはDocker Swarm 'yaml'ファイルを使用している場合、この変更はシームレスに行われ、ユーザー側での操作は必要ありません。サービスの中断はありません。

ただし、Helmチャートをカスタマイズした場合や、上書きファイルを使用する場合は、移行に役立つ追加情報について、コミュニティページの「再バランシングのガイダンス」を参照してください。

APIリクエストのページ数制限の最大値

システムリソースの管理を改善する継続的な取り組みで、最大ページ数の制限が特定のAPIリクエストに導入されました。最大ページ数制限は1000ページに設定されますが、Black Duckの今後のバージョンで変更される可能性があります。2022.2.0バージョンで影響を受けるAPIリクエストのリストについては、以下の「APIの機能強化」セクションを参照してください。

廃止されたAPI

Black Duck 2022.2.0では、/cpes/{cpeId}/variantsエンドポイントが廃止され、/cpes/{cpeId}/originsに置き換えられます。/cpes/{cpeId}/variantsは、Black Duck 2022.4.0で削除されます。/api/cpesのメタデータ内のAPIリンクも、/api/cpes/{cpeId}/variantsではなく、/api/cpes/{cpeId}/originsを返すように更新されています。

今後のリソースガイダンスの変更

次回のBlack Duck 2022.4.0リリースでは、デフォルトのリソース設定が更新され、すべてのスキャンボリュームの推奨設定が増加します。2022.4.0リリースには、既存の設定を引き続き使用する方法についての説明が付属しています。

正確な推定スキャンスループットは、スキャンサイズ、タイプ、コンポジションによって異なることに注意してください。しかしながら、この内訳を社内テストで使用して、以下の表に情報を収集しました。

- 50%フル署名スキャン
- 40%フルパッケージマネージャスキャン
- 10%開発者パッケージマネージャスキャン

ファイル編成の変更

2022.4.0以降では、上記の変更に加え、リソース上書きYAMLファイルの編成が変更されます。

Kubernetesの場合、Helmチャート内のリソース上書きYAMLファイルの編成が変更されます。

- valuesフォルダの名前がsizes-gen01に変更されます。
- 以前の4つのサイズ（S、M、L、XL）のファイル（small.yamlなど）は、新しいsizes-gen02ディレクトリに移動します。
- 新しいディレクトリ（sizes-gen03）には、次の表に示す各構成のリソース上書きファイルが含まれます。これらのファイルには、10sph.yaml、120sph.yamlなどの名前が付けられています。

Swarmの場合、Black Duckはコンテナリソースを直接docker-compose.ymlに割り当てなくなります。代わりに、リソースは別の上書きファイルで指定されます。現在のリソース割り当てはsizes-gen02/resources.yamlに移動されます。Black Duck 2022.4.0以降では、sizes-gen03 folderで複数の割り当てが可能になります。

KubernetesとSwarmのどちらの場合も、1時間あたりの平均スキャン数で測定された負荷に基づいて、7つの割り当てがあります。予想される負荷が事前定義された割り当てのいずれにも一致しない場合は切り上げます。たとえば、1時間に100スキャンと予想される場合、sizes-gen03/120sph.yamlを選択します。

リソースガイダンスとコンテナの拡張性

これらの設定は、KubernetesとSwarmの両方のインストールに適用されます。

名前	スキャン/時間	Black Duckサービス	PostgreSQL	合計
10sph	10	CPU:10コア メモリ:29 GB	CPU:2コア メモリ:8 GB	CPU:12コア メモリ:37 GB
120sph	120	CPU:12コア メモリ:46 GB	CPU:4コア メモリ:16 GB	CPU:16コア メモリ:62 GB
250sph	250	CPU:16コア メモリ:106 GB	CPU:6コア メモリ:24 GB	CPU:22コア メモリ:131 GB
500sph	500	CPU:27コア メモリ:208 GB	CPU:10コア メモリ:40 GB	CPU:37コア メモリ:249 GB
1000sph	1000	CPU:47コア メモリ:408 GB	CPU:18コア メモリ:72 GB	CPU:65コア メモリ:480 GB
1500sph	1500	CPU:66コア メモリ:593 GB	CPU:26コア メモリ:104 GB	CPU:92コア メモリ:697 GB
2000sph	2000	CPU:66コア メモリ:593 GB	CPU:34コア メモリ:136 GB	CPU:100コア メモリ:729 GB

PostgreSQLの設定

PostgreSQLコンテナを使用しているお客様は、ALTER SYSTEMを使用して手動で値を設定する必要があり、shared_buffersへの変更は、次回PostgreSQLを再起動するまで有効になりません。これらの設定は、KubernetesとSwarmの両方のインストールに適用されます。

名前	スキャン/時間	PostgreSQL CPU/メモリ	shared_buffers(MB)	effective_cache_size(MB)
10sph	10	CPU:2コア メモリ:8 GB	2654	3185
120sph	120	CPU:4コア メモリ:16 GB	5338	6406
250sph	250	CPU:6コア メモリ:24 GB	8018	9622
500sph	500	CPU:10コア メモリ:40 GB	13377	16053
1000sph	1000	CPU:18コア メモリ:72 GB	24129	28955
1500sph	1500	CPU:26コア メモリ:104 GB	34880	41857
2000sph	2000	CPU:34コア メモリ:136 GB	45600	54720

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2021.10.0が日本語にローカライズされました。

簡体字中国語

UI、オンラインヘルプ、およびリリースノートのバージョン2021.10.0が簡体字中国語にローカライズされました。

バージョン2022.2.0の新機能および変更された機能

Logstashの更新

CVE-2021-44832の脆弱性に対処するため、Black Duckで使用されるLogstashイメージは、Log4j2バージョン2.17.1を使用する7.16.3にアップグレードされました。

強化された署名生成

「発表」で述べたように、署名スキャナはデフォルトでは、サーバーではなくクライアント上で署名を生成するようになります。

Black Duckでホストされるサービスを使用している場合、またはこのリリースに含まれているHelmチャートまたはDocker Swarm 'yaml'ファイルを使用している場合、この変更はシームレスに行われ、手動の操作は必要ありません。サービスの中断はありません。

ただし、Helmチャートをカスタマイズした場合や、上書きファイルを使用する場合は、移行に役立つ追加情報について、コミュニティの「再バランシングのガイダンス」の記事を参照してください。

コミュニティでは、PrometheusとGrafanaを使用したBlack Duckの監視に関する詳細も記載されています。

高速スキャンの機能強化

同じエンドポイントが使用されますが、高速スキャンモードを受け入れるために新しいヘッダーが追加されました。新しいHTTPヘッダーは「X-BD-RAPID-SCAN-MODE」という名前であり、次の値を受け入れます。

- ALL：デフォルトの操作。RAPIDまたは（RAPIDおよびFULL）であるポリシールールを評価します。ヘッダーがnullの場合は、これがデフォルトになります。
- BOM_COMPARE：ALLなどのすべてのポリシールールを評価しますが、ポリシールールモードのタイプに基づいて別々に評価を行います。ポリシールールが（RAPIDおよびFULL）の場合は、BOM_COMPARE_STRICTと同様に動作しますが、ポリシールールが（RAPID）のみである場合は、ALLと同様に動作します。RAPIDのみのポリシーは、結果にnullのポリシーステータスが表示されます。
- BOM_COMPARE_STRICT：（RAPIDおよびFULL）であるポリシールールのみを評価します。陽性結果に含まれるすべてのポリシールールのステータスは、NEWまたはRESOLVEDになります。ポリシー違反は、既存のプロジェクトバージョンの構成表と比較されます。ポリシー違反が既知で、すでに構成表に表示されていた場合（アクティブまたは上書き）、そのポリシー違反は高速スキャンの陽性結果には含まれませんが、既存の制限に従った完全な結果には含まれます。

BOM_COMPAREモードのいずれかを実行するには、HUBに既存のプロジェクトバージョンが必要です。

PostgreSQL 11コンテナの移行

CentOS PostgreSQL 9.6コンテナは、Black Duck PostgreSQL 11コンテナに置き換えられました。新しいblackduck-postgres-upgraderコンテナは、PostgresSQL 9.6からPostgreSQL 11にデータベースを移行し、完了すると終了します。

コア以外のPG拡張機能を使用しているお客様の場合は、移行前にそれらをアンインストールし、移行が正常に完了した後に再インストールすることを強くお勧めします。そうしないと、移行が失敗する可能性があります。

レプリケーションを設定しているお客様は、移行前に、pg_upgradeのドキュメントの手順に従う必要があります。そこで説明されている準備が行われていない場合、移行はおそらく成功しますが、レプリケーションの設定が壊れます。

重要：移行を開始する前に：

- システムカタログのデータコピーによるディスクの使用に起因する予期しない問題を回避するため、10%ほどの余裕をディスク容量に確保してください。
- ディスク容量が不足するとLinuxシステムが中断する可能性があるため、ルートディレクトリの容量とボリュームマウントを確認してください。

synossysctlを使用して2022.2.0に更新すると、次のタスクが実行されます。

- Black Duckインスタンスを停止する
- Synopsys提供のPGコンテナのユーザー向けにデータベース移行ジョブを実行する
- インスタンスを更新して再起動する

KubernetesおよびOpenShiftユーザーの場合：

- 移行は1回限りのジョブによって実行されます。
  - Black Duckを停止します。例：

    ```
    kubectl scale --replicas=0 -n <your_namespace> deployments --selector
     app=blackduck
    ```

  - アップグレードジョブを実行します。例：

    ```
    helm upgrade <your_deployment_name> . -n <your_namespace>
     <your_normal_helm_options> --set status=Stopped --set runPostgresMigration=true
    ```

  - helm upgradeで通常どおりBlack Duckを再起動します。
  - この移行により、CentOS PostgreSQLコンテナの使用がSynopsys提供のコンテナに置き換えられます。また、synopsys-initコンテナは、blackduck-postgres-waiterコンテナに置き換えられます。
- プレーンなKubernetesでは、アップグレードジョブのコンテナはルートとして実行されます。ただし、唯一の要件は、ジョブがPostgreSQLデータボリュームの所有者と同じUIDで実行されることです。
- OpenShiftでは、アップグレードジョブは、PostgreSQLデータボリュームの所有者と同じUIDで実行されることを前提としています。

Swarmユーザーの場合：

- 移行は完全に自動化されているため、Black Duckの標準アップグレードの操作以外に追加の操作は必要ありません。
- 上記のレイアウトとUIDの変更を行うには、blackduck-postgres-upgraderコンテナをルートとして実行する必要があります。
- その後のBlack Duckの再起動時に、blackadu-postgres-upgraderは移行が不要であると判断し、すぐに終了します。
- オプション：移行が成功した後は、blackduck-postgres-upgraderコンテナをルートとして実行する必要はありません。

更新したセキュリティリスクランキング

一般的な業界動向に基づいて、デフォルトのセキュリティリスクランキングでは、脆弱性スコアの精度を高めるため、CVSS 3.0スコアをBDSAとともに主要スコアメトリックとして使用するようになりました。

新しいデフォルトのランキングは次のとおりです。

- BDSA（CVSS v3.x）

- NVD（CVSS v3.x）
- BDSA（CVSS v2）
- NVD（CVSS v2）

この更新では、新規インストールのランキングのみが変更されます。既存のインスタンスへのアップグレードでは、以前に設定されたランキング順序が維持されます。

バージョン詳細コンポーネントレポートの機能強化

新しい[コンポーネントリンク]列がバージョン詳細コンポーネントレポートに追加されました。この列には、コンポーネントの詳細ページを表示するときに表示されるコンポーネントのURLが含まれます。このレポートは、ダッシュボードで目的のプロジェクトを選択し、バージョンを選択し、[レポート]タブをクリックして、[作成]ボタンをクリックし、[バージョン詳細レポート]を選択することによって生成されます。次のポップアップで、[コンポーネント]チェックボックスがオンになっていることを確認し、新しい[コンポーネントリンク]列を含むコンポーネントレポートを生成します。

脆弱性警告表示の機能強化

プロジェクトのコンポーネントの脆弱性を表示するとき、当該の脆弱性のリンク済みBDSAが、このプロジェクトバージョンで使用されるコンポーネントのバージョンに関連付けられていない場合に、Black Duckが警告を表示するようになりました。指定した脆弱性を表示すると、次のいずれかのメッセージが表示されます。

関連するNVDレコードがBDSAの脆弱性に存在しない場合：

> Black Duckセキュリティアドバイザリ（BDSA）チームは、<脆弱性ID>をこのコンポーネントバージョンにマッピングしましたが、これは、National Vulnerability Database（NVD）の関連レコードには含まれていませんでした。

関連するBDSAレコードがNVDの脆弱性に存在しない場合：

> National Vulnerability Database（NVD）は、<脆弱性ID>をこのコンポーネントバージョンにマッピングしましたが、Black Duckセキュリティアドバイザリチームは、これは影響を受けていないと判断しました。

BDSAの脆弱性の詳細については、Black Duckのヘルプドキュメントを参照してください。

JobRunnerヒープおよびCPUベースのスロットル

Black Duck 2022.2.0以降、JobRunnerコンテナはヒープとCPUの使用状況を監視し、現在のリソース使用状況に基づいてワークロードを削減できるようになります。たとえば、ヒープ使用率が90%を超えた場合、JobRunnerはメモリリソースが回復するまでそれ自体を一時停止することができます。リソースが使用可能になると、JobRunnerは使用可能なリソースに比例してワークロードを増加します。

JobRunnerが一時停止した場合は、[管理] > [診断] > [システム情報] > [JobRunner]ページに表示されます。次のようなエントリが表示されます。

> 1アクティブJobRunnerエンドポイント：
>
> docker-swarm_jobrunner_1.docker-warm_default/58993e70a84c(172.23.0.15), paused=true

"paused=true"は、このJobRunnerがリソース制約の結果としてこれ以上作業していないことを示します。リソース使用率が回復すると、エントリはpaused=falseに変わり、JobRunnerは新しい作業を開始します。

ソースレポートでの無視されたスニペット

無視されたスニペットがソースレポートに含まれるように環境を設定できるようになりました。これは、環境変数INCLUDE_IGNORED_COMPONENTS_IN_REPORT=TRUEを設定することによって実行できます。

コンポーネント検索バージョン数の機能強化

プロジェクトに追加するコンポーネントを検索するときに、特定のコンポーネントにあるバージョンの数を確認できるようになります。この数は、コンポーネント名を入力すると動的に検索結果に表示されます。

セキュリティ脆弱性修正の機能強化

プロジェクトの修正ステータスを変更しようとする際の混乱を防ぐために、セキュリティの脆弱性を修正するプロセスが明確化されました。プロジェクトのセキュリティ脆弱性を表示するときに、ハッシュ化された行が表示され、修正対象として選択できない場合があります。これは、BDSAまたはCVEのいずれかのリンクタイプのセキュリティ脆弱性レコードがプロジェクトにあることが原因です。セキュリティリスクランキングでその脆弱性レコードの優先順位が高くない場合、そのプロジェクトに対して修正計画は実行できません。優先順位の高いセキュリティ脆弱性レコードに切り替えると、そのプロジェクトの修正計画を更新できるようになります。

プロジェクトバージョンのクローン作成の機能強化

プロジェクトバージョンのクローンを作成するときに、ディープライセンスデータを含めることができるようになりました。これを行うには、ダッシュボードでプロジェクトを選択し、プロジェクトのバージョンを表示しているときに[設定]タブをクリックします。

プロジェクトタグでの検索

[検索]ページでタグによってプロジェクトを検索および選択できるようになりました。これにより、タグでグループ化されたプロジェクトに対して保存済み検索の作成が可能になり、タグで識別される共通アプリケーション内にあるプロジェクトのダッシュボードがサポートされます。

ポリシーの新しい脆弱性条件ルール

脆弱性IDの新しいポリシー条件が追加されました。新しいポリシー条件では、特定の脆弱性（CVEまたはBDSA）IDをターゲットにしてコンポーネントにフラグを付けられるようにするポリシーを作成または編集できます。

新しいソフトウェア構成表（SBOM）レポートSPDX形式

プロジェクトのソフトウェア構成表レポートをSPDX形式でエクスポートできるようになりました。これを行うには、プロジェクトバージョンを表示して[レポート]タブをクリックし、[レポートの作成]ボタンをクリックします。現在は、SPDX 2.2をサポートしており、今後のBlack Duckバージョンでは、他の形式もサポートする予定です。

強化された署名スキャンリクエストボリューム管理

強化された署名スキャンで特定の期間に発生する可能性のある大量のリクエストをより適切に管理するため、スキャンサービスは最大動作限度に達した場合、クライアントで処理されるようにHTTP 429（TOO MANY REQUESTS）エラーを返すようになりました。この場合、クライアントは10分間、30秒ごとに再試行してから、スキャンが失敗したことを通知します。

[検索]ページの新しいソートオプション

[検索]ページの[プロジェクトグループ]でプロジェクトをソートできるようになり、組織内の特定のプロジェクトグループに割り当てられているプロジェクトを簡単に検索できるようになりました。

/api/search/project-versions用の新しいprojectGroupMembershipフィルタ

このフィルタを使用すると、特定のプロジェクトグループの下位にあり、他のフィルタで指定された条件に一致するすべてのプロジェクトバージョンが返されます。projectGroupMembershipフィルタは、ユーザーがアクセス権を持つプロジェクトグループのみを返します。使用例は/api/search/projectversions?filter=projectGroupMembership:PG~{projectGroupId}です。

レポートデータベースの機能強化

レポートスキーマに新しいビューが追加されました。

- reporting.scan_view

Black Duckとアイデンティティプロバイダ（IdP）間の保護された通信

Black Duckは、SAML認証要求に署名するための5年の有効期間を持つ自己署名証明書を作成するようになりました。管理者は、[管理者] > [システム設定] > [ユーザー認証]に移動し、[外部認証]セクションで[SAML]を選択し、[署名付き認証要求を送信]チェックボックスをオンにすることで、要求に署名する必要があるかどうかを設定できます。

このオプションのデフォルト設定はオフになっているか、不要です。有効にすると、Black Duck公開証明書をダウンロードするリンクが利用可能になり、IdPが認証要求を確認できるようにユーザーにこのリンクを配布する必要があります。

既知のコンポーネントへの一致しないコンポーネントの割り当て

構成表スキャン中に検出された一致しないコンポーネントを既知のコンポーネントに割り当てることができるようになりました。

新しい高速スキャンコンポーネントの依存関係ツリー

高速スキャン出力でプロジェクト内の脆弱なコンポーネントのインスタンスすべての依存関係ツリーを表示するようになりました。これにより、そのコンポーネントが、他の参照コンポーネントやサブプロジェクトなどでどのように参照されているかを明確に確認できます。3つの親依存関係を持つjackson-core コンポーネントの高速スキャンの例は次のようになります。

"componentName": "jackson-core",

"versionName": "2.9.6",

"dependencyTrees": [

[

"io.jitpack:module2:2.0-SNAPSHOT:module2:maven",

"com.fasterxml.jackson.module:jackson-module-kotlin:2.9.6",

"com.fasterxml.jackson.core:jackson-databind:2.9.6",

"com.fasterxml.jackson.core:jackson-core:2.9.6"

]

],

プロジェクトグループの役割名の更新

プロジェクトグループに関連付けられた役割の名前が更新され、「プロジェクトグループ」という表現が削除されました。役割の機能は、この更新では変更されていません。役割がどのように更新されたかについては、以下のリストを参照してください。

- プロジェクトグループマネージャ→プロジェクトマネージャ
- プロジェクトグループセキュリティマネージャ→セキュリティマネージャ
- プロジェクトグループ構成表アノテーター→構成表アノテーター
- プロジェクトグループ構成表マネージャ→構成表マネージャ
- プロジェクトグループコードスキャナ→プロジェクトコードスキャナ

- プロジェクトグループポリシー違反レビュー担当者→ポリシー違反レビュー担当者
- プロジェクトグループビューア→プロジェクトビューア

プロジェクトおよびプロジェクトグループ管理の機能強化

複数のユーザーとプロジェクトグループをプロジェクトやプロジェクトグループに簡単に追加できるようになりました。ユーザーまたはプロジェクトグループの1回の追加操作で複数を選択できるように、ドロップダウンメニューが拡張されました。

Logstashコンテナメモリの増加

メモリ不足の問題によってクラッシュまたは再起動が発生する可能性があるため、Logstashコンテナに割り当てられるメモリを1024 MBから2560 MBに増やしました。これにより、操作に影響が及ぶWebアプリケーションの中断が減少します。

プロジェクトグループの削除の機能強化

既存のポリシールール式で参照されているプロジェクトグループは、削除できなくなりました。

文字列検索時の新しい拡張子の追加

ナレッジベースでのFLLD/FLCDスキャンとの拡張子の互換性を維持するために、以下の拡張子が、文字列検索で有効な拡張子のリストに追加されました。

- pkginfo
- properties
- pc

サポートされるブラウザのバージョン

- Safariバージョン15.0（16612.1.29.41.4、16612）
  - Safariバージョン13.0以前はサポートされなくなりました
- Chromeバージョン94.0.4606.71（公式ビルド）（x86_64）
  - Chromeバージョン71以前はサポートされなくなりました
- Firefoxバージョン92.0.1（64ビット）
  - Firefoxバージョン71以前はサポートされなくなりました
- Microsoft Edgeバージョン94.0.992.38（公式ビルド）（64ビット）
  - Microsoft Edgeバージョン78以前はサポートされなくなりました

コンテナバージョン

- blackducksoftware/blackduck-postgres:11-2.7
- blackducksoftware/blackduck-authentication:2022.2.0
- blackducksoftware/blackduck-webapp:2022.2.0
- blackducksoftware/blackduck-scan:2022.2.0
- blackducksoftware/blackduck-jobrunner:2022.2.0
- blackducksoftware/blackduck-cfssl:1.0.5
- blackducksoftware/blackduck-logstash：1.0.16

- blackducksoftware/blackduck-registration:2022.2.0
- blackducksoftware/blackduck-nginx：2.0.12
- blackducksoftware/blackduck-documentation:2022.2.0
- blackducksoftware/blackduck-upload-cache：1.0.21
- blackducksoftware/blackduck-redis:2022.2.0
- blackducksoftware/blackduck-bomengine:2022.2.0
- blackducksoftware/blackduck-matchengine:2022.2.0
- blackducksoftware/blackduck-webui:2022.2.0
- sigsynopsys/bdba-worker:2021.12.1
- blackducksoftware/rabbitmq：1.2.6

APIの機能強化

新規または変更されたAPIリクエストの詳細については、Black Duckで入手可能なAPIドキュメントを参照してください。

新しい署名付き認証要求フィールド

Black Duckが署名付き認証要求をIdPに送信するかどうかを判断するために、新しいsendSignedAuthenticationRequestフィールドが以下のAPIリクエストに追加されました。このフィールドのデフォルト値はFALSEです。証明書をダウンロードするためのメタリンクは、署名付き認証要求構成がTRUEに設定されている場合にのみ使用できます。

. `GET, POST /api/sso/configuration`

新しい/api/active-usersエンドポイント

この新しいクエリは、指定された日付以降にシステムにログインしたユーザーのすべてのユーザー最終ログイン情報を返します。このクエリでは、休眠ユーザーと同じsinceDaysクエリパラメータを使用します。

新規プロジェクトバージョンレポートのエンドポイント

タイプ（通知ファイル、バージョンレポート、脆弱性修正、脆弱性ステータス、脆弱性更新、ソフトウェア構成表レポート）に関係なくすべてのバージョンレポートをサポートするために、次のパブリックエンドポイントが追加されました。

. `GET /api/projects/{projectId}/versions/{projectVersionId}/reports`
. `GET /api/projects/{projectId}/versions/{projectVersionId}/reports/{reportId}`
. `DELETE /api/projects/{projectId}/versions/{projectVersionId}/reports/{reportId}`
. `GET /api/projects/{projectId}/versions/{projectVersionId}/reports/{reportId}/contents`
. `GET /api/projects/{projectId}/versions/{projectVersionId}/reports/{reportId}/download`

新しいポリシールールパブリックエンドポイント

アクティブなポリシールールを取得するために、新しいパブリックAPIリクエストが追加されました。

. `GET /api/projects/{projectId}/versions/{projectVersionId}/policy-rules`

新しい/api/cpes/{cpeId}/originsエンドポイント

Black Duck 2022.2.0では、/api/cpes/{cpeId}/variantsエンドポイントが廃止され、/api/cpes/{cpeId}/originsに置き換えられます。/api/cpes/{cpeId}/variantsは、Black Duck 2022.4.0で削除されます。/api/cpesのメタデータ内のAPIリンクも、/api/cpes/{cpeId}/variantsではなく、/api/cpes/{cpeId}/originsを返すように更新されています。

APIリクエストのページ制限の最大値

システムリソースの使用量を抑えるために、次のAPIリクエストにページ制限の最大値が設定されるようになりました。この制限は現在1000項目に設定されています。

. `GET /api/projects/<id>/versions/<id>/components`
. `GET /api/projects/<id>/versions/<id>/vulnerable-bom-components`
. `GET /api/codelocations`
. `GET /api/projects/<id>/versions`
. `GET /api/projects`
. `GET /api/users`

APIエンドポイント用の新しいソートフィルタ

parentProjectGroupNameという新しいソートオプションが次のAPIエンドポイントに利用できるようになりました。これにより、親プロジェクトグループ名でプロジェクトバージョンをソートできます。

. `/api/search/project-versions`
. `/api/watched-projects`
. `/api/dashboards/users/{id}/saved-searches/{id}`

新しいGET /api/scan-readiness APIエンドポイント

すべてのスキャンコンテナの準備状態を取得する新しいパブリックAPIエンドポイントが追加されました。

. `GET /api/scan-readiness`

応答例:


```
{
 "readiness": "ACCEPTING",
 "items": [
  {
   "id": "9dc7653a462b",
   "service": "scan",
   "readiness": "ACCEPTING",
   "updatedAt": "2021-12-21T17:26:01.495Z",
   "versionId": 1
  }
 ]
}
```


- マルチスキャンレプリカ環境で、すべてのスキャンコンテナレプリカが正常な場合、集約状態はACCEPTINGになります。システムは、新しいスキャンを問題なく受け入れて処理できます。
- マルチスキャンレプリカ環境で、1つのスキャンコンテナが正常ではなく、他のレプリカが正常な場合、集約状態はPARTIALになります。この状態では、システムが過負荷になります。スキャンパフォーマンスが低下する可能性があります。スキャンは、タイムアウトまたは失敗する可能性がわずかにあります。

- マルチスキャンレプリカ環境で、一部のスキャンコンテナが正常ではない場合、集約状態はDEGRADEDになります。システムは過負荷状態になり、新しいスキャンを受け入れられません。拒否するように設定すると、新しいスキャン要求は受け入れられなくなり、HTTP 429リターンコードが返されます。
- コンテナがダウンした場合、そのエントリは5分後（間隔は設定可能）に削除されます。

GET /api/codelocations/{codeLocationId}/scan-summariesの応答の更新

/api/codelocations/{codeLocationId}/scan-summariesに対して生成されたAPI応答内のscanType値は、あいまいさを避けるために各タイプに分割されるようになりました。新しい値には、次のものが含まれます。

. PACKAGE_MANAGER
. BINARY
. BOM_IMPORT
. SIGNATURE

従来のスキャンでは、scanType値にBDIOが引き続き使用されます。

この変更はBlack Duck 2021.8.0で導入されているので注意してください。

2022.2.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- （HUB-31267）。グローバルな役割を持たないユーザーが、スキャンページまたはプロジェクトURLから直接すべてのプロジェクトにアクセスできる問題が修正されました。スキャン権限のないユーザーには、projects/.../versions/.../codelocations画面に[スキャンのアップロード]ボタンが表示されなくなりました。
- （HUB-31734）。[コンポーネント]ページのフィルタがプロジェクトレベルのユーザーには機能しない問題が修正されました。
- （HUB-31993）。アップロードされたBDIOファイルのバージョン/リリース値がnullの場合にスキャンが失敗する可能性がある問題が修正されました。バージョン/リリース値がない場合でも、スキャンは失敗しなくなりました。
- （HUB-31964）。JDBCクエリのパラメータが多すぎた結果としてプロジェクトバージョンのVersionReportJobが失敗することにより一部のレポートを生成できない問題が修正されました。
- （HUB-30479、HUB-31842）。優先順位の低い脆弱性レコードを修正に使用したときに、BDSAとCVEレコードの両方を含む脆弱性の修正が機能しない問題が修正されました。脆弱性を修正するには、優先順位の高い脆弱性レコードタイプを使用する必要があります。
- （HUB-31207）。アーカイブされたプロジェクト下の脆弱性を修正しても、一旦適用されるとセキュリティ上のリスクの数は更新されない問題が修正されました。アーカイブされたプロジェクトバージョンの脆弱性をユーザーが修正することはできないため、プロジェクトバージョンがアーカイブされたら、脆弱性修正の[更新]ボタンはグレー表示にされるようになりました。
- （HUB-32029）。一部の「無視された」コンポーネントが、再スキャン後に「無視を解除」になる可能性がある問題が修正されました。
- （HUB-31768）。通知ファイルの生成時に、無視されたスニペットに基づいた著作権が誤って含まれる問題が修正されました。
- （HUB-32296、HUB-32255）。REST API GET /api/vulnerabilities/CVE-2021-44228/affected-projectsが0項目を返す問題が修正されました。また、検索結果とエンドポイントの両方の、影響を受けるプロジェクト数では、関連する脆弱性を持つコンポーネントもカウントされるようになったことにも注意してください。
- （HUB-31801、HUB-32424）。著作権の[更新]ボタンがスーパーユーザーの役割に表示される問題が修正されました。この機能は、著作権を更新する権限を持つ役割にのみ表示されるようになりました。

- （HUB-32692）。コンポーネントに複数の脆弱性があり、それぞれの脆弱性ステータスが異なる場合、コンポーネントのすべての脆弱性が選択したポリシールールに一致しない限り、ポリシールールがポリシー違反をトリガーしない問題が修正されました。
- （HUB-32357）。コンポーネント、コンポーネントのバージョン、ライセンス、NVD脆弱性、およびBDSA脆弱性に関するKBの更新を処理するナレッジベースアクティビティジョブに関する問題が修正されました。これまでは、エラーや問題が発生した場合、該当するすべてのプロジェクトバージョンで単一の更新を処理することにフォールバックしていました。この場合、多くのチャーンが発生し、KB更新ジョブの処理速度が低下する可能性があります。
- （HUB-32543）。プロジェクトマネージャとプロジェクトグループマネージャの役割を割り当てることにより、プロジェクトマネージャの役割に対する設定がオフになった場合に、これらの役割がポリシーを上書きし、脆弱性を修正する可能性がある問題が修正されました。セキュリティ上の役割は、これらの権限を持つプロジェクトマネージャまたはスーパーユーザーによってのみ割り当てることができるようになりました。
- （HUB-31129）。Hubでのプロジェクトバージョンレポート（脆弱性の詳細レポートなど）に印刷される脆弱性のURLに、BDSAレコードを含むCVEが含まれる（コンポーネントにもBDSAレコードがある場合）問題が修正されました。BDSA番号が付加されたCVEリンクは、脆弱性レポートに印刷されなくなります。
- （HUB-31044）。カスタムフィールドID値が正しくないAPIを使用してポリシーを設定すると、後でポリシー画面が正しく表示されなくなる問題が修正されました。
- （HUB-31753）。CollectScanStatsJobジョブが完了するまでに予想よりも時間がかかり、データベースの不要な肥大化を招く可能性がある問題が修正されました。
- （HUB-31663）。QuartzSearchDashboardRefreshJobが、このジョブの複数インスタンスをスケジュールしようとして、データベースへのクエリが大量にブロックされる可能性がある問題が修正されました。
- （HUB-31862）。日本語ローカライゼーションで構成表アノテーターの役割に関する翻訳が欠落していた点が修正されました。
- （HUB-31208）。構成表およびコンポーネントバージョンセキュリティタブではIBM COS SDK For Java 2.10.0コンポーネントが脆弱であると表示されていたのに、コンポーネントバージョンページでは脆弱性が表示されない問題が修正されました。
- （HUB-31735）。レポート（source.csv）と[ソース]ページ間のスニペットレコードの不一致に関する問題が修正されました。無視されたスニペットがレポートに含まれている場合は、INCLUDE_IGNORED_COMPONENTS_IN_REPORT環境変数も機能するようになりました。
- （HUB-31566）。ジョブのオーバースケジュール、メモリ不足問題、および/または長時間のジョブにより、サービスでデータベース接続エラーが発生する可能性がある問題が修正されました。
- （HUB-31997）。json-schema v0.3.0コンポーネントの脆弱性情報が修正されました。
- （HUB-32527）。通知ファイルレポートを作成するときに、次のモーダルで正しくないレポートタイプ名が表示される問題が修正されました。
- （HUB-31750）。BDSA-2021-0395ページに表示される壊れたリンクが修正されました。
- （HUB-31976）。「スーパーユーザー」の役割を持つユーザーが、プロジェクトバージョンスキャンページ内でスキャンを管理できない問題が修正されました。
- （HUB-32566）。ユーザーがファイルをApache Pulsarコンポーネントにマッピングできない問題が修正されました。
- （HUB-31201）。プロジェクト（グループ）ビューアの役割のみでユーザーをプロジェクト（グループ）に割り当てることができない問題が修正されました。
- （HUB-31251）。カスタムフィールドオプションを削除するとポリシーAPIが壊れる可能性がある問題が修正されました。
- （HUB-29676、HUB-32912）。[コンポーネントの追加/編集]ダイアログボックスで一部のコンポーネントのバージョンを選択できない問題が修正されました。

- （HUB-30847）。webappコンテナが非ルートユーザーとして実行されたときに、webapp-logstashポッドで権限拒否エラーが発生しクラッシュする問題が修正されました。
- （HUB-31375）。プロジェクト概要の「最終更新日」と、[検索] > [プロジェクト]の「更新日」の値が一致しない問題が修正されました。
- （HUB-30004）。Detectを使用した正常なバイナリスキャンによってHUB上で空の構成表が生成される可能性がある、OpenShift環境での権限の問題が修正されました。
- （HUB-32159）。カスタム署名レベルに空の値を送信すると、誤ったエラーメッセージが生成される問題が修正されました。
- （HUB-32142）。権限がないためにRabbitMQがOpenShiftにインストールできない可能性がある問題が修正されました。
- （HUB-32216）。ユーザーがコンポーネントのポリシー違反を上書きしようとし、その後特定のバージョンでそのコンポーネントバージョンのポリシー違反を元に戻そうとしても何も起こらない問題が修正されました。
- （HUB-32312）。KBUpdateWorkflowジョブコンポーネントバージョン更新でメモリを飽和させ使い切ってしまい、タイムスタンプを進められない問題が修正されました。
- （HUB-31916）。UIページが更新されるまで、プロジェクト設定更新APIが有効にならないように見える問題が修正されました。
- （HUB-30088）。SSOアカウントからログアウトするときにログアウトページが表示されない問題が修正されました。
- （HUB-32442）。依存関係パスの取得に使用されたAPIクエリの完了が、予想よりも大幅に時間がかかる問題が修正されました。
- （HUB-32538、HUB-32541）。kbUpdateJobが失敗し、詳細な更新にフォールバックして、完了までに大幅に時間がかかる可能性がある問題が修正されました。
- （HUB-32708）。実行に時間がかかり、PostgreSQL 11を実行しているAzureシステムで全体的な速度低下を引き起こす、Black Duck 2021.10.0で導入された統計クエリが削除されました。この問題は、問題を調査しているMicrosoftのサポート担当者から報告されています。その他のインストールは、この問題の影響を受けません。
- （HUB-32364、HUB-31606）。テーブルに15を超えるスキャンがあり、ユーザーがそれらを一括削除しようとした場合に、スキャンページがフリーズして応答しなくなる可能性がある問題が修正されました。
- （HUB-32602）。IPコードパスを介して行われたパッケージマネージャスキャンの現在のスキャンステータスが、ScanPurgeJobプロセスにより誤ってFAILEDに変更される可能性がある問題が修正されました。
- （HUB-31122）。ScanPurgeJobプロセスがバックグラウンドで実行されているために、BomEngineでスキャンがスキップされることがある問題が修正されました。
- （HUB-30882）。レポートの脆弱性修正のターゲットの日付/実際の日付が、タイムゾーン変換のために入力した日付より1日前になる問題は修正されました。
- （HUB-32434）。ベルアイコンをクリックしてすべての通知を表示してから、通知を生成したプロジェクト名をクリックするとエラーが発生する問題が修正されました。
- （HUB-32027）。日本語のローカライゼーションで推移的な依存関係バイナリに対する間違った翻訳が修正されました。
- （HUB-30788）。タイプに関係なくすべてのバージョンレポートをサポートする新しいエンドポイントが追加されました。詳細については、上記の「APIの機能強化」のセクションを参照してください。
- （HUB-32843）。日本語のローカライゼーションで、プロジェクトバージョンページの[コンポーネント]タブにおける「スニペット」の翻訳の欠落が修正されました。
- （HUB-31964）。JDBCのパラメータが多すぎた結果としてプロジェクトバージョンのVersionReportJobが失敗することにより一部のレポートを生成できない問題が修正されました。

- （HUB-32393）。構成表にスニペットマッチが存在する場合、結果がフィルタされても上位ビューにセキュリティ/ライセンス/運用上のリスクが設定されないことがある問題が修正されました。
- （HUB-32604）。環境変数BLACKDUCK_CORS_ALLOWED_ORIGINS_PROP_NAMEがワイルドカードに設定されている場合、CORS機能が動作しない問題が修正されました。

5. Black Duckバージョン2021.10.x

バージョン2021.10.3の発表

Apache Log4J2のセキュリティアドバイザリ(CVE-2021-45046およびCVE-2021-45105)

Apache Organizationは、Log4j2コンポーネントの新しいバージョン(2.17.0)をリリースしました。これは、バージョン2.15.0および2.16.0で修正されていない追加の脆弱性に対処するものです。

CVE-2021-45046では、コンテキストルックアップまたはスレッドコンテキストマップパターンのいずれかを使用するデフォルト以外のパターンレイアウトが、ログ構成で使用されているときに、攻撃者がスレッドコンテキストマップ(MDC)入力データを制御して、JNDIルックアップパターンを使った悪意のある入力データを作成することができ、その結果サービス拒否(DOS)攻撃が引き起こされます。

CVE-2021-45105では、攻撃者がスレッドコンテキストマップ(MDC)入力データを制御して、再帰的なルックアップを含む悪意のある入力データを作成でき、その結果、プロセスを終了させるStackOverflowErrorが発生し、サービス拒否(DOS)攻撃が引き起こされます。

詳細については、ApacheのLog4jセキュリティ脆弱性のページを参照してください。

Black Duck 2021.10.2バージョンで述べられているように、Synopsysの製品、サービス、およびシステムに対する露出は限定的であると考えられます。露出があった範囲に対しては、状況を修正済みであるか、修正の過程にあります。今後の更新については、コミュニティページを引き続きご確認ください。

バージョン2021.10.3の新機能および変更された機能

Log4jの更新

Apache Log4j 2 Javaライブラリは、重要なCVE-2021-45046およびCVE-2021-45105の脆弱性に対処するために2.17.0に更新されました。

Logstashの更新

Black Duckで使用されるLogstashイメージは、Log4j2バージョン2.17.0を使用する7.16.2にアップグレードされました。

コンテナバージョン

- blackducksoftware/blackduck-postgres:9.6-1.4
- blackducksoftware/blackduck-authentication:2021.10.3
- blackducksoftware/blackduck-webapp:2021.10.3
- blackducksoftware/blackduck-scan:2021.10.3
- blackducksoftware/blackduck-jobrunner:2021.10.3
- blackducksoftware/blackduck-cfssl:1.0.4
- blackducksoftware/blackduck-logstash:1.0.15
- blackducksoftware/blackduck-registration:2021.10.3
- blackducksoftware/blackduck-nginx:2.0.9

- blackducksoftware/blackduck-documentation:2021.10.3
- blackducksoftware/blackduck-upload-cache：1.0.19
- blackducksoftware/blackduck-redis:2021.10.3
- blackducksoftware/blackduck-bomengine:2021.10.3
- blackducksoftware/blackduck-matchengine:2021.10.3
- blackducksoftware/blackduck-webui:2021.10.3
- sigsynopsys/bdba-worker:2021.9.2
- blackducksoftware/rabbitmq：1.2.5

2021.10.3で修正された問題

このリリースでは、次の問題が修正されています。

- （HUB-32233）。CVE-2021-45046およびCVE-2021-45105に対応して、Log4jをバージョン2.17.0にアップグレードしました。
- （HUB-32295）。Bitnami LogstashをLog4j 2.17.0を使用する7.16.2バージョンに更新しました。

バージョン2021.10.2の発表

Apache Log4J2のセキュリティアドバイザリ（CVE-2021-44228）

Synopsysは、プロジェクトのGitHubを介して2021年12月9日に公開された、Log4Shell（またはLogJam）と呼ばれるオープンソースのApache Log4j 2 Javaライブラリに関連するセキュリティの問題を認識しています。この脆弱性により、認証されていないリモートコードの実行が可能になり、Apache Log4j 2バージョン2.0～2.14.1に影響が及んでいます。詳細については、CVEの公式投稿を参照してください。

現時点でわかっている知見に基づいて、Synopsysの製品、サービス、システムに対する露出は限定的であると考えています。露出があった範囲に対しては、状況を修正済みであるか、修正の過程にあります。今後の更新については、コミュニティページを引き続きご確認ください。

https://www.synopsys.com/blogs/software-security/zero-day-exploit-log4j-analysis/も参照してください。

バージョン2021.10.2の新機能および変更された機能

Log4jの更新

Apache Log4j 2 Javaライブラリは、重要なCVE-2021-44228の脆弱性に対処するために2.15.0に更新されました。

コンテナバージョン

- blackducksoftware/blackduck-postgres:9.6-1.4
- blackducksoftware/blackduck-authentication:2021.10.2
- blackducksoftware/blackduck-webapp:2021.10.2
- blackducksoftware/blackduck-scan:2021.10.2
- blackducksoftware/blackduck-jobrunner:2021.10.2
- blackducksoftware/blackduck-cfssl:1.0.4

- blackducksoftware/blackduck-logstash：1.0.13
- blackducksoftware/blackduck-registration:2021.10.2
- blackducksoftware/blackduck-nginx：2.0.9
- blackducksoftware/blackduck-documentation:2021.10.2
- blackducksoftware/blackduck-upload-cache：1.0.19
- blackducksoftware/blackduck-redis:2021.10.2
- blackducksoftware/blackduck-bomengine:2021.10.2
- blackducksoftware/blackduck-matchengine:2021.10.2
- blackducksoftware/blackduck-webui:2021.10.2
- sigsynopsys/bdba-worker:2021.9.2
- blackducksoftware/rabbitmq：1.2.5

2021.10.2で修正された問題

このリリースでは、次の問題が修正されました。

- （HUB-32174）。CVE-2021-44228に対応して、Log4jをバージョン2.15.0にアップグレードしました。

バージョン2021.10.1の新機能および変更された機能

RestResponseErrorHandlerの改善

RestResponseErrorHandleは、Black Duck機能の信頼性を向上させるために、ナレッジベースおよびネットワーク内の他のサーバーからの予期しない応答をより適切に処理できるようになりました。

コンテナバージョン

- blackducksoftware/blackduck-postgres:9.6-1.4
- blackducksoftware/blackduck-authentication:2021.10.1
- blackducksoftware/blackduck-webapp:2021.10.1
- blackducksoftware/blackduck-scan:2021.10.1
- blackducksoftware/blackduck-jobrunner:2021.10.1
- blackducksoftware/blackduck-cfssl:1.0.4
- blackducksoftware/blackduck-logstash：1.0.11
- blackducksoftware/blackduck-registration:2021.10.1
- blackducksoftware/blackduck-nginx：2.0.9
- blackducksoftware/blackduck-documentation:2021.10.1
- blackducksoftware/blackduck-upload-cache：1.0.19
- blackducksoftware/blackduck-redis:2021.10.1
- blackducksoftware/blackduck-bomengine:2021.10.1
- blackducksoftware/blackduck-matchengine:2021.10.1

- blackducksoftware/blackduck-webui:2021.10.1
- sigsynopsys/bdba-worker:2021.9.1
- blackducksoftware/rabbitmq：1.2.5

2021.10.1で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- （HUB-31129）。Hubでのプロジェクトバージョンレポート（脆弱性の詳細レポートなど）に印刷される脆弱性のURLに、BDSAレコードを含むCVEが含まれる（コンポーネントにもBDSAレコードがある場合）問題が修正されました。BDSA番号が付加されたCVEリンクは、脆弱性レポートに印刷されなくなります。
- （HUB-31293）。2021.8.xにアップグレードした後、Pythonの推移的な依存関係が直接的な依存関係に変更される問題が修正されました。
- （HUB-31764）。脆弱性の修正ステータスが更新されるときに、構成表の計算中にNullポインタ例外を引き起こす問題が修正されました。
- （HUB-30004）。Detectを使用した正常なバイナリスキャンによってHUB上で空の構成表が生成される可能性がある、OpenShift環境での権限の問題が修正されました。
- （HUB-31879）。構成表の作成フェーズ中にスキャンがスタックする可能性がある問題が修正されました。詳細については、上記の「新機能および変更された機能」セクションの「RestResponseErrorHandlerの改善」を参照してください。
- （HUB-31896）。パブリックAPIを介した構成表の脆弱性に対する修正の更新が、再スキャン後に持続しない問題が修正されました。
- （HUB-31753）。CollectScanStatsJobジョブが完了するまでに予想よりも時間がかかり、データベースの不要な肥大化を招く可能性がある問題が修正されました。
- （HUB-31663）。QuartzSearchDashboardRefreshJobが、このジョブの複数インスタンスをスケジュールしようとして、データベースへのクエリが大量にブロックされる可能性がある問題が修正されました。
- （HUB-31755）。プロジェクトバージョンレポートの生成時に、プロジェクト構造が循環しているためにVersionReportJobでメモリ不足になる可能性がある問題が修正されました。
- （HUB-31566）。ジョブのオーバースケジュール、メモリ不足問題、および/または長時間のジョブにより、サービスでデータベース接続エラーが発生する可能性がある問題が修正されました。

バージョン2021.10.0の発表

強化された署名スキャン

2021.8.0リリースのPackage Manager Scanningで導入されたパフォーマンス強化機能は、2021.10.0リリースの署名スキャンで利用可能になっています。これらの強化の主要部分は、重複する構成表の検出です。この機能を使用した場合、特定のプロジェクトおよびバージョンに関連付けられている構成表が署名スキャンによって変更されない限り、構成表の計算はバイパスされます。

さらに、強化された署名スキャンでは、新たなパッケージマネージャスキャンまたは署名スキャンの処理で、JobRunnerは役割を果たさなくなりました。強化された署名スキャンの実行では、システムリソースがさらに必要になることはありませんが、コンテナの微妙なバランス調整が必要になる可能性があります。バランス調整が必要かどうかについては、Synopsysのサポートにお問い合わせください。当社は強化された機能の活用をすべてのお客様に推奨しています。

Black Duck 2021.8.0ではDetect 7.4を明確化

完全な機能性および互換性を維持する場合、Black Duckバージョン2021.8.0には、Detect 7.4が必要になります。Black Duckで旧バージョンのDetectは引き続き使用できますが、集約BDIOファイルの使用時に、依存関係タイプやソースビューの不整合が構成表内で生じる可能性があります。

Detect 7.4へのアップグレードで、構成表内の不整合を回避できます。

PostgreSQLコンテナの9.6から11への移行

Black Duckは、2022.2.0リリースでPostgreSQLイメージをバージョン9.6からバージョン11に移行します。SynopsysのPostgreSQLイメージを使用していないお客様には影響はありません。

Black Duck PostgreSQL 9.6の廃止

Black Duckは、Black Duck 2020.6.0リリースで表明したとおり、2021.6.0リリースで実装された外部PostgreSQL 9.6のサポートを終了することになりました。2022.2.0リリース以降の場合、Black DuckはPostgreSQL 9.6と連動しなくなります。さらにPostgreSQL 9.6インスタンスを参照している場合は、Black Duckが起動しなくなります。

PostgreSQLサポートのスケジュール

将来の2022.10.0リリース以降、Black Duckは外部PostgreSQL 11のサポートを終了します。今後のPostgreSQLバージョンに関しては、サポートの開始日と終了日を以下の表で確認してください。

PGバージョン	最初のリリース	最終リリース	BD外部サポートの追加	BD外部サポートの終了
16.x	2023年後半	2028年後半	2024.10.0	2026.10.0
15.x	2022年後半	2027年後半	2023.10.0	2025.10.0
14.x	2021年9月	2026年11月	2022.10.0	2024.10.0
13.x	2020年9月	2025年11月	2021.8.0	2023.10.0
12.x	2019年10月	2024年11月	X	X
11.x	2018年10月	2023年11月	2020.6.0	2022.10.0

2021.10.0以降にデータベースbds_hub_reportは廃止

2021.10.0以降、Black Duckの新インストールでは、bds_hub_reportデータベースが作成されなくなります。最終的に2022.10.0でbds_hub_reportを削除する予定です。

またbds_hub_reportが存在しない場合でも、hub_create_data_dump.shおよびhub_db_migrate.shスクリプト（当社のオーケストレーションファイルとともに配布）は正常に動作するようになります。

- bds_hub_reportが存在する場合、それをhub_create_data_dump.shスクリプトはダンプしますが、存在しない場合でも、スクリプトがエラーになることはありません。bds_hub_reportが存在しない場合、スクリプトはスキップを通知するメッセージを出力します。
- hub_db_migrate.shスクリプトは、bds_hub_reportが存在する場合（ダンプファイルが存在するかどうかに関係なく）、そのリストアを試行します（先行リリースの動作とマッチ）。bds_hub_reportが存在しない場合、ダンプファイルが存在するかどうかに関係なく、リストアは試行されません。

- 新しいスクリプトhub_recreate_reportdb.shが追加されました。2021.8.x以前のbds_hub_report DBから2021.10.0以降の新インストールにデータをコピーする場合、この新しいスクリプトによってbds_hub_reportが再作成されます。この場合、次のようになります。
  - 以前のBDインスタンスでhub_create_data_dump.shを実行します。
  - 新しいBDインスタンスでhub_recreate_reportdb.shを実行します。
  - 新しいBDインスタンスでhub_db_migrate.shを実行し、ダンプはステップ#1で作成します。

APIリクエストに最大ページ数の制限を適用する予定

Black Duck 2022.2.0以降、APIリクエストには最大ページ数の制限が適用されます。単一のリクエストを作成する場合には、文書化されたページ制限以下の値で制限リクエストパラメータを指定する必要があります。文書化された制限を超えたページリクエストは切り捨てられ、許容される最大ページ数のみが返されます。ページサイズのリクエストは拒否されませんが、ページリクエストあたりの最大結果数が返されます。

アプリケーションの安定性を高め、不当に大きなリクエストによるパフォーマンスの低下を防ぐために、以降のリリースではこの制限が継続的に適用されます。

廃止されたAPI

以下の廃止されたエンドポイントは「404 NOT FOUND」エラーを返し、ターゲットリソースへのアクセスが利用できなくなったことを示します。

- GET /oauthclients
- POST /oauthclients
- DELETE /oauthclients/{oAuthClientId}
- GET /oauthclients/{oAuthClientId}
- PUT /oauthclients/{oAuthClientId}
- POST /vulnerabilities/vulndb-copy

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2021.8.0が日本語にローカライズされました。

簡体字中国語

UI、オンラインヘルプ、およびリリースノートのバージョン2021.8.0が簡体字中国語にローカライズされました。

バージョン2021.10.0の新機能および変更された機能

強化された署名生成のためにエラーメッセージを更新

署名スキャンのサーバー側エラーメッセージが更新されました。エラーメッセージの完全なリストは、今後のリリースのユーザーガイドに記載されます。

マップされていないスキャンデータの保持構成設定

マップされていないスキャンのデフォルト保持期間を管理者が変更できるように、新しい構成設定が利用可能になりました。Black Duck 2021.10.0以降、この設定はデフォルトで有効になり、期間は30日（以前は365日）に設定されます。この保持設定は更新でき、最も短い場合は1日、最も長い場合は365日に設定できます。

UIでこの設定を変更するには、 

をクリックし、[設定]、[データの保管]の順にクリックします。

推定セキュリティリスク

この推定リスク統計は、セキュリティ脆弱性の重大度カテゴリ別にソートされたコンポーネントの全バージョンを参照し、コンポーネントバージョンごとに各重大度カテゴリの最大脆弱性数を計算することで算出されます。各重大度カテゴリの最大脆弱性数は、セキュリティリスクの構成表の[重大度カテゴリ別の推定セキュリティリスク]に表示されます。重大度が最高値になっているカテゴリ数は、複数の異なるコンポーネントバージョンを参照している可能性があります。以下に例を示します。

- バージョン1.1では、重大2、高3、中15、低4になっています
- バージョン1.2では、重大2、高4、中12、低1になっています
- この例で、コンポーネントのバージョンが不明の場合、重大度カテゴリ別の推定セキュリティリスクは、構成表で重大2、高4、中15、低4になります。

推定リスクではなく、正確なリスクを表示するには、アプリケーションで使用されている正確なバージョンを選択する必要があります。この推定リスク情報は、どのコンポーネントを最初にレビューすべきかの優先順位付けに役立ちます。企業のセキュリティポリシーに基づいて優先順位をさらに明確にし、コンポーネントの最初の選別が実行できるように、推定リスク情報とともにBDポリシー管理を使用することをお勧めします。

注： 表示される情報は統計データの推定のみです。結果的に、推定セキュリティリスクにはCVEデータは含まれません。

ディープライセンスデータが有効の場合に通知レポートを生成する

通知ファイルは、宣言されたライセンスを追加ライセンスの前に配置するようになりました。宣言されたライセンスと追加ライセンスは、アルファベット順にソートされます。

[ソース]ビューと[ソース]レポートにコメントを追加する

プロジェクトの[ソース]ビューでは、エントリにコメントを追加できるようになりました。ファイルコメントは、スニペットビューにも表示されます。ソースレポートでは、これらのコメントは「コメント」というラベルの付いた新しい列にも表示されます。ソースレポートを作成するには、[レポート]タブで[バージョン詳細レポート]の[ソース]チェックボックスをオンにします。

[ソース]タブの特定エントリに関するコメントは、次の方法で入力できます。

- そのコンポーネントの行の末尾にあるアイコンをクリックし、ドロップダウンメニューから[コメント]を選択します。また、すでにコメントがある場合はアイコンをクリックします。
- [ソース]ビューでエントリをクリックし、コンポーネントの名前をクリックします。次にアイコンをクリックし、ドロップダウンメニューから[コメント]を選択します。また、すでにコメントがある場合はアイコンをクリックします。

ポリシー管理の機能強化 – プロジェクトグループ

Black Duckユーザーは、プロジェクトグループとその下位アイテムにポリシールールを適用できるようになりました。

適用するには、[ポリシー管理]に移動し、[ポリシールールの作成]ボタンまたはボタンをクリックして[編集]を選択します。[ポリシールールの作成/編集]モーダルが開いたら、[プロジェクトのサブセット。フィルタの内容...]オプションが有効になっており、[プロジェクトの条件]フィルタドロップダウンが表示されることを確認します。

ポリシー管理の機能強化 – 脆弱性条件に(RCE)リモートコード実行を追加

Black Duckユーザーは、ポリシーの作成または編集時に、フィルタオプションとしてリモートコード実行(RCE)を追加できるようになりました。適用するには、[ポリシー管理]に移動し、[ポリシールールの作成]ボタンまたは ボタンをクリックして[編集]を選択します。[脆弱性の条件]ドロップダウンメニューには、新しい(RCE)リモートコード実行の値が表示されます。

プロジェクトグループマネージャの権限の変更

以前は、脆弱性の修正やポリシーの上書きをプロジェクトマネージャに許可するグローバル設定によって、プロジェクトグループマネージャの実際の権限が影響を受けることはありませんでした。現在では、プロジェクトグループマネージャの役割の権限は、プロジェクトマネージャの役割設定に基づいて調整されるようになりました。

署名スキャナのドライラン更新

以前は、署名スキャナのドライランを実行すると、出力でJSONファイルが生成されていました。Black Duck 2021.10.0以降、生成される出力ファイルには.bdio拡張子が付けられ、zip形式で圧縮されています。出力ファイルは、従来の署名スキャンと同様に、今後もドライランと同じディレクトリに生成されます。

サポートされるブラウザのバージョン

- Safariバージョン15.0(16612.1.29.41.4、16612)
  - Safariバージョン13.0以前はサポートされなくなりました
- Chromeバージョン94.0.4606.71(公式ビルド)(x86_64)
- Firefoxバージョン92.0.1(64ビット)
- Microsoft Edgeバージョン94.0.992.38(公式ビルド)(64ビット)
  - Microsoft Edgeバージョン79以前はサポートされなくなりました

コンテナバージョン

- blackducksoftware/blackduck-postgres:9.6-1.3
- blackducksoftware/blackduck-authentication:2021.10.0
- blackducksoftware/blackduck-webapp:2021.10.0
- blackducksoftware/blackduck-scan:2021.10.0
- blackducksoftware/blackduck-jobrunner:2021.10.0
- blackducksoftware/blackduck-cfssl:1.0.4
- blackducksoftware/blackduck-logstash:1.0.11
- blackducksoftware/blackduck-registration:2021.10.0
- blackducksoftware/blackduck-nginx:2.0.9
- blackducksoftware/blackduck-documentation:2021.10.0
- blackducksoftware/blackduck-upload-cache:1.0.19
- blackducksoftware/blackduck-redis:2021.10.0
- blackducksoftware/blackduck-bomengine:2021.10.0
- blackducksoftware/blackduck-matchengine:2021.10.0
- blackducksoftware/blackduck-webui:2021.10.0

- sigsynopsys/bdba-worker:2021.9.1
- blackducksoftware/rabbitmq：1.2.5

APIの機能強化

GET /api/project-groupsの権限の修正

GET /api/project-groups apiエンドポイントには、次の修正が加えられています。

- GET api/project-groups ユーザーが検索結果として表示することを許可されているプロジェクトグループのみが返されます。
- GET api/project-groups/<project group ID> スーパーユーザーの役割を持つユーザーには「HTTP 200 OK」が返され、それ以外のユーザーには「HTTP 403 Forbidden」メッセージが返されます。

GET /api/users/{userId}の権限の変更

GET /api/users/{userId}エンドポイントでは、権限チェックが実行されなくなりました（以前はUSERMGMT_READ チェックが必要でした）。

- GET /api/users/エンドポイント（全ユーザーをリスト）は、今後もUSERMGMT_READ権限で保護されます。
- /api/projects/{projectId} APIのprojectOwnerユーザー（ユーザーの権限ステータスに関係なく）は今後も提供されます。
- Black Duckバージョン2021.8.2でプロジェクトの役割に追加されたUSERMGMT_READ権限は削除されます。

GET /api/project-groupsの新しいフィルタパラメータ

特定のプロジェクトグループを検索するために、exactNameという新しいフィルタパラメータが追加されました。[真]の場合、exactName フィルタはqの名前値とマッチするプロジェクトグループのみを返します。プロジェクトグループの検索条件では、大文字と小文字は区別されません。マッチするグループがない場合は、何も返されません。また、exactName フィルタが[真]の場合は、qパラメータを指定する必要があります。指定しない場合は、プロジェクトグループは返されません。

/api/project-groupsリクエストでフィルタを使用する方法については、以下を参照してください。

```
/api/project-groups?q=name:<project group name>&filter=exactName:true
```

CPEサポートAPIの改善

次の3つの新しいパブリックAPIが追加されました。

- GET /api/cpes [searchParamは必須です。マッチするCPE IDが返されます]
- GET /api/cpes/{cpeId}/versions [CPE IDにマッチするコンポーネントバージョンが返されます]
- GET /api/cpes/{cpeId}/variants [CPE IDにマッチするコンポーネント取得元が返されます]

Copyright 2.0データおよび新しいレガシーエンドポイント

Black Duckは現在、新しい著作権データを提供するために、既存のエンドポイント（以下）を使用してCopyright 2.0データを展開しようとしています。削除または追加される応答フィールドはありません。

```
GET /api/components/{componentId}/versions/{componentVersionId}/origin/{originId}/file-copyrights
```

新しいエンドポイントを作成して、Copyright 1.0（akaレガシー）データを引き続き提供します。

```
GET /api/components/{componentId}/versions/{componentVersionId}/origin/{originId}/file-copyrights-legacy
```

注:この新しいエンドポイントは、Black Duck UIでは直接使用されず、パブリックAPIを介してのみ使用されます。また現在、既存のエンドポイントではCopyright 2.0データが返されるため、Black Duckのすべてのお客様(使用しているバージョンに関係なく)にこの新しいデータが表示されます。

パブリックAPIを使用したlastScanDateの公開

現在、以下のAPIはパブリックAPI応答でlastScanDateを公開しています。

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

2021.10.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (HUB-29413)。[コンポーネントの追加]または[コンポーネントの編集]モーダルでは、コンポーネントの検索がより正確になっており、カスタムコンポーネントを簡単に検索できるようになりました
- (HUB-26545およびHUB-30185)。次のPublic REST APIエンドポイントは、componentModification、componentModified、componentPurposeコンポーネントの条件を想定どおりに更新しませんでしたが、その問題は修正されました。
  . `/api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}`
  . `/api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}`
- (HUB-30474)。ユーザーが特定プロジェクトにアクセスできない場合、[影響を受けるプロジェクト]ページに表示されるカウントが実際の結果とマッチしませんでしたが、その問題は修正されました。
- (HUB-30623)。クライアントが原因で多数のエラーが発生した場合、スタックトレースのログ記録によって大きなログファイルが生成されたり、実際よりも深刻なログレベルで誤ってエラーが記録されたりしていましたが、その問題は修正されました。
- (HUB-30099)。既存の構成表で、脆弱性ステータスが更新されませんでしたが、KBの更新によってその問題は修正されました。構成表コンポーネント - 現在のステータスがユーザー更新またはシステム更新ではない場合に、修正ステータスが変化すると、バージョン脆弱性修正(構成表 - セキュリティビューにある)は、KB更新ジョブによって更新されるようになりました。
- (HUB-29773)。/api/projects/<project ID>/versions/<version ID>/vulnerable-bom-componentsエンドポイントの応答時間が想定よりも長くなっていましたが、その問題は修正されました。このリクエストには、バージョン構成表コンポーネントごとに1つのライセンス定義のみが含まれるようになりました。この変更により、応答時間が短縮されました。ライセンスの上書きでProtex構成表をインポートした場合は、表示される結果の件数が少なくなっています。
- (HUB-26924)。SAML SSOユーザーがログインに失敗したときに、ユーザーフレンドリーなエラーメッセージが表示されるように修正されました。SSO構成が間違っている場合は、構成の問題を通知するためにエラーページが表示されます。HUBでユーザーが無効になっている場合は、エラーページが表示され、ユーザーはシステム管理者に連絡するか、未許可のページにアクセスするように指示されます。
- (HUB-31176)。修正ステータスが特定のプロジェクトバージョンに関連付けられている場合、高速スキャンポリシー評価で構成表ステータスがチェックされませんでしたが、その問題は修正されました。
- (HUB-30808)。プロジェクトの構成表でコンポーネントの「追加フィールド」をレビューする場合、カスタムフィールド管理の[構成表コンポーネント]タブで作成されたカスタムフィールドが返されませんでしたが、その問題は修正されました。構成表コンポーネントのカスタムフィールドを編集する場合、最大100個のカスタムフィールドが表示されます。
- (HUB-30922)。プロジェクトバージョンレベルの説明が表示されないという問題は修正されました。現在、このフィールドには、プロジェクトレベルで使用する説明が表示されるようになりました。

- （HUB-31482）。HUB 2021.6.2以降、[スニペット確認]ページにライセンスが表示されませんでしたが、その問題は修正されました。
- （HUB-31003）。脆弱性を一括で修復しようとすると、「HTTP 500 Internal Server Error」が発生していましたが、その問題は修正されました。
- （HUB-31425）。バージョン詳細レポートで、以前のバージョンのHUBと比較しようとしてクエリを実行すると、完了までにかなりの時間がかかっていましたが、その問題は修正されました。
- （HUB-29598）。コンポーネントページの[印刷]ボタンで生成したPDFでは、脆弱性の件数が多く、バーが長くなり過ぎてプッシュアウトされていましたが、その問題は修正されました。
- （HUB-30133）。Helm導入環境のt-shirt sizing ymlsにはwebuiコンテナがあり、XL導入用のメモリは小さくなっていましたが、その問題は修正されました。webuiコンテナのメモリ制限は、x-large.yaml tshirtサイズで1024 Miに引き上げられました。
- （HUB-28889）。RabbitMQにアクセスできない場合、構成表エンジンは起動できませんんでしたが、その問題は修正されました。
- （HUB-30215）。BDSA-2020-1311で間違ったレポートが生成され、その回避策もありませんでしたが、その問題は修正されました。
- （HUB-30857）。[影響を受けるプロジェクト]ページの脆弱性については、表示される項目で、無視されるコンポーネントからの脆弱性の件数は除外されていましたが、項目の総合計の数を確認すると、実際にはその数値が含まれていました。このバグは修正されました。現在では、項目の総数からも、無視されるコンポーネントの脆弱性件数は除外されています。
- （HUB-30603）。プロジェクトの[セキュリティ]タブで、BDSAまたはCVEレコードの下にあるコメントはグレー表示になっていましたが、ユーザーはコメントの内容をすべて確認できました。その問題は修正されました。
- （HUB-28753）。Dockerで作成された場合、BomEngineはHUB_PROXY_PASSWORD_FILEシークレット値を受け入れず、407 AUTHENTICATION REQUIREDエラーを返していました。その問題は修正されました。
- （HUB-31483）。日本語ローカライゼーションの場合、[ポリシー違反]モーダルでは、ポリシー上書き日とユーザー情報が誤って表示されていましたが、その問題は修正されました。

6. Black Duckバージョン2021.8.x

バージョン2021.8.8の新機能および変更された機能

Black Duck バージョン2021.8.8はメンテナンスリリースであり、新機能や変更された機能はありません。認証されていないリモート攻撃者がクロスサイトスクリプティング攻撃を実行できるようになるCVE-2022-30278に対処するために、オンラインヘルプを修正しました。

コンテナバージョン

- blackducksoftware/blackduck-postgres:9.6-1.1
- blackducksoftware/blackduck-authentication:2021.8.8
- blackducksoftware/blackduck-webapp:2021.8.8
- blackducksoftware/blackduck-scan:2021.8.8
- blackducksoftware/blackduck-jobrunner:2021.8.8
- blackducksoftware/blackduck-cfssl:1.0.3
- blackducksoftware/blackduck-logstash：1.0.15
- blackducksoftware/blackduck-registration:2021.8.8
- blackducksoftware/blackduck-nginx：2.0.6
- blackducksoftware/blackduck-documentation:2021.8.8
- blackducksoftware/blackduck-upload-cache：1.0.18
- blackducksoftware/blackduck-redis:2021.8.8
- blackducksoftware/blackduck-bomengine:2021.8.8
- blackducksoftware/blackduck-matchengine:2021.8.8
- blackducksoftware/blackduck-webui:2021.8.8
- sigsynopsys/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq：1.2.3

2021.8.8で修正された問題

お客様から報告された次の問題が修正されました。

- （HUB-32811）。JDBCのパラメータが多すぎた結果としてプロジェクトバージョンのVersionReportJobが失敗することにより一部のレポートを生成できない問題が修正されました。

バージョン2021.8.7の発表

Apache Log4J2のセキュリティアドバイザリ（CVE-2021-45046およびCVE-2021-45105）

Apache Organizationは、Log4j2コンポーネントの新しいバージョン（2.17.0）をリリースしました。これは、バージョン2.15.0および2.16.0で修正されていない追加の脆弱性に対処するものです。

CVE-2021-45046では、コンテキストルックアップまたはスレッドコンテキストマップパターンのいずれかを使用するデフォルト以外のパターンレイアウトが、ログ構成で使用されているときに、攻撃者がスレッドコンテキストマップ(MDC)入力データを制御して、JNDIルックアップパターンを使った悪意のある入力データを作成することができ、その結果サービス拒否(DOS)攻撃が引き起こされます。

CVE-2021-45105では、攻撃者がスレッドコンテキストマップ(MDC)入力データを制御して、再帰的なルックアップを含む悪意のある入力データを作成でき、その結果、プロセスを終了させるStackOverflowErrorが発生し、サービス拒否(DOS)攻撃が引き起こされます。

詳細については、ApacheのLog4jセキュリティ脆弱性のページを参照してください。

Black Duck 2021.8.6バージョンで述べられているように、Synopsysの製品、サービス、およびシステムに対する露出は限定的であると考えられます。露出があった範囲に対しては、状況を修正済みであるか、修正の過程にあります。今後の更新については、コミュニティページを引き続きご確認ください。

バージョン2021.8.7の新機能および変更された機能

Log4jの更新

Apache Log4j 2 Javaライブラリは、重要なCVE-2021-45046およびCVE-2021-45105の脆弱性に対処するために2.17.0に更新されました。

Logstashの更新

Black Duckで使用されるLogstashイメージは、Log4j2バージョン2.17.0を使用する7.16.2にアップグレードされました。

コンテナバージョン

- blackducksoftware/blackduck-postgres:9.6-1.1
- blackducksoftware/blackduck-authentication:2021.8.7
- blackducksoftware/blackduck-webapp:2021.8.7
- blackducksoftware/blackduck-scan:2021.8.7
- blackducksoftware/blackduck-jobrunner:2021.8.7
- blackducksoftware/blackduck-cfssl:1.0.3
- blackducksoftware/blackduck-logstash:1.0.15
- blackducksoftware/blackduck-registration:2021.8.7
- blackducksoftware/blackduck-nginx:2.0.6
- blackducksoftware/blackduck-documentation:2021.8.7
- blackducksoftware/blackduck-upload-cache:1.0.18
- blackducksoftware/blackduck-redis:2021.8.7
- blackducksoftware/blackduck-bomengine:2021.8.7
- blackducksoftware/blackduck-matchengine:2021.8.7
- blackducksoftware/blackduck-webui:2021.8.7
- sigsynopsys/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

2021.8.7で修正された問題

次の問題が修正されました。

- （HUB-32233）。CVE-2021-45046およびCVE-2021-45105に対応して、Log4jをバージョン2.17.0にアップグレードしました。
- （HUB-32295）。Bitnami LogstashをLog4j 2.17.0を使用する7.16.2バージョンに更新しました。

バージョン2021.8.6の発表

Apache Log4J2のセキュリティアドバイザリ（CVE-2021-44228）

Synopsysは、プロジェクトのGitHubを介して2021年12月9日に公開された、Log4Shell（またはLogJam）と呼ばれるオープンソースのApache Log4j 2 Javaライブラリに関連するセキュリティの問題を認識しています。この脆弱性により、認証されていないリモートコードの実行が可能になり、Apache Log4j 2バージョン2.0～2.14.1に影響が及んでいます。詳細については、CVEの公式投稿を参照してください。

現時点でわかっている知見に基づいて、Synopsysの製品、サービス、システムに対する露出は限定的であると考えています。露出があった範囲に対しては、状況を修正済みであるか、修正の過程にあります。今後の更新については、コミュニティページを引き続きご確認ください。

https://www.synopsys.com/blogs/software-security/zero-day-exploit-log4j-analysis/も参照してください。

バージョン2021.8.6の新機能および変更された機能

Log4jの更新

Apache Log4j 2 Javaライブラリは、重要なCVE-2021-44228の脆弱性に対処するために2.15.0に更新されました。

コンテナバージョン

- blackducksoftware/blackduck-postgres:9.6-1.1
- blackducksoftware/blackduck-authentication:2021.8.6
- blackducksoftware/blackduck-webapp:2021.8.6
- blackducksoftware/blackduck-scan:2021.8.6
- blackducksoftware/blackduck-jobrunner:2021.8.6
- blackducksoftware/blackduck-cfssl:1.0.3
- blackducksoftware/blackduck-logstash：1.0.13
- blackducksoftware/blackduck-registration:2021.8.6
- blackducksoftware/blackduck-nginx：2.0.6
- blackducksoftware/blackduck-documentation:2021.8.6
- blackducksoftware/blackduck-upload-cache：1.0.18
- blackducksoftware/blackduck-redis:2021.8.6
- blackducksoftware/blackduck-bomengine:2021.8.6
- blackducksoftware/blackduck-matchengine:2021.8.6

- blackducksoftware/blackduck-webui:2021.8.6
- sigsynopsys/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq：1.2.3

2021.8.6で修正された問題

次の問題が修正されました。

- （HUB-32174）。CVE-2021-44228に対応して、Log4jをバージョン2.15.0にアップグレードしました。

バージョン2021.8.5の新機能および変更された機能

Black Duck バージョン2021.8.5はメンテナンスリリースであり、新機能や変更された機能はありません。

コンテナバージョン

- blackducksoftware/blackduck-postgres:9.6-1.1
- blackducksoftware/blackduck-authentication:2021.8.5
- blackducksoftware/blackduck-webapp:2021.8.5
- blackducksoftware/blackduck-scan:2021.8.5
- blackducksoftware/blackduck-jobrunner:2021.8.5
- blackducksoftware/blackduck-cfssl:1.0.3
- blackducksoftware/blackduck-logstash：1.0.10
- blackducksoftware/blackduck-registration:2021.8.5
- blackducksoftware/blackduck-nginx：2.0.6
- blackducksoftware/blackduck-documentation:2021.8.5
- blackducksoftware/blackduck-upload-cache：1.0.18
- blackducksoftware/blackduck-redis:2021.8.5
- blackducksoftware/blackduck-bomengine:2021.8.5
- blackducksoftware/blackduck-matchengine:2021.8.5
- blackducksoftware/blackduck-webui:2021.8.5
- sigsynopsys/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq：1.2.3

2021.8.5で修正された問題

- （HUB-31482）。Black Duckバージョン2021.6.2以降、[スニペット確認]ページにライセンスが表示されませんでしたが、その問題は修正されました。
- （HUB-31663）。QuartzSearchDashboardRefreshJobが、ジョブの複数インスタンスをスケジュールしようとして、ブロックされたクエリが大量に発生していましたが、その問題は修正されました。

バージョン2021.8.4の新機能および変更された機能

Black Duck バージョン2021.8.4はメンテナンスリリースであり、新機能や変更された機能はありません。

コンテナバージョン

- blackducksoftware/blackduck-postgres:9.6-1.1
- blackducksoftware/blackduck-authentication:2021.8.4
- blackducksoftware/blackduck-webapp:2021.8.4
- blackducksoftware/blackduck-scan:2021.8.4
- blackducksoftware/blackduck-jobrunner:2021.8.4
- blackducksoftware/blackduck-cfssl:1.0.3
- blackducksoftware/blackduck-logstash：1.0.10
- blackducksoftware/blackduck-registration:2021.8.4
- blackducksoftware/blackduck-nginx：2.0.6
- blackducksoftware/blackduck-documentation:2021.8.4
- blackducksoftware/blackduck-upload-cache：1.0.18
- blackducksoftware/blackduck-redis:2021.8.4
- blackducksoftware/blackduck-bomengine:2021.8.4
- blackducksoftware/blackduck-matchengine:2021.8.4
- blackducksoftware/blackduck-webui:2021.8.4
- sigsynopsys/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq：1.2.3

2021.8.4で修正された問題

- （HUB-31425）。バージョン詳細レポートで、以前のバージョンのHUBと比較しようとしてクエリを実行すると、完了までにかなりの時間がかかっていましたが、その問題は修正されました。

バージョン2021.8.3の新機能および変更された機能

レポートデータベースの機能強化

次のデータをレポートスキーマの下のscan_stats_viewに追加しました。

- scan_size

コンテナバージョン

- blackducksoftware/blackduck-postgres:9.6-1.1
- blackducksoftware/blackduck-authentication:2021.8.3
- blackducksoftware/blackduck-webapp:2021.8.3
- blackducksoftware/blackduck-scan:2021.8.3

- blackducksoftware/blackduck-jobrunner:2021.8.3
- blackducksoftware/blackduck-cfssl:1.0.3
- blackducksoftware/blackduck-logstash：1.0.10
- blackducksoftware/blackduck-registration:2021.8.3
- blackducksoftware/blackduck-nginx：2.0.6
- blackducksoftware/blackduck-documentation:2021.8.3
- blackducksoftware/blackduck-upload-cache：1.0.18
- blackducksoftware/blackduck-redis:2021.8.3
- blackducksoftware/blackduck-bomengine:2021.8.3
- blackducksoftware/blackduck-matchengine:2021.8.3
- blackducksoftware/blackduck-webui:2021.8.3
- sigsynopsys/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq：1.2.3

2021.8.3で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- （HUB-29959、HUB-30391、HUB-30397）。構成表の準備中にナレッジベースからの「500 内部エラー」応答によりスキャンが完了しない問題が修正されました。
- （HUB-31047）。バージョン構成表コンポーネントページを表示する際、UIがバックエンドの呼び出しを重複して作成しており、データベースに不要な負荷がかかっていましたが、その問題は修正されました。
- （HUB-30074）。アップロードソース情報が更新される前に、非常に小さなコードの場所のスニペットスキャンが終了することがあり、アップロードされたソースが失われたように見えるという問題が修正されました。

バージョン2021.8.2の新機能および変更された機能

Black Duck バージョン2021.8.2はメンテナンスリリースであり、新機能や変更された機能はありません。

コンテナバージョン

- blackducksoftware/blackduck-postgres:9.6-1.1
- blackducksoftware/blackduck-authentication:2021.8.2
- blackducksoftware/blackduck-webapp:2021.8.2
- blackducksoftware/blackduck-scan:2021.8.2
- blackducksoftware/blackduck-jobrunner:2021.8.2
- blackducksoftware/blackduck-cfssl:1.0.3
- blackducksoftware/blackduck-logstash：1.0.10
- blackducksoftware/blackduck-registration:2021.8.2
- blackducksoftware/blackduck-nginx：2.0.6
- blackducksoftware/blackduck-documentation:2021.8.2

- blackducksoftware/blackduck-upload-cache：1.0.18
- blackducksoftware/blackduck-redis:2021.8.2
- blackducksoftware/blackduck-bomengine:2021.8.2
- blackducksoftware/blackduck-matchengine:2021.8.2
- blackducksoftware/blackduck-webui:2021.8.2
- sigsynopsys/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq：1.2.3

2021.8.2で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- （HUB-31078）。Kubernetesの環境では、インストール/アップグレードの一部として--reuse-valuesフラグを使用すると、Black Duck 2021.8のインストール/アップグレードが正常に終了しませんでした。その問題は文書化されました。詳細については、Helmチャートの下にあるREAME.mdを参照してください。
- （HUB-31086）。いくつかのプロジェクトバージョンで、[構成表]ページの右上にあるスニペットボックスが欠落していましたが、その問題は修正されました。
- （HUB-31156）。プロジェクトレベルで構成表マネージャの役割を持っていても、グローバルな役割または全般的な役割は持っていないユーザーの場合、プロジェクト構成表にアクセスできませんでした。その問題は修正されました。

バージョン2021.8.1の新機能および変更された機能

Black Duck バージョン2021.8.1はメンテナンスリリースであり、新機能や変更された機能はありません。

コンテナバージョン

- blackducksoftware/blackduck-postgres:9.6-1.1
- blackducksoftware/blackduck-authentication:2021.8.1
- blackducksoftware/blackduck-webapp:2021.8.1
- blackducksoftware/blackduck-scan:2021.8.1
- blackducksoftware/blackduck-jobrunner:2021.8.1
- blackducksoftware/blackduck-cfssl:1.0.3
- blackducksoftware/blackduck-logstash：1.0.10
- blackducksoftware/blackduck-registration:2021.8.1
- blackducksoftware/blackduck-nginx：2.0.6
- blackducksoftware/blackduck-documentation:2021.8.1
- blackducksoftware/blackduck-upload-cache：1.0.18
- blackducksoftware/blackduck-redis:2021.8.1
- blackducksoftware/blackduck-bomengine:2021.8.1
- blackducksoftware/blackduck-matchengine:2021.8.1
- blackducksoftware/blackduck-webui:2021.8.1

- sigsynopsys/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

2021.8.1で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (HUB-31029)。個人/グループのスーパーユーザーの役割は、プロジェクトマネージャの役割設定で上書きされていました。その問題は修正されました。
- (HUB-30808)。プロジェクトの構成表でコンポーネントの「追加フィールド」をレビューする場合、カスタムフィールド管理の[構成表コンポーネント]タブで作成されたカスタムフィールドが返されませんでしたが、その問題は修正されました。
- (HUB-30655)。スーパーユーザーの役割を持たないユーザーが、[管理]メニューの[プロジェクトグループ管理]オプションを表示できましたが、その問題は修正されました。
- (HUB-31077)。Helmチャートのプロパティに変更が加えられたため、Kubernetesの導入環境では、Black Duck HUB 2021.6.0を2021.8.xにアップグレードできませんでした。その問題は修正されました。他の旧バージョンには影響はありません。

バージョン2021.8.0の発表

Black Duck 2021.8.0リリースに必要なDetect 7.4

Black Duckバージョン2021.8.0を実行するには、Detect 7.4が必要です。アップグレードする際には、この最小バージョン要件を満たしていることを確認してください。

CentOS-7上のDesktop Scanner

依存関係が更新されたため、最新バージョンのDesktop ScannerはCentOS-7では実行されません。そのため、古いバージョンのElectron 12で動作するCentOS-7ビルド専用に別のRPMが作成されました。Electron 12がサポートされている限り、この個別のCentOS-7ビルドを維持します。

現在のダウンロードに加えて、ツールページにCentOS-7ダウンロード専用のリンクが追加されました。通常のRPM、Debianパッケージ、macOSおよびWindowsインストーラが利用できます。

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2021.6.0が日本語にローカライズされました。

簡体字中国語

UI、オンラインヘルプ、およびリリースノートのバージョン2021.2.0が簡体字中国語にローカライズされました。

廃止されたAPI

次のエンドポイントは削除されました。

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

以下の廃止されたエンドポイントは「410 GONE」エラーを返し、ターゲットリソースへのアクセスが利用できなくなったことを示します。

- GET /oauthclients
- POST /oauthclients

- DELETE /oauthclients/{oAuthClientId}
- GET /oauthclients/{oAuthClientId}
- PUT /oauthclients/{oAuthClientId}
- POST /vulnerabilities/vulndb-copy

バージョン2021.8.0の新機能および変更された機能

PostgreSQL 13の外部データベースのサポート

Black Duckは、外部PostgreSQLを使用する新規インストール用にPostgreSQL 13をサポートおよび推奨するようになりました。2021.8.xへの移行では、PostgreSQL 13への移行は必要ありません。

内部PostgreSQLコンテナのユーザーは、アクションは必要ありません。

PostgreSQL 12はサポートされていません。

インストールマニュアルは、今後のリリースで更新される予定です。

Azureをご利用のお客様へのお知らせ

Azure PostgreSQL 13でのBlack Duckのサポートは、Azure PostgreSQL 13のフルリリースまでは努力目標となり、問題の解決は保証されません。したがって、本番環境への導入にAzure PostgreSQL 13を使用しないことを強くお勧めします。Azure PostgreSQL 11を使用する必要があります。

PostgreSQL 13のAzureサポートの詳細については、https://docs.microsoft.com/en-us/azure/postgresql/concepts-version-policyを参照してください。

スキャンの新しいシステム設定：コンポーネント依存関係の重複感度

この設定では、スキャン中に検出されたコンポーネントの重複パッケージIDを[ソース]ページに表示する方法を変更できます。以前のリリースおよび2021.8.0のデフォルト設定（1に設定）では、スキャン中の検出頻度に関係なく、1つのパッケージIDのみが[ソース]ページに表示されます。この設定を1より大きい値に変更すると、より多くのエントリが表示されるため、レイヤーごとの洞察が深まり、各コンポーネントがどのレイヤーから発生したかを判断することができます。この機能は、[構成表集約を使用して検出]を有効にしてスキャンし、1つのスキャンに集約されたさまざまなモジュールにおけるパッケージID参照を表示する場合に特に便利です。

スキャンの新しいシステム設定：最小スキャン間隔

この設定では、LCAの強化された署名スキャンを使用するときに、特定のコードの場所に対して署名スキャンを実行できる最小時間間隔を変更できます。デフォルト設定は0、または最小スキャン間隔が設定されていないため、頻度に関係なくスキャンが実行されます。0より大きい値に設定すると、設定されたスキャン間隔より前に署名スキャンが実行された場合、スキャンは処理されません。たとえば4に設定すると、4時間が経過するまで署名の再スキャンが許可されません。この設定は、[管理]>[システム設定]>[スキャン]ページでグローバルに設定するか、Detectクライアントのコマンドラインオプションを使用して設定できます。注：この設定は、パラメータ--detect.blackduck.signature.scanner.arguments='--signature-generation'を使用してスキャンした場合にのみ使用されます。

注： この機能を有効にすると、スキャン間隔が原因で署名スキャンが実行されなかった場合でも、Detectを使用した署名スキャンは成功ステータスで終了します。スキャンが実行されなかったことを示す警告メッセージがログに表示されますが、他の情報は表示されません。

高速スキャンのポリシー適用の変更

高速スキャンユーザーは、フルスキャン（従来）、高速スキャン、またはその両方の結果にポリシーを適用する方法を設定できるようになりました。バージョン2021.8.0以降のBlack Duckの新規インストールのデフォルト設定は、フルスキャンにのみ適用されるように設定されます。高速スキャンを使用して、ポリシーに関係なくすべての脆弱性を検出するには、1つのポリシーを作成し、条件の重大度を0以上に設定します。

実行された高速スキャン数の自動累積カウントの追加

このカウントは正確であり、データが失われることはありませんが、一部のスキャンが後続日のデータから取得されるタイミングの問題がある場合があります。

高速スキャンの脆弱性条件のポリシー管理への追加

ポリシー管理では、次の脆弱性の条件が利用可能になりました。

- CWE ID
- ソリューションが利用可能
- 回避策が利用可能
- 攻撃が利用可能
- ソースから到達可能
- 修正ステータス

プロジェクトグループ管理

Black Duckでは、Hub内のすべてのプロジェクトを論理的にグループ化できるようになりました。これにより、どのプロジェクトがどのビジネスユニットに属しているかを整理できるため、組織全体のリスクを簡単に確認できます。プロジェクトグループには、プロジェクトと他のプロジェクトグループの両方を含めることができ、マルチレベルの階層を提供できます。

ユーザーとグループは、任意の数の役割を持つプロジェクトグループに割り当てることができます。この割り当てにより、割り当てが下位レベルで明示的に上書きされない限り、指定された役割を持つグループの下のプロジェクトにアクセスできるようになります。この概念により、まだ作成されていないプロジェクトへのデフォルトアクセス権をユーザーに設定できます。

さらに、検索ダッシュボードが拡張され、ユーザーがプロジェクトグループを介してアクセスできるプロジェクトの検索結果が返されるようになりました。

新しいユーザーの役割であるグローバルリリース作成者とプロジェクトグループ構成表アノテーター、および既存の役割への変更

プロジェクト作成者とグローバルコードスキャナという役割が持っていたグローバルリリース作成のアクセス権が取り消され、所有していない、またはアクセス権を持っていないプロジェクトのリリースを作成できなくなりました。この機能に依存しているユーザーのギャップを埋めるために、グローバルリリース作成者という新しい役割が追加されました。プロジェクト作成者やグローバルコードスキャナを使用している現在のすべてのユーザーは、アップグレード移行スクリプトの一部としてこの役割を自動的に継承します。つまり、この変更は、より狭いセキュリティの変更を利用したいと考えている現在のユーザーのためのものです。

プロジェクトグループ構成表アノテーターには、割り当てられたプロジェクトグループ内のすべてのプロジェクトに対する構成表アノテーター権限があります。つまり、プロジェクトグループに関連付けられているプロジェクトのコメントの追加や編集、カスタムフィールドの編集ができます。

Protex BOMツールトークンアクセスサポートの強化

Protex BOMツールでは、BD_HUB_TOKEN環境変数をサポートして、ProtexからエクスポートされたJSONをHubにアップロードできるようになりました。トークンを設定するには、コマンドプロンプトを使用して「-T」を追加します。

BD_HUB_TOKEN=[insert token here]変数を.bash_profileに追加して、変更を永続的にします。

脆弱性の通知の機能強化

新しい環境変数を追加しました：blackduck-config.evファイル内のBLACKDUCK_NOTIFY_WHEN_REMEDIATEDデフォルトはtrueですが、falseに設定すると、Black Duckでは「無視、修復完了、緩和、またはパッチ適用済み」の修正ステータスを持つ脆弱性に対する「新しい」脆弱性通知を送信または作成できなくなります。

署名スキャンタイムアウトメッセージの拡張

署名スキャン中のネットワークタイムアウト（HUBからの応答を待機中）では、I/Oエラーではなくネットワークタイムアウトを示す正確なエラーメッセージ（コード74）が返されるようになりました。新しいメッセージ形式Scan <Corresponding Scan ID> failed: [<Reason why it happened and whether to contact an administrator or retry the scan>]が表示されます。

Black Duck Hubの再試行要求メカニズムの機能強化

ウェイターが導入され、HTTP 502/503/504応答を受信したときにスキャンのHubへのアップロードが再試行されるようになりました。スキャンが失敗したことを通知する前に、30秒ごとに10分間再試行します。

[スキャン]ページの拡張機能

[作成]列が[スキャン]ページに新しく追加され、スキャンが作成された日時を確認できるようになりました。列に表示される日付により、[作成日]オプションを使用してスキャンをフィルタリングするときに日付を簡単に比較できます。

バージョンのないコンポーネントの表層ライセンスリスク情報

不明なバージョンのコンポーネントのデフォルトライセンスを決定するための新しいロジックが導入されました。これは、コンポーネントの上位1,000バージョンで表示される最大回数に基づく推定ライセンスです。これにより、バージョンを選択しなくてもライセンスリスクを計算できます。ただし、より正確な結果を得るには、これらのコンポーネントを確認し、手動でバージョンを指定することをお勧めします。

レポートデータベースの機能強化

次のデータをレポートスキーマの下のscan_stats_viewに追加しました。

- user_id
- project_id
- project_name
- version_id
- version_name
- scan_id
- scan_name
- code_location_id
- code_location_name
- scan_type
- scan_status

- scan_start_at
- scan_end_at
- scan_duration
- scan_age
- scan_archived_at
- application_id

ポリシールール条件の機能強化

総合スコアのポリシールール脆弱性条件カテゴリに、新しいポリシー条件演算子が追加されました。ポリシールールを作成または編集するときに、[次の値以下]を選択できるようになりました。

コンテナバージョン

- blackducksoftware/blackduck-postgres:9.6-1.1
- blackducksoftware/blackduck-authentication:2021.8.0
- blackducksoftware/blackduck-webapp:2021.8.0
- blackducksoftware/blackduck-scan:2021.8.0
- blackducksoftware/blackduck-jobrunner:2021.8.0
- blackducksoftware/blackduck-cfssl:1.0.3
- blackducksoftware/blackduck-logstash：1.0.10
- blackducksoftware/blackduck-registration:2021.8.0
- blackducksoftware/blackduck-nginx：2.0.5
- blackducksoftware/blackduck-documentation:2021.8.0
- blackducksoftware/blackduck-upload-cache：1.0.18
- blackducksoftware/blackduck-redis:2021.8.0
- blackducksoftware/blackduck-bomengine:2021.8.0
- blackducksoftware/blackduck-matchengine:2021.8.0
- blackducksoftware/blackduck-webui:2021.8.0
- sigsynopsys/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq：1.2.3

APIの機能強化

- スニペットマッチを一括確認/確認解除、一括無視/無視解除するための新しいAPIが追加されました。

  . `PUT /api/projects/{projectId}/versions/{versionId}/bulk-snippet-bom-entries Media Type: application/vnd.blackducksoftware.bill-of-materials-6+json`

- 次のAPIエンドポイントが更新され、ユーザーがプロジェクトグループメンバーシップを介してアクセスできるプロジェクトが考慮されるようになりました。クエリパラメータもnameからentityNameに変更され、応答内容と同等になりました。
  - `GET /api/users/{userId}/assignable-projects`
  - `GET /api/users/{userId}/assignable-project-groups/`
  - `GET /api/usergroups/{userGroupId}/assignable-projects`
  - `GET /api/usergroups/{userGroupId}/assignable-project-groups`

2021.8.0で修正された問題

- (HUB-29341)。--include-filesフラグを使用してProtexから構成表をエクスポートし、Hubインスタンスにインポートすると、Javaヒープ領域エラーが発生するという問題が修正されました。
- (HUB-29005)。構成表にまったく同じ名前でUUIDが異なる2つのコンポーネントがある場合、フィルタAPI(/api/projects/projectId/versions/versionId/components-filters?filterKey=bomComponents)は名前によってそれらをグループ化するのではなく、IDとそのバージョン(存在する場合)に基づいて2つの独立したコンポーネントを返すべきであるという問題を修正しました。
- (HUB-29567)。「更新日時」(または2021.8.0では「最終設定更新日時」)のタイムスタンプが更新されても、[プロジェクトバージョン]>[詳細]のユーザー名で更新されない問題が修正されました。「最終設定更新日時」タイムスタンプとユーザー名で更新されたタイムスタンプは、プロジェクトのバージョンの詳細が変更された場合にのみ更新されるようになりました。
- (HUB-30139)。Protex BOMツールの問題を修正しました。--include-filesフラグを使用しているときに「Unmarshalling Error:Illegal character」が発生していました。
- (HUB-12280)。bdioファイルのアップロード時に、「bdioツリー」の下層にある場合、プロジェクトとの関連性が表示されない問題を修正しました。
- (HUB-29481)。同じ名前で大文字が異なるライセンスが通知レポートから除外される問題が修正されました。
- (HUB-30143)。Protex BOMツール 2021.6.0が最新のJDK(11.0.11)で動作しない問題を修正しました。
- (HUB-29274)。[構成表]ページに循環参照がある場合にVersionReportJobによってjobrunnerにメモリ不足の問題を発生させる問題を修正しました。
- (HUB-29381)。プロジェクトバージョンがコンポーネントとして追加されたときに([追加]>[プロジェクト]を使用)、コンポーネントエントリに無効な[運用リスク]レベルが表示される問題が修正されました。
- (HUB-30087)。バージョン名にマルチバイトの英数字が含まれている場合に、プロジェクトバージョンクエリでバージョンが見つからない問題が修正されました。
- (HUB-23686)。ノードファイルに対してDetectを実行しているときに、署名スキャナがスタックする問題を修正しました。
- (HUB-25592)。コンポーネント(またはコンポーネントのバージョン)の調整が構成表から自動的に削除される問題を修正しました。
- (HUB-25552)。「マッチ」タイプの調整を含むコンポーネント(またはコンポーネントのバージョン)が構成表から自動的に追加/削除される問題を修正しました。
- (HUB-29196)。ポリシー違反ポップアップをクリックしても非表示にならず、マウスカーソルがポリシー違反シンボルからすばやく離れる問題が修正されました。
- (HUB-29573)。ポリシー違反モーダルの表示時にポリシールールの説明の改行が無視される問題を修正しました。
- (HUB-30611)。データベース移行スクリプトで、数値のユーザー名がエラーの原因となっている問題が修正されました。

- （HUB-26611）。Detectで集約を使用したときに、直接的/推移的な依存関係が正しく報告されない問題を修正しました。この修正は、Detect 7.4を使用している場合にのみ解決され、Detectで新しいサブプロジェクトdetect.bom.aggregate.remediation.modeを使用する必要があることに注意してください。
- （HUB-22379）。一部のインスタンスでプロジェクトのタグ付けとタグポリシーの設定に数時間かかるパフォーマンスの問題が修正されました。
- （HUB-30141）。サポートされていない「リンク」オプションを含むHubスウォームdocker-compose.ymlの問題を修正しました。
- （HUB-29549）。アクセス権チェックによる[構成表]ページのロードに関するパフォーマンスの問題が修正されました

7. Black Duckバージョン2021.6.x

バージョン2021.6.2の新機能および変更された機能

Black Duck バージョン2021.6.2はメンテナンスリリースであり、新機能や変更された機能はありません。

コンテナバージョン

- blackducksoftware/blackduck-postgres:9.6-1.1
- blackducksoftware/blackduck-authentication:2021.6.2
- blackducksoftware/blackduck-webapp:2021.6.2
- blackducksoftware/blackduck-scan:2021.6.2
- blackducksoftware/blackduck-jobrunner:2021.6.2
- blackducksoftware/blackduck-cfssl:1.0.2
- blackducksoftware/blackduck-logstash：1.0.10
- blackducksoftware/blackduck-registration:2021.6.2
- blackducksoftware/blackduck-nginx：2.0.5
- blackducksoftware/blackduck-documentation:2021.6.2
- blackducksoftware/blackduck-upload-cache：1.0.17
- blackducksoftware/blackduck-redis:2021.6.2
- blackducksoftware/blackduck-bomengine:2021.6.2
- blackducksoftware/blackduck-matchengine:2021.6.2
- blackducksoftware/blackduck-webui:2021.6.2
- sigsynopsys/bdba-worker：2021.06
- blackducksoftware/rabbitmq：1.2.2

2021.6.2で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- （HUB-30493）。NGINX構成でAlertのプロキシ証明書の場所を指定することにより、ホストされたユーザーがBlackduck Alertインスタンスにアクセスできない問題が修正されました。

バージョン2021.6.1の新機能および変更された機能

Black Duckセキュリティアドバイザリ（BDSA）のリモートコード実行手順

Black Duckは、2021.6.1リリースにおいて、リモートでのコード実行（RCE）を可能にする脆弱性に注目しています。Black DuckのUIでは、BDSAの脆弱性にRCEタグがある場合、BDSAのフルレコード、脆弱性の表、および特定のコンポーネントの[セキュリティ]タブに表示されます。

脆弱性APIは、bdsaTagsという名前の配列を使用して脆弱性を報告します。bdsaTag配列に「RCE」が含まれている場合、この脆弱性によりリモートでコードが実行される可能性があります。

- /api/components/{componentId}/vulnerabilities
- /api/components/{componentId}/versions/{componentVersionId}/vulnerabilities
- /api/components/{componentId}/versions/{componentVersionId}/origin/{componentVersionOriginId}/vulnerabilities
- /api/projects/{projectId}/versions/{versionId}/components/{componentId}/versions/{componentVersionId}/origins/{componentVersionOriginId}/vulnerabilities

コンテナバージョン

- blackducksoftware/blackduck-postgres:9.6-1.1
- blackducksoftware/blackduck-datadog:1.0.1
- blackducksoftware/blackduck-solr:1.0.0
- blackducksoftware/blackduck-authentication:2021.6.1
- blackducksoftware/blackduck-webapp:2021.6.1
- blackducksoftware/blackduck-scan:2021.6.1
- blackducksoftware/blackduck-jobrunner:2021.6.1
- blackducksoftware/blackduck-cfssl:1.0.2
- blackducksoftware/blackduck-logstash：1.0.10
- blackducksoftware/blackduck-registration:2021.6.1
- blackducksoftware/blackduck-nginx：2.0.3
- blackducksoftware/blackduck-documentation:2021.6.1
- blackducksoftware/blackduck-upload-cache：1.0.17
- blackducksoftware/blackduck-redis:2021.6.1
- blackducksoftware/blackduck-bomengine:2021.6.1
- blackducksoftware/blackduck-matchengine:2021.6.1
- blackducksoftware/blackduck-webui:2021.6.1
- sigsynopsys/bdba-worker：2021.06
- blackducksoftware/rabbitmq：1.2.2

2021.6.1で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- （HUB-29202）。2021.4.0のバイナリスキャンコンテナ（bdba-worker）が、タイムアウト値と再試行値を増やすとDocker Swarmで動作しない問題を修正しました。
- （HUB-29405）。core_i7アーキテクチャの識別により、マッチが破棄される問題が修正されました。
- （HUB-30134）。RabbitMQ接続の問題により、構成表エンジンが警告なしで起動に失敗する問題が修正されました。
- （HUB-30170）。デュアルスタックKubernetesを使用しているときに、Dockerエントリポイントの設定が正しくないためRedisが起動しない問題が修正されました。

- （HUB-30202）。[脆弱性の詳細]ページで、ユーザーがクリックしてBDSAスコアとNVDスコアを切り替えたときに、スコアメトリックの表示が正しく変更されない問題が修正されました。

バージョン2021.6.0の発表

外部データベース用のPostgreSQLバージョン9.6のサポート終了

Black Duck 2021.6.0リリースの時点で、Synopsysは外部データベース用のPostgreSQLバージョン9.6のサポートを終了しました。

Black Duck は、外部データベース用のPostgreSQLバージョン11.xのみをサポートするようになりました。

廃止されたページ

以前にお知らせしたように、[スキャン] > [コンポーネント]ページは削除されました。

廃止されたAPI

次のエンドポイントは廃止されました。

- GET /oauthclients
- POST /oauthclients
- DELETE /oauthclients/{oAuthClientId}
- GET /oauthclients/{oAuthClientId}
- PUT /oauthclients/{oAuthClientId}
- POST /vulnerabilities/vulndb-copy

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2021.4.0が日本語にローカライズされました。

バージョン2021.6.0の新機能および変更された機能

新しいコンテナとシステム要件の変更

2021.6.0リリースでは、次のようになります。

- 新しいコンテナblackduck-webuiが追加され、Black Duckのパフォーマンスの向上、キャッシュ機能の向上、将来の拡張性が実現されました。
- 高速スキャン機能は、すべてのBlack Duckのお客様が使用できるようになりました。この機能を使用するには、blackduck-matchengineという新しいコンテナが必要です。このコンテナは、Black Duckナレッジベースへの接続を管理し、ナレッジベースの結果を短い間隔でキャッシュします。

以下は、すべてのコンテナの単一インスタンスの実行に必要な最小ハードウェアです。メモリ要件は、サポートする同時高速スキャンの数によって異なることに、注意してください。

- 7 CPU

- Redisの最小構成の場合は28.5 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は31.5 GB RAM。これにより、最大100の同時高速スキャンがサポートされます。

  Redisの最小構成の場合は30 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は33 GB RAM。これにより、150以上の高速スキャンがサポートされますが、サポートされる高速スキャンの最大数は現在判定中です。
- データベースおよびその他のBlack Duckコンテナ用に250 GBの空きディスク容量
- データベースバックアップに適した容量

以下は、Black Duck – Binary AnalysisでBlack Duckを実行するために必要な最小ハードウェアです。

- 8 CPU
- Redisの最小構成の場合は32.5 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は35.5 GB RAM。これにより、最大100の同時高速スキャンがサポートされます。

  Redisの最小構成の場合は34 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は37 GB RAM。これにより、150以上の高速スキャンがサポートされますが、サポートされる高速スキャンの最大数は現在判定中です。
- データベースおよびその他のBlack Duckコンテナ用に350 GBの空きディスク容量
- データベースバックアップに適した容量

注： binaryscannerコンテナを1個追加するごとに、1 CPU、2 GB RAM、100 GBの空きディスク容量の追加が必要になります。

高速スキャン

高速スキャンはすべてのお客様にご利用いただけます。

Black Duckの高速スキャンは、開発者が、プロジェクトに含まれているオープンソースコンポーネントのバージョンが、オープンソースの使用に関する企業ポリシーに違反しているかどうかを迅速に判断する方法を提供します。Synopsys Detectを使用すると、高速スキャンがパッケージマネージャのスキャンのみを使用し、Black Duckサーバーデータベースとやり取りしないので、迅速に結果が返されます。クイックフィードバックが必要な場合や、Black Duckでデータを保持する必要がない場合は、高速スキャンを使用します。

高速スキャンを使用すると、Black Duckの追加のインスタンスを展開しなくても、何千ものスキャンを実行できます。プロジェクトバージョンなしで、またはBlack Duckのユーザーインターフェイスにアクセスせずに使用できる、実用的な結果（ビルドの失敗など）を提供します。

新しいジョブサブシステム

ジョブサブシステムが新しい実装に置き換えられました。

- ジョブのステータスには次のようなものがあります。
  - 保留
  - 進行中
  - 完了
  - エラー
- 定期的またはオンデマンドのスケジュールに基づいてジョブをフィルタリングできます。

- 新しい実装では、次のジョブが追加されました。
  - BomAggregatePurgeOrphansCheckJob：構成表データがプロジェクトバージョンに関連付けられていないかどうかを確認し、必要なジョブを開始します。
  - BomVulnerabilityDataRecomputationCheckJob：特定の設定が変更されたときに構成表の計算が必要かどうかをチェックし、必要なジョブを開始します。
  - BomVulnerabilityDataRecomputationJob：ナレッジベースから受信したコンポーネント情報を更新します。
  - HierarchicalVersionBomCheckJob：階層的な構成表計算が必要かどうかをチェックし、その処理に必要なジョブを開始します
  - JobHistoryStatsJob-Calculate Daily Statistics：ジョブアクティビティに基づいて日次統計を計算します。
  - JobHistoryStatsJob-Calculate Five Minute Statistics：ジョブアクティビティに基づいて、5分間隔で統計情報を計算します。
  - JobHistoryStatsJob-Calculate Hourly Statistics：ジョブアクティビティに基づいて、1時間の統計情報を計算します。
  - JobHistoryStatsJob-Prune Job History：保持設定に基づいて、ジョブ履歴から古いレコードをプルーニングします。
  - KBUpdateCheckJob：ナレッジベースから受信した更新を開始します。
  - KbUpdateWorkflowJob-BDSA Vulnerability Update：ナレッジベースから受信したBDSAの脆弱性情報を更新します。
  - KbUpdateWorkflowJob-Component Update：ナレッジベースから受信したコンポーネント情報を更新します。
  - KbUpdateWorkflowJob-Component Version Update：ナレッジベースから受信したコンポーネントバージョンの更新を処理します。
  - KbUpdateWorkflowJob-License Update：ナレッジベースから受信したライセンス情報を更新します。
  - KbUpdateWorkflowJob-NVD Vulnerability Update：ナレッジベースから受信したNVD脆弱性情報を更新します。
  - KbUpdateWorkflowJob-Summary：最新のナレッジベース更新に関するサマリーレポートを発行します。
  - LicenseTermFulfillmentCheckJob：ライセンスの履行処理が必要かどうかを確認し、必要なジョブを開始します。
  - NotificationPurgeCheckJob：クリーンアップが必要な通知があるかどうかを確認し、必要なジョブを開始します。
  - QuartzVersionBomEventCleanupJob：保持ポリシーに基づいて構成表イベントをクリーンアップします。
  - VersionBomComputationCheckJob：構成表の計算が必要かどうかをチェックし、必要なジョブを開始して処理します。
  - VersionBomNotificationCheckJob：構成表計算結果の通知を発行します。
  - WatchdogJob：定期的なジョブを監視して正常に実行されていることを確認し、問題があると判断されたジョブの報告または修正を行います。
- 次のジョブは削除されました。
  - KbUpdateJob

レポートの機能強化

- 新しいプロジェクトバージョンレポートlicense_conflicts_date_time.csvが追加されました。このプロジェクトバージョンのライセンス競合を一覧表示します。このレポートには、次のカラムがあります。
  - コンポーネントID
  - バージョンID
  - コンポーネント名
  - コンポーネントバージョン名
  - 使用法
  - ライセンスID
  - ライセンス名
  - ソース/タイプ
  - ライセンス条項の責任
  - ライセンス条項のカテゴリ
  - ライセンス条項名
  - 説明
  - 競合ライセンスID
  - 競合ライセンス名
  - 競合ライセンス条項のソースタイプ
  - 競合ライセンス条項の責任
  - 競合ライセンス条項のカテゴリ
  - 競合ライセンス条項名
  - 競合ライセンス条項の説明
- components_date_time.csvプロジェクトバージョンレポートの末尾に、新しい列[ライセンス競合あり]が追加されました。この列は、このコンポーネントバージョンにライセンス競合があるかどうかを示します。
- レポートのファイル名では、UTCではなくシステムタイムゾーンが使用されるようになりました。

Black Duckナレッジベースの著作権情報を更新する機能

Black Duckでは、コンポーネントの取得元に関して、更新されたBlack Duckナレッジベース著作権情報を表示できるようになりました。新しいデータまたは更新されたデータがある場合、Black Duckは表示情報を更新しますが、編集内容は保持されます。

新しい役割

BOM Annotatorという新しい役割がBlack Duckに追加されました。この役割を持つユーザーは、プロジェクトへの読み取り専用アクセス権を持ち、構成表のコメントの追加または編集、構成表カスタムフィールドの更新を実行できます。

LDAPまたはSAMLグループの同期

Black DuckにLDAPまたはSAMLを設定するときにグループ同期を有効にすると、外部認証システム（LDAPまたはSSO）内のこのグループの名前が、[グループ名]ページの[外部グループ名]フィールドに表示されるようになりまし

た。これで、外部システムでグループ名が変更された場合は、そのグループ名を編集して、外部認証システムのグループ名とBlack Duckのグループ名を同期させられるようになりました。

必須カスタムフィールドの強制

Black Duckでは、必須カスタムフィールドを持つオブジェクトを編集する際にユーザーが値を入力する必要があるオプションが用意されました。

プロジェクト検索用の新しいフィルタ

Black Duckでは、プロジェクトの検索時に次のフィルタを新しく提供します。

- スキャンなし:このフィルタは、スキャンの一部になったことがないプロジェクトバージョンをすべて検索します。
- スキャンされていない期間:このフィルタは、選択した期間以降にスキャンされていないプロジェクトバージョンをすべて検索します。

マップされていないコードの場所の保存期間

マップされていないコードの場所のデフォルト保存期間が365日から30日に変更されました。

[コンポーネントの追加/編集]ダイアログボックスの追加情報

使用するコンポーネントをより簡単に判別できるように、[コンポーネントの追加/編集]ダイアログボックスに、コンポーネントのホームページURLと、このコンポーネントを使用するプロジェクトバージョン番号が表示されるようになりました。

ポリシーの機能強化

次のコンポーネント条件には、「偽」オプションが含まれるようになりました。

- プロジェクトバージョンとのライセンス競合
- 未履行のライセンス条項
- 不明なコンポーネントバージョン

C/C++マッチングの改善

2021.6.0リリースでは、LinuxドメインでC/C++をスキャンするお客様の構成表精度が向上しています。

新しいマッチタイプ

2021.6.0リリースでは、2つの新しいマッチタイプが追加されました。

- 直接的な依存関係バイナリ:スキャンにより、使用中のバイナリに直接的な依存関係があると判定されました。
- 推移的な依存関係バイナリ:スキャンにより、使用中のバイナリに推移的な依存関係があると判定されました。

サポートされるブラウザのバージョン

- Safariバージョン14.0.3(15610.4.3.1.7、15610)
- Chromeバージョン90.0.4430.72(公式ビルド)(x86_64)
- Firefoxバージョン88.0(64ビット)
- Microsoft Edgeバージョン90.0.818.41(公式ビルド)(64ビット)

コンテナバージョン

- blackducksoftware/blackduck-postgres:9.6-1.1
- blackducksoftware/blackduck-authentication:2021.6.0
- blackducksoftware/blackduck-webapp:2021.6.0
- blackducksoftware/blackduck-scan:2021.6.0
- blackducksoftware/blackduck-jobrunner:2021.6.0
- blackducksoftware/blackduck-cfssl:1.0.2
- blackducksoftware/blackduck-logstash：1.0.10
- blackducksoftware/blackduck-registration:2021.6.0
- blackducksoftware/blackduck-nginx：2.0.0
- blackducksoftware/blackduck-documentation:2021.6.0
- blackducksoftware/blackduck-upload-cache：1.0.17
- blackducksoftware/blackduck-redis:2021.6.0
- blackducksoftware/blackduck-bomengine:2021.6.0
- blackducksoftware/blackduck-matchengine:2021.6.0
- blackducksoftware/blackduck-webui:2021.6.0
- sigsynopsys/bdba-worker：2021.03
- blackducksoftware/rabbitmq：1.2.2

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2021.4.0が日本語にローカライズされました。

APIの機能強化

- ジョブサブシステムの変更：
  - GET /jobs/{jobID}は、特定のジョブのジョブの詳細をIDで取得する呼び出しです。この呼び出しは、404 Not Foundステータスコードを返します。
  - 次の呼び出しは、Black Duckバージョン2020.2.0以降では使用停止になり、404 Not Foundステータスコードを返し、Black Duckバージョン2021.6.0でも引き続き機能しません。
    - PUT /jobs/{jobID} これは、ジョブを再スケジュールする呼び出しです。
    - DELETE /jobs/{jobID} この呼び出しは、ジョブを終了します。

    この機能は、将来のリリースで利用可能になる新しいJob Rest APIの実装に変わります。
- 高速スキャンタイプを識別するために、ポリシービュー（/api/policy-rules/{policyRuleId}）の式（"developerScanExpression"）に新しいブール値フィールドを追加しました。

2021.6.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- （Hub-21613）。scan.cliバージョン2019.8.xで、使用しているJavaバージョンが原因でパフォーマンスが低下するという、意味のない警告メッセージが表示される問題が修正されました。

- （Hub-25227、25521）。[スキャン]ページでスキャンのステータスがスキャン完了になり、誤解を招くという問題が修正されました。
- （Hub-26108）。Black DuckにAlertを展開する場合に、顧客証明書の使用時にnginxアラート設定ファイルを手動で操作しなければならないという問題を修正しました。
- （Hub-26924）。SAML SSOユーザーがログインに失敗したときに、ユーザーフレンドリーなエラーメッセージが表示されるように修正されました。
- （Hub-27209）。VersionBomComputationJobが次のエラーで失敗する問題を修正しました：″Error in job execution: could not extract ResultSet; SQL [n/a]; constraint [cvss2_severity].″
- （Hub-27681）。カスタムセキュリティコンテキストを使用してKubernetesに展開するときに、ルートユーザーがBOM Engineを起動する必要がある問題を修正しました。
- （Hub-27894）。新しいBlack Duck検索でリセットが0に設定されるように修正されました。
- （Hub-28171）。1件のプロジェクトで著作権検索が失敗する問題を修正しました。
- （Hub-28305）。ログに次のエラーが表示される問題を修正しました：Failed class com.blackducksoftware.job.integration.domain.impl.JobMaintenanceJob
- （Hub-28347）。スニペットの調整が重複キーSnippetAdjustmentエラーになる問題が修正されました。
- （Hub-28351）。構成表ライセンスの変更を保存する際のパフォーマンスの問題を修正しました。
- （Hub-28469）。Docker 20.10.xでカスタム証明書を設定できない問題を修正しました。
- （Hub-28726）。プロジェクトのクローンを作成した後に、プロジェクトのクローンを作成したユーザーの名前がコンポーネントレビュー担当者の名前としてBlack Duckに表示される問題が修正されました。
- （Hub-28909）。ユーザーアカウントがロックアウトされた後、Black Duck UIに誤ったエラーメッセージが表示される問題を修正しました。
- （Hub-29071）。スニペットを一括編集する際のパフォーマンスの問題を修正しました。
- （Hub-29168）。プロジェクトバージョンにマッピングされたスキャンに一致するものがない場合に、プロジェクトレベルのファイル調整がそのプロジェクトバージョンに適用されないという問題が修正されました。

8. Black Duckバージョン2021.4.x

バージョン2021.4.1の新機能および変更された機能

Black Duck バージョン2021.4.1はメンテナンスリリースであり、新機能や変更された機能はありません。

2021.4.1で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (Hub-28347)。スニペットの一括調整が次のエラーで失敗する問題を修正しました:"Adjustment Failed: The server encountered an error, please check your connection and try again."
- (Hub-28807)。Artifactoryプラグインに次のエラーが表示される問題を修正しました:"Too many parameters error on /api/projects/<projectID>/versions/<projectVersionID>/components/<componentID>/versions/<componentVersionID>?offset=0&limit=100."
- (Hub-29002)。[スニペット確認]ウィンドウで無視を解除されたスニペットをフィルタリングすると、システム全体のスニペットが表示されるという問題が修正されました。
- (Hub-29448)。LDAPユーザー認証に失敗し、「IncorrectResultSizeDataAccessException」エラーが発生する問題を修正しました。

バージョン2021.4.0の発表

新しいコンテナとシステム要件の変更

2021.6.0リリースでは、次のようになります。

- 新しいコンテナblackduck-webuiが追加され、Black Duckのパフォーマンスの向上、キャッシュ機能の向上、将来の拡張性が実現されます。
- 高速スキャン機能は、すべてのBlack Duckのお客様が使用できます。この機能を使用するには、現在blackduck-kbと呼ばれる新しいコンテナが必要です。このコンテナは、Black Duckナレッジベースへの接続を管理し、ナレッジベースの結果を短い間隔でキャッシュします。

以下は、すべてのコンテナの単一インスタンスの実行に必要な最小ハードウェアです。メモリ要件は、サポートする同時高速スキャンの数によって異なることに、注意してください。

- 7 CPU
- Redisの最小構成の場合は28.5 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は31.5 GB RAM。これにより、最大100の同時高速スキャンがサポートされます。

  Redisの最小構成の場合は30 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は33 GB RAM。これにより、150以上の高速スキャンがサポートされますが、サポートされる高速スキャンの最大数は現在判定中です。
- データベースおよびその他のBlack Duckコンテナ用に250 GBの空きディスク容量
- データベースバックアップに適した容量

以下は、Black Duck - Binary AnalysisでBlack Duckを実行するために必要な最小ハードウェアです。

- 8 CPU

- Redisの最小構成の場合は32.5 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は35.5 GB RAM。これにより、最大100の同時高速スキャンがサポートされます。

  Redisの最小構成の場合は34 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は37 GB RAM。これにより、150以上の高速スキャンがサポートされますが、サポートされる高速スキャンの最大数は現在判定中です。
- データベースおよびその他のBlack Duckコンテナ用に350 GBの空きディスク容量
- データベースバックアップに適した容量

注： binaryscannerコンテナを1個追加するごとに、1 CPU、2 GB RAM、100 GBの空きディスク容量の追加が必要になります。

マップされていないコードの場所の保存期間

Black Duck 2021.6.0リリースでは、マップされていないコードの場所のデフォルトの保存期間が365日間から30日間に変更されます。

廃止されたAPI

次のエンドポイントは廃止され、今後のリリースでは削除される予定です。

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

次のエンドポイントは2021年4月30日をもって廃止されます。

```
GET /api/components/{componentId}/versions/{componentVersionId}/origins/{originId}/
direct-dependencies
```

2021.6.0リリースでの新しいジョブ実装

Black Duckバージョン2021.6.0では、ジョブサブシステムが新しい実装に変わっているため、以下のジョブのRest API呼び出しは機能しません。

. `GET /jobs/{jobID}`

  これは、特定のジョブのジョブの詳細をIDで取得する呼び出しです。Black Duck 2021.6.0リリースでは、この呼び出しは404 Not Foundステータスコードを返します。

次の呼び出しは、Black Duckバージョン2020.2.0以降では使用停止になり、404 Not Foundステータスコードを返し、Black Duckバージョン2021.6.0でも引き続き機能しません。

. `PUT /jobs/{jobID}`

  これは、ジョブを再スケジュールする呼び出しです。

. `DELETE /jobs/{jobID}`

  この呼び出しは、ジョブを終了します。

この機能は、将来のリリースで利用可能になる新しいJob Rest APIの実装に変わります。

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2021.2.0が日本語にローカライズされました。

バージョン2021.4.0の新機能および変更された機能

高速スキャン – お客様の使用が制限された機能

Black Duckの高速スキャンは、開発者が、プロジェクトに含まれているオープンソースコンポーネントのバージョンが、オープンソースの使用に関する企業ポリシーに違反しているかどうかを迅速に判断する方法を提供します。Synopsys Detectを使用すると、高速スキャンがパッケージマネージャのスキャンのみを使用し、Black Duckサーバーデータベースとやり取りしないので、迅速に結果が返されます。クイックフィードバックが必要な場合や、Black Duckでデータを保持する必要がない場合は、高速スキャンを使用します。

高速スキャンを使用すると、Black Duckの追加のインスタンスを展開しなくても、何千ものスキャンを実行できます。プロジェクトバージョンなしで、またはBlack Duckのユーザーインターフェイスにアクセスせずに使用できる、実用的な結果(ビルドの失敗など)を提供します。

注： 高速スキャンは、2021.4.0リリースの限定的なカスタマーアクセス機能です。高速スキャンを使用するには、Synopsysのアカウント管理チームにお問い合わせください。

重複している構成表の検出

Black Duck では重複している構成表の検出が追加されました。これは、新しいパッケージマネージャスキャンが既存の構成表を重複させるかどうかを判断し、重複させる場合はスキャンの処理を停止し、完了として指定します。冗長な(同一の)データを生成する高周波スキャンの場合、Black Duckの重複構成表検出により、パフォーマンスが大幅に向上します。

Black Duck 2021.4.0では、Synopsys Detectによって検出された一連の依存関係が前のスキャンのセットと同一の場合にのみ、この機能がパッケージマネージャ(依存関係)スキャンに影響を与えます。この機能は今後のリリースで拡張される予定です。

プロジェクトマネージャの役割を構成する機能

Black Duck では、システム管理者が、プロジェクトマネージャの役割がポリシー違反を管理できるかどうか(ポリシー違反を上書きするか、上書きを削除するか)、またはプロジェクトのセキュリティ脆弱性を修正できるかどうかを定義できるようになりました。

デフォルトでは、プロジェクトマネージャの役割を持つユーザーは、ポリシー違反を管理し、セキュリティの脆弱性を修正できます。バージョン2021.4.0にアップグレードしたユーザーでは、プロジェクトマネージャの役割に変更はありません。

複数ライセンス編集の機能強化

ナレッジベースまたはカスタムコンポーネントのライセンスを編集するときに、Black Duckでは、ルートレベルまたは元のライセンスと同じレベルでコンポーネントの新しい複数ライセンスシナリオを簡単に作成したり、既存の複数ライセンスシナリオを編集したりすることができるようになりました。

ディープライセンスデータの機能拡張

Black Duckでは、ファイルレベルのディープライセンスを追加したり、手動で追加したライセンスを削除したりできるようになりました。

レポートの機能強化

- コンポーネントプロジェクトバージョンレポート（component_date_time.csv）では、次の機能が強化されています。
  - 新しい列[コンポーネント取得元ID]がレポートの最後に追加されました。この列には、以前はAPIを使用してのみ取得できたコンポーネントの取得元ID値が表示されます。
  - コメント列に一覧表示されている各コメントにユーザー名、日付、および時刻が追加されました。
- アップグレードガイダンスプロジェクトバージョンレポート（project_version_upgrade_guidance_date_time.csv）の最後に、新しい列[ナレッジベースのタイムアウト]が追加されました。コンポーネントのバージョン/取得元のアップグレードガイダンスデータの取得中にBlack Duckナレッジベースでタイムアウトエラーが発生したかどうかを示します。

ポリシー管理の機能強化

- ポリシールールで使用可能なプロジェクトおよびコンポーネントの条件を、容易に見つけて選択できるようにするために、条件がカテゴリに再編成されました。また、プロジェクトとコンポーネントのカスタムフィールドは、カスタムフィールドのタイプによって分離されています。
- 新しいライセンス条件である、宣言済みライセンスまたはディープライセンスの[ライセンスの有効期限の比較]では、ライセンスの有効期限をプロジェクトバージョンのリリース日と比較できます。

脆弱性の影響の機能強化

ポリシールールの新しい脆弱性条件[ソースから到達可能]が利用可能になり、到達可能と識別された脆弱性のポリシールールを作成できるようになりました。この条件を使用して、優先度が異なる（より高い）脆弱性に優先順位を付けます。

LDAPまたはSAMLグループの同期化の変更

認証エラーを減らすために、Black DuckはLDAPまたはSAMLグループの同期化を変更しました。現在は、LDAPまたはSAMLをBlack Duck用に設定するときにグループ同期を有効にした場合、LDAPまたはSAMLサーバー上のグループ名とBlack Duckサーバーが同一である必要があります。Black Duckでグループの名前を変更する場合は、LDAPまたはSAMLサーバー上のグループの名前も変更して、新しい名前に一致させる必要があります（その逆も同様です）。名前が同一でない場合、グループが同期されなくなる可能性があり、そのグループのユーザーの権限が失われます。

コンテナの拡張

Binaryscannerコンテナにヘルスチェックが追加されました。

[ソース]タブの機能強化

新しいフィルタ[コードビュー使用可能]がプロジェクトバージョンの[ソース]タブに追加されました。

コンポーネントおよびプロジェクト検索の機能強化

コンポーネントおよびプロジェクト検索の[検索]ページに、検索結果をソートする機能が追加されました。

保存済み検索の機能強化

ソートされた検索結果は、保存済み検索でサポートされており、ダッシュボードページで関心がある順序で結果を表示できます。

[プロジェクト名]ページのパフォーマンスの向上

パフォーマンスを向上させるには、ポリシー違反アイコン( )または上書きアイコン( )を選択して、[プロジェクト名]ページの[概要]タブにポリシー違反情報を表示する必要があります。

クローンの作成の機能強化

プロジェクトバージョンのクローンの作成に、次の機能強化が行われました。

- デフォルトのクローンの作成オプションが変更されました。これで、プロジェクトの作成時にすべてのクローンの作成オプションが有効になります。
- 新しいオプション[バージョン設定]が追加され、次の値のクローンが作成されます。
  - ライセンス
  - 注記
  - ニックネーム
  - リリース日
  - フェーズ
  - 配布
- [プロジェクト名]ページから[クローン作成]選択すると、新しい[クローンバージョン]ダイアログボックスが表示されます。[バージョン設定]のクローン作成オプションが有効になっている場合は、新しいバージョン名のみがダイアログボックスに表示されます。
- 混乱を避けるため、[クローンを作成するバージョン]フィールドは[新規バージョンを作成]ダイアログボックスから削除されました。

ライセンス競合の機能強化

[ライセンス競合]または[コンポーネント]タブを使用してコンポーネントまたはプロジェクトバージョンのライセンスの使用方法を変更するなど、構成表を手動で編集すると、ライセンス競合が再計算されます。

[システム情報]ページの機能強化

[システム情報]ページの使用カテゴリが拡張されました。

- [使用方法:プロジェクト]セクションで、[プロジェクト別スキャン]セクションに[プロジェクト別上位10スキャン]が表示されるようになりました。
- [使用方法:高速スキャン完了]セクションで、[ユーザー別高速スキャン]に[ユーザー別上位10の高速スキャン]が表示されるようになりました。
- [使用方法:スキャン完了]セクションはテーブルに再フォーマットされ、重複している構成表の検出のための[同一パッケージマネージャ]行が含まれています。次の2つの新しいテーブルも追加されました。[コードの場所概要情報]と[重複構成表情報]です。

これらのページには、6か月のデータ、またはシステムにデータがある月数のいずれか小さい方が表示されます。

新しいジョブCollectScanStatsJobは、[システム情報]ページの[使用方法:スキャン完了]セクションに表示されるスキャン統計情報を収集します。

インストールガイドの削除

「Installing Black Duck Using Kubernetes 」および「Installing Black Duck Using OpenShift」ガイドがドキュメントセットから削除されました。これらのドキュメントには、最新のドキュメントへのリンクのみが含まれていました。これらのリンクは、各PDFのBlack Duckドキュメントページおよびオンラインヘルプのホームページに追加されています。

[プロジェクト名]ページの機能強化

[プロジェクト名]ページが再編成されて強化され、各プロジェクトバージョンの最後のスキャン日が含まれるようになりました。

[ダッシュボード]ページの機能強化

[ダッシュボード]ページのポリシー違反円グラフの「なし」のポリシー違反値は、以前は100%（違反なし）または0%（いくつかの違反）のどちらかを返していましたが、違反の実際の割合を反映するようになりました。

サポートされるブラウザのバージョン

- Safariバージョン14.0.3（15610.4.3.1.7、15610）
- Chromeバージョン90.0.4430.72（公式ビルド）（x86_64）
- Firefoxバージョン88.0（64ビット）
- Microsoft Edgeバージョン90.0.818.41（公式ビルド）（64ビット）

コンテナバージョン

- blackducksoftware/blackduck-postgres：1.0.16
- blackducksoftware/blackduck-authentication:2021.4.0
- blackducksoftware/blackduck-webapp:2021.4.0
- blackducksoftware/blackduck-scan:2021.4.0
- blackducksoftware/blackduck-jobrunner:2021.4.0
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash：1.0.9
- blackducksoftware/blackduck-registration:2021.4.0
- blackducksoftware/blackduck-nginx：1.0.31
- blackducksoftware/blackduck-documentation:2021.4.0
- blackducksoftware/blackduck-upload-cache：1.0.16
- blackducksoftware/blackduck-redis:2021.4.0
- blackducksoftware/blackduck-bomengine:2021.4.0
- sigsynopsys/bdba-worker：2021.03
- blackducksoftware/rabbitmq：1.2.2

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2021.2.0が日本語にローカライズされました。

APIの機能強化

- APIドキュメントでPostmanコレクションを生成する機能を、/api-doc/postman-collection-public.jsonから追加しました。ユーザーは、PostmanコレクションとしてPostmanにpostman-collection-public.jsonファイルをインポートできます。
- /api-doc/openapi3-public.jsonを介してお客様向けエンドポイントのOpenAPI Specification（OAS）を生成する機能を追加しました。

- /api/projects?filter=ownerを使用してプロジェクト所有者別にプロジェクトをフィルタリングする機能を追加しました。この機能はユーザーのURLを取得してユーザーが所有するプロジェクト（例：/api/projects?filter=owner:https://<bd_server>/api/users/）を検索します。
- ライセンス所有権情報を新しい所有権フィールドとして/projects/{projectId}/versions/{projectVersionId}/componentsエンドポイントに追加しました。
- 次のアプリケーション設定を読み取り、変更するためのAPIが追加されました。
  - 分析設定の読み取り

    ```
    GET /api/settings/analysis
    ```
  - 解析設定の読み取り

    ```
    PUT /api/settings/analysis
    ```
  - ブランディング設定の読み取り

    ```
    GET /api/settings/branding
    ```
  - ブランディング設定の更新

    ```
    PUT /api/settings/branding
    ```
  - ライセンスレビュー設定の読み取り

    ```
    GET /api/settings/license-review
    ```
  - ライセンスレビュー設定の更新

    ```
    PUT /api/settings/license-review
    ```
  - 役割設定の読み取り

    ```
    GET /api/settings/role
    ```
  - 役割設定の更新

    ```
    PUT /api/settings/role
    ```
- 特定の日付または特定のコンポーネントに基づいてナレッジベースからコンポーネントの移行データを取得するための/api/component-migrationsおよび/api/component-migrations/{componentOrVersionId}エンドポイントが追加されました。
- /license-dashboardAPを公開し、ユーザーが使用中のライセンスを表示できるようにしました。
- 脆弱性が100を超える参照を持っている場合に、api/vulnerabilities/{vulnerabilityId}エンドポイントがヘッダーオーバーフローエラーを返す問題を解決しました。エンドポイントは警告を表示し、応答ヘッダーで25以上のリンクヘッダーが返されたときに、応答本文にメタリンクを含めます。
- [トリガータイプ]フィルタは[ユーザー]タイプにのみ使用されるため、このフィルタをアクティビティ/ジャーナルエンドポイントから削除しました。

2021.4.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- （Hub-24015、26281）。Black Duckユーザーインターフェイスに表示される断続的なアクセス権限拒否エラーを修正しました。
- （HUB-25116）。UCS-2でエンコードされたファイルの[スニペットビュー]ダイアログボックスに赤いドットが表示され、テキストが読み取れない問題をが修正しました。
- （HUB-25549）。codeLocationNameに日本語の文字が含まれている場合に、作成されたコードの場所がプロジェクトバージョンにマップされなかった/api/uploadsの問題を修正しました。
- （HUB-25550）。プロジェクトバージョンのアクティビティ/ジャーナルに構成表更新日時を追加しました。

- (HUB-25605, 27618)./api/tokens/authenticateを使用してAPIトークンで認証を行う場合の問題を修正しました。この問題では、トークンの期限が切れた後に、HTTPクライアントがSAMLプロバイダページにリダイレクトされるか、PDFレポートの生成中にエラーが発生していました。
- (Hub-25993)。重複したレコードが原因で、Job Runnerログに次のエラーメッセージが表示される問題を修正しました。「A conflicting object already exists」
- (Hub-26481)。新しい修正ステータスを保存した後に、ページが完全に更新される問題を修正しました。
- (HUB-26588)。android-studio-ide-201.7199119-windows.exeでバイナリスキャンを実行できない問題を修正しました。
- (Hub-26695)。一日の特定の時間帯にスキャンにかなり時間がかかる問題を修正しました。
- (Hub-26897)。[コンポーネント名]ページに一覧表示されていない無効なバージョンについて404 Not Foundエラーコードが表示されるように、問題を修正しました。
- (Hub-26911)。代替スニペットマッチを選択したときに、コンポーネントが暗号化されていると誤って識別される問題を修正しました。
- (Hub-27159)。「過去1年間のコントリビュータ」、「過去1年間のコミット」、または「新しいバージョン数」コンポーネント条件を使用するポリシールールの問題を修正しました。これらの条件は、値が0の場合に違反をトリガーするように定義されていますが、値が0より大きい場合、またはコンポーネントにコミット履歴がない場合にポリシー違反がトリガーされました。

  注： この修正により、新しいスキャンまたは再スキャンによって、以前にトリガーされたいくつかのポリシー違反が削除されることがあります。
- (Hub-27167)。グローバルプロジェクトビューアの役割を持つ非アクティブなグループに割り当てられたアクティブなユーザーが、ダッシュボードですべてのプロジェクトを表示できる問題を修正しました。
- (Hub-27175)。[コンポーネント名]ページの[使用数]の値が、コンポーネントのバージョンではなく、コンポーネントの取得元の数に基づいていたために不正確だった問題を修正しました。
- (Hub-27282)。構成表のポリシー違反ポップアップが開いたままになっていることがあり、ページを更新しない限り閉じられない問題を修正しました。
- (Hub-27284、27660)。推移的な依存関係のマッチタイプを持つ一部の動的にリンクされたコンポーネントで、プロジェクトバージョン構成表の[ソース]列にマッチ情報が欠落していた問題を修正しました。
- (Hub-27287)。[プロジェクト名]ページの[概要]タブに表示されるリスク数が、コンポーネント取得元ではなく、コンポーネントのバージョン値を使用するように([構成表]ページと同じように)、問題を修正しました。
- (Hub-27293)。「レビュー済み」とマークされたコンポーネントが、プロジェクトの再スキャン時に「未レビュー」とマークされる問題を修正しました。
- (Hub-27306)。通知レポートでコンポーネントが大文字と小文字を区別する順序で一覧表示トされる問題を修正しました。
- (Hub-27308)。コンポーネントバージョンのライセンスが変更された後に、Black Duck KB [コンポーネント名]ページに脆弱性の数が正しく表示されない問題を修正しました。
- (Hub-27326)。プロジェクト[設定]タブを使用してアプリケーションIDを削除しても、実際にはアプリケーションIDが削除されない問題を修正しました。
- (Hub-27613)。[ソース]タブでバイナリのソースファイルに移動できない問題を修正しました。
- (Hub-27961)。[ダッシュボード]ページのグラフの凡例を修正して、クリック可能な状態で表示されないようにしました。
- (Hub-27982)。バイナリスキャンでMSIアーカイブの最初と最後のファイルのみが識別される問題を修正しました。

- （Hub-27985）。Black Duckが構成表を作成しているときに表示されるメッセージの問題を修正しました。構成表ページを下にスクロールすると表示されなくなります。
- （Hub-28094）。/api/usergroupsエンドポイントが検索語で「_」または「%」を正しく使用しない問題を修正しました。
- （Hub-28165）。構成表ページでライセンスを編集する際に[キャンセル]/[閉じる]を選択しても変更が適用される問題を修正しました。
- （Hub-28208）。[登録]ページに表示されるコードベースサイズが正しくない問題を修正しました。
- （Hub-28226）。1つまたは複数のポリシーに違反しているコンポーネントが、そのコンポーネントが配置されたコードの場所がマップされていないか削除された場合に、「ポリシークリア済み」通知を生成するように問題を修正しました。
- （Hub-28259）。SQLクエリ解析の「未レビュー/無視を解除」に関する問題を修正しました。
- （Hub-28292）。HELM Tシャツのサイズ設定.ymlファイルが構成表エンジンコンテナをスケールしなかった問題を修正しました。
- （Hub-28370）。構成表の比較ビューを使用しているときに重大な脆弱性が表示されなかった問題を修正しました。
- （Hub-28375）。CVEまたはBDBAレコードの[影響を受けるプロジェクト]タブに無視されたコンポーネントの脆弱性が表示されないように、問題を修正しました。
- （Hub-28383）。[プロジェクト名]ページがフィルタにかけられ、結果としてページに1つのバージョンしか表示されない場合、バージョンを削除できなかった問題を修正しました。
- （Hub-28416）。ライセンスのグループのANDまたはOR演算子を変更できない問題を修正しました。
- （Hub-28458）。SnippetScanAutoBomジョブに「Error in job execution：Duplicate key」エラーメッセージが表示される問題を修正しました。
- （Hub-28562）。スキャンが事後処理を完了できず、次のエラーメッセージが表示されるバイナリスキャンの問題を修正しました。「Path is not a parent of null.」
- （Hub-28580）。[マイアクセストークン]ページにアクセスしようとすると、「アプリケーションに不明なエラーが発生しました」というエラーが発生する問題を修正しました。
- （Hub-28639）。プロジェクト名に英語と中国語の両方の文字が含まれている場合、ダウンロードしたレポートファイルのサフィックスに.zipの代わりに.json拡張子が付いていた問題を修正しました。
- （Hub-28681）。マッチタイプが直接または推移的な依存関係である場合に、[ソース]タブに使用状況が表示されるように、問題を修正しました。
- （Hub-28765）。[構成表]ページに確認済みと無視済みの両方のスニペットが表示される問題を修正しました。
- （Hub-28773）。hub-webserver.envファイルのTLS_PROTOCOLSオプションからTLSv1.1が削除されるように、問題を修正しました。

9. Black Duckバージョン2021.2.x

バージョン2021.2.1の新機能および変更された機能

Black Duck バージョン2021.2.1はメンテナンスリリースであり、新機能や変更された機能はありません。

2021.2.1で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- （Hub-23928）。確認済みスニペットマッチが再スキャン後に変更される問題を修正しました。
- （Hub-26898）。スキャンが完了したように見えても、Black Duckからbom_complete通知を取得できなかったためにSynopsys Detectがタイムアウトになる問題を修正しました。
- （Hub-27688）。マッチしたファイルのAPI呼び出しで、推移的な依存関係と直接の依存関係のマッチに関する情報が返されない問題を修正しました。
- （Hub-28410）。KubernetesでRabbitMQコンテナを起動できない問題を修正しました。この問題は永続的ボリュームを導入することで解決されました。
- （Hub-28208、28386）。[製品登録]ページに誤ったコードベースサイズが表示される問題を修正しました。
- （Hub-28278）。RabbitMQコンテナの永続ボリュームが見つからないために構成表エンジンに過剰なログが記録され、スキャンが失敗する問題を修正しました。
- （Hub-28292）。構成表エンジンコンテナのスケーリングに関する問題を修正しました。

バージョン2021.2.0の発表

Azureをご利用のお客様へのお知らせ

Black Duckバージョン2021.2.0は、Azure Kubernetes Services（AKS）で展開し、Azure Database for PostgreSQLを外部データベースとして使用するお客様に影響を与える既知の問題とともにリリースされています。これは、Azureプラットフォーム上のBlack Duckのお客様に推奨される標準構成であることに注意してください。現時点では、外部データベースを備えたAzureプラットフォームで実行しているお客様が2021.2.0にアップグレードすることはお勧めしません。これを行うと、システムが動作不能のままになり、インストールを前の状態に戻すように強制されます。

この問題は今後のBlack Duckリリースで解決される予定であり、リリースの詳細が判明した時点で発表されます。

AKS上で実行しており、内部PostgreSQLデータベースを使用する場合は、問題はなく、システムは期待どおりに動作します。ただし、これは、AKSプラットフォームでの変則的なインストールです。

ご不明な点やご質問がある場合は、Black Duckサポートにお問い合わせください。

外部データベース用のPostgreSQLバージョン9.6のサポート廃止

Synopsysは、Black Duck 2021.6.0リリース以降で、外部データベース用のPostgreSQLバージョン9.6のサポートを廃止する予定です。

Black Duck 2021.6.0リリース以降では、Black Duckは、外部データベース用にPostgreSQLバージョン11.xのみをサポートします。

Internet Explorer 11はサポートされなくなりました

SynopsysはInternet Explorer 11のサポートを終了しました。

廃止されたページ

[スキャン] > [コンポーネント]ページは、2021.2.0リリースで廃止され、今後のリリースでは削除される予定です。

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2020.12.0が日本語にローカライズされました。

バージョン2021.2.0の新機能および変更された機能

新しいカスタム脆弱性ダッシュボード

2021.2.0では、セキュリティダッシュボードが、保存済み脆弱性検索を使用できるカスタム脆弱性ダッシュボードに切り替わり、重要な脆弱性を簡単に表示できるようになりました。Black Duckでは、さまざまな属性を使用してプロジェクトおよび/またはBlack Duckナレッジベース内で使用される脆弱性を検索し、検索を保存してから、この[ダッシュボード]ページを使用して保存済み検索からダッシュボードを表示できるようになりました。

脆弱性ごとに、カスタム脆弱性ダッシュボードに次の情報が表示されます。

- BDSAまたはNVDの脆弱性ID。脆弱性IDを選択すると、追加のスコア値など、脆弱性に関する詳細情報が表示されます。
- この脆弱性の影響を受けるプロジェクトのバージョンの数と、この脆弱性の影響を受けるプロジェクトのバージョンが一覧表示された脆弱性の[影響を受けるプロジェクト]タブを表示するリンク。
- 全体的なリスクスコア。
- ソリューション、回避策、または攻撃が利用可能かどうか。
- 脆弱性が最初に検出、公開、および最終変更された日付。
- このセキュリティ脆弱性の共通脆弱性タイプ一覧（CWE）番号。

脆弱性検索の機能強化

脆弱性の検索は、脆弱性の検索に使用できる属性と、検索結果に表示される情報によって強化されています。プロジェクトの脆弱性を検索するか、Black Duckナレッジベースの脆弱性を検索するかどうかを選択できます。

脆弱性を検索する場合は、次の属性を使用できます。

- 影響を与えるプロジェクト
- デフォルトの修正
- 到達可能
- 悪用
- 最初の検出
- 修正ステータス
- 解決方法
- ベーススコア
- 攻撃される可能性のスコア

- 影響スコア
- 総合スコア
- 公開された年
- 重大度
- ソース（BDSAまたはNVD）
- 一時スコア
- 回避策

これらの脆弱性は、前述のように、検索結果を保存して[ダッシュボード]ページに表示できるようになりました。

プロジェクトのライセンス競合を管理する機能

ライセンス違反のリスクを軽減するため、構成表内のコンポーネントに、プロジェクトの宣言されたライセンスに対して齟齬がある条項を含むライセンスがある場合を理解する必要があります。Black Duckでは、これらのライセンス条項の競合を特定し、それを[法]タブにある新しい[ライセンス競合]に表示するようになりました。

コンポーネントのライセンスがプロジェクトバージョンのライセンスと競合する場合にトリガーされるポリシールールを設定することもできます。

Black Duckは、ライセンスのリスクが高いコンポーネントバージョンのライセンス競合のみを判断することに注意してください。Black Duckライセンスリスクモデルでは、「高リスク」とは、このビジネスシナリオ（配布タイプとコンポーネントの使用法の組み合わせ）の下で、このファミリのライセンスが競合する傾向があることを意味します。中程度または低リスクとは、ビジネスシナリオが変更された場合（または誤って定義された場合）、またはライセンス以外の競合要因が原因でリスクが発生する可能性があることを意味します。

依存関係

Synopsys Detectスキャンで直接的または推移的な依存関係が検出された場合、Black Duckは、プロジェクトバージョンの[セキュリティ]タブで、依存関係の各タイプの一致数を一覧表示するようになりました。

推移的な依存関係の場合、依存関係ツリーには、この依存関係をもたらしたコンポーネント、重大度レベル別の脆弱性、およびその依存関係パスでコンポーネントが導入された回数のマッチ数が表示されます。

レポートデータベースの機能強化

無視されたコンポーネントの新しいテーブル（component_ignored）がレポートデータベースに追加されました。次のカラムがあります。

- id。ID
- project_version_id。プロジェクトバージョンID。
- component_id。コンポーネントID。
- component_version_id。コンポーネントバージョンID。
- component_name。コンポーネント名。
- component_version_name。コンポーネントバージョン名。
- version_origin_id。バージョン取得元ID。
- origin_id。取得元ID。
- origin_name。取得元名。
- ignored。コンポーネントが無視されるかどうかを示すブール値。
- policy_approval_status。ポリシーの承認ステータス。

- review_status。コンポーネントのレビューステータス。
- reviewed_by。コンポーネントをレビューしたユーザー。
- reviewed_on。コンポーネントがレビューされた日時。
- security_critical_count。重要なセキュリティ脆弱性の数。
- security_high_count。高セキュリティ脆弱性の数。
- security_medium_count。中程度のセキュリティ脆弱性の数。
- security_low_count。低セキュリティ脆弱性の数。
- security_ok_count。セキュリティの脆弱性が存在しない数。
- license_high_count。高ライセンスリスクの数。
- license_medium_count。中ライセンスリスクの数。
- license_low_count。低ライセンスリスクの数。
- license_ok_count。ライセンスリスクなしの数。
- operational_high_count。高い運用リスクの数。
- operational_medium_count。中程度の運用リスクの数。
- operational_low_count。低い運用リスクの数。
- operational_ok_count。運用リスクなしの数。

ユーザー情報の新しいテーブル（user）がレポートデータベースに追加されました。次のカラムがあります。

- id。ID。
- first_name。ユーザーの名。
- last_name。ユーザーの姓。
- username。Black Duckのユーザーのユーザー名。
- email。ユーザーの電子メールアドレス。
- active。このユーザーがアクティブかどうかを示すブール値。
- last_login。ユーザーがBlack Duckに最後にログインした時刻。

ライセンス編集の機能強化

構成表でライセンスを編集する際に、次の機能強化が行われました。

- コンポーネントのライセンスを編集するときに、Black Duckでは、ルートレベルまたは元のライセンスと同じレベルで構成表内のコンポーネントの新しい複数ライセンスシナリオを簡単に作成したり、既存の複数ライセンスシナリオを編集したりすることができるようになりました。
- コンポーネントに別のライセンスを選択した場合は、Black Duckナレッジベースで定義されたとおりに、ライセンスを元のライセンスに戻すことができます。
- [<コンポーネント名 バージョン>コンポーネントライセンス]ダイアログボックスの新しいオプションにより、編集モードがあることを容易に識別できます。

レポートの機能強化

source_date_time.csvプロジェクトバージョンレポートの最後に、新しいカラム[アーカイブのコンテキストとパス]が追加されました。このカラムは、既存のパスとアーカイブコンテンツのカラムに表示される情報を連結して、各コンポーネントのフルパスを提供します。

通知ファイルレポート

通知ファイルレポートが改善され、著作権データに単一のコンポーネント取得元の重複情報が含まれなくなりました。

バイナリスキャンの機能拡張

バイナリスキャンでは、完全一致に加えて部分一致が返されるようになりました。

ディープライセンスデータの機能拡張

ファイル内のディープライセンスデータの証拠を確認するときに、Black Duckでは、ライセンステキストの一致をトリガーしたライセンステキストが強調表示されるようになりました。

BOM Engine

Black Duck UIの応答時間を改善するために、ライセンスの更新はBOM Engineによって実行されるようになりました。このプロセスは、構成表からアクセス可能な[構成表処理ステータス]ダイアログボックスで、[ライセンスの更新]または[ライセンス条項の履行の更新]イベントとして表示されます。

Black Duckチュートリアル

Black Duckのトレーニングを簡単に表示するには、Black Duck UIの[ヘルプ]メニュー()から、[Black Duckチュートリアル]を選択します。

パスワードの構成の変更

システム管理者の役割を持つユーザーは、ローカルBlack Duckアカウントのパスワード要件を設定できるようになりました。スーパーユーザーの役割を持つユーザーは、パスワード要件を構成できなくなりました。

ポリシールールの機能強化

ポリシー管理では、ブール値、日付、ドロップダウン、複数選択、単一選択、およびテキストフィールドタイプのプロジェクトバージョンのカスタムフィールドに基づいて、ポリシールールを作成する機能が提供されるようになりました。

ホスティングロケーション: Synopsys Detect

外部接続が制限されているBlack Duckのお客様は、Synopsys Detectの内部ホスティングロケーションを定義できるようになりました。これらのユーザーは、この情報を使用して、Code Sightを利用して開発者ベース全体に展開し、オンデマンドのソフトウェアコンポジション解析(SCA)スキャンを実行できます。

保存済み検索ダッシュボードの機能強化

[ダッシュボード]ページに表示される保存済み検索ごとに、検索が最後に更新された日時がBlack Duckに一覧表示されるようになりました。ポップアップに保存された検索フィルタとリンクが表示されるので、[検索]ページを開いて、改訂された保存済み検索を編集および保存できます。

スニペットのトリアージの機能拡張

未確認スニペット()、確認済みスニペット()、無視されたスニペット()を区別しやすくするために、[ソース]タブにアイコンが追加されました。

サポートされるブラウザのバージョン

- Safariバージョン14.0.3(15610.4.3.1.6, 15610)

- Chromeバージョン88.0.4324.150（公式ビルド）（x86_64）
- Firefoxバージョン85.0.2（64ビット）
- Microsoft Edgeバージョン88.0.705.63（公式ビルド）（64ビット）

コンテナバージョン

- 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

サポートされるDockerのバージョン

Black Duckのインストールでは、Dockerバージョン18.09.x、19.03.x、および20.10.x（CEまたはEE）がサポートされています。

Docker webapp-volume

Docker webapp-volumeは、オーケストレーションでは使用されなくなりました。必要に応じて、ユーザーはDocker webapp-volumeをバックアップおよびプルーニングできます。それ以外の場合は、アクションは必要ありません。

Ubuntuオペレーティングシステム

UbuntuのDocker環境にBlack Duckをインストールするための推奨オペレーティングシステムは、バージョン18.04.xです。

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2020.12.0が日本語にローカライズされました。

APIの機能強化

- APIドキュメントは、https://<Black Duck server URL>/api-doc/public.htmlでのみ入手できるようになりました。
- 作成日でコードの場所（/api/codelocations）をフィルタリングする機能が追加されました。

- 以前のバージョンで正しく動作していなかったSAML IDプロバイダのメタデータXMLファイル（api/sso/idp-metadataエンドポイント）のダウンロードに使用されるAPIを修正しました。
- remediation-guidanceエンドポイント（GET /api/components/{componentId}/versions/{componentVersionId}/remediating）は、「410 GONE」応答を返さなくなりました。upgrade-guidanceエンドポイント（GET /api/components/{componentId}/versions/{componentVersionId}/upgrade-guidance）に切り替える必要があります。このエンドポイントは、削除されたremediation-guidanceエンドポイントと互換性がありません。
- コンポーネントの依存関係パスを表示するために、レポートのdependency-pathsエンドポイントが追加されました。

  /api/project/{projectId}/version/{projectVersionId}/origin/{originId}/dependency-paths
- [システム設定]ページでSynopsys Detect URIの読み取りを設定または更新するためにのみ使用されるSynopsys Detect URIエンドポイントが追加されました。

  /external-config/detect-uri

2021.2.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- （Hub-22103）。ライセンスステータスを更新するときに、Black Duckサーバーが時間内に応答しなかった問題が修正されました。
- （Hub-22623）。UIにロードするときに、概要ダッシュボードが企業顧客に対して頻繁にタイムアウトする問題を修正しました。
- （Hub-24332）。同じコードの場所をスキャンすると通知が重複する問題が修正されました。
- （Hub-25374）。データベースazure_maintenanceの権限エラーを修正しました。
- （Hub-25580）。構成表に表示されているコンポーネントが9ページ以降に正しくソートされない問題を修正しました。
- （Hub-25666）。エンドポイント/usergroups/<group #>/rolesのページネーションの問題を修正しました。
- （Hub-26030）。アクションの実行後に、ダッシュボードのソートオプションがプロジェクト名で保持されない問題を修正しました。
- （Hub-26324）。エラー「java.lang.IllegalStateException: Parent of [file:/C:/src/External/PackageManager/ProjectTemplates/com.unity.template.universal-10.1.0.tgz] does not exist」がスキャンのアップロード時に発生する問題を修正しました。
- （Hub-26343）。登録コンテナのヒープ領域が不足しているため、Black Duckを登録できない問題が修正されました。
- （Hub-26493）。ユーザーがプロジェクトのメンバーとして自分自身を削除したときに表示される紛らわしいエラーメッセージが修正されました。
- （Hub-26501）。[コンポーネントの編集]ダイアログボックスでcordova-plugin-inappbrowserコンポーネントを選択できない問題を修正しました。
- （Hub-26536）。ウォッチするプロジェクトがページヘッダーにウォッチしないアイコン（  ）を表示する問題を修正しました。
- （Hub-26540）。Black Duckを再起動しないとSAMLの初期構成が有効にならないという問題を修正しました。
- （Hub-26615）。プロジェクトAでプロジェクトマネージャの役割を持ち、プロジェクトBでプロジェクトマネージャとプロジェクトコードスキャナの役割を持つユーザーが、スキャンをプロジェクトAにアップロードできるという問題が修正されました。

- （Hub-26616）。スニペットを無視しようとすると、次のエラーメッセージで失敗する問題が修正されました。「コンシューマ、プロデューサー、調整タイプ、開始行、終了行の変更がサポートされていないため、既存のスニペット調整を更新できません。」
- （Hub-26712、26962）。スニペットマッチが確認された後、[ソース]タブのツリービューに表示されるスニペットアイコンがクリアされない問題を修正しました。
- （Hub-26726）。ポリシールールを作成するときに、カスタムフィールドで「not in」オプションを使用できない問題が修正されました。
- （Hub-26807）。構成表コンポーネントバージョンのカスタムフィールドを取得しようとしたときに、HTMLステータスコード404を受信する問題が修正されました。
- （Hub-26815）。SAML統合設定を保存するとページが再ロードされ、IDプロバイダのメタデータ設定が切り替わる問題が修正されました。
- （Hub-26904）。[設定]タブのプロジェクトバージョンの[アクティビティ]セクションに表示されるマッチ数値が[スキャン名]ページと異なる問題が修正されました。
- （Hub-26930）。コンポーネントの通知がトリガーされない問題を修正しました。
- （Hub-27002）。クローン作成されたプロジェクトが作成されたときに誤った通知が送信される問題を修正しました。
- （Hub-27049）。ユーザーにライセンスマネージャの役割が割り当てられていないと、プロジェクトバージョンレポートのライセンス条項カテゴリが、Black Duck UIに表示されないという問題が修正されました。
- （Hub-27208）。SAMLの構成時にSynopsys Alertの読み込みに失敗するblackduck-nginxの問題を修正しました。
- （Hub-27227）。スニペットのマッチングが完了するまでに時間がかかる問題を修正しました。
- （Hub-27264）。コンポーネントを確認すると、その使用状況がデフォルト値にリセットされる問題が修正されました。
- （Hub-27681）。カスタムセキュリティコンテキストを使用してKubernetesに展開するときに、ルートユーザーがBOM Engineを起動する必要がある問題を修正しました。

10. Black Duckバージョン2020.12.x

バージョン2020.12.0の発表

新しいコンテナとシステム要件の変更

新しいコンテナが2つ追加されています。2020.12.0リリース向けのBOM EngineおよびRabbitMQ（今後は必須コンテナ）です。

すべてのコンテナの単一インスタンスを実行するための最小システム要件は次のとおりです。

- 6 CPU
- Redisの最小構成の場合は26 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は29 GB RAM
- データベースおよびその他のBlack Duckコンテナ用に250 GBの空きディスク容量
- データベースバックアップに適した容量

Black Duck – Binary AnalysisでBlack Duckを実行するために必要な最小ハードウェアは次のとおりです。

- 7 CPU
- Redisの最小構成の場合は30 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は33 GB RAM
- データベースおよびその他のBlack Duckコンテナ用に350 GBの空きディスク容量
- データベースバックアップに適した容量

注： binaryscannerコンテナを1個追加するごとに、1 CPU、2 GB RAM、100 GBの空きディスク容量の追加が必要になります。

Internet Explorer 11のサポートの終了

Internet Explorer 11のサポートは廃止されます。Synopsysは、Black Duck 2021.2.0 リリース以降でのInternet Explorer 11のサポートを終了します。

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2020.10.0が日本語にローカライズされました。

バージョン2020.12.0の新機能および変更された機能

新しいコンテナとシステム要件の変更

新しいコンテナが2つ追加されています。2020.12.0リリース向けのBOM EngineおよびRabbitMQ（今後は必須コンテナ）です。

すべてのコンテナの単一インスタンスを実行するための最小システム要件は次のとおりです。

- 6 CPU
- Redisの最小構成の場合は26 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は29 GB RAM

- データベースおよびその他のBlack Duckコンテナ用に250 GBの空きディスク容量
- データベースバックアップに適した容量

Black Duck – Binary AnalysisでBlack Duckを実行するために必要な最小ハードウェアは次のとおりです。

- 7 CPU
- Redisの最小構成の場合は30 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は33 GB RAM
- データベースおよびその他のBlack Duckコンテナ用に350 GBの空きディスク容量
- データベースバックアップに適した容量

注： binaryscannerコンテナを1個追加するごとに、1 CPU、2 GB RAM、100 GBの空きディスク容量の追加が必要になります。

パスワードの構成

スーパーユーザーの役割を持つユーザーが、ローカルBlack Duckアカウントのパスワード要件を設定できるようになりました。有効にすると、新しいパスワードがお客様の要件を満たしていることが、Black Duckにより確認されます。また、脆弱と見なされるパスワード(「password」、「blackduck」、ユーザーのユーザー名や電子メールアドレスなど)は拒否されます。

スーパーユーザーは次の操作を実行できます。

- 最小パスワード長を定義します。
- パスワードの最小文字種数を定義します。使用可能な文字種は、小文字、大文字、数字、特殊文字です。
- 現在のユーザーがBlack Duckにログインするときにパスワード要件を適用するかどうかを選択します。

デフォルトでは、パスワード要件は有効で、次のように設定されています。

- 最小パスワード長は8文字です。
- 必要な文字種は1つだけです。
- Black Duckにログインしている現在のユーザーにはパスワード要件が適用されません。

ライセンスの機能強化

ライセンスリスクを適切に管理できるように、Black Duckでは、構成表のコンポーネントについてマルチライセンスシナリオを新規に作成したり既存のものを編集したりできるようになりました。

脆弱性の影響解析の機能強化

- 新しいプロジェクトバージョンレポートvulnerability_matches_date_time.csvが追加されました。脆弱性によって到達される可能性のあるコンポーネントごとに、コンポーネント、脆弱性データ、および脆弱性の影響解析データが一覧表示されます。このレポートには、次のカラムがあります。
  - コンポーネント名
  - コンポーネントID
  - 使用中
  - コンポーネントバージョン名
  - バージョンID
  - チャネルバージョン取得元
  - 取得元ID
  - 取得元名ID
  - 脆弱性ID
  - 脆弱性ソース
  - CVSSバージョン
  - セキュリティ上のリスク
  - ベーススコア
  - 総合スコア
  - ソリューションが利用可能
  - 回避策が利用可能
  - 攻撃が利用可能
  - 呼び出された関数
  - 修飾名
  - 行番号
- 新しいテーブルとして、脆弱性メソッドマッチ（vulnerability_method_matches）がレポートデータベースに追加されました。次のカラムがあります。
  - id。ID。
  - project_version_id。到達可能な脆弱性があるプロジェクトバージョンのUUID。
  - vuln_source。脆弱性のソース。脆弱性の影響解析の場合、値はBDSAです。
  - vuln_id。脆弱性ID（BDSA-2020-1234など）。
  - qualified_name。関数が呼び出されるクラスの名前。
  - called_function。コード内で脆弱性を到達可能にする脆弱な関数呼び出しの名前。
  - line_number。コード内で脆弱な関数が呼び出される行番号。
- 脆弱性レポート（脆弱性修正レポート、脆弱性ステータスレポート、および脆弱性更新レポート）には、セキュリティ脆弱性が到達可能か（真）、または到達不能か（偽）を示すために、レポートの末尾に[到達可能]という新しいカラムが追加されました。

構成表の計算情報

Black Duckでは、プロジェクトバージョン構成表の計算ステータスに関する詳細情報が提供されるようになりました。

Black Duck UIのプロジェクトバージョンヘッダーにある新しい[ステータス]インジケータ([コンポーネント]インジケータに代わるもの)は、構成表の現在のステータスを示し、構成表イベントの処理の状態を通知します。更なる情報として、新しい[構成表処理ステータス]ダイアログボックスに、保留中、処理中、または失敗したイベントが表示されます。

また、Black Duckでは、構成表イベントクリーンアップジョブ(VersionBomEventCleanupJob)の頻度も構成できます。このジョブは、処理エラーまたはトポロジ変更によってスタックした可能性のある構成表イベントをクリアします。

ポリシーの機能強化

- ポリシー管理では、次のカスタムフィールドに基づいてポリシールールを作成する機能が提供されます。
  - ブール、日付、ドロップダウン、複数選択、単一選択、テキストの各フィールドタイプ用のコンポーネントカスタムフィールド。
  - ブール、日付、ドロップダウン、複数選択、単一選択、テキストの各フィールドタイプ用のコンポーネントバージョンカスタムフィールド。
- これらの条件のポリシールールを作成する際に、宣言されたライセンスデータとディープ(埋め込み)ライセンスデータを区別できるようになりました。
  - ライセンス
  - ライセンスの有効期限
  - ライセンスファミリ

  注:
  これらのライセンス条件を使用する既存のポリシールールは、宣言されたライセンスにのみ適用されるようになりました。これらのライセンス条件に対しては、ディープ(埋め込み)ライセンス用に、個別のポリシールールを作成する必要があります。

レポートの機能強化

以前はグローバルレベルまたはプロジェクトレベルでのみ利用可能だった脆弱性レポート(脆弱性修正レポート、脆弱性ステータスレポート、および脆弱性更新レポート)が、プロジェクトバージョンで利用できるようになりました。

スニペットファイルサイズの構成

スニペットでスキャンされるデフォルトの最大ファイルサイズが変更可能になり、1 MBから16 MBまでの値を選択できるようになりました。

マップされていないコードの場所のクリーンアップ構成

Black Duckでは、マップされていないコードの場所データを365日ごとにパージします。この機能を無効にして、マップされていないコードの場所データがパージされないようにすることができます。また、定期的にスキャンしてデータを頻繁に破棄するために、保持期間の日数をより短く設定することもできます。

アクセストークン

ユーザーアクセストークンのスコープのオプションは、読み取りまたは読み書きになりました。

サポートされるブラウザのバージョン

- Safariバージョン14.0.1(14610.2.11.51.10)
- Chromeバージョン87.0.4280.88(公式ビルド)(x86_64)

- Firefox 83.0（64ビット）
- Internet Explorer 11 11.630.19041.0

  Internet Explorer 11のサポートは廃止されます。Synopsysは、Black Duck 2021.2.0 リリース以降でのInternet Explorer 11のサポートを終了します。
- Microsoft Edge 87.0.664.60（公式ビルド）（64ビット）

コンテナバージョン

- 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

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2020.10.0が日本語にローカライズされました。

APIの機能強化

- createdAtフィールドでプロジェクト（api/projects）を並べ替える機能が追加されました。
- ある日付の前後に作成されたプロジェクトのapi/projectsエンドポイントにフィルタを適用する機能が追加されました。
- 脆弱性の影響解析機能の一部として、脆弱性マッチを表示するAPIが追加されました。

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

- 次の構成表エンドポイントが追加されました。
  - 構成表ステータス概要の取得:

    GET /api/projects/{projectId}/versions/{projectVersionId}/bom-status
  - 構成表のイベントのリスト:

    GET /api/projects/{projectId}/versions/{projectVersionId}/bom-events
  - 失敗した構成表イベントの削除:

    DELETE /api/projects/{projectId}/versions/{projectVersionId}/bom-events/{bomEventId}
  - 失敗したすべてのイベントの構成表からの削除:

    DELETE /api/projects/{projectId}/versions/{projectVersionId}/bom-events
- 新しいパスワード設定エンドポイント:
  - パスワード設定の取得:

    GET /api/password/security/settings
  - システムパスワード設定の取得:

    GET /api/password/management/settings
  - システムパスワード設定の更新:

    PUT /api/password/management/settings
  - パスワードの検証:

    POST /api/password/security/validate
- /api/catalog-risk-profile-dashboard APIは、HTTP 404（Not Found）を返すようになりました。

2020.12.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- （Hub-24839）。[コンポーネントの追加/編集]ダイアログボックスで一部のコンポーネントのオリジナルIDを選択できなかった問題を修正しました。
- （Hub-24911）。KBUpdateJobが失敗してコンポーネントの更新がスキップされる問題を修正しました。
- （Hub-25230）。ユーザーがライセンステキストを開いたり編集したりする際に、ライセンステキストウィンドウが表示されない問題を修正しました。
- （Hub-25452）。[ソース]タブでライセンス検索結果ページを表示する際にライセンスタイプを選択すると、[検出タイプ]フィルタが自動的に追加される問題を修正しました。
- （Hub-25489）。サブフォルダが変更されたときに[ソース]タブのフィルタがリセットされる問題を修正しました。
- （Hub-25603）。別のパスを選択したときに、[スニペットビュー]ダイアログボックスの[ソース]タブにある[マッチしたファイルパス]フィールドに表示されるパスが更新されるように、問題を修正しました。
- （Hub-25681）。汎用/未指定コンポーネントバージョンのライセンスをProtex BOMツールでインポートできない問題を修正しました。
- （Hub-25715）。マウスを使用しない限り、[カスタムフィールドの管理]ページの[アクティブ]ステータスを変更できない問題を修正しました。
- （Hub-25739）。構成表コンポーネントのすべてのコメントを表示できない問題を修正しました。
- （Hub-25874）。データが同じカラム名にあるにもかかわらず、bom_component_custom_fields_date_time.csvレポートにcomponents_date_time.csvレポートと異なるデータがリストされる問題を修正しました。

- （Hub-26442）。プロジェクト所有者がスキャンをプロジェクトバージョン内から削除できない問題を修正しました。
- （Hub-26496）。コンポーネントの使用法が変更されたときにライセンスリスクが変更されたにもかかわらず、ライセンスリスクに対するポリシー違反が引き続きトリガーされる問題を修正しました。

11. Black Duckバージョン2020.10.x

バージョン2020.10.1の新機能および変更された機能

コンテナバージョン

- 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

2020.10.1で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (Hub-25489)。別のフォルダを選択したときに[ソース]タブで選択されているフィルタがリセットされる問題を修正しました。
- (Hub-25515)。ホストインスタンスでTLS 1.3が動作している場合に、アップロード時に署名スキャナが失敗し、エラーメッセージ「エラー:ホストへの接続を保護できません」が表示される問題を修正しました。
- (Hub-25791)。バージョン2020.4.2からバージョン2020.6.1/2020.6.2にアップグレードした後に、スキャンにかかる時間が大幅に増加する問題を修正しました。
- (Hub-26027)。エラーメッセージ「エラー:アプリケーションに不明なエラーが発生しました。(正しくないリクエスト)エラー。error.{core.rest.common_error」が、Synopsys Detectスキャンのアップロード時にBlack Duckに表示される問題を修正しました。
- (Hub-26085)。バイナリスキャンで2番目の空のスキャンが追加される問題を修正しました。

バージョン2020.10.0の発表

2020.12.0リリースまで延期された新しいコンテナとシステム要件の変更

以前にBlack Duckは、2020.10.0リリース向けに、BOM EngineおよびRabbitMQ（現在は必須コンテナ）という2つのコンテナが追加されると発表しました。この要件は、2020.12.0リリースに延期されました。

2020.12.0リリースでは、すべてのコンテナの単一インスタンスを実行するための最小システム要件は次のようになります。

- 6 CPU
- Redisの最小構成の場合は26 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は29 GB RAM
- データベースおよびその他のBlack Duckコンテナ用に250 GBの空きディスク容量
- データベースバックアップに適した容量

2020.12.0リリースでは、Black Duck – Binary AnalysisでBlack Duckを実行するために必要とされる最小ハードウェアは次のようになります。

- 7 CPU
- Redisの最小構成の場合は30 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は33 GB RAM
- データベースおよびその他のBlack Duckコンテナ用に350 GBの空きディスク容量
- データベースバックアップに適した容量

注： binaryscannerコンテナを1個追加するごとに、1 CPU、2 GB RAM、100 GBの空きディスク容量の追加が必要になります。

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2020.8.0が日本語にローカライズされました。

バージョン2020.10.0の新機能および変更された機能

新しいカスタムコンポーネントダッシュボード

2020.10.0では、コンポーネントダッシュボードが、保存済みコンポーネント検索を使用できるカスタムコンポーネントダッシュボードに切り替わり、重要なコンポーネントバージョンを簡単に表示できるようになりました。Black Duckでは、さまざまな属性を使用してプロジェクト内で使用されるコンポーネントを検索し、検索を保存してから、この[ダッシュボード]ページを使用して保存済み検索からダッシュボードを表示できるようになりました。

カスタムコンポーネントダッシュボードでは、コンポーネントバージョンごとに次の情報が表示されます。

- 当該コンポーネントバージョンを使用しているプロジェクトバージョンの数、および各プロジェクトバージョンのフェーズ、ライセンス、レビューステータス、セキュリティ上のリスク
- リスクカテゴリ別の脆弱性の数
- ライセンスおよび運用上のリスク
- ポリシー違反
- 承認済みステータス

- 当該コンポーネントバージョンが最初に検出された日付
- Black Duckナレッジベースに基づく、コンポーネントがリリースされた日付
- 新しいバージョンの数
- このコンポーネントの脆弱性が最後に更新された日時

コンポーネント検索およびBlack Duckナレッジベース検索の機能強化

コンポーネントの検索は、コンポーネントの検索に使用できる属性と、検索結果に表示される情報によって強化されています。プロジェクトで使用されるコンポーネント検索とBlack Duckナレッジベースでのコンポーネント検索を簡単に区別できるように、UIも機能強化されました。

Black Duckナレッジベース検索の検索属性は変更されていませんが、Black Duckプロジェクトで使用されているコンポーネントバージョンを検索する場合に、次の属性を使用できます。

- セキュリティ上のリスク
- ライセンスリスク
- 運用上のリスク
- ポリシールール
- ポリシー違反の重大度
- レビューステータス
- コンポーネントの承認済みステータス
- 最初の検出
- ライセンスファミリ
- カスタムフィールドデータがない
- リリース日
- ライセンス
- 脆弱性CWE
- 脆弱性報告日

検索条件に一致するコンポーネントバージョンごとに、次の情報が表示されます。

- 当該コンポーネントバージョンを使用しているプロジェクトバージョンの数、および各プロジェクトバージョンのフェーズ、ライセンス、レビューステータス、セキュリティ上のリスク
- リスクカテゴリ別の脆弱性の数
- ライセンスおよび運用上のリスク
- ポリシー違反
- 承認済みステータス
- 当該コンポーネントバージョンが最初に検出された日付
- Black Duckナレッジベースに基づく、コンポーネントがリリースされた日付
- 新しいバージョンの数
- このコンポーネントの脆弱性が最後に更新された日時

これらのコンポーネントは、前述のように、検索結果を保存して[ダッシュボード]ページに表示できるようになりました。

ナレッジベースコンポーネント検索結果ごとに、次の情報が表示されます。

- 当該コンポーネントを使用しているプロジェクトバージョンの数、各プロジェクトバージョンのリスト、フェーズ、使用されているコンポーネントバージョン、関連するセキュリティ上のリスク
- コミットアクティビティ推移
- 最終コミット日
- コンポーネントバージョンの数
- このコンポーネントのタグ

保存済み検索の機能強化

Black Duckの[ダッシュボード]ページでは、保存済み検索をフィルタにかけたり並べ替えたりできるようになりました。

ライセンスの競合

2020.10.0リリースでは、齟齬があるカスタムライセンス条項を指定できるようになりました。Black Duckナレッジベース条項またはユーザーのカスタムライセンス条項と競合している禁止/必須アクションに対しては、カスタムのライセンス条項を定義できます。

注： 現在、プロジェクトバージョン構成表では、齟齬があるライセンス条項を表示することはできません。この機能は、将来のBlack Duckリリースで利用可能になる予定です。

ライセンス管理の機能強化

次の新しい3つのフィルタが、[ライセンス管理]の[ライセンス条項]タブに追加されました。

- ライセンスに関連付けられている
- 齟齬がある条項が含まれている
- 責任

新しいコンポーネントの使用状況

Black Duckは、コンポーネントの使用状況を調べる必要があることを示すためにユーザーが使用できる使用法[未指定]を追加しました。[動的にリンク]などの既存のデフォルト値の代わりに、この使用法をデフォルト値として使用すると便利な場合があります。この場合、コンポーネントに正しい使用法値またはデフォルト値が割り当てられているかどうかの混乱が解消されます。

新しい階層

Black Duckは、最重要階層として指定できる階層0を追加しました。

この新しい階層により、次のデフォルトポリシールールが階層0を含むように変更されました。

- 脆弱性が高1よりも大きい外部階層0、階層1、または階層2プロジェクトなし
- 脆弱性が中3よりも大きい外部階層0、階層1、または階層2プロジェクトなし

既存の階層に変更はありません。

カスタムフィールドの機能強化

カスタムフィールドに対して、次の機能拡張が行われました

- Black Duck で、カスタムフィールドが必須であることを示す機能が追加されました。
  - カスタムフィールド情報を表示すると、警告メッセージ「*その他のフィールドは必須です」が表示されます。ただし、必須のカスタムフィールドにデータが入力されていない場合でも、ユーザーは、カスタム以外のフィールド情報と必須以外のカスタムフィールドの情報をページで表示したり保存したりできます。
  - 情報が欠落しているプロジェクトバージョン構成表内のコンポーネントを表示できるように、新しいフィルタ[カスタムフィールドデータがない]が構成表に追加されました。
- ブール型や単一選択フィールドタイプで、カスタムフィールド情報を表示する際にも、選択を解除できるオプションが追加されました。

許可された署名リスト

スキャンしたコードに含まれるオープンソースソフトウェアを判定するために、署名リストで、Black DuckがBlack Duckナレッジベースウェブサービスに送信する署名を定義します。署名スキャナ に、新しい2つのパラメータが追加されました。このパラメータを使用して、バイナリファイル拡張子またはソースファイル拡張子の許可された署名リストを作成できます。各リストはオプションであり、他のリストとは独立して動作します。

- --BinaryAllowedList x, y, x（x、y、zは、SHA-1（バイナリ）ファイルの承認済みファイル拡張子です）
- --SourceAllowedList a, b, c（a、b、cは、クリーンなSHA-1（ソースコード）ファイルの承認済みファイル拡張子です）

脆弱性の影響解析の機能強化

脆弱性の影響解析に対して、次の機能強化が行われました。

- セキュリティ脆弱性が到達可能（真）であるか到達不能（偽）であるかを示すために、security_date_time.csvプロジェクトバージョンレポートの最後に新しい列[到達可能]が追加されました。
- 新しいフィルタ[到達可能]がプロジェクトバージョンの[セキュリティ]タブに追加されました。

レポートの機能強化

次のレポート機能が強化されました。

- components_date_time.csvプロジェクトバージョンレポートの最後に新しい列[コメント]が追加され、各コンポーネントのコメントが一覧表示されるようになりました。
- マッチタイプを判定するために、vulnerability-status-report_date_time.csvレポートの最後に新しい列[マッチタイプ]が追加されました。

レポートデータベースの機能強化

次のカラムがコンポーネントマッチ表（component_matches）に追加されました。

- match_confidence。スニペット、バイナリ、または部分的なファイルマッチを除いたうえで、マッチの信頼性を表します。
- match_archive_context。プロジェクトのルートディレクトリを基準とした、アーカイブ済みファイルへのローカルパスです。
- snippet_confirmation_status。スニペットマッチのステータスをレビューします。

HTTP/2およびTLS 1.3

ブラウザに表示されるBlack Duck UIのセキュリティとレンダリングを改善するために、Black Duckは、Black Duck NGINXウェブサーバーでHTTP/2およびTLS 1.3をサポートするようになりました。Black Duck NGINXウェブサーバーは、HTTP/1.1およびTLS 1.2も引き続きサポートします。

スキャンパージのためのジョブに対する変更

BomVulnerabilityNotificationJobとLicenseTermFulfillmentJobでも、古い監査イベントが削除されました。

サポートされるブラウザのバージョン

- Safariバージョン13.1.2（14609.3.5.1.5）
- Chromeバージョン86.0.4240.80
- Firefox 82（64ビット）
- Internet Explorer 11.572.19041.0

  Internet Explorer 11のサポートは廃止されます。Synopsysは、Black Duck 2021.2.0 リリース以降でのInternet Explorer 11のサポートを終了します。
- Microsoft Edge 86.0.622.51（公式ビルド）（64ビット）

コンテナバージョン

- 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

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2020.8.0が日本語にローカライズされました。

APIの機能強化

- Black Duckのシングルサインオン（SSO）ステータスを確認するためのエンドポイントが追加されました。

  GET /api/sso/status

- SAML/LDAP構成を取得するためのエンドポイントが追加されました（管理者専用）。
  - SSO構成の読み取り：

    GET /api/sso/configuration
  - IDPメタデータファイルのダウンロード：

    GET /api/sso/idp-metadata
  - また以下のSSOエンドポイントも追加されました。
    - SSO構成の更新：

      POST /api/sso/configuration
    - IDPメタデータファイルのアップロード：

      POST /api/sso/idp-metadata
- 次の構成表階層型コンポーネントエンドポイントが追加されました。
  - 階層型ルートコンポーネントのリスト：

    GET /api/projects/{projectId}/versions/{projectVersionId}/hierarchical-components
  - 階層型子コンポーネントのリスト：

    GET /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/hierarchical-components/{hierarchicalId}/children
  - 階層型子コンポーネントバージョンのリスト：

    GET/api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/hierarchical-components/{hierarchicalId}/children
- 脆弱性の通知APIに新しいフィールドが追加され、通知をさらに分類できるようになりました。これらの通知には、構成表で変更された脆弱性情報が含まれ、次のフィールドが含まれます。
  - vulnerabilityNotificationCause

    発生し、通知をトリガーした脆弱性イベントの種類についての情報。脆弱性の追加/削除、コメントの変更、修正の詳細の変更、脆弱性の重大度の変更、ステータスの変更などです。
  - eventSource

    通知を生成したソースの情報。スキャン、Black Duck KB更新、ユーザーアクション（修正、優先順位の変更、調整）などです。
- /api/catalog-risk-profile-dashboard APIは、HTTP 410（GONE）を返すようになりました。

2020.10.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- （Hub-20559、22100）。異なるルートディレクトリから同じコードの場所をスキャンしたとき、またはプロジェクトバージョンを複製したときに、スニペットの調整が失われていた問題を修正しました。
- （Hub-21421）。大規模プロジェクトで印刷機能が動作しない問題を修正しました。
- （Hub-23705、25560）。ユーザーが作成したレポートをユーザーが削除できなかった問題を修正しました。
- （Hub-23709）。スキャン時に次のscan.cli.sh警告メッセージが表示されていた問題を修正しました。「すべてのマニフェストからマニフェストを検出できません」
- （Hub-24330）。ProtexプロジェクトをBlack Duckバージョン2019.10.3にインポートしようとすると、エラーメッセージ「キー値の重複は一意の制約に違反しています」が表示されていましたが、この問題を修正しました。

- （Hub-24673）。コンポーネント数が32,000を超えていると、[ダッシュボード]ページから移動するときに失敗する問題を修正しました。
- （Hub-24675）。root_bom_consumer_node_idが正しく設定されていなかった問題を修正しました。
- （Hub-24871）。リリース2019.10.0以降のPostgreSQLデータベースの拡張に関する問題を修正しました。
- （Hub-24772）。構成表印刷時のデフォルト.pdfファイル名がプロジェクト名とバージョン名でなかった問題を修正しました。
- （Hub-24839）。[コンポーネントの追加/編集]ダイアログボックスで一部のコンポーネントのオリジナルIDを選択できなかった問題を修正しました。
- （Hub-24947）。構成表にプロジェクトを追加した際に、検索結果の表示で一貫性が損なわれていた問題を修正しました。
- （Hub-25171）。APIを使用して修正した場合に、再スキャン（PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/origins/{originId}/vulnerabilities/{vulnerabilityId}/remediation）するまで、脆弱性の件数が更新されなかった問題を修正しました。
- （Hub-25219）。APIを使用してレポートを作成する際の問題（localeに指定したja_JPが無視されるなど、locale指定時の問題）を修正しました。生成レポートの言語は、localeフィールドで正しく設定されるようになりました。
- （Hub-25234）。構成表を印刷する[印刷]ボタンに、バーグラフのカウントが表示されないことがあった問題を修正しました。
- （Hub-25240）。ブラウザまたはAPIが特定の脆弱性（BDSA-2020-1674）の呼び出しで失敗していた問題を修正しました。
- （Hub-25241）。VersionBomComputationJobが次のエラーメッセージでスキャンに失敗する問題を修正しました。「データ整合性違反（Constraint:not_null, Detail: on column source_start_lines）」。
- （Hub-25244）。Black Duckリリース2020.4.2にアップグレードした後に、手動で追加したコンポーネントが構成表から削除されていた問題を修正しました。
- （Hub-25247）。Black Duck PostgreSQLログに、次のエラーメッセージが表示されていた問題を修正しました。エラー：キー値の重複は一意の制約「scan_component_scan_id_bdio_node_id_key」に違反しています。
- （Hub-25321）。構成表ページをスクロールすると、テキストを表示すべきでないページ領域にテキストが表示されていた問題を修正しました。
- （Hub-25324）。[スキャン名]ページで、ワードラップが行われなかった問題を修正しました。
- （Hub-25478）。[セキュリティ]ページのセキュリティリスクフィルタが表示されなかった問題を修正しました。
- （Hub-25508）。以前のメディアタイプ（v4およびv5）がポリシールールAPI（GET /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/policy-rules）に対して機能しないことがあった問題を修正しました。
- （Hub-25522、25523）。Chrome for Black Duckバージョン2020.8.0の構成表印刷プレビューウィンドウで発生していた表示形式の問題を修正しました。
- （Hub-25548）。階層ビューで新しいコンポーネントマッチを選択しても、ソースビューのコンポーネントマッチが更新されなかった問題を修正しました。
- （Hub-25570）。[セキュリティダッシュボード]ページで一部の領域が読み込まれなかった問題を修正しました。
- （Hub-25608）。脆弱性更新レポートの[新しい脆弱性]および[新たに修正された脆弱性]カテゴリで、脆弱性が2回カウントされていた問題を修正しました。
- （Hub-25649）。[ダッシュボード]ページのポリシー違反ポップアップウィンドウが閉じなかった問題を修正しました。
- （Hub-25841）。テキストデータ型のカスタムフィールドに入力した数値が日付形式に変換されていた問題を修正しました。

12. 既知の問題と制限事項

Black Duckの既知の問題と制限事項は次のとおりです。

新しい既知の問題

·

現在の既知の問題と制限事項

- ユーザーの認証にLDAPディレクトリサーバーを使用している場合は、次の点を考慮してください。
  - Black Duck は、単一のLDAPサーバーをサポートしています。複数のサーバーはサポートされていません。
  - ユーザーがディレクトリサーバーから削除されても、Black Duckユーザーアカウントはアクティブと表示され続けます。ただし、認証情報は有効ではなくなり、ログインに使用できません。
  - グループがディレクトリサーバーから削除されても、Black Duckグループは削除されません。グループは手動で削除してください。
- タグ付けでは、文字、数字、プラス(+)および下線(_)のみがサポートされています。
- Black Duckがユーザーを認証している場合、ログイン中にユーザー名の大文字と小文字は区別されません。LDAPユーザー認証が有効になっている場合、ユーザー名の大文字と小文字は区別されます。
- コードの場所に大規模な構成表がある場合、コードの場所を削除すると、ユーザーインターフェイスのタイムアウトエラーで失敗することがあります。