




リリースノート

バージョン2021.8.0



このエディションの『リリースノート』は、バージョンBlack Duckの2021.8.0を対象としています。

本ドキュメントは2022年4月29日に作成または更新されました。

コメントおよび提案については、次の宛先までお送りください。

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

Copyright © 2021 by Synopsys.

All rights reserved.本ドキュメントの使用はすべて、Black Duck Software, Inc.とライセンス所有者の間の使用許諾契約に準拠します。本ドキュメントのいかなる部分も、Black Duck Software, Inc.の書面による許諾を受けることなく、どのような形態または手段によっても、複製または譲渡することが禁じられています。

Black Duck、Know Your Code、およびBlack Duckロゴは、米国およびその他の国におけるBlack Duck Software, Inc.の登録商標です。Black Duck Code Center、Black Duck Code Sight、Black Duck Hub、Black Duck Protex、およびBlack Duck Suiteは、Black Duck Software, Inc.の商標です。他の商標および登録商標はすべてそれぞれの所有者が保有しています。

CH: 章1: 製品発表	1
バージョン2021.8.0の発表	1
Black Duck 2021.8.0リリースに必要なDetect 7.4	1
CentOS-7上のDesktop Scanner	1
日本語	1
簡体字中国語	1
廃止されたAPI	1
バージョン2021.6.0の発表	2
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	2
廃止されたページ	2
廃止されたAPI	2
日本語	2
バージョン2021.4.0の発表	2
新しいコンテナとシステム要件の変更	2
マップされていないコードの場所の保存期間	3
廃止されたAPI	3
2021.6.0リリースでの新しいジョブ実装	3
日本語	4
バージョン2021.2.0の発表	4
Azureをご利用のお客様へのお知らせ	4
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	4
Internet Explorer 11はサポートされなくなりました	4
廃止されたページ	4
日本語	4
バージョン2020.12.0の発表	5
新しいコンテナとシステム要件の変更	5
Internet Explorer 11のサポートの終了	5
日本語	5
バージョン2020.10.0の発表	5
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	5
日本語	6
バージョン2020.8.0の発表	6
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	6

2020.10.0リリースで廃止されたAPI	6
日本語	6
バージョン2020.6.1の発表	6
Internet Explorer 11のサポートの終了	6
バージョン2020.6.0の発表	7
今後のリリースでの新しいコンテナとシステム要件の変更	7
Internet Explorer 11のサポートの廃止	8
PostgreSQL 11の外部データベースのサポート	8
バージョン2020.2.0の発表	8
個別のファイルマッチ	8
Docker Composeのサポート	8
CH: 章2: リリース情報	9
バージョン2021.8.0	9
バージョン2021.8.0の新機能および変更された機能	9
2021.8.0で修正された問題	13
バージョン2021.6.2	14
バージョン2021.6.2の新機能および変更された機能	14
2021.6.2で修正された問題	15
バージョン2021.6.1	15
バージョン2021.6.1の新機能および変更された機能	15
2021.6.1で修正された問題	16
バージョン2021.6.0	16
バージョン2021.6.0の新機能および変更された機能	16
2021.6.0で修正された問題	21
バージョン2021.4.1	22
バージョン2021.4.1の新機能および変更された機能	22
2021.4.1で修正された問題	22
バージョン2021.4.0	23
バージョン2021.4.0の新機能および変更された機能	23
2021.4.0で修正された問題	28
バージョン2021.2.1	30
バージョン2021.2.1の新機能および変更された機能	30
2021.2.1で修正された問題	30
バージョン2021.2.0	30
バージョン2021.2.0の新機能および変更された機能	30
2021.2.0で修正された問題	35
バージョン2020.12.0	37
バージョン2020.12.0の新機能および変更された機能	37
2020.12.0で修正された問題	41
バージョン2020.10.1	42
バージョン2020.10.1の新機能および変更された機能	42

2020.10.1で修正された問題	43
バージョン2020.10.0	43
バージョン2020.10.0の新機能および変更された機能	43
2020.10.0で修正された問題	48
バージョン2020.8.2	50
バージョン2020.8.2の新機能および変更された機能	50
2020.8.2で修正された問題	50
バージョン2020.8.1	50
バージョン2020.8.1の新機能および変更された機能	50
2020.8.1で修正された問題	51
バージョン2020.8.0	51
バージョン2020.8.0の新機能および変更された機能	51
2020.8.0で修正された問題	57
バージョン2020.6.2	58
バージョン2020.6.2の新機能および変更された機能	58
2020.6.2で修正された問題	58
バージョン2020.6.1	59
バージョン2020.6.1の新機能および変更された機能	59
2020.6.1で修正された問題	59
バージョン2020.6.0	59
バージョン2020.6.0の新機能および変更された機能	59
2020.6.0で修正された問題	64
CH: 章3: 既知の問題と制限事項	66

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>を参照するか、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]を選択してください。

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。

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 to 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2021.6.0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。

現在Black Duckは、外部データベース用のPostgreSQLバージョン11.xのみをサポートします。

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2021.4.0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個追加することにより、1 CPU、2GB RAM、100GB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2021.2.0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、2GB RAM、100GB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2020.10.0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個追加することにより、1 CPU、2GB RAM、100GB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2020.8.0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 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。

2020.10.0リリースで廃止されたAPI

Black Duck 2020.10.0リリースでは、/api/catalog-risk-profile-dashboard APIは、HTTP 410(GONE) を返します。Black Duck 2020.12.0リリース以降で、このAPIは使用できなくなります。

/api/catalog-risk-profile-dashboardを置き換える新しいAPIは、2020.10.0リリースで発表されます。

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2020.6.0が日本語にローカライズされました。

バージョン2020.6.1の発表

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。

バージョン2020.6.0の発表

今後のリリースでの新しいコンテナとシステム要件の変更

2020.8.0リリース

2020.8.0リリースでは、新しいRedisコンテナがBlack Duckに追加されます。このコンテナでは、Black Duckのキャッシュ機能の整合性が向上し、アプリケーションのパフォーマンスが改善します。

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。

- 5 CPU
- Redisの最小構成の場合は21 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24 GB RAM
- データベースおよびその他のBlack Duckコンテナ用に250GB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。

- 6 CPU
- Redisの最小構成の場合は25 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28 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、CPU、2GB RAM、100GBの空きディスク容量の追加が必要です。

2020.10.0リリース

2020.10.0リリースでは、Black Duckは次の2つのコンテナを追加します。BOM EngineとRabbitMQは必須コンテナです。これらのコンテナは、アプリケーションのパフォーマンスを向上させるために使用され、主にプロジェクトバージョンの構成表パフォーマンスを向上させます。

初期テストで示される、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

初期テストで示される、Black Duck - Binary AnalysisでBlack Duckを実行させ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個追加することにより、CPU、2GB RAM、100GBの空きディスク容量の追加が必要です。

これらのシステム要件は、初期テスト結果に基づいていることに注意してください。最終的なシステム要件は、この記載内容よりも小さい場合がありますが、記載内容より大きくなることはありません。

Internet Explorer 11のサポートの廃止

Synopsysは、Black Duck 2021.2.0リリース以降でInternet Explorer 11のサポートを廃止する予定です。

PostgreSQL 11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 11.7をサポートするようになりました。PostgreSQL 9.6は引き続き外部PostgreSQLインスタンスに対して完全にサポートされていますが、Synopsysは、外部PostgreSQLを使用する新規インストールには、PostgreSQL 11.7を推奨しています。

内部PostgreSQLコンテナのユーザーの場合は、PostgreSQL 9.6が引き続きBlack Duck 2020.6.0でサポートされるバージョンです。

バージョン2020.2.0の発表

個別のファイルマッチ

事前に通知したとおり、あいまいマッチによる誤検出を減らすために、署名スキャンの一環としての個別のファイルマッチの実行は、Black Duck CLIおよびSynopsys Detectスキャンのデフォルト動作ではなくなりました。

個別のファイルマッチでは、1つのファイルのチェックサム情報に基づいてコンポーネントを識別します。Black Duckでは、少数のファイル拡張子のセット(.js、.apklib、.bin、.dll、.exe、.o、.so)を対象に、定期的に署名スキャンを行い、1つのファイルに一致するチェックサムに基づいてファイルとコンポーネントをマッチングします。残念ながら、このマッチは常に正確であるとは限らず、かなりの量の誤検出が発生しました。広範なSynopsys顧客ベース全体にわたり開発者のエクスペリエンスを向上させるために、個別のファイルマッチはデフォルト動作ではなくなり、現在では、オプション機能になっています。

2020.2.0にアップグレードすると、個別のファイルマッチがオフになり、一部のコンポーネントが構成表から削除される場合があります。構成表への影響を推定するには、マッチタイプを「完全ファイル」に限定してコンポーネントを探し、構成表から削除される可能性のあるコンポーネントを確認してください。Dockerイメージをスキャンする場合、「完全ファイル」マッチはこの変更の影響を受けません。ご注意ください。

署名スキャンには、個別のファイルマッチを有効にする新しいパラメータがあります。スキャンにSynopsys Detectを使用している場合、バージョン6.2には、個別のファイルマッチのオン/オフをサポートする新しいパラメータがあり、デフォルトは[オフ]になっています。

Docker Composeのサポート

事前に通知したとおり、2020.2.0リリースでDocker Composeはサポートされるオーケストレーションメソッドではなくなりました。

バージョン2021.8.0

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

この設定により、ユーザーは、署名スキャンにLCAインテリジェント永続機能を使用するときに、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ツールの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 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。

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

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

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-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-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-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。
- (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。

バージョン2021.6.2

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のため、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

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

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

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をBlack Duck - Binary Analysisで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、2GB RAM、100GB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。

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。

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。

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

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。

バージョン2021.4.1

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

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。

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。
- Added the capability to generate OpenAPI Specification (OAS) for `/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입]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。

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。

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 `.yaml` 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BDBAL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。

バージョン2021.2.1

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

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、ポリシーールを作成する機能が提供されるようになりました。

Synopsys Detectのホスティングロケーション

外部接続が制限されているBlack Duckのお客は、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。

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

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。

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、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。

バージョン2020.12.0

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個追加することにより、1 CPU、2GB RAM、100GB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可能になり、1MBから16MB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日ごとにページします。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ペ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 Duck2021.2.0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

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。

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。

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。

バージョン2020.10.1

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

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, z`(`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。

スキャンペ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。

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。

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。

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。

バージョン2020.8.2

バージョン2020.8.2の新機能および変更された機能

Black Duckバージョン2020.8.2はメンテナンスリリースのため、新機能や変更された機能はありません。

2020.8.2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-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-25967)。コンポーネントの使用法変更に整合性がなかった問題が修正されました。

バージョン2020.8.1

バージョン2020.8.1の新機能および変更された機能

マッピングされていないコードの場所を時間でクリーンアップする機能

Black Duckでは、Docker Swarmの実装のために、`blackduck-config.env`ファイル内に`blackduck.scan.processor.scanpurge.cronstring`変数を設定して、スキャンパージcronジョブを設定できるようになりました。

ポリシーの機能強化

Black Duckでは、脆弱性の修正ステータスに対して、ポリシーを作成できるようになりました。

コンテナバージョン

- `blackducksoftware/blackduck-postgres`: 1.0.13
- `blackducksoftware/blackduck-authentication`: 2020.8.1
- `blackducksoftware/blackduck-webapp`: 2020.8.1
- `blackducksoftware/blackduck-scan`: 2020.8.1
- `blackducksoftware/blackduck-jobrunner`: 2020.8.1
- `blackducksoftware/blackduck-cfssl`: 1.0.1
- `blackducksoftware/blackduck-logstash`: 1.0.6
- `blackducksoftware/blackduck-registration`: 2020.8.1
- `blackducksoftware/blackduck-nginx`: 1.0.25
- `blackducksoftware/blackduck-documentation`: 2020.8.1
- `blackducksoftware/blackduck-upload-cache`: 1.0.15

- blackducksoftware/blackduck-redis:2020.8.1
- sigsynopsys/bdba-worker:2020.06-2
- blackducksoftware/rabbitmq: 1.2.1

2020.8.1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-24149)。実行した操作に関係なく「エラー: StatusLoggerが認識されていません...」というエラーメッセージが表示される、Protex構成表ツールの問題を修正しました。
- (Hub-24480)。Black Duckをバージョン2020.4.1にアップグレードした場合に、Protexからインポートしたコンポーネントが、無視済みステータスを失っていた問題を修正しました。
- (Hub-25254)。配布タイプの変更にポリシー違反が誤ってトリガーされていた問題を修正しました。
- (Hub-25269、25416)。長時間実行中のクエリにより、スキャンがブロックされたり、PostgreSQLデータベースでデッドロックが発生したりする問題を修正しました。
- (Hub-25387)。KbUpdateJobが断続的に失敗する問題を修正しました。
- (Hub-25509)。Black Duckバージョン2020.4.2でデータベースサイズが増加していた問題を修正しました。

バージョン2020.8.0

バージョン2020.8.0の新機能および変更された機能

脆弱性の影響を解析する機能

Black Duckでは、最初に対処すべき脆弱性を優先できるように、Javaアプリケーションから呼び出される外部のパブリックメソッドが既知の脆弱性に関与している可能性があるかどうかを判別できるようになりました。Black Duckは、ソースコード内で呼び出される完全修飾パブリック機能名を判定し、脆弱性によって悪用される既知の関数名と照合できます。自分のJavaアプリケーションから呼び出す外部パブリックメソッドが既知の脆弱性に関与している可能性があるかどうかを把握することで、どの脆弱性に集中する必要があるかを優先付けできます。

この機能は、Synopsys Detect/バージョン6.5以降(およびSynopsys Detect6.5以降を使用するSynopsys Detect(Desktop))で、Javaアプリケーションのみを対象に使用できます。

次の点に注意してください。

- Synopsys Detectが検出できるのは、脆弱な可能性のある関数を呼び出すJavaパブリックメソッド内の脆弱性のみです。
- この機能では、BDSAでの到達可能な関数のみが表示されます。

新しいコンテナおよびシステム要件

新しいRedisコンテナがBlack Duckに追加されました。このコンテナにより、Black Duckのキャッシュ機能の整合性が向上し、アプリケーションのパフォーマンスが改善します。

すべてのコンテナの単一インスタンスを実行するために必要な現在の最小ハードウェアは次のようになりました。

- 5 CPU
- Redisの最小構成の場合は21 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

合は24 GB RAM

- データベースおよびその他のBlack Duckコンテナ用に250GB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ようになりました。

- 6 CPU
- Redisの最小構成の場合は25 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28 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個追加することにより、CPU、2GB RAM、100GBの空きディスク容量の追加が必要です。

カスタムシステムアナウンス

システム管理者は、Black Duckユーザーに対して、カスタムのサインオンメッセージやサインオン後メッセージを作成できるようになりました。

たとえば、近日中に実施されるイベントについてユーザーに通知する場合や、不正使用により引き起こされる事態を示す免責事項を表示する必要がある場合に、システムアナウンスを使用できます。

次の4種類のメッセージを作成できます。

- ログイン。ユーザーがBlack Duckにログインするときに表示されるメッセージ。
- バナー。すべてのページの上部に表示されるメッセージ。
- フッター。すべてのページのフッターに表示されるメッセージ。
- よこそ。ユーザーがBlack Duckにログインした後に表示されるメッセージ。

プロジェクトバージョンレポートの機能強化

新しい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

プロジェクトバージョンレポートに、新しいレポート、`project_version_upgrade_guidance_date_time.csv`が追加されました。

このレポートの内容：

- コンポーネントバージョンの詳細(取得元の情報や脆弱性の総数を含む)
- アップグレード先のバージョン/取得元、およびその詳細(脆弱性の総数など)を含むコンポーネント(存在する場合)の短期的なアップグレードガイダンス
- アップグレード先のバージョン/取得元、およびその詳細(脆弱性の総数など)を含むコンポーネント(存在する場合)の長期的なアップグレードガイダンス

このレポートの列：

- コンポーネントID
- コンポーネントバージョンID

- コンポーネント 取得元ID
- コンポーネント 名
- コンポーネント バージョン名
- コンポーネント 取得元 名
- コンポーネント 取得元ID
- コンポーネント 取得元 バージョン名
- 既知の脆弱性の総数
- 短期推奨バージョンID
- 短期推奨バージョン名
- 短期推奨コンポーネント 取得元ID
- 短期推奨取得元名
- 短期推奨取得元ID
- 短期推奨取得元バージョン名
- 短期的に緊急の脆弱性
- 短期的に高の脆弱性
- 短期的に中の脆弱性
- 短期的に低の脆弱性
- 長期推奨バージョンID
- 長期推奨バージョン名
- 長期推奨コンポーネント 取得元ID
- 長期推奨取得元名
- 長期推奨取得元ID
- 長期推奨取得元バージョン名
- 長期的に緊急の脆弱性
- 長期的に高の脆弱性
- 長期的に中の脆弱性
- 長期的に低の脆弱性

`security_date_time.csv`レポートに追加された新しい列

`security_date_time.csv`プロジェクトバージョンレポートに追加された新しい列:

- CVSSバージョン。脆弱性評価システムのバージョン: CVSS 2.0またはCVSS 3.x。
- マッチタイプ。

署名スキャナの機能強化

署名スキャナからBlack Duckにスキャンデータをストリーム(バッファ)する方法を制御する2つの新しいプロパティが署名スキャナに追加されました。まれに、ネットワークに合わせてこれらの値の変更が必要になることがあります。たとえば、ネットワークに問題がある場合は値を下げ、ネットワークが非常に安定している場合はデフォルト値を大きくします。

- **--max-request-body-size**. スキャンされたパスのスキャンデータをアップロードするメインリクエストのサイズ。
- **--max-update-size**. 署名スキャナが個別のURI(スキャンされたパス)のデータの更新を完了したときに、Black Duckに通知する更新リクエストのバッファサイズ。

APIの機能強化

- 特定のBlack Duckユーザーの最終ログイン日を取得します。

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

2020.8.0へのアップグレードに伴い、すべてのユーザーのデフォルトの最終ログイン日がアップグレード日になりますが、それ以降は実際のログインデータが使用されます。デフォルトでは、このエンドポイントには、過去30日間にログインしていないすべてのユーザーが表示されますが、`?sinceDays=クエリパラメータ`を追加して、検索期間を任意の日数に変更できます。また、作成済みのユーザーの内、システムにログインしたことのないユーザーも表示されます。

- 活動していないユーザーを検索します。

GET /api/dormant-users

- アナウンス用に新しく追加されたエンドポイント：

- ログインアナウンスを作成します。

POST /api/manage-announcement/login

- ようこそアナウンスを作成します。

POST /api/manage-announcement/welcome

- バナーアナウンスを作成します。

POST /api/manage-announcement/banner

- フッターアナウンスを作成します。

POST /api/manage-announcement/footer

- ログインアナウンスを編集します。

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

- ようこそアナウンスを編集します。

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

- バナーアナウンスを編集します。

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

- フッターアナウンスを編集します。

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

- ログインアナウンスを削除します。

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

- ようこそアナウンスを削除します。

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

- バナーアナウンスを削除します。

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

- フッターアナウンスを削除します。

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

- ログインアナウンスを取得します。

GET /api/manage-announcement/login

- ようこそアナウンスを取得します。

GET /api/manage-announcement/welcome

- バナーアナウンスを取得します。

GET /api/manage-announcement/banner

- フッターアナウンスを取得します。

GET /api/manage-announcement/footer

- ID別にログインアナウンスを取得します。

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

- ID別にようこそアナウンスを取得します。

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

- ID別にバナーアナウンスを取得します。

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

- ID別にフッターアナウンスを取得します。

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

- ユーザーログインアナウンスを取得します。

GET /api/announcement/login

- ユーザーようこそアナウンスを取得します。

GET /api/announcement/welcome

- ユーザーバナーアナウンスを取得します。

GET /api/announcement/banner

- ユーザーフッターアナウンスを取得します。

GET /api/announcement/footer

- ID別にユーザーログインアナウンスを取得します。

GET /api/announcement/login/{announcementId}

- ID別にユーザーようこそアナウンスを取得します。

GET /api/announcement/welcome/{announcementId}

- ID別にバナーアナウンスを取得します。

GET /api/announcement/banner/{announcementId}

- ID別にユーザーフッターアナウンスを取得します。

GET /api/announcement/footer/{announcementId}

- ようこそアナウンスを抑制します。

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

- API取得元応答に、新しいオプションのoriginUrlフィールドが追加されました。
- api/projects/id/versions/id/referencesに、構成表API(api/projects/id/versions/id/components) リファレンスが追加されました。
- api/codelocations/id/scan-summariesの応答に、createdByUsernameが追加されました。
- /api/projects/versions/hierarchical-componentsにcomponentTypeフィールドが追加され、アイテムのcomponentTypeがSUB_PROJECTの場合、メタデータにprojectおよびprojectVersionリンクを含むようになりました。
- vulnerabilityWithRemediationブロックの下にある/api/projects/{projectId}/versions/{projectVersionId}/vulnerable-bom-componentsに、relatedVulnerabilityリンクが追加されました。
- /api/projects/{projectId}/versions/{projectVersionId}/vulnerable-bom-componentsに、remediationCreatedByおよびremediationUpdatedByが追加されました。
- 非推奨のエンドポイント：
 - 修正オプションの一覧表示 : GET /api/components/{componentId}/versions/{componentVersionId}/remediating.

このエンドポイントは、GET /api/components/{componentId}/versions/{componentVersionId}/upgrade-guidanceで置き換えられました。

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84.0.4147.125(公式ビルド) (64ビット)
- Firefox 79.0(64ビット)
- Internet Explorer 11.450.19041.0

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 44.19041.423.0
- Microsoft EdgeHTML 18.19041

コンテナバージョン

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

日本語

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2020.6.0が日本語にローカライズされました。

2020.8.0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-23467)。マッチ数が1,300件以上ある場合に、[スキャン]ページに「サーバーが時間内に応答しませんでした」というエラーメッセージが表示される問題を修正しました。
- (Hub-23892)。[スキャン]ページの[スキャンサイズ]列が空だった問題を修正しました。
- (Hub-23937、24799)。[ライセンス管理]ページのロードが失敗する問題を修正しました。
- (Hub-24009)。Synopsys Detectの出力で、コード400で構成表インポートが直ちに失敗し、`hub_scan_errors.log`に「ドキュメントnullのドキュメントデータの保存に失敗しました」というメッセージが表示される問題を修正しました。
- (Hub-24112)。プロジェクトバージョンの[ソース]タブで選択されているノードがなくなったときでも、ユーザーがマッチ数フィルタビューに戻ることができるように、問題を修正しました。
- (Hub-24278)。バイナリスキャンファイルのアップロードが、次のエラーメッセージが表示されて失敗する問題を修正しました:「バイナリスキャンのアップロード時の不明なステータスコード: 0, null」。
- (Hub-24291)。32,767を超えるコンポーネントを表示しようとしたときに、[構成表]ページに「アプリケーションに不明なエラーが発生しました」と表示される問題を修正しました。
- (Hub-24407)。スニペットのクローンを作成するときに「文字列からシリアル化を解除できません」というエ

ラーメッセージが表示される問題を修正しました。

- (Hub-24432)。32,000を超えるプロジェクトを表示しようとしたときに[ダッシュボード]ページが読み込まれない問題を修正しました。
- (Hub-24451)。認証プロキシを使用してBlack Duckナレッジベースを呼び出したときに、HUB_PROXY_PASSWORD_FILE docker secretが無視される問題を修正しました。
- (Hub-24480)。ProtexをBlack Duck 2020.4.1にインポートしたときにコンポーネントの変更が失われる問題を修正しました。
- (Hub-24529)。Black Duckナレッジベースで「パッチ適用済み」ステータスが示されているコンポーネントに対して、誤ってポリシー違反がトリガーされる問題を修正しました。
- (Hub-24583、25244)。Black Duckナレッジベースが更新されたときに手動で追加したコンポーネントが削除される問題を修正しました。
- (Hub-24646)。Black Duckのアップグレード時に発生していた、[ライセンス管理]ページでナレッジベースライセンスが更新されても、その変更を行ったユーザーが識別されない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[コンポーネント]ページに移動するときに失敗する問題を修正しました。
- (Hub-24716)。無視しているコンポーネントの脆弱性通知が表示される問題を修正しました。
- (Hub-24739)。LDAPユーザーの電子メールアドレスを変更できない問題を修正しました。
- (Hub-24740)。bom_component_custom_fields_date_time.csvレポートに、無視しているコンポーネントのみが表示される問題を修正しました。
- (Hub-24758)。スニペットを並列表示したときに、プロジェクトバージョンの[ソース]タブの左側で、マッチしたコードが完全には強調表示されない問題を修正しました。
- (Hub-24845)。[概要]タブの[統計情報]セクションが更新されない問題を修正しました。
- (Hub-24866)。ルートのサブディレクトリの一部を除外して、ディスク上のルート全体をスキャンしようとしたときに、署名スキャナが「正しくないリクエスト」エラーを報告する問題を修正しました。
- (Hub-24885)。階層ビューでプロジェクトバージョンの[ソース]タブにマッチを表示しようすると、「アプリケーションに不明なエラーが発生しました」というメッセージが表示される問題を修正しました。
- (Hub-24968)。セキュリティダッシュボードを表示しようとしたときに、「Black Duckサーバーが時間内に応答しませんでした」というエラーメッセージが表示される問題を修正しました。
- (Hub-25072)。名前にチルダ文字(~)が含まれるコンポーネントのポリシーを作成すると、「アプリケーションに不明なエラーが発生しました」というエラーメッセージが表示される問題を修正しました。
- (Hub-25115)。パラメータの数が32,767個を超えるとスキャンが失敗する問題を修正しました。
- (Hub-25166)。Istio環境でのpostgres-initポッドの問題を修正するために、preおよびpostコマンドを追加しました。

バージョン2020.6.2

バージョン2020.6.2の新機能および変更された機能

Black Duckバージョン2020.6.2はメンテナンスリリースのため、新機能や変更された機能はありません。

2020.6.2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-24918)。BdioDataTransferJobおよびVersionBomComputationジョブがスキャンデータを正しく読み取っていなかったことが原因でスキャンの結果が返されないことがある問題を修正しました。

バージョン2020.6.1

バージョン2020.6.1の新機能および変更された機能

Black Duckバージョン2020.6.1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。

2020.6.1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-23970)。著作権オプションが選択されていると通知ファイルを生成できない問題を修正しました。
- (Hub-24106)。ナレッジベースサービスにアクセスできないことが原因でKbUpdateジョブが失敗する問題を修正しました。
- (Hub-24651)。プロジェクトマネージャおよび構成表マネージャの役割を持つユーザーが/api/projects/ページでリリースフェーズフィルタを使用できない問題を修正しました。
- (Hub-24721)。Black Duckセキュリティアドバイザリ(BDSA)がライセンスされたモジュールではない場合に、構成表コンポーネントレポートが失敗する問題を修正しました。
- (Hub-24739)。LDAPユーザーの電子メールアドレスを変更できない問題を修正しました。
- (Hub-24765)。SNIPPET_MATCHINGオプションを使用してスキャンしたときにスニペットが識別されないことがある問題を修正しました。

バージョン2020.6.0

バージョン2020.6.0の新機能および変更された機能

保存された検索を含む新しいプロジェクトダッシュボード

Black Duckには、プロジェクトの1つ以上のバージョンに含まれるコンポーネントに関連する、リスクのタイプと重大度およびポリシー違反を表示できるように、ダッシュボードが用意されています。ダッシュボードは、すべてのプロジェクトとプロジェクトバージョンにわたる全体的なビューです。

重要なプロジェクトとプロジェクトのバージョンを表示できるように、2020.6.0では、プロジェクトダッシュボードが2つの新しいデフォルトダッシュボードに代わり、無制限の数のカスタムダッシュボードを作成できるようになりました。

Black Duckには、次の2つのデフォルトのダッシュボードが表示されます。

- **ウォッチ**。ウォッチするプロジェクト。
- **マイプロジェクト**。ウォッチしていないプロジェクトを含むすべてのプロジェクト。

これらのダッシュボードは、プロジェクトレベルの新しい[ダッシュボード]ページに情報を表示します。[プロジェクトダッシュボード]ページが、この[ダッシュボード]ページに代わりました。

さらに、重要なプロジェクトバージョンをすばやく表示できるように、カスタムダッシュボードを作成することもできます。Black Duckでは、さまざまな属性を使用してプロジェクトを検索し、検索を保存してから、このページを使用して保存された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。保存された検索に基づくダッシュボードには、プロジェクトのバージョンレベルで情報が表示されます。

[ウォッチ]ダッシュボードと[マイプロジェクト]ダッシュボードに表示される情報は、リアルタイムに更新されます。新し

いジョブSearchDashboardRefreshJobは、5分ごとにカスタムダッシュボードを更新します。



をクリックすると、ダッシュボードが表示されます。表示されていない場合は、**[ダッシュボード]**を選択してこれらのダッシュボードを表示します。

プロジェクト検索の機能強化

プロジェクトの検索は、プロジェク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。

次の属性を使用して、Black Duckでプロジェクトを検索できるようになりました。

- ウォッチ。このプロジェクトがウォッチするプロジェクトかどうかを選択します。
- セキュリティリスク。
- ライセンスリスク。
- 運用リスク。
- ポリシールール。リストからポリシールールを選択して、このポリシーに違反するプロジェクトを検索します。
- ポリシー違反。ポリシールールの重大度レベル。
- 配布。
- 最終スキャン日。
- リリースフェーズ。
- 階層。

検索結果には、検索条件を満たすプロジェクトバージョンが表示されます。プロジェクトのバージョンごとに、次の数を表示できます。

- 検出された結果とデータベースが最後に更新された時刻。
- セキュリティ、ライセンス、または運用リスクが最も高いレベルにあるコンポーネント。
- リスクカテゴリごとのコンポーネント。
- このプロジェクトバージョンのポリシーの重大度が最も高いコンポーネント。
- 重大度レベル別のポリシー違反のあるコンポーネント。

プロジェクトバージョンごとに、検索結果に次の情報も表示されます。

- このプロジェクトバージョンのコンポーネントの数。
- 最終スキャン日。
- このプロジェクトバージョンが最後に更新された日時です。
- このプロジェクトバージョンのライセンス。
- このプロジェクトバージョンのフェーズ。
- このプロジェクトバージョンの配布。

前述のように、検索結果を保存してダッシュボードに表示できるようになりました。

埋め込み著作権情報の検出

Black Duckでは、埋め込み著作権情報のインスタンスを検出できるようになりました。コードのスキャン時に著作権データの検出を有効にすることで、ライセンスコンプライアンスに重点を置いたユーザーは、オープンソースソフト

ウェアや専有著作権情報を検出して管理することで、ライセンスコンプライアンスのリスクを軽減できます。

この機能を使用して、Black Duckは著作権文字列のテキスト検索を実行し、見つかったテキストを[ソース]タブに表示します。

必要に応じてソースファイルをアップロードし、レビュー担当者が検出されたファイル内の著作権テキストを[ソース]タブ内から表示できるようにします。

プロジェクトのクローン作成

Black Duckでは、プロジェクトのクローンを作成する機能が提供されるようになりました。プロジェクトのクローン作成を使用して、既存のプロジェクトを新しいプロジェクトにフォークします。クローンの作成により、既存のプロジェクトで定義したデータ、分析、および解決策を、新しいプロジェクトのベースラインとして使用することにより作業量を削減できます。

プロジェクトを作成できるユーザーは、プロジェクトのクローンを作成できます。プロジェクトごとに、クローンを作成するバージョンとプロジェクトの属性(プロジェクトの設定、プロジェクトメンバー、グループなど)を選択します。

ポリシー管理の機能強化

- ポリシー管理では、次に基つ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。
 - ライセンスの有効期限
 - ブール、日付の構成表コンポーネントカスタムフィールド。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。
 - プロジェクトフィルタに、ブール型、複数選択型、テキストフィールド型のプロジェクトカスタムフィールドが含まれるようになりました。
- 複数のライセンスを持つコンポーネントのライセンスポリシー条件を評価するためのロジックが変更され、新しいポリシー違反が発生したり、コンポーネントがポリシー違反をトリガーしなくなったりする可能性があります。

1つ以上のライセンス条件(ライセンス、ライセンスステータス、ライセンスファミリ、および/またはライセンス有効期限)を使用して作成されたポリシールールに対して複数のライセンスを持つコンポーネントを評価する場合、各ライセンスが評価され、ポリシー違反に対してすべてのライセンス条件が真でなければなりません。ライセンスリスクがポリシー条件として含まれている場合、ライセンスリスクは個別に評価されます。他のライセンスポリシー条件を満たすライセンスだけでなく、コンポーネントのすべてのライセンスが評価されます。したがって、あるライセンスが複数の条件のポリシールールを満たし、そのコンポーネントの別のライセンスがライセンスリスク条件を満たしている場合に、ポリシー違反がトリガーされることがあります。

外部データベースでサポートされるPostgreSQL 11.7

Black Duckは、外部PostgreSQLを使用する新規インストール用にPostgreSQL 11.7をサポートするようになりました。PostgreSQL 9.6は引き続き外部PostgreSQLインスタンスに対して完全にサポートされていますが、Synopsysは、外部PostgreSQLを使用する新規インストールには、PostgreSQL 11.7を推奨しています。

内部PostgreSQLコンテナのユーザーの場合は、PostgreSQL 9.6が引き続きBlack Duck 2020.6.0でサポートされるバージョンです。

数値ユーザー名は、外部PostgreSQLデータベースでサポートされます

外部PostgreSQLインスタンスは、数字のみで構成されるユーザー名がサポートされるようになりました。

通知ファイルレポートの機能強化

不明なライセンスファミリのライセンスは、通知ファイルレポートから除外されるようになりました。

個々のプロジェクトで利用可能になったグローバル脆弱性レポート

脆弱性修正レポート、脆弱性ステータスレポート、脆弱性更新レポートは、アクセス権を持つ1つ以上のプロジェクトに対して実行できるようになりました。

レポートがグローバルレベルかプロジェクトレベルかを区別するために、これらのレポートのファイル名は次のように変更されています。

- レポートのグローバルバージョンの場合、vulnerability-remediation-report_all_assigned_projects_YYYY-MM-DD_HHMMSS(UTCのタイムスタンプ)
- 1つ以上のプロジェクトの場合、vulnerability-remediation-report_YYYY-MM-DD_HHMMSS(UTCのタイムスタンプ)
- レポートのグローバルバージョンの場合、vulnerability-status-report_all_assigned_projects_YYYY-MM-DD_HHMMSS(UTCのタイムスタンプ)
- 1つ以上のプロジェクトの場合、vulnerability-status-report_YYYY-MM-DD_HHMMSS(UTCのタイムスタンプ)
- レポートのグローバルバージョンの場合、vulnerability-update-report_all_assigned_projects_YYYY-MM-DD_HHMMSS(UTCのタイムスタンプ)
- 1つ以上のプロジェクトの場合、vulnerability-update-report_YYYY-MM-DD_HHMMSS(UTCのタイムスタンプ)

ソースプロジェクトバージョンレポートに追加された詳細情報

source_date_time.csvレポートは次の情報で拡充されました。

- [スキャン]列がレポートの最後に追加されました。プロジェクトバージョンの構成表には、プロジェクトバージョンにマッピングされた複数のスキャンを含めることができるため、この列には、この一致が見つかったスキャンが一覧表示されます。
- [パス]列に依存関係マッチに関する情報が表示されるようになりました。直接的な依存関係の場合、列に依存関係のIDが表示され、一致コンテンツ値が表示されます。推移的な依存関係の場合、列には最上位レベルのコンポーネントから宣言されたコンポーネントへの完全な依存関係パスが表示されます。

CVSSv3.1のサポート

Black DuckはCVSS v3.1スコアをサポートするようになりました。CVSSv3.1では、スコアリングの実行方法を明確にするスコア基準が更新されました。新しいメトリックベクトルや値はありませんが、明確化により全体的なスコアが変化する可能性があります。

レポートデータベースの機能強化

CVSS 3.xをサポートするために、component_vulnerabilityの表に次の列が追加されました。

- severity_cvss3
- base_score_cvss3
- exploit_score_cvss3

- impact_score_cvss3
- temporal_score_cvss3

再スキャン時に部分的なスニペット調整を保持するオプション

Black Duckでは、ファイルを再スキャンするときに部分的なスニペットマッチから識別情報を適用できるように設定することができるようになりました。これにより、再識別が必要なスニペットの数が最小限に抑えられます。

新しい監査イベント

監査イベントは、ユーザーが次の操作を行うと表示されるようになりました。

- ポリシーを作成し、Black Duckがプロジェクトバージョンを評価します。
- ポリシーを更新し、Black Duckがプロジェクトバージョンを評価します。
- ポリシーを有効化し、Black Duckがプロジェクトバージョンを評価します。
- ポリシーを無効化し、Black Duckは対応するポリシー違反をクリアします。
- ポリシーを削除し、Black Duckは対応するポリシー違反をクリアします。

構成表ページの新しい情報アイコン

[構成表]ページでは、情報アイコン(ⓘ)を使用して、調整フィールドまたはカスタムフィールドの追加情報があるかどうかを示します。

- アイコンにカーソルを合わせると、調整があるか、追加のフィールドがあるかが表示されます。
- アイコンを選択して、追加情報を表示する[コンポーネントの詳細]ダイアログボックスを開きます。

APIの機能強化

- 一致操作中に発生するコンポーネントインポートイベントのリストを提供する新しいエンドポイントが追加されました。

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

- 一致操作中に発生するコンポーネントインポートイベントの数(ステータス別)を提供する新しいエンドポイントが追加されました。

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

- 構成表がどのスキャンに属しているかを調べるためのAPIが追加されました。このAPIは、関連するスキャンによって検出されたエントリのリストを提供します。

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

- 著作権検索のサポートが追加され、ソースビューAPIの著作権検索用に新しいフィルタが追加されました。
- 最新のスキャンサマリAPIを改善しました。

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

サポートされるブラウザのバージョン

- Safariバージョン13.1.1(14609.2.9.1.3)
- Chromeバージョン83.0.4103.97(公式ビルド)(64ビット)

- Firefox 77.0.1(64ビット)
- Internet Explorer 11.836.18362.0
- Microsoft Edge 44.18362.449.0

コンテナバージョン

- blackducksoftware/blackduck-postgres: 1.0.13
- blackducksoftware/blackduck-authentication:2020.6.0
- blackducksoftware/blackduck-webapp:2020.6.0
- blackducksoftware/blackduck-scan:2020.6.0
- blackducksoftware/blackduck-jobrunner:2020.6.0
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash: 1.0.6
- blackducksoftware/blackduck-registration:2020.6.0
- blackducksoftware/blackduck-nginx: 1.0.25
- blackducksoftware/blackduck-documentation:2020.6.0
- blackducksoftware/blackduck-upload-cache: 1.0.14
- sigsynopsys/bdba-worker:2020.03-1
- blackducksoftware/rabbitmq: 1.0.3

日本語

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2020.4.0が日本語にローカライズされました。

2020.6.0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-20003) 。[コンポーネントの追加]ダイアログボックスでカスタムコンポーネントが識別されるように問題を修正しました。
- (Hub-22599) プロジェクトバージョンのクローン作成時にUIがタイムアウトになる問題を修正しました。
- (Hub-22695) プロジェクトバージョンをクローン作成して再スキャンした後、手動で識別されたコンポーネントが欠落していた問題を修正しました。
- (HUB-22812) 構成表の印刷時にフィルタが無視される問題を修正しました。
- (HUB-23502) --certificate-file-pathパラメータを指定せずにBlack DuckをOpenShiftネイティブモードで展開した場合、証明書に「サブジェクトの別名」が生成されない問題を修正しました。
- (HUB-23601) プロジェクト名[設定]タブの[所有者]ド롭ダウンメニューに、可能なすべての選択項目が表示されるように問題を修正しました。
- (HUB-23736) HierarchicalVersionBomJobが正常に実行されない問題を修正しました。
- (HUB-23798) サブプロジェクトを[コンポーネント]ダッシュボードからコンポーネントとして編集するときに404エラーが表示される問題を修正しました。
- (HUB-23909、23925) プロジェクトバージョンの[セキュリティ]タブで、ステータスに関係なく脆弱性を表示できない問題を修正しました。
- (Hub-23984) 役割が割り当てられていないユーザーのGET /api/projectsエンドポイントに対して、すべての

プロジェクトが返される問題を修正しました。

- (Hub-23985) 一致を選択するか、[ファイルツリーに表示]オプションを使用しても、ソースツリー内のファイルまでスクロールしない問題を修正しました。
- (Hub-23994) Black Duck - Binary Analysisが、アップロードされたバイナリファイルをクリーンアップしなかった問題を修正しました。
- (Hub-24011) スニペット スキャンで「413リクエストのエンティティが大きすぎます」というエラーメッセージが表示される問題を修正しました。
- (Hub-24040) jobrunnerがハングし、ジョブが完了しない問題を修正しました。
- (Hub-24097) コンポーネントのバージョンを更新した後、使用法の編集内容が保持されない問題を修正しました。
- (Hub-24107) 著作権オプションを選択したときに、通知ファイルレポートがパラメータが多すぎて失敗する問題を修正しました。
- (Hub-24239) `api/projects/<projectid>/versions/<versionid>/policy-status`に400エラーが表示される問題を修正しました。
- (Hub-24286) [コンポーネント名バージョン]ページに、コンポーネントバージョンがソフト削除されたにもかかわらず、表示される問題を修正しました。
- (Hub-24308) 空のサブプロジェクトが[構成表]ページのソースとして「componentCountコンポーネント」を表示する問題を修正しました。

Black Duckの既知の問題と制限事項は次のとおりです。

- 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。