Qualys クラウドプラットフォーム（VM、PC）v10.x

リリースノート

バージョン 10.2

2020 年 7 月 9 日（2020 年 7 月 28 日更新）

Qualys クラウドプラットフォーム (VM、PC) の新リリースでは、Vulnerability Management と Policy Compliance が改善されています。

Qualys クラウドプラットフォーム

認証レコードメニューの再構築
「Agentless Tracking Identifier」および「Asset Tracking & Data Merging」の変更
Unix 認証レコードに対象の種類を追加するためのサポート

Qualys Policy Compliance（PC）

MS SharePoint に対する新しい Vault のサポート
新しい OCA テクノロジのサポート
Microsoft Windows 2008、2012、2016 の認証局
IBM Sterling Connect: Direct 4.x（Unix）

Qualys Vulnerability Management（VM）

ユーザ削除機能の強化

Qualys 10.2 では、多くの改善と更新が実施されました。詳細

無断複写・転載を禁じます。2020 年 クォリスジャパン株式会社

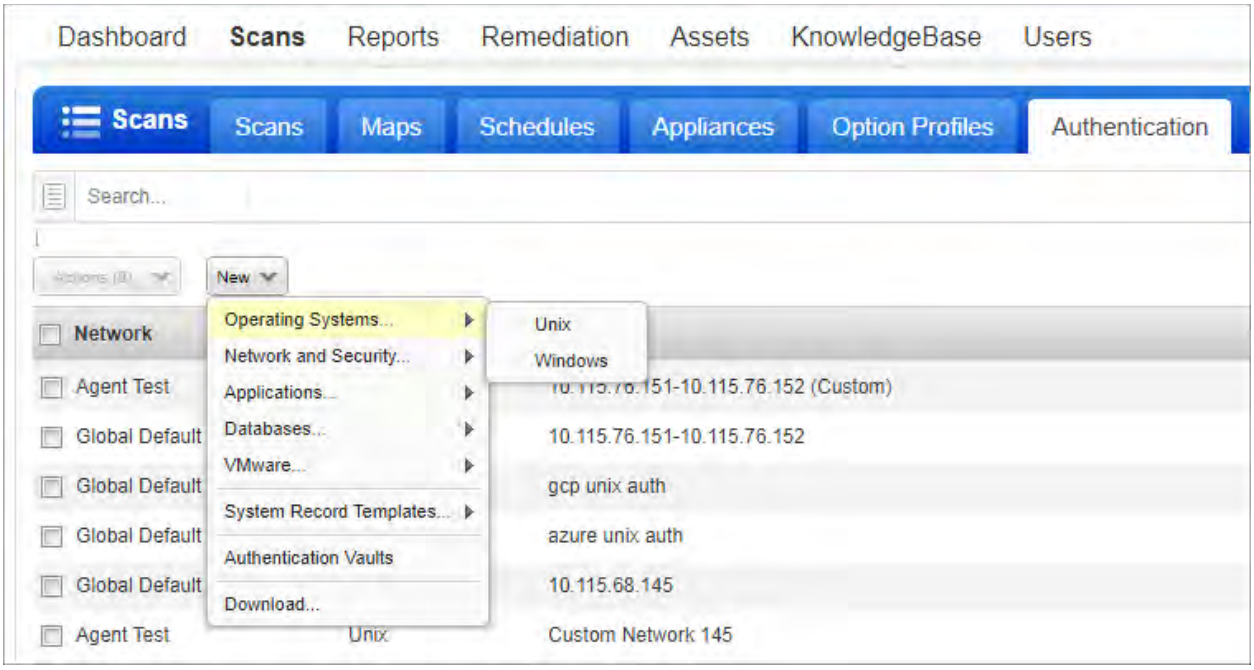
Qualys クラウドプラットフォーム

認証レコードメニューの再構築

認証レコードのメニュー項目を再構築し、認証レコードをレコードタイプやファミリに基づくカテゴリに論理的にまとめました。タイプ/ファミリが同じ認証レコードが同じカテゴリに分類されるようになります。

例えば、次のようになります。「Operating Systems」では、Unix や Windows などのオペレーティングシステムの認証レコードを作成するためのオプションが表示されます。同じように、「Applications」カテゴリには、Apache Web Server や Docker といったアプリケーションの認証レコードを作成するためのオプションが含まれます。その他にも、「Network and Security」、「Databases」、「VMware」、「System Record Templates」といったカテゴリがあります。

認証レコードにアクセスするには、VM および PC モジュールで「Scans」→「Authentication」を選択します。



次の表に、新しい構造に基づくカテゴリとそのカテゴリに分類される認証レコードをリストします。この表において、PC + SCA と記載されている認証レコードは、PC + SCA モジュールでのみ使用できます。また、VM のみと記載されている認証レコードは、VM モジュールでのみ使用できます。それ以外の（PC + SCA）または（VM のみ）という記載がない認証レコードはすべて VM と PC の両方で使用できます。

カテゴリ	認証レコード
Operating Systems	- Unix - Windows
Network and Security	- CheckPoint Firewall（PC + SCA） - Cisco - Palo Alto Networks Firewall - SNMP
Application Records	- Apache Web Server（PC + SCA） - Docker（PC + SCA） - HTTP Record（VM のみ） - IBM WebSphere App Server（PC + SCA） - JBoss Server - MS Exchange Server（PC + SCA） - MS IIS（PC + SCA） - MS SharePoint（PC + SCA） - Oracle HTTP Server（PC + SCA） - Oracle WebLogic Server - Tomcat Server
Databases	- IBM DB2 - Informix DB - MariaDB（PC + SCA） - MongoDB - MS SQL（PC + SCA） - MySQL - Oracle Listener - Oracle Record - Pivotal Greenplum（PC + SCA） - PostgreSQL（PC + SCA） - Sybase
VMWare	- vCenter Mapping List - vCenter Mapping Upload - vCenter - VMware ESXi
System Record Templates	Oracle System Record Template
Authentication Vaults	変更なし
Download	変更なし

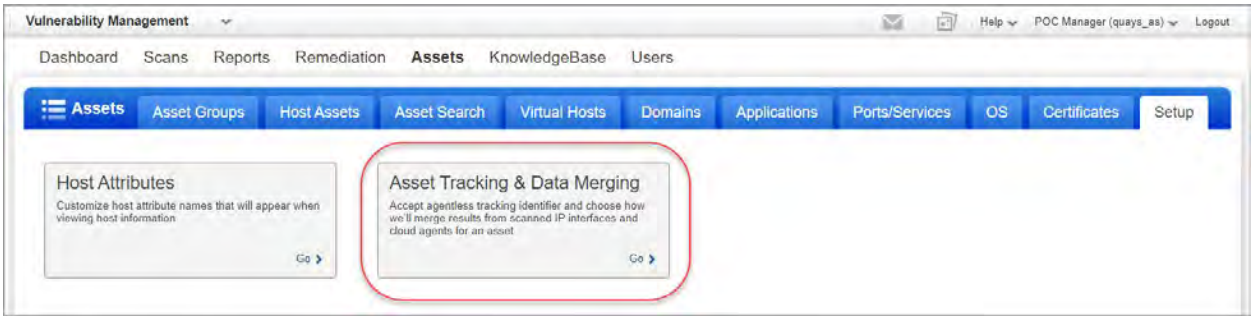
「Agentless Tracking Identifier」および「Asset Tracking & Data Merging」の変更

「Assets」の下に「Asset Tracking & Data Merging」という新しい設定オプションを追加したことで、エージェントレス追跡識別子機能を承認したり、アセットについてスキャンした IP インタフェースおよびクラウドエージェントからの結果をマージする方法を選択したりできるようになります。これらすべてを同じ設定ウィンドウで行うことができます。これにより、設定の利便性が向上します。

この新しい設定オプションは、以下に代わるものです。

- これまで「Scans」→「Setup」にあった「Agentless Tracking」オプション

- これまで「Users」→「Setup」にあった「Cloud Agent Setup」オプション

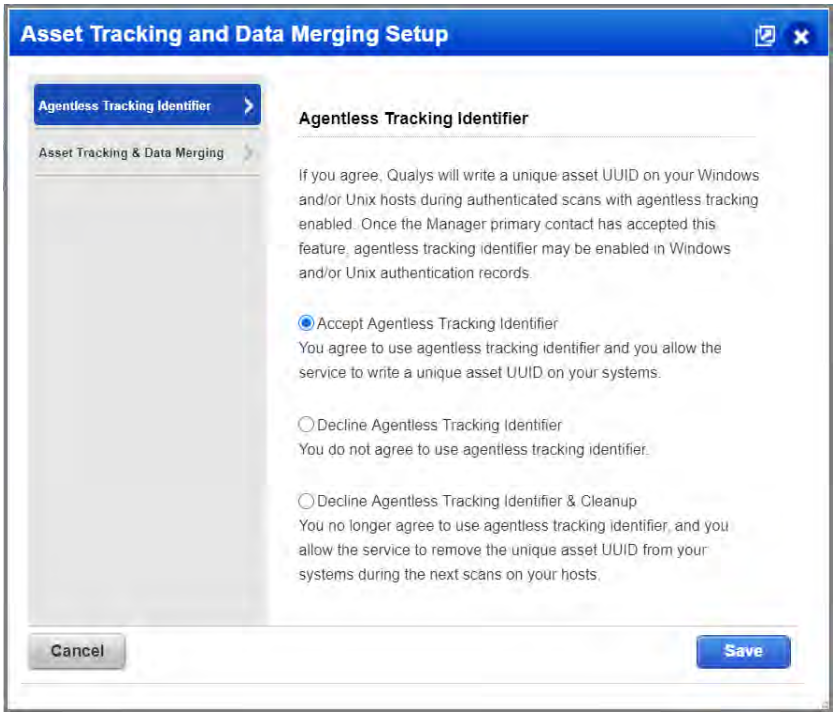


Agentless Tracking Identifier

この項では、一次連絡先となるマネージャがエージェントレス追跡識別子機能を承認または拒否することができます。エージェントレス追跡識別子を使用してホストをスキャンすると、一意のアセット UUID でホストが追跡されます。

設定手順

「Assets」→「Setup」→「Asset Tracking & Data Merging」→「Agentless Tracking Identifier」を選択します。この機能を承認または拒否するために適切なオプションを選択します。エージェントレス追跡識別子の使用を止め、次回のスキャン時にシステムから一意のアセット UUID を削除する場合は、「Decline Agentless Tracking Identifier and Cleanup」オプションを選択します。

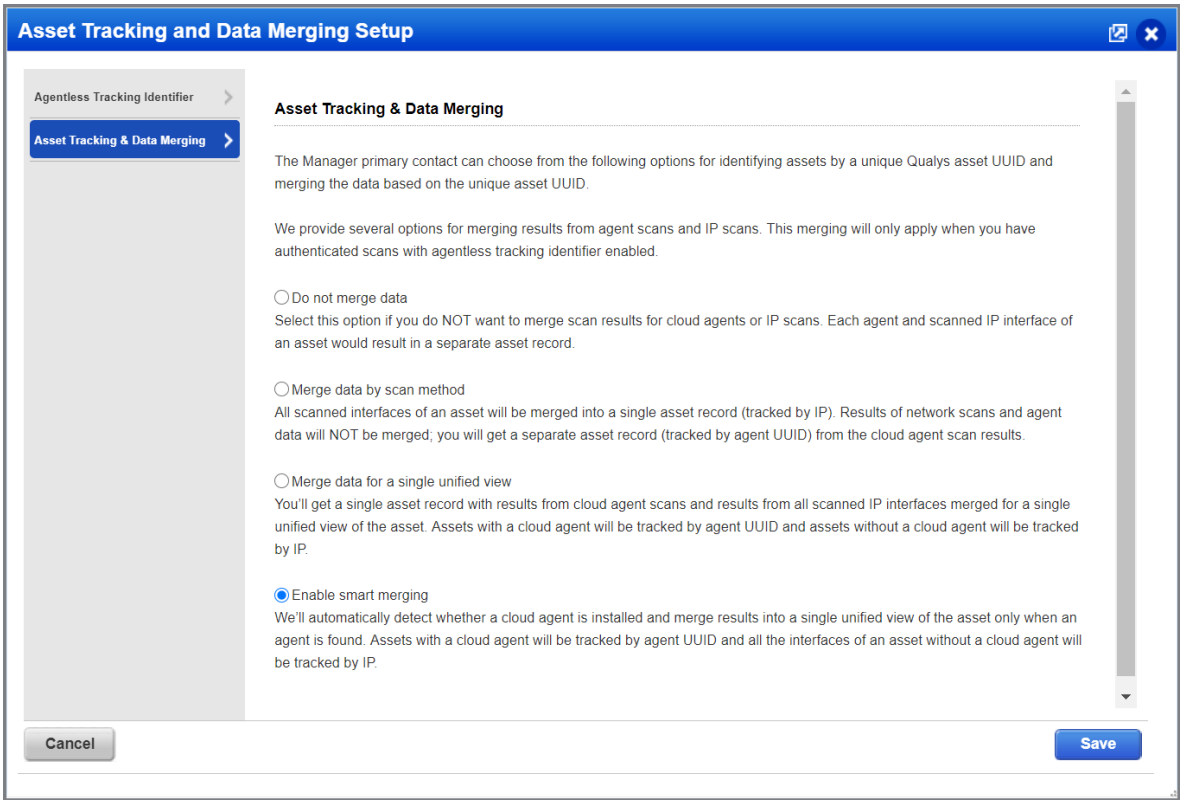


Asset Tracking & Data Merging

この項では、一次連絡先となるマネージャが一意のアセット UUID でアセットを識別したり、一意のアセット UUID に基づいてデータをマージしたりするためのオプションを提供します。今回のリリースでは、クラウドエージェントスキャンおよび IP スキャンからのスキャン結果をマージするための新しいオプションがいくつか導入され、より細かくコントロールできるようになります。適切なオプションを選択してください。なお、結果のマージは、エージェントレス追跡識別子を有効にした状態でスキャンを認証している場合に限り適用されます。

設定手順

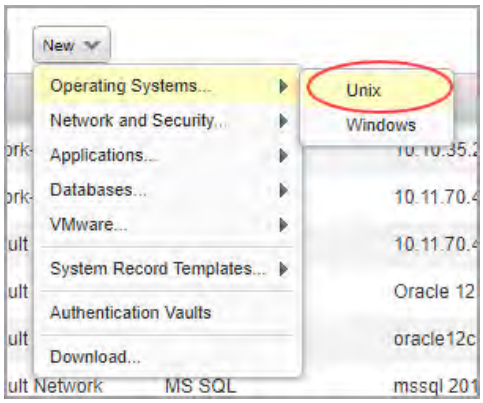
「Assets」→「Setup」→「Asset Tracking & Data Merging」→「Asset Tracking & Data Merging」を選択します。ページのいずれかのマージオプションを選択します。



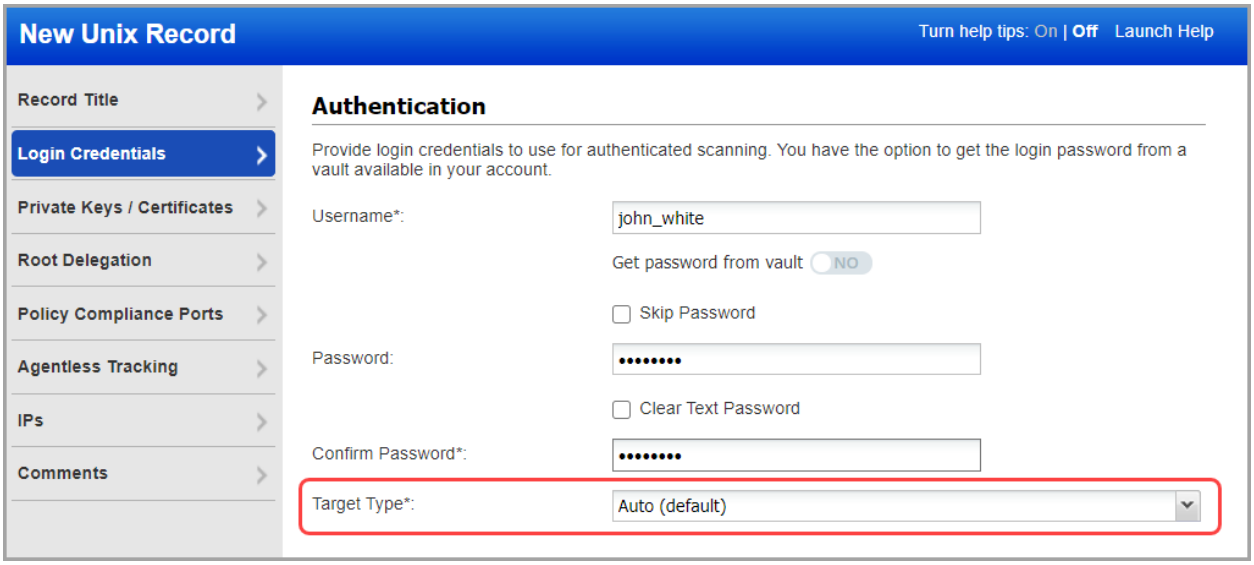
Unix 認証レコードに対象の種類を追加するためのサポート

Unix（SSH2）認証レコードの作成または更新時に対象の種類を指定できるようになります。このフィールドが追加されたことで、シェルベース以外の対象の種類を SSH2 認証レコードで定義することができます。標準の Unix シェルの対象は引き続き自動検出されます。今回のリリースでは、「Auto (default)」オプションのみを提供します。その他の対象の種類については、今後のリリースで提供していく予定です。

新しい Unix レコードを作成するには、「Scans」→「Authentication」→「New」に移動し、「Operating Systems」から「Unix」を選択します。



レコード作成ウィザードで、「Login Credentials」タブに移動すると、「Target Type」で「Auto (default)」値が選択されます。



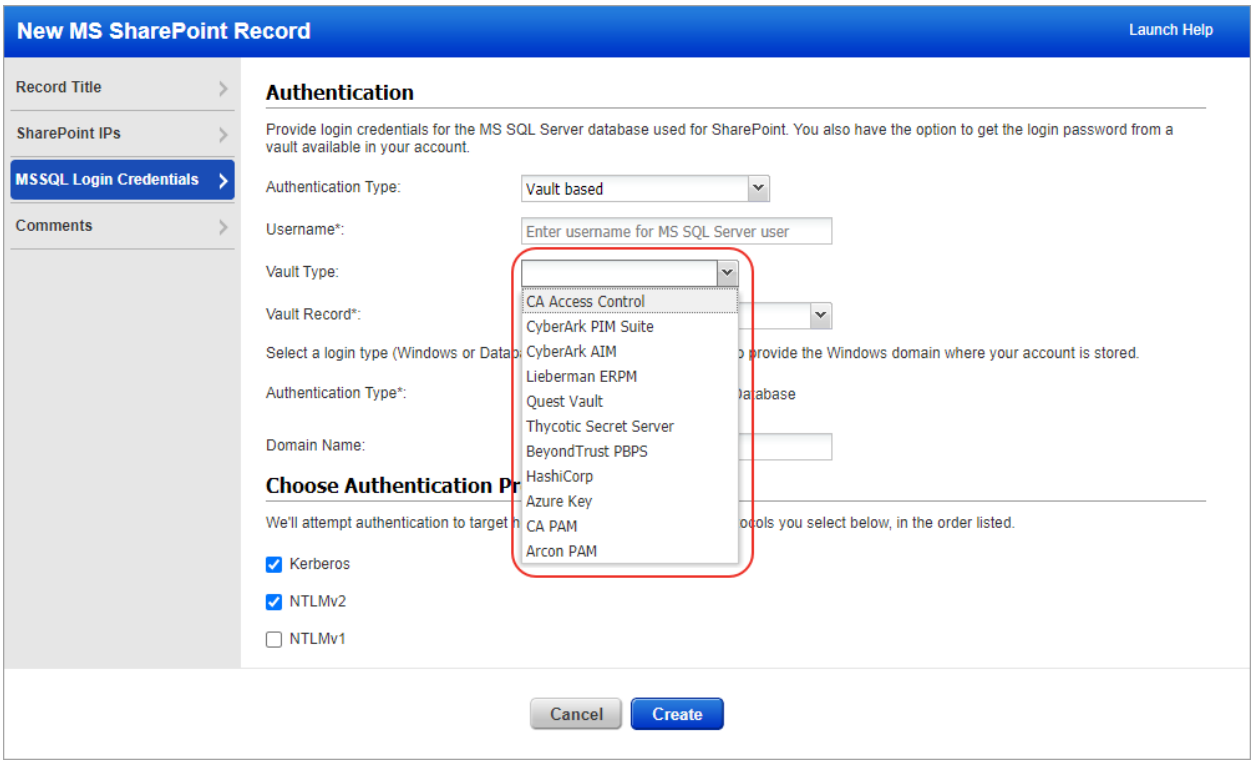
編集のために既存の認証レコードを開くと、「Target Type」フィールドが表示されるようになります。このようなレコードに対して、対象の種類が「Auto (default)」に設定されます。

Qualys Policy Compliance（PC）

MS SharePoint に対する新しい Vault のサポート

MS SharePoint 認証にサポートされる Vault が増えたことで、ログイン資格情報を取得するためのオプションが多くなります。MS SharePoint 認証レコードで、更に Arcon PAM、Azure Key、CA Access Control、HashiCorp、Lieberman ERPM といった Vault が表示されるようになります。また、BeyondTrust PBPS、CA PAM、CyberArk AIM、CyberArk PIM Suite、Quest Vault、および Thycotic Secret Server の Vault については、MS SharePoint レコードで今後もサポートされます。

Vault を使用して新しい MS SharePoint レコードを作成するには、「Scans」→「Authentication」→「New」→「Application Records」→「MS SharePoint」を選択します。「MSSQL Login Credentials」タブで「Authentication Type」ドロップダウンから「Valut based」を選択し、Vault のタイプを選択します。



新しい OCA テクノロジのサポート

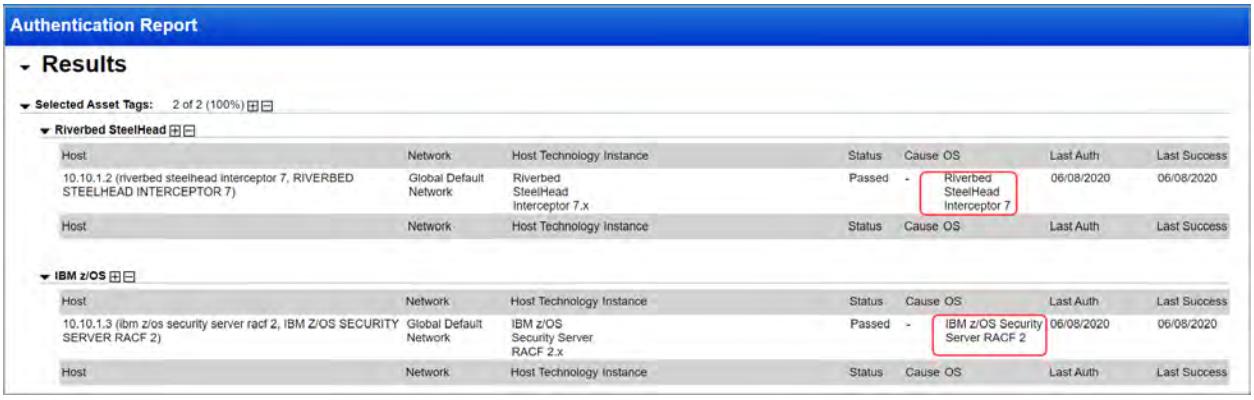
Out-of-Band Configuration Assessment（OCA）追跡を使用してデータを収集するアセット上で、次の新しいテクノロジがサポートされるようになりました。

- Riverbed SteelHead Interceptor 7.x
- IBM z/OS Security Server RACF 2.x

コンプライアンス状態を表示するには、「Reports」タブに移動し、これらのテクノロジのポリシーコンプライアンスレポートと認証レポートを実行するだけです。

レポートのサンプル

次の例は、Riverbed SteelHead Interceptor 7.x および IBM z/OS Security Server RACF 2.x の認証レポートのサンプルです。



Authentication Report

Results

Selected Asset Tags: 2 of 2 (100%)

Riverbed SteelHead

Host	Network	Host Technology Instance	Status	Cause OS	Last Auth	Last Success
10.10.1.2 (riverbed steelhead interceptor 7, RIVERBED STEELHEAD INTERCEPTOR 7)	Global Default Network	Riverbed SteelHead Interceptor 7.x	Passed	-	Riverbed SteelHead Interceptor 7	06/08/2020	06/08/2020
Host	Network	Host Technology Instance	Status	Cause OS	Last Auth	Last Success

IBM z/OS

Host	Network	Host Technology Instance	Status	Cause OS	Last Auth	Last Success
10.10.1.3 (ibm z/os security server racf 2, IBM Z/OS SECURITY SERVER RACF 2)	Global Default Network	IBM z/OS Security Server RACF 2.x	Passed	-	IBM z/OS Security Server RACF 2	06/08/2020	06/08/2020
Host	Network	Host Technology Instance	Status	Cause OS	Last Auth	Last Success

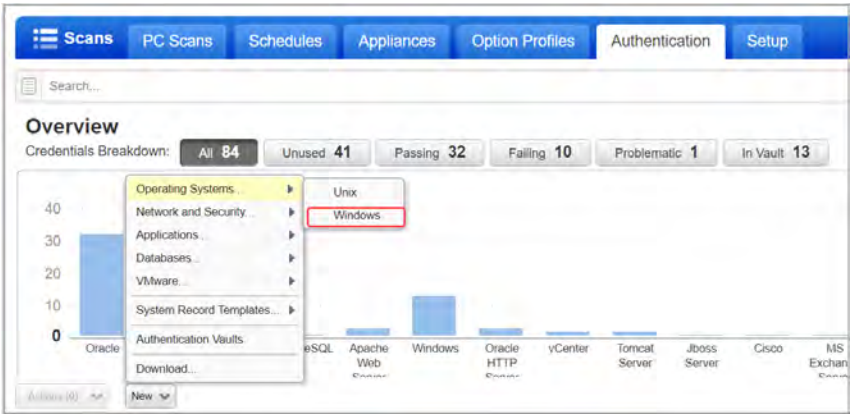
Microsoft Windows 2008、2012、2016 の認証局

Windows 認証のサポートが拡張され、Windows 2008、2012、2016 の認証局が対象となりました。

Windows 2008、2012、2016 の認証局を認証し、コンプライアンススキャンを実行するには、Windows レコードが必要です。

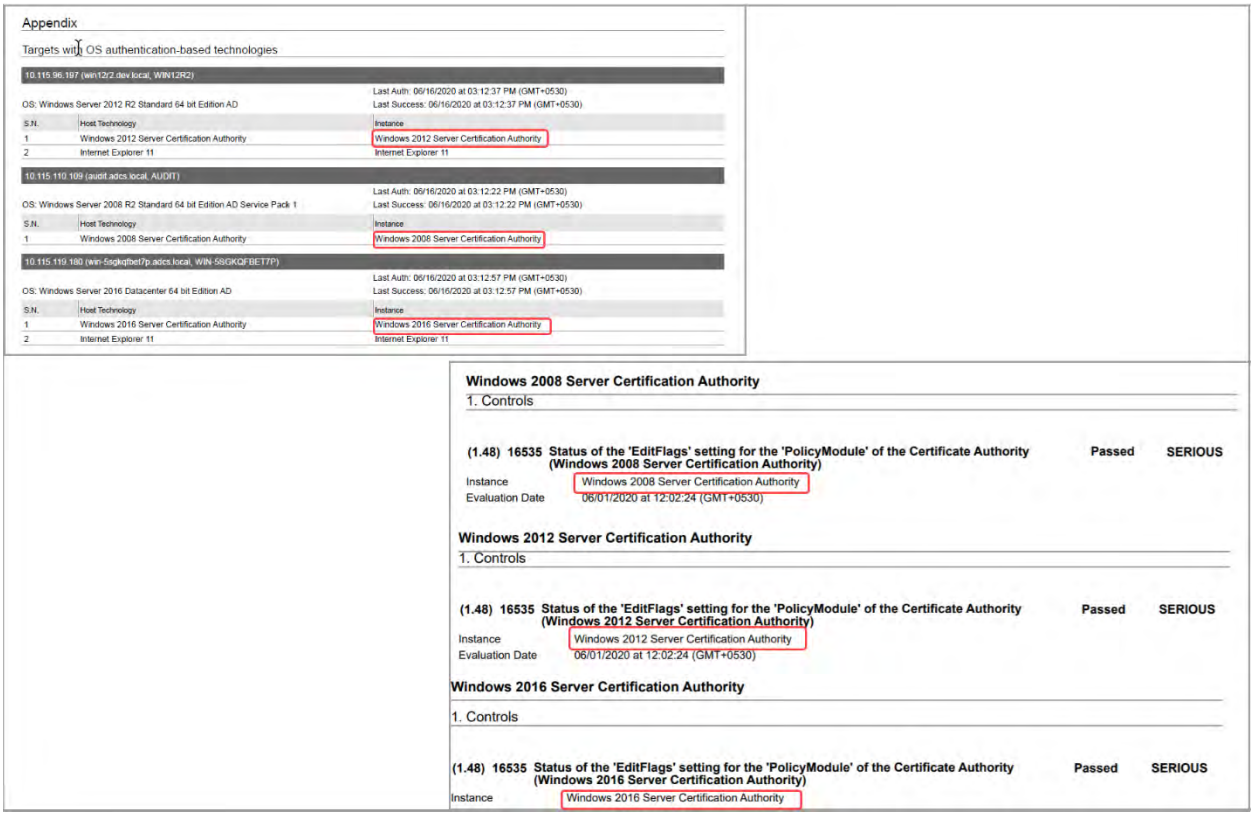
操作手順

「Scans」→「Authentication」を選択し、「New」→「Operating Systems」を選択します。



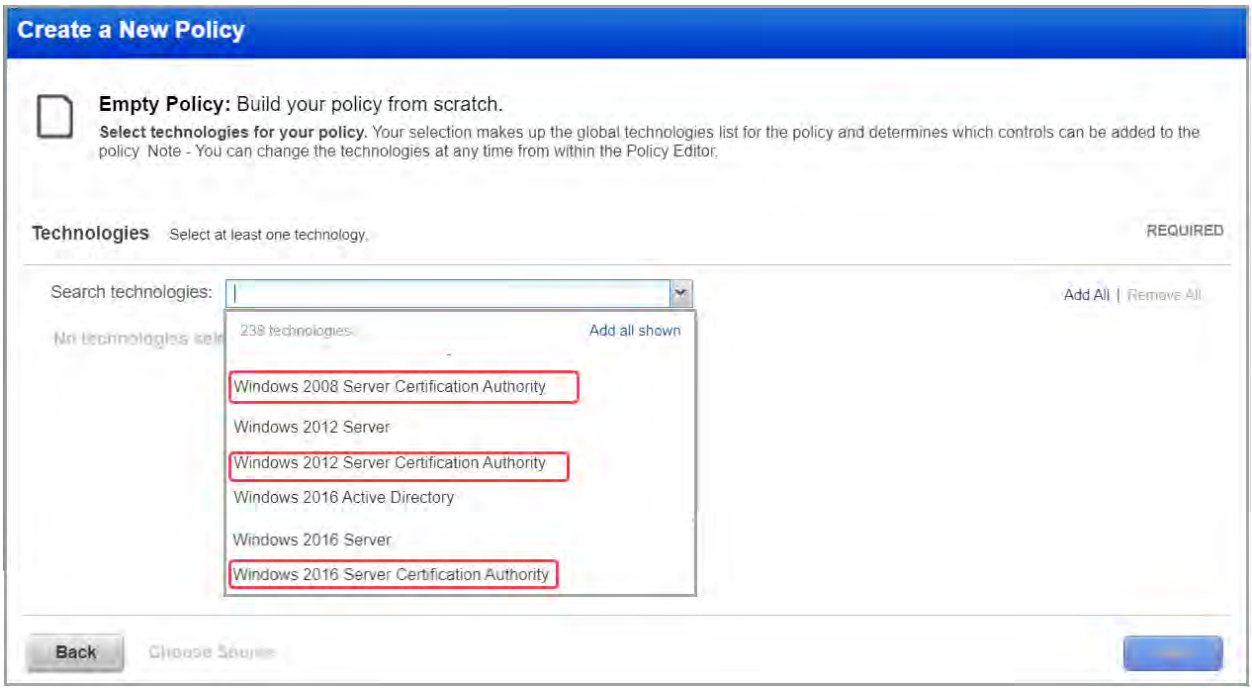
レポートのサンプル

認証レポートとポリシーレポートに、Windows 2008、2012、2016 の認証局インスタンスが表示されます。



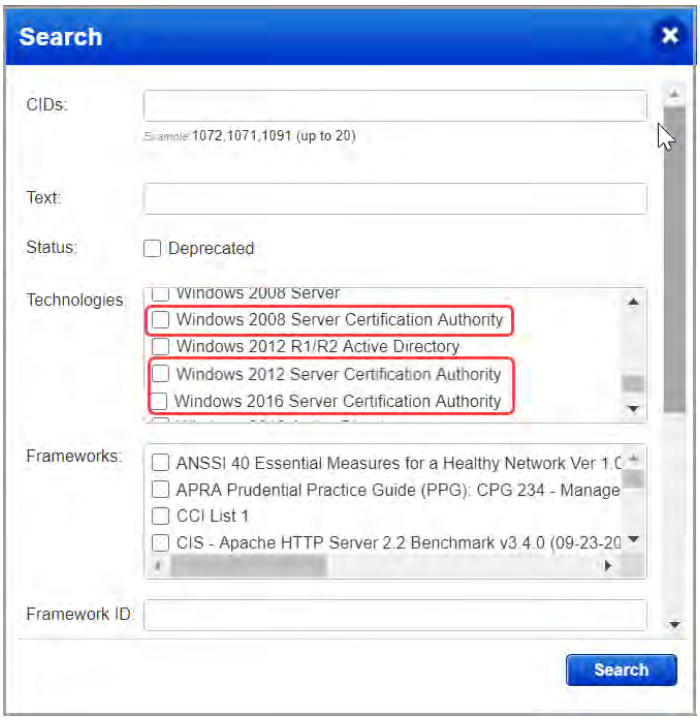
ポリシーとコントロール

新しいポリシーを作成するときにも、テクノロジのリストに Windows 2008、2012、2016 の認証局が表示されます。



コントロールの検索

テクノロジでコントロールを検索するときに、Windows 2008、2012、2016 の認証局が表示されます。



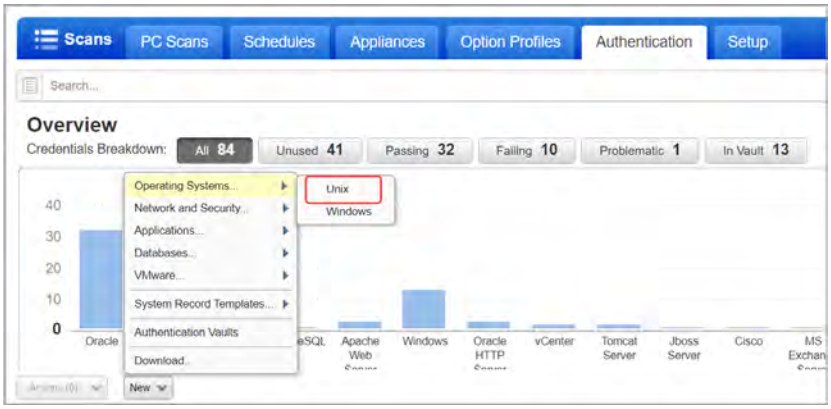
IBM Sterling Connect: Direct 4.x（Unix）

Unix 認証のサポートが拡張され、IBM Sterling Connect: Direct 4.x（Unix）が対象となりました。

IBM Sterling Connect: Direct 4.x（Unix）を認証し、コンプライアンススキャンを実行するには、Unix レコードが必要です。

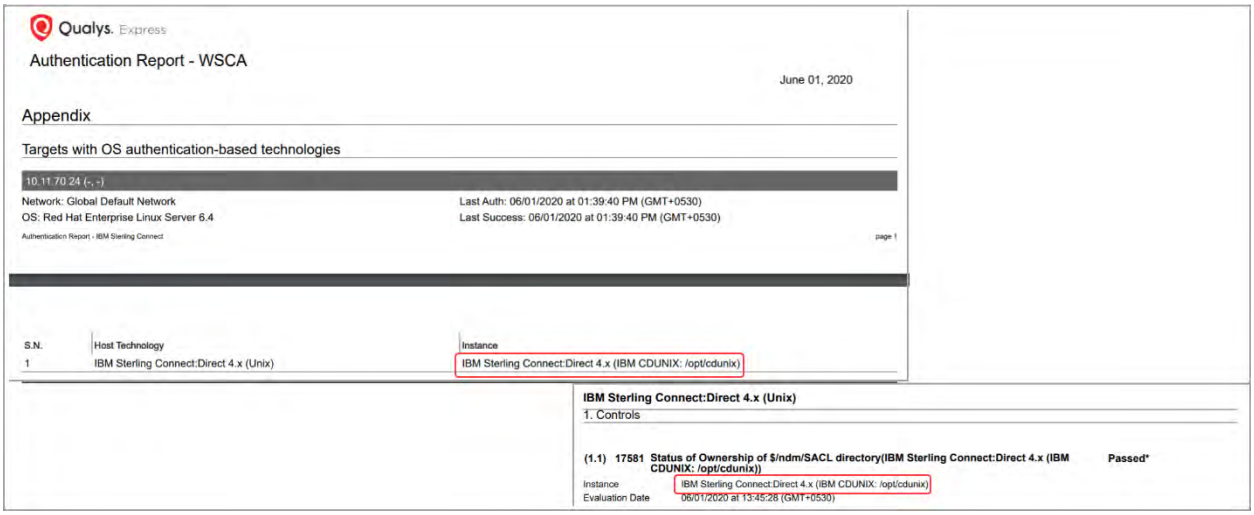
操作手順

「Scans」→「Authentication」を選択し、「New」→「Operating Systems」→「Unix」を選択します。



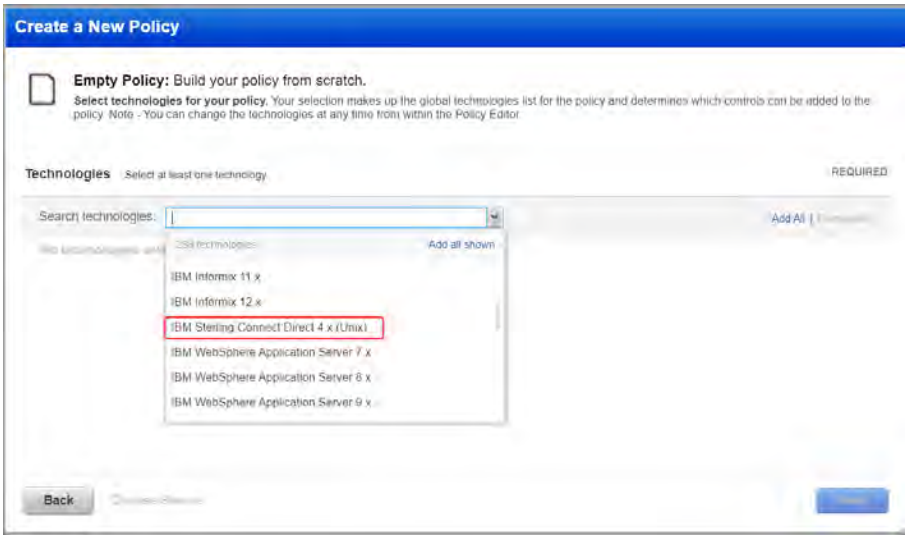
レポートのサンプル

認証レポートとポリシーレポートに、IBM Sterling Connect: Direct 4.x（Unix）インスタンスが表示されます。



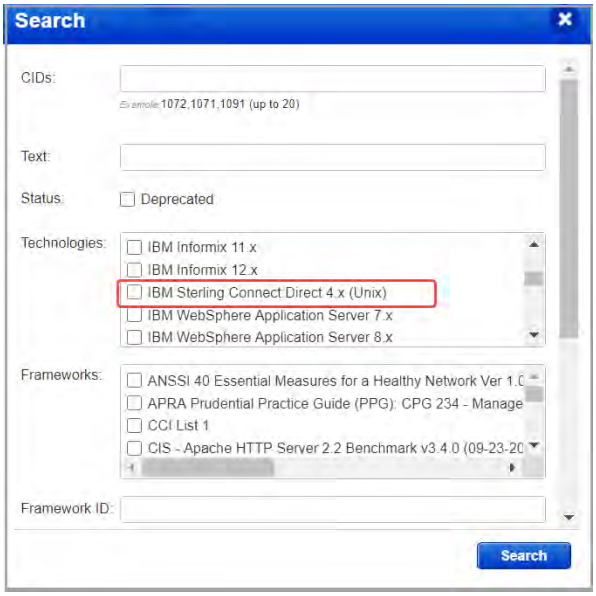
ポリシーとコントロール

新しいポリシーを作成するときに、テクノロジのリストに IBM Sterling Connect: Direct 4.x（Unix）も表示されます。



コントロールの検索

テクノロジでコントロールを検索するときに、IBM Sterling Connect: Direct 4.x（Unix）が表示されます。



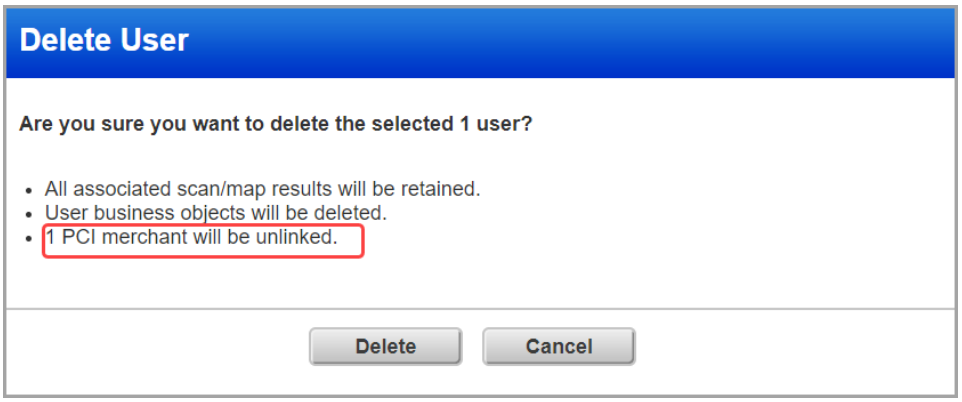
Qualys Vulnerability Management（VM）

ユーザ削除機能の強化

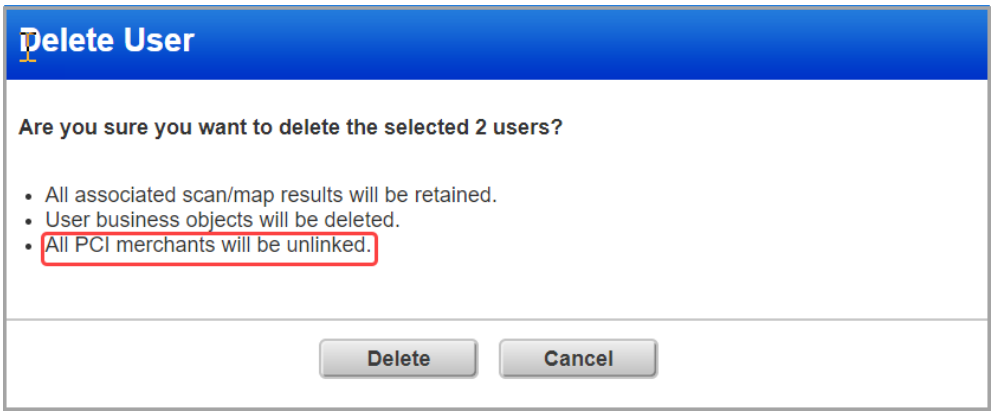
ユーザ削除機能を次のように強化しました。

VM ユーザを削除すると、PCI アカウントから自動的にリンクが解除され、次のような通知メッセージが表示されます。

1）1 人のユーザを削除する場合は、次のメッセージが表示されます。



複数のユーザを削除する場合は、次のメッセージが表示されます。



2）PCI アカウントにリンクされているユーザを削除した場合、同じ PCI アカウントを別のユーザにリンクさせることができます。

問題点の改善

- サブスクリプションに設定されている同時制限に達したためにスキャンが遅延した場合、スケジュールされている開始時間ではなく、スキャンの実際の開始時間に基づいてスキャンのキャンセル時間が計算されるという問題が修正されました。
- ユーザ定義コントロールの「References」ページで「Delete」リンクが機能しないという問題が修正されました。
- 期待値に一重引用符が含まれるコントロールのポリシーを保存できないという問題が修正されました。
- アセット数が 8000 を超えるアセットグループで対話形式レポートを実行しようとすると、コントロール/ホスト選択ページが読み込まれないというパフォーマンスの問題が修正されました。
- データが含まれ、複数のモジュールに存在するアセットをパージすると、データ全体がパージされるという問題が修正されました。
- 状態 API の CSV 出力で合格/不合格日付列に正しい値が表示されないという問題が修正されました。API 呼び出しで、改善情報の有無に関係なく、正しい CSV 出力が表示されるようになります。
- エクスポートしたポリシーでユーザ定義コントロールの評価に設定した期待値が、このポリシーを PC にインポートすると、元の値にリセットされるという問題が修正されました。修正後は、ユーザ定義コントロールに設定された新しい期待値が、インポートしたポリシーでも保持されるようになります。
- IP アドレスを使用してホストアセットを追加する場合、IP アドレスに非表示/特殊文字が存在することでエラーになっていたという問題が修正されました。
- 期待値の自動更新を選択した場合の FIM/DI UDC の処理のパフォーマンスが改善されました。これにより、ポリシーのコントロールを更新/評価する際の遅延が解消されます。
- 最初のホストで最初に不合格となったコントロールの XML レポートで、「Cause of Failure」の <Unexpected>/<Unexpected> 項に複数の基準がリストされるという問題が修正されました。インスタンスに単一の基準または予期される基準が表示されるようになります。
- ポリシーコンプライアンススコアカードレポートに関連するパフォーマンスの問題が修正されました。
- 非ネットワークアカウントに対する IP アセット選択を使用した STIG レポート生成に関する問題が修正されました。
- コントロールの参照フィールドに一重引用符が含まれる場合、ポリシーを保存できないという問題が修正されました。
- ホストリスト API 応答で EC2_INSTANCE_ID パラメータが表示されない問題が修正されました。
- 問題が修正され、Unix/Windows 設定パラメータがない MariaDB 認証レコードを API から更新できるようになりました。
- 状態 API データでアセットの DNS ホスト名に余分なスペースが追加されていた問題が修正されました。
- API ユーザガイドのセッションログインのための”パスワード ”入力パラメータの説明が更新され、-d および -u を使用した curl リクエストの作成方法が明確になりました。
- オンラインヘルプが更新され、アプライアンスのインジケータがアイコンでどのように表現されるかが記載されるようになりました。
- オンラインヘルプが更新され、ファイアウォールインスタンスへの認証のために、Palo Alto Networks Firewall レコードを作成する方法が記載されるようになりました。
- API ユーザガイドが更新され、/msp/ignore_vuln.php に対する API の詳細に関する情報が追加されました。
- MongoDB 認証のオンラインヘルプが更新され、サポートされている認証のタイプが正確にリストされるようになりました。