Qualys Global AssetView/CyberSecurity Asset 管理 v2.x リリースノート

バージョン 2.16

2023 年 8 月 30 日(2023 年 9 月 11 日更新)

新着情報

Global AssetView/CyberSecurity Asset Management 2.16 の新機能は次の通りです。

CSAM CyberSecurity Asset Management

- CSAM EASM トグル
- サードパーティアセットのインポート
- 新しい QQL トークン
- EASM プロファイルの新しいオプション設定
- ドメインと組織の検証の機能強化
- アセットオープンポート詳細レポート

GAV CSAM Global AssetView/CyberSecurity Asset Management

- サードパーティのコネクタによって識別されたアセットの消去
- VM、PC、および CERT モジュールのアセットをアクティブ化する
- アセットのアクティベーション履歴の表示
- パージ・ルール作成の新しいオプション

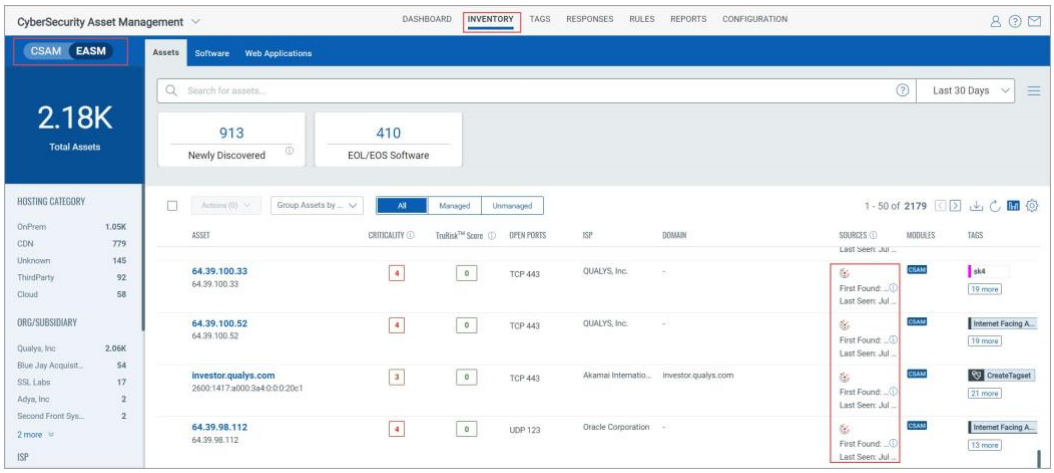
GlobalAssetView/CyberSecurity Asset Management 2.16は、さらに多くの改善とアップ デートをもたらします! 詳しくはこちらをご覧ください。

CSAM EASM トグル CSAM

CSAM 2.16.0.0 リリースより以前のバージョンは、EASM タブと INVENTORY タブが使用可能でした。INVENTORY タブの EASM から、または、EASM タブの EASM タグでタグ付けされたインベントリ ソースの 1 つとして EASM を含むアセットすべてのインベントリソースを含むアセットを表示できました。

将来の機能拡張の範囲を考慮すると、[EASM] タブと [CSAM] タブの両方に複数のタブが追加される可能性があります。そのため、CSAM 2.16.0.0 リリースでは、ナビゲーションを容易にするために CSAM EASM トグルを導入することで、これらのタブの両方を置き換えました。

INVENTORY タブをクリックすると、CSAM EASM トグルが表示されます。既定では、トグルは CSAM アセットを表示するように設定されています。それぞれのアセットインベントリを表示するには、トグルを CSAM または EASM に切り替えます。残りの機能はそのままです。



たとえば、CSAM に切り替えて CSAM インベントリ リストからアセットをクリックすると、Asset Summary ページから Asset Details タブにリダイレクトされます。
EASM に切り替えて EASM インベントリ リストからアセットをクリックすると、Asset Details ページから External Attack Surface タブにリダイレクトされます。

サードパーティアセットのインポート CSAM

このリリースでは、サードパーティのデータ コネクタを使用して Qualys アセットデータを強化するための新機能 "サードパーティアセットのインポート" が導入されました。この機能を使用すると、Webhook、Active Directory、ServiceNow などのさまざまなコネクタによってスキャンされたサードパーティのアセットを識別し、CSAM にインポートできます。

注: 「サードパーティアセットのインポート」は、ベータフェーズの新機能です。初期段階にあり、リクエストベースでのみ利用できます。詳細については、テクニカル アカウント マネージャー (TAM) にお問い合わせください。

エンドツーエンドの機能ワークフローを理解するには、オンラインヘルプを参照してください。

この機能の要点は、すべてのサードパーティのアセットまたはデータが Qualys アセットとマージされるか、新しい管理されていないアセットが作成され、アセットの重複排除方法が可視化されることです。

すぐに使用できるサードパーティ製コネクタ

IT アセットを効果的に管理するには、すべてのアセットの信頼性の高い包括的なインベントリを用意することが不可欠です。サードパーティのデータ コネクタを使用すると、Qualys で使用できない非エージェントまたは非スキャナーアセットを検索し、Qualys で管理されていないアセットを作成できます。その後、それらを脆弱性管理プログラムに追加できます。

Qualys コネクタは、すべてのクラウド環境で継続的な可視性とセキュリティを実現します。コネクタを構成し、クラウド アカウント内のアセットを検出できます。コネクタ統合を使用すると、サードパーティ サービス用のコネクタを作成し、リソースを検出し、CSAM などの必要な Qualys モジュールに情報を渡すことができます。

1. Webhook: Webhook コネクタを使用すると、サードパーティ製のインベントリのアセットへ接続して検出できます。その後、検出されたアセットを CSAM アプリケーションで表示できます。CSAM API は、サード パーティのサービスとの接続を確立するために必要です。Webhook コネクタの場合は、API 要求を送信してアセットを識別または検出し、CSAM インベントリに取り込む必要があります。詳細については、*API v2 ユーザーガイド*の「サードパーティアセットのインポート」セクションを参照してください。

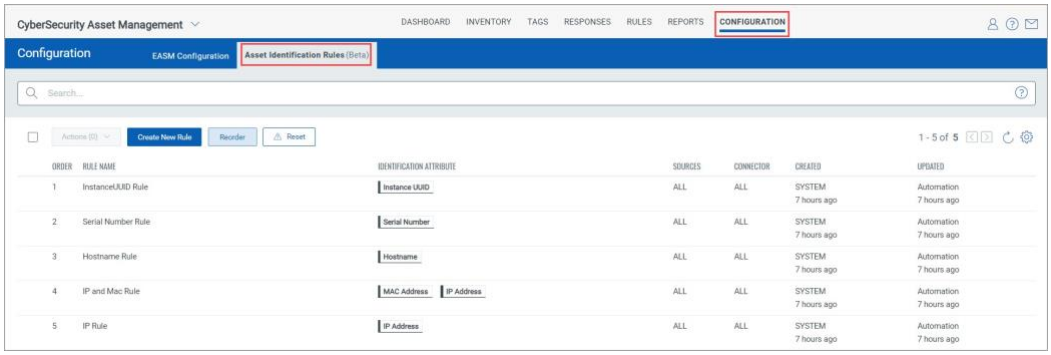
2. Active Directory: Active Directory コネクタを使用すると、Azure AD サーバーからアセットデータをフェッチできます。コネクタは、このデータを CSAM アプリケーションに渡します。

3. ServiceNow: ServiceNow インベントリ コネクタを使用すると、ServiceNow インベントリのリソースに接続して検出できます。その後、検出されたアセットを CSAM アプリケーションで表示できます。

Asset Identification Rules

[設定] > [アセット識別ルール (ベータ)]
タブに移動して、サードパーティアセットを識別してインポートします。

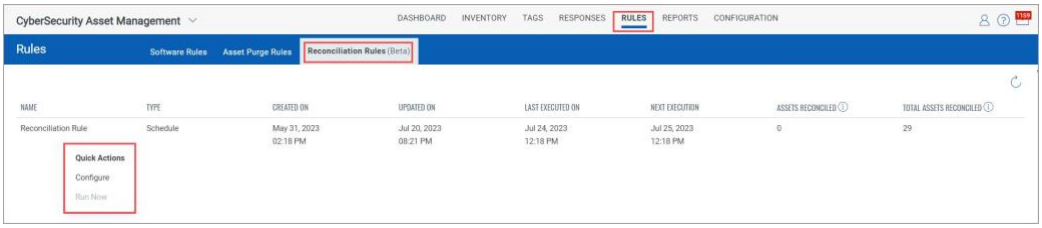
アセットを CSAM にインポートするために必要な識別属性とコネクタ
ソースを選択することで、アセット
識別ルールを作成できます。詳細については、オンラインヘルプを参照してください。



Reconciliation Rules

Reconciliation Rules (Beta) は、別のスケジュールで再度検出される前に、サードパーティのソースによって既に識別されているアセットがある場合に、Qualys エージェントやスキャナーなどの Qualys ネイティブ センサーからのアセットをマージする場合に不可欠です。

Rules > Reconciliation Rules (Beta) タブに移動します。On Demand または Recurring Reconciliation Rule を構成し、そのようなアセットをマージできます。詳細については、オンラインヘルプを参照してください。



また、Webhook、ServiceNow、Active Directory コネクタなどのサードパーティ製コネクタによって検出されたアセットを消去することもできます。

新しい QQL トークン CSAM

Inventory タブから次の新しい QQL トークンを使用できます。詳細については、*IT アセットの検索トークンを参照してください*。

トークン名	説明
connectors.connectorId	ユーザーが作成した特定のコネクタから供給されるアセットを検索します。 **注:** このトークンは「サードパーティアセット」用です ベータフェーズの新機能である「インポート」。初期段階にあり、リクエストベースでのみ利用できます。詳細については、テクニカル アカウント マネージャー (TAM) にお問い合わせください。
connectors.firstDiscovered	検出結果が最初に検出された日時を特定します。
connectors.lastDiscovered	検出結果が最初に検出された日時を特定します。

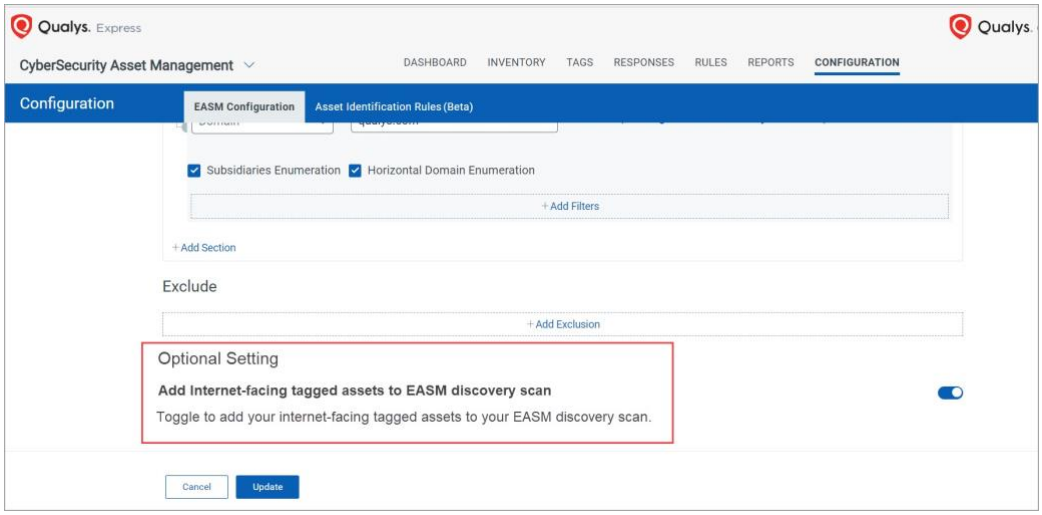
Asset Idenfification Rules (Beta) タブから次の新しい QQL トークンを使用できます 。詳細については、*IT アセットの検索トークンを参照してください*。

注: これらのトークンは、ベータフェーズの新機能である「サードパーティアセットのインポート」用です。初期段階にあり、リクエストベースでのみ利用できます。詳細については、テクニカル アカウント マネージャー (TAM) にお問い合わせください。

トークン名	説明
ruleName	正確なルール名またはルール名のフラグメントを指定して、アセット識別ルールを取得します。
identificationAttribute	指定した属性を使用して作成されたアセット識別ルールを取得します。

EASM プロファイルの新しいオプション設定 CSAM

新しいオプション設定、Add internet-facing tagged assets to ESAM discovery scan が EASM プロファイル構成に追加されます。



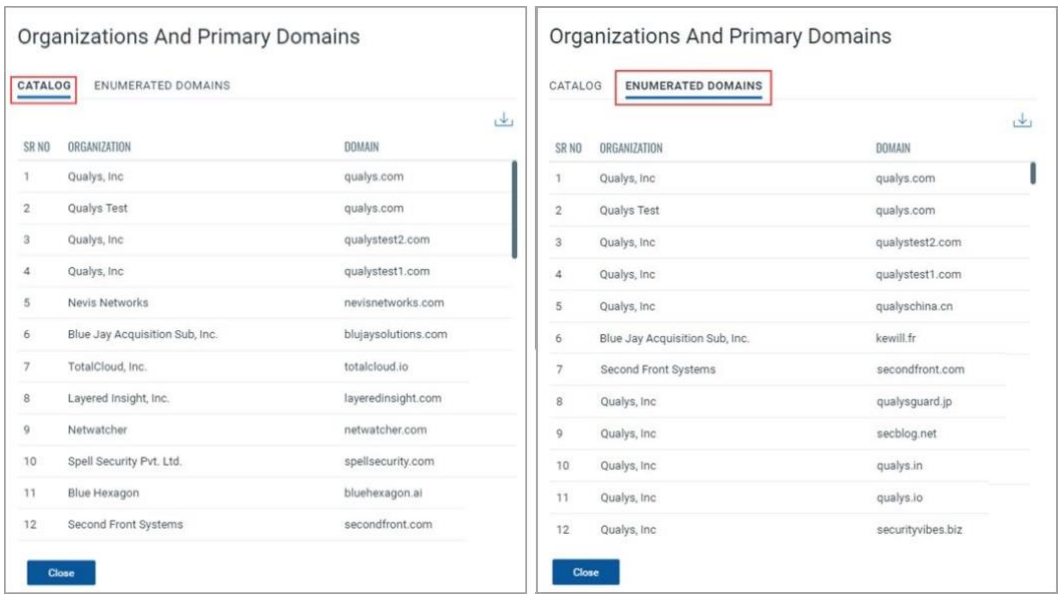
通常、EASM のサードパーティソースからデータを取得する場合、さまざまな理由でインターネットに接続するすべてのアセットを利用できない場合があります。たとえば、ファイアウォールによって許可されているインターネットに接続されたアセットのみが Qualys スキャナーにアクセスできる場合や、インターネットに接続するアセットに、関連付けられたドメイン、サブドメイン、組織の ASN などの十分な属性がない場合などです。その場合、EASM のサードパーティソースは、そのようなアセットをすぐに検出することはできません。
このようなシナリオでは、トグルをオンにすると、このような IP アドレスは EASM 検出プロセスの一部と見なされます。同期後、Asset Details ページで外部攻撃対象領域の詳細を確認できます。

トグルをオフにすると、タグやソースなど、EASM に関連するインターネットに接続されたタグ付きアセット情報がすべて Asset Details ページから削除されます。

ドメインと組織の検証の機能強化 CSAM

CSAM 2.16.0.0 リリースより以前は、ドメインと組織の検証が成功した後に、組織とドメインの詳細を表示できました。

CSAM 2.16.0.0 リリースでは、Organizations and Primary Domains ポップアップが拡張され、Catalog タブと ENUME DOMAINS タブの下に詳細が表示されるようになりました。



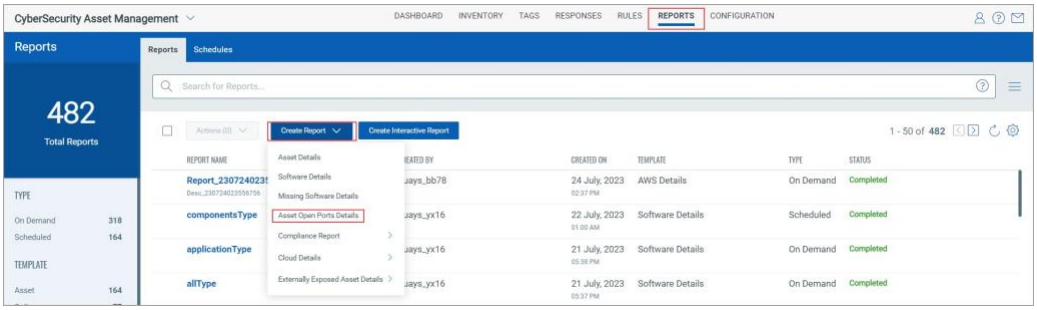
EASM カタログ DB で使用可能なドメインと組織のリストは、CATALOG タブから確認できます 。

他の関連するドメインとサブドメインは、水平列挙と WHOIS DB を介して表示できます ENUMERATED DOMAINS タブから。入力ソースは、カタログ DB またはユーザー指定の入力です。

その結果、カタログのデータと WHOIS を区別できます。

アセットオープンポート詳細レポート CSAM

アセットオープンポートの詳細レポートを作成できるようになりました。Reports > **Create Report** > **Asset Open Ports Details** に移動してレポートを作成し、選択したアセットの開いているポート、プロトコル、説明、検出されたサービス、IP アドレスなどの詳細を取得します。詳細については、オンラインヘルプを参照してください。

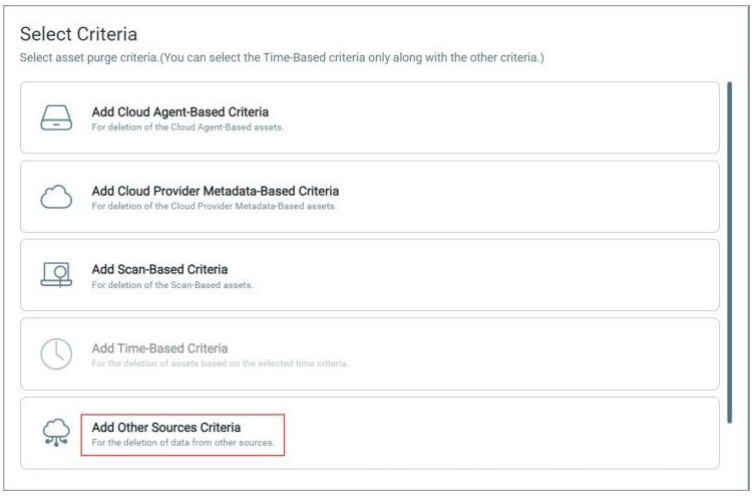


サードパーティのコネクタによって識別されたアセットの消去 GAV CSAM

アセットパージルールワークフローを作成するための **Add Other Sources** 基準の導入により、Webhook、ServiceNow、Active Directory コネクタなどのサードパーティコネクタによって検出されたアセットをパージできるようになりました。

注: Add Other Sources 基準を使用して他のパージ基準を追加することはできません。

詳細については、オンラインヘルプを参照してください。

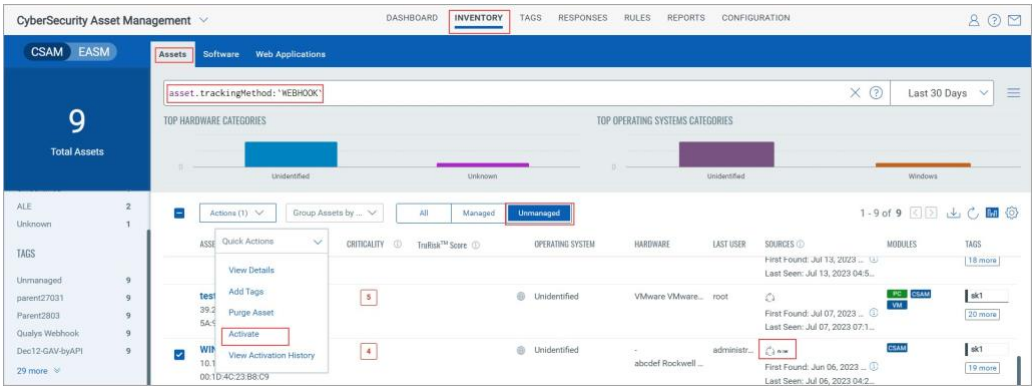


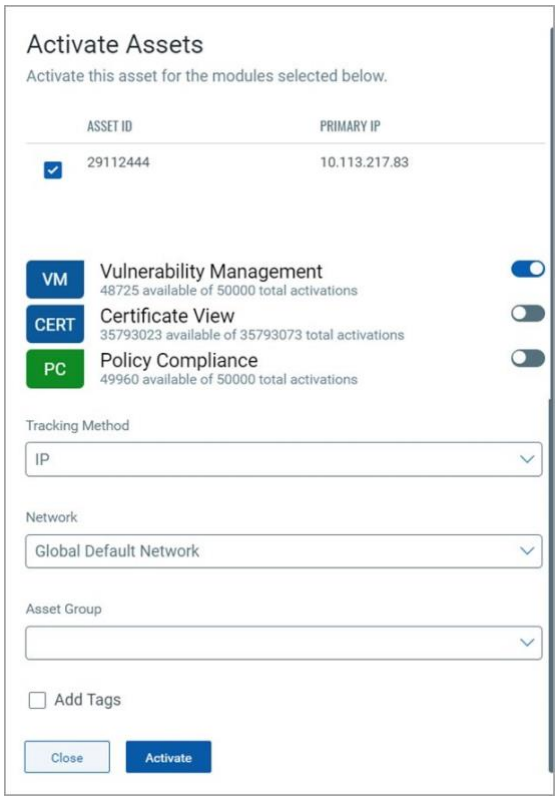
VM、PC、および CERT モジュールのアセットをアクティブ化する GAV CSAM

サイバーセキュリティアセットマネージメント (CSAM) から、脆弱性マネージメント (VM)、ポリシーコンプライアンス (PC)、証明書ビュー (CERT) モジュールのために、EASM、PS、サードパーティなどのソースを通じて検出されたアセットをアクティブ化できます。

注: アセットのアクティベーションは、AWS、Azure、GCP のクラウドアセットおよび QAGENT アセットの追跡方法ではサポートされていません。

アセットは、個々のモジュールまたは 3 つのモジュールすべてに対して同時にアクティブ化できます。すべてのモジュールに対してアセットをアクティブ化すると、**Activate** オプションがオフになります。
Inventory > Assets タブに移動し、アセットの Quick Actions メニューから Activate をクリックして、VM、PC、または CERT モジュールのアセットをアクティブ化します。





それぞれのモジュールの横にあるトグルを有効にして、アセットを割り当てる追跡方法、ネットワーク、およびアセットグループを選択します。

また、必要に応じて、アセットにタグを追加し、Activate をクリックします。.

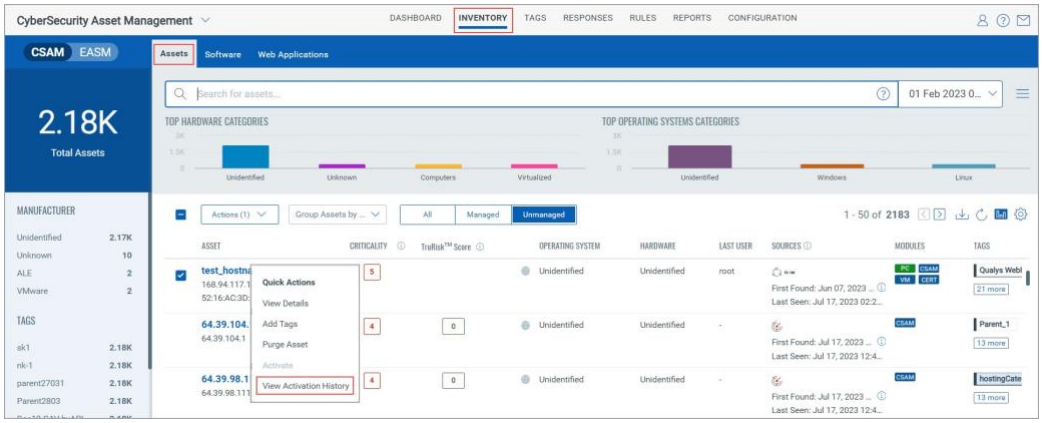
必要なモジュールのアセットをアクティブ化すると、そのアセットの IP アドレスがそれぞれのモジュールスキャン用に追加されます。

詳細は Online Help をご欄下さい。

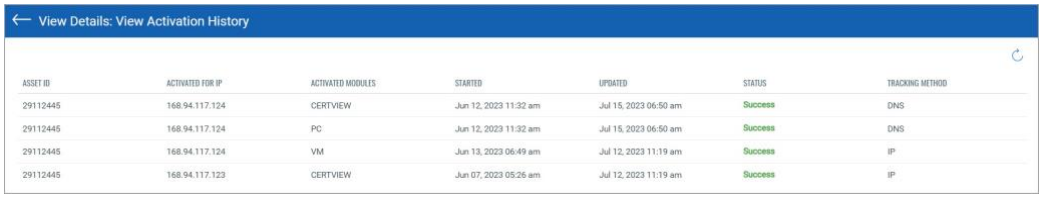
アセットのアクティベーション履歴の表示 GAV CSAM

VM、PC、または CERT モジュールをアクティブ化したアセットのアクティブ化履歴を表示できます。

Inventory > Assets タブに移動し、アセットの Quick Actions メニューから View Activation History をクリックします。



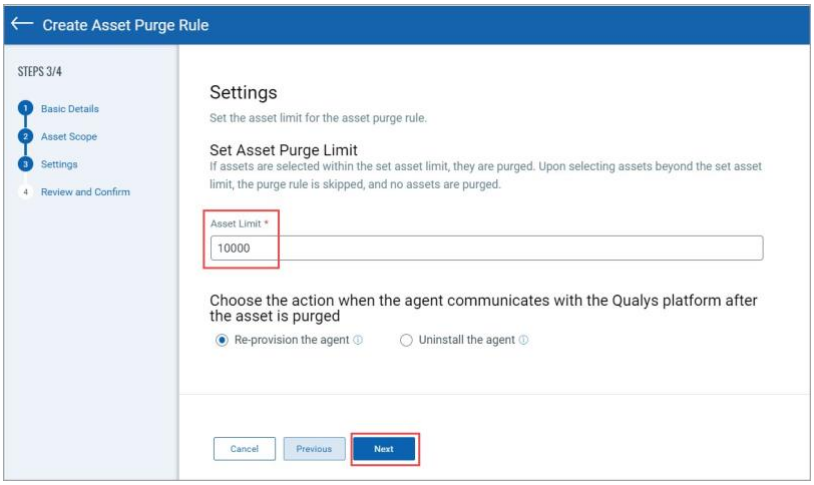
アセット ID、アクティブ化されたモジュール、状態などのアクティブ化の詳細を確認できます。



パージ・ルール作成の新しいオプション GAV CSAM

このリリースでは、アセットパージルールの作成ワークフローに新しいオプションが導入されました。
アセットが消去された後にエージェントが Qualys プラットフォームと通信するときに、エージェントで新しいアセットを作成するか、エージェントをアンインストールするかを決定できます。
詳細については、オンラインヘルプを参照してください。

注:デフォルトでは、**Re-provision the agent** が選択されており、その結果、エージェントは新しいアセットを作成します。**Uninstall Agent** を選択すると、エージェントはホストからアンインストールされます。
また、新規および既存のルールに対して **Re-provision the agent** が既定で選択されています。



対処された問題

- 一部のコネクタでコネクタの処理が完了する際にエラーが発生する問題を修正しました。
- インストールされているアセットに対して誤ったバージョンの Oracle Web Logic サーバー ソフトウェアが表示される問題を修正しました。
- クラウドエージェントアセットの CSAM UI での OS 名の表示方法に関する不整合の問題を修正しました。

- asset.cpuCount とプロセッサ.numberOfCpu トークンを使用する QQL クエリで誤った結果が表示される問題を修正しました。
- 新しくカタログ化された ″その他″ ソフトウェアに対して誤ったハッシュキーが生成され、不明とされるソフトウェアの正規化が正しく行われない問題を修正しました。
- 複数のスーパー ユーザーを持つ顧客で、レポートの生成要求を送信しなかったスーパー ユーザーから EASM 概要レポート通知が送信されるという問題が観察されました。
- この問題が修正され、EASM サマリー レポートの生成時に、レポートを生成したスーパー ユーザーから通知が送信されるようになりました。