Tenable Identity Exposure 3.x ユーザーおよび管理者ガイド

最終更新日: 2024 年 4 月 5 日

目次

Tenable Identity Exposure にようこそ

最終更新日: 2024/04/30

Tenable Identity Exposure (旧 Tenable.ad) は、脅威を予測し、侵害を検出し、インシデントや攻撃に対応することにより、お客様がインフラのセキュリティを確保できるようにします。直感的に操作できるダッシュボードを使って Active Directory をリアルタイムで監視すれば、最も重大な脆弱性とそれに推奨される修正方法を一目で把握できます。Tenable Identity Exposure の攻撃インジケーターと露出インジケーターにより、Active Directory に影響を与える潜在的な問題を見つけたり、危険な信頼関係を特定したり、攻撃を詳しく分析したりできます。

> 攻撃インジケーターと露出インジケーターの機能は、ライセンスの種類によって利用範囲が異なります。

使い始めるには、Tenable Identity Exposure の使用を開始するを参照してください。

> **注意:** Tenable Identity Exposure は、単独で、または Tenable One パッケージの一部として購入できます。詳細は、Tenable One を参照してください。

> **ヒント:** *Tenable Identity Exposure ユーザーガイド*は、英語、日本語、ドイツ語、韓国語、中国語 (簡体字)、中国語 (繁体字) で提供されています。*Tenable Identity Exposure* のユーザーインターフェースは、英語、日本語、ドイツ語、フランス語、韓国語、中国語 (簡体字)、中国語 (繁体字) で提供されています。ユーザーインターフェース言語を変更するには、ユーザー環境設定をご覧ください。

Tenable Identity Exposure の詳細は、次のカスタマー向け説明資料で確認してください。

- Tenable Identity Exposure セルフヘルプガイド
- Tenable Identity Exposure はじめに (Tenable University)

Tenable One サイバーエクスポージャー管理プラットフォーム

Tenable One は、サイバーエクスポージャー管理プラットフォームです。DX 時代のアタックサーフェス全体の可視化、起こり得る攻撃を防ぐための取り組みへのフォーカス、サイバーリスクの正確な伝達を支援することで、最大限のビジネスパフォーマンスを発揮できるようにします。

このプラットフォームは、Tenable Research による高速で広範な脆弱性カバレッジを基盤に構築されており、IT 資産、クラウドリソース、コンテナ、ウェブアプリケーション、認証システムを合わせて網羅する、業界で最大の脆弱性カバレッジを提供します。包括的な分析機能も、対応措置の優先順位を付け、サイバーリスクを伝達してくれます。Tenable One を使用する企業は以下のことができます。

- DX 時代のアタックサーフェス全体を把握できる可視性を得る
- 起こり得る脅威に先駆けた攻撃防止対策の優先順位付け
- より適切な判断を可能にするサイバーリスクの伝達

Tenable Identity Exposure はスタンドアロン製品として存在しますが、Tenable One サイバーエクスポージャー管理プラットフォームの一部としても購入できます。

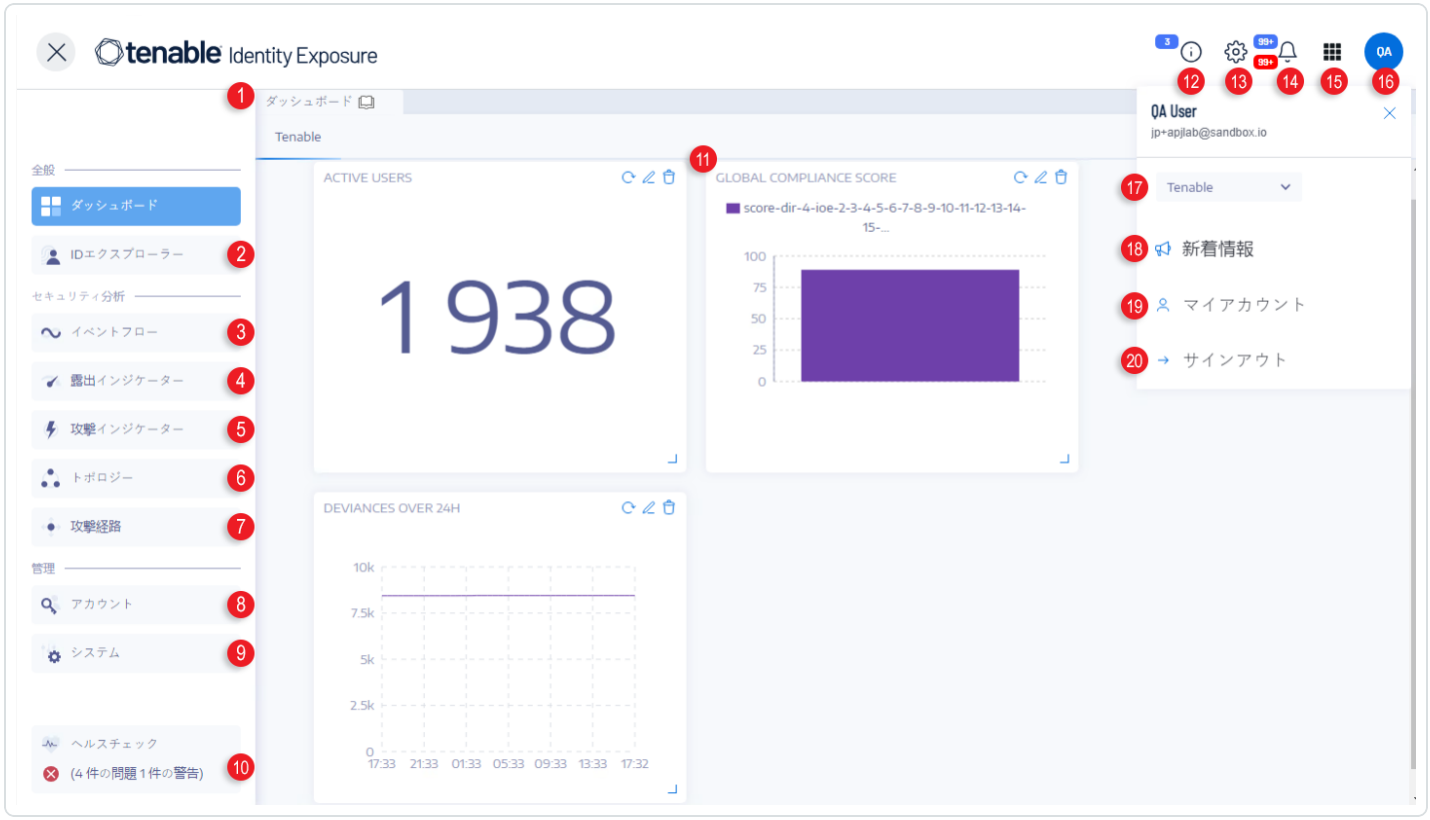
ヒント: Tenable One 製品の使用開始の詳細については、Tenable One デプロイメントガイドを参照してください。

Tenable Identity Exposure のナビゲーション

Tenable Identity Exposure にログインすると、この例に示すようなホームページが開きます。

サイドナビゲーションバーを展開または折りたたむには

- 展開するには、ウィンドウの左上にある ☰ メニューをクリックします。
- 折りたたむには、ウィンドウの左上にある **X** をクリックします。



#	名称	機能
1	ダッシュボード	ダッシュボードを使用すると、AD インフラのセキュリティを視覚的な方法で効率的に管理し、監視できます。
2	アイデンティティエクスプローラー	Tenable Identity Exposure のアイデンティティエクスプローラービューは、Active Directory と Microsoft Entra ID の両方のアイデンティティを統合します。この

		ビューには、リストされている各資産のアイデンティティリスクスコア(ベータ版)と、アイデンティティの侵害の考えられる到達範囲が表示されます。
3	イベント情報	イベント情報は、Active Directory に影響を与えるイベントのリアルタイムの監視と分析の結果を表示します。
4	露出インジケーター	Tenable Identity Exposure は露出インジケーター(IoE)を使用して、Active Directory のセキュリティの成熟度を測定し、監視と分析の対象となっているイベントの情報に深刻度レベル(重大、高、中、低)を割り当てます。
5	攻撃インジケーター	Tenable Identity Exposure は攻撃インジケーターを使用して攻撃をリアルタイムで検出できます。
6	Topology	トポロジーページは、Active Directory をインタラクティブなグラフで視覚化します。フォレスト、ドメイン、およびそれらの間に存在する信頼関係が表示されます。
7	攻撃経路	攻撃経路ページは、Active Directory の関係性をグラフで表します。 • 影響範囲: 侵害された可能性のある資産から発生した AD 内のラテラルムーブメントを評価します。 • 攻撃経路: 特定のエントリポイントから資産に到達する権限昇格の手法を予測します。 • 露出資産: サイバー空間に露出

		した資産の視覚化を使用して資産の脆弱性を測定し、すべての昇格経路に対処します。
8, 9	マネジメント **必要なユーザーロール**: 適切なアクセス許可を持つ組織のユーザー	このセクションでは、以下を設定できます。 • アカウント: ユーザーアカウント、ロール、セキュリティプロファイル • システム: フォレストとドメイン、アプリケーションサービス、アラート、認証 詳細は、Tenable Identity Exposure 管理者ガイドを参照してください。
10	ヘルスチェック	ヘルスチェックを使用すると、ドメインとサービスアカウントの設定を 1 つの統合ビューでリアルタイムに可視化でき、そこからドリルダウンして詳細情報を表示できます。
11	ウィジェット	ウィジェットは、ダッシュボード上のカスタマイズ可能なデータセットです。棒グラフ、折れ線グラフ、カウンターを含めることができます。
12	製品のアップデート	製品の最新機能に関する情報。
13	設定	システム設定、フォレストとドメインの管理、ライセンス、ユーザーとロールの管理、プロファイル、アクティビティログへのアクセス。
14	通知 (ベル)	確認待ちの攻撃アラートや露出アラートはベルのアイコンとバッジのカウントで通知されます。

15	アプリケーションスイッチャー	Tenable ワークスペースからアプリケーションを切り替えるには、このアイコンをクリックします。
16, 19	ユーザープロファイルアイコン (ユーザー環境設定)	このアイコンをクリックして、セキュリティプロファイル、リリースノート、アクティビティログ、環境設定、サインアウトのサブメニューにアクセスします。
17	セキュリティプロファイル	セキュリティプロファイルを使用すると、さまざまなタイプのユーザーが、さまざまなレポートの視点からセキュリティ分析をレビューすることができます。
18	新機能	クリックすると、Tenable Identity Exposure の最新バージョンのリリースノートが開きます。
20	サインアウト	クリックすると Tenable Identity Exposure からサインアウトします。

Tenable Identity Exposure にログインする

Tenable Identity Exposure のウェブアプリケーションにはクライアント URL からアクセスします。

Tenable Identity Exposure にログインするには、次のオプションのいずれかを選択します。

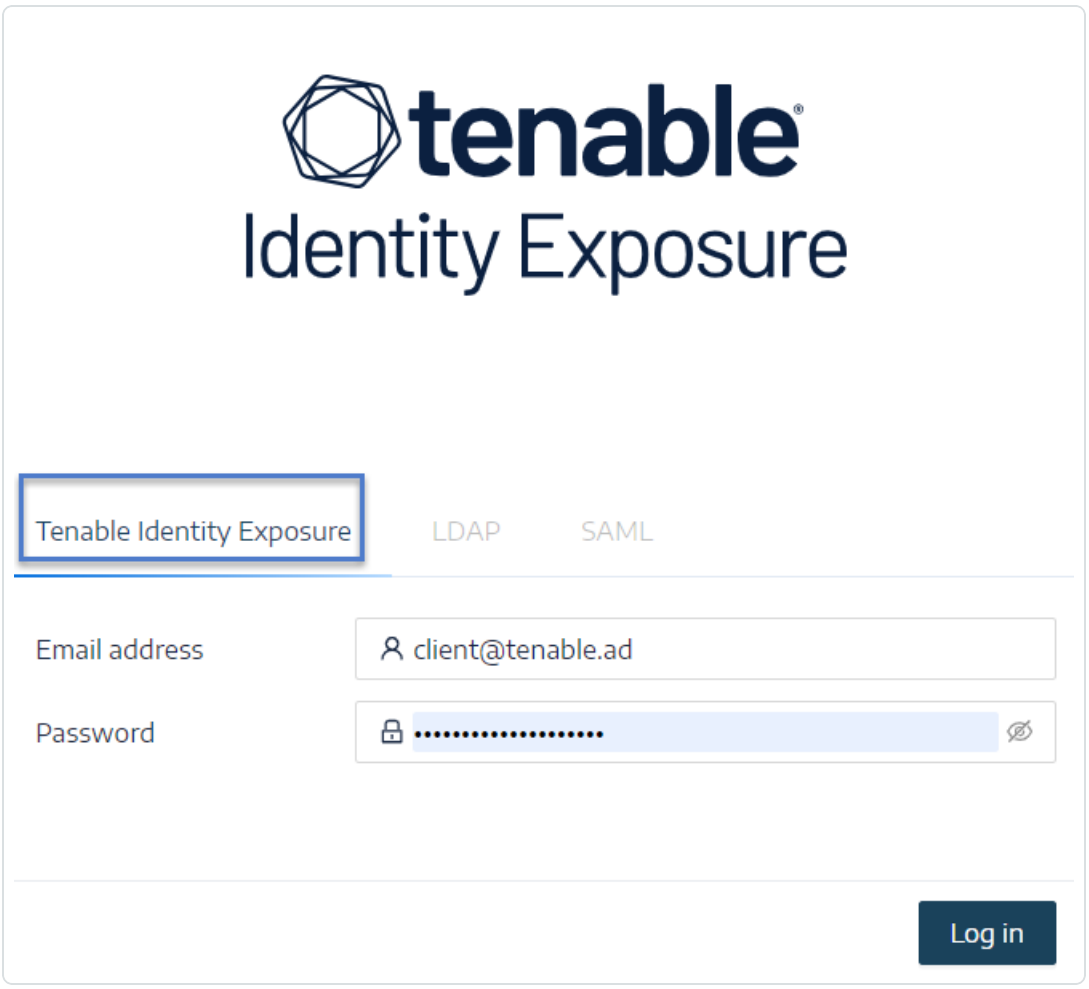
- ◦ Tenable Identity Exposure アカウントを使用する
  - ◦ LDAP アカウントを使用する
  - ◦ SAML を使用する

Tenable Identity Exposure アカウントを使用する

Tenable Identity Exposure アカウントを使用してサインインするには

1. 任意のブラウザのアドレスバーにクライアント URL (例: client.tenable.ad) を入力します。

   [ログイン] ウィンドウが表示されます。



2. **[Tenable Identity Exposure]** タブをクリックします。
3. メールアドレスを入力します。
4. パスワードを入力します。
5. **[ログイン]** をクリックします。

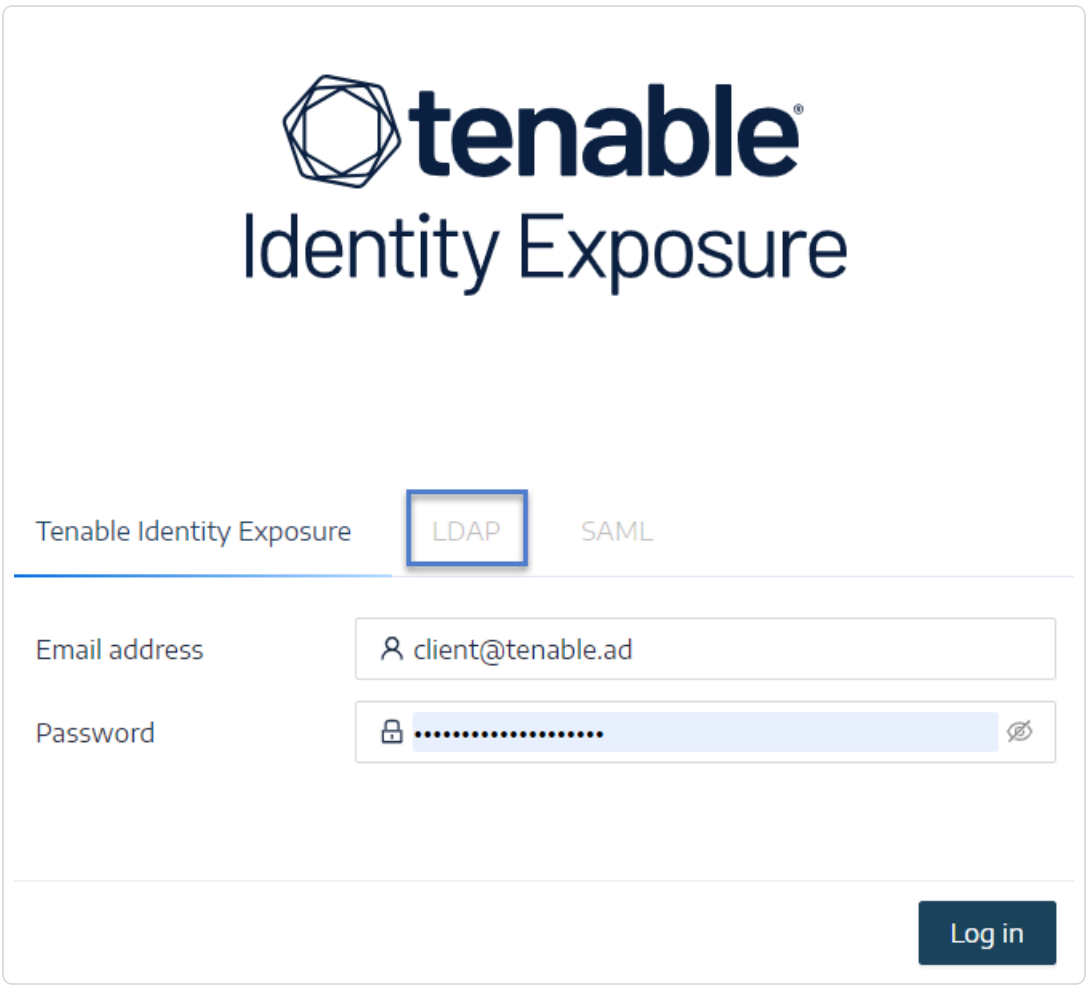
   Tenable Identity Exposure ページが開きます。

LDAP アカウントを使用する

LDAP を使用してサインインするには

1. 任意のブラウザのアドレスバーにクライアント URL (例: client.tenable.ad) を入力します。

   [ログイン] ウィンドウが表示されます。



2. **[LDAP]** タブをクリックします。
3. LDAP アカウント名を入力します。
4. LDAP パスワードを入力します。
5. **[ログイン]** をクリックします。

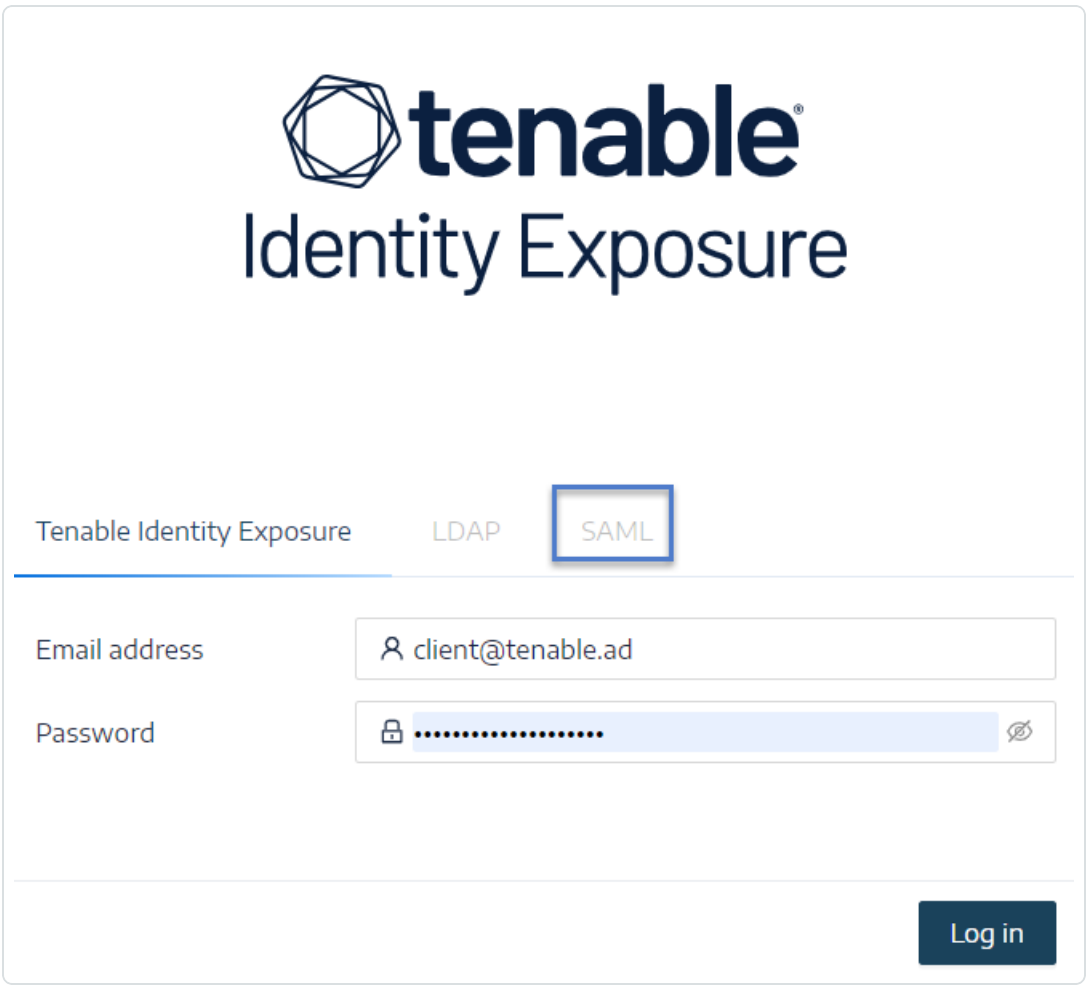
   Tenable Identity Exposure ページが開きます。

SAML を使用する

SAML を使用してサインインするには

1. 任意のブラウザのアドレスバーにクライアント URL (例 : client.tenable.ad) を入力します。

   [ログイン] ウィンドウが表示されます。



2. **[SAML]** タブをクリックします。
3. ID プロバイダー (IDP) へのリンクをクリックします。

   Tenable Identity Exposure により認証のために SAML サーバーにリダイレクトされます。
4. IDP で会社の認証情報を入力します。

   ログインユーザーとして Tenable Identity Exposure にリダイレクトされます。

警告: ログインに繰り返し失敗すると、Tenable Identity Exposure によってアカウントがロックされます。アカウントがロックされた場合は、管理者に連絡してください。

Tenable Identity Exposure からサインアウトするには

1. Tenable Identity Exposure で、**ユーザーアイコンをクリックします**。

   サブメニューが表 示されます。

2. **[サインアウト]** をクリックします。

   Tenable Identity Exposure **のログインページに戻ります**。

ワークスペースへのアクセス

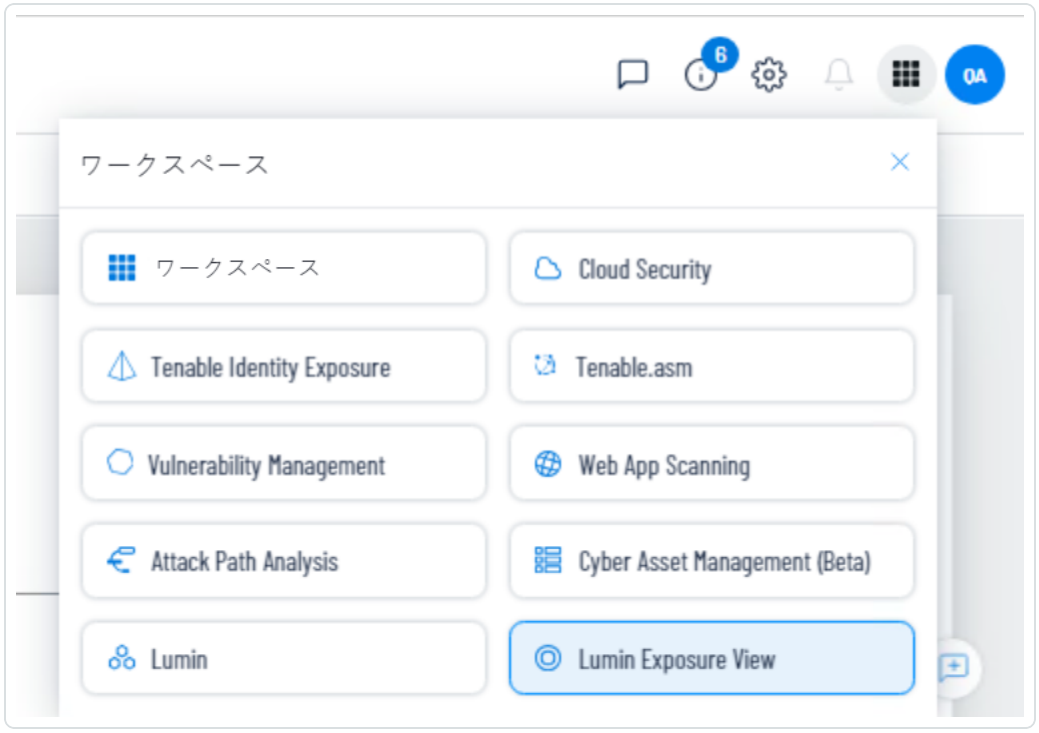
Tenable にログインすると、デフォルトで **[ワークスペース]** ページが表示されます。**[ワークスペース]** ページで、Tenable アプリケーションを切り替えたり、デフォルトのアプリケーションを設定して今後 **[ワークスペース]** ページをスキップするようにしたりできます。上部のナビゲーションバーに表示される **[ワークスペース]** メニューから、アプリケーションを切り替えることもできます。

ワークスペースメニューを開く

[ワークスペース] メニューを開く方法

1. いずれかの Tenable アプリケーションの右上隅にある ボタンをクリックします。

   [ワークスペース] メニューが表示されます。



2. アプリケーションタイルをクリックして開きます。

ワークスペースページを表示する

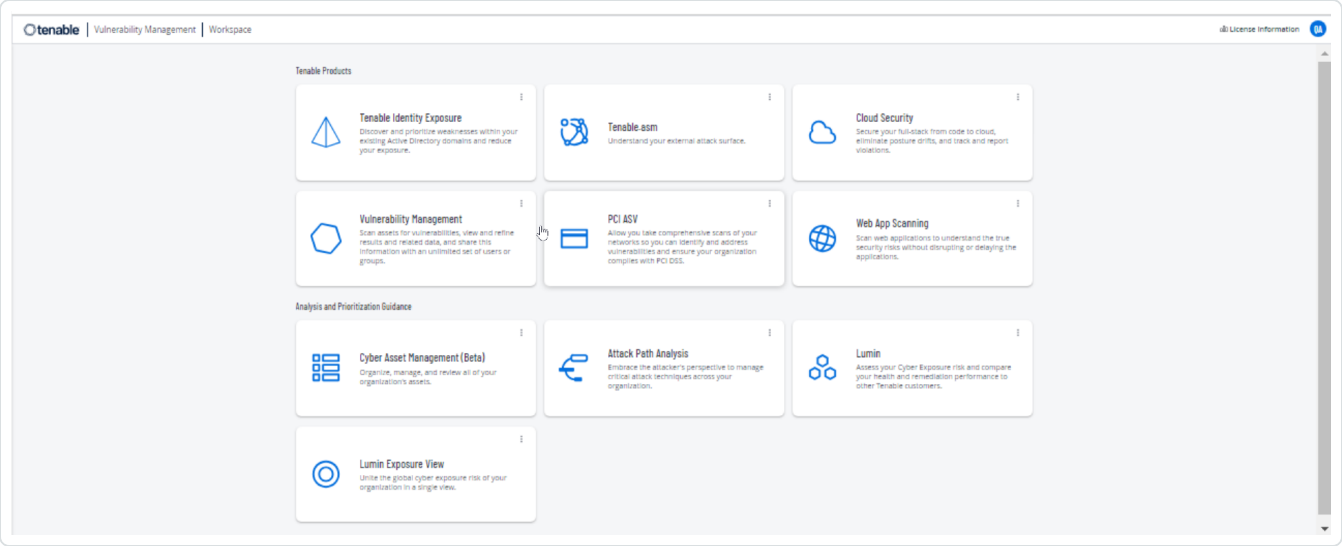
[ワークスペース] ページを表示する方法

1. いずれかの Tenable アプリケーションの右上隅にある ボタンをクリックします。

   [ワークスペース] メニューが表示されます。

2. **[ワークスペース]** メニューの **[ワークスペース]** をクリックします。

   [ワークスペース] ページが表示されます。



デフォルトのアプリケーションを設定する

Tenable にログインすると、デフォルトで **[ワークスペース]** ページが表示されます。ただし、今後 **[ワークスペース]** ページをスキップするように、デフォルトアプリケーションを設定することもできます。

> デフォルトでは、**管理者**、**スキャンマネージャー**、**スキャンオペレーター**、**標準**、**基本**のロールを持つユーザーは、デフォルトのアプリケーションを設定できます。別のロールをお持ちの場合は、管理者に連絡して、**[マイアカウント]** から **[管理]** アクセス許可をリクエストしてください。詳細については、カスタムロールを参照してください。

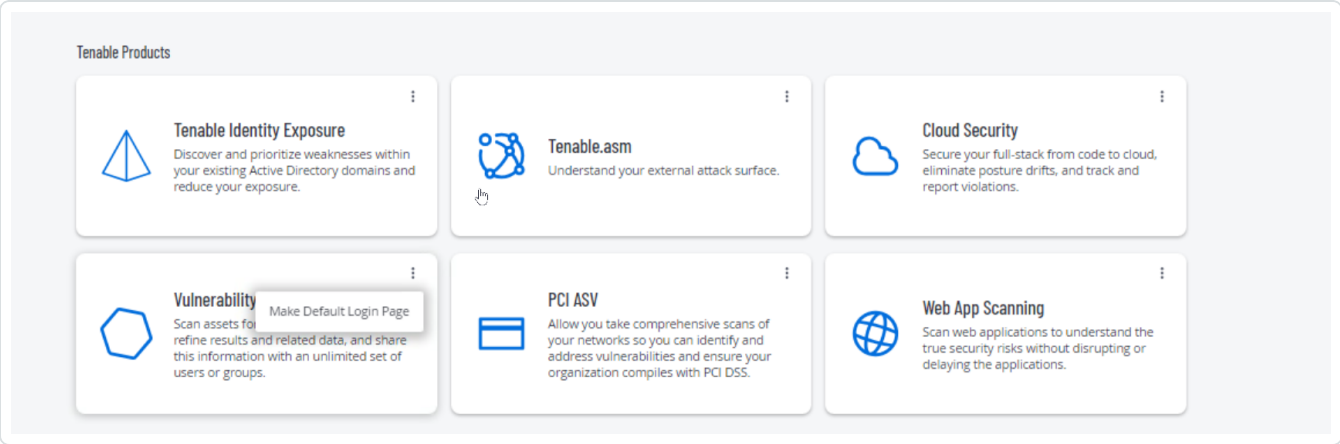
デフォルトのログインアプリケーションを設定する方法

1. Tenable にログインします。

   [ワークスペース] ページが表示されます。

2. 選択するアプリケーションの右上にある ボタンをクリックします。

   メニューが表示されます。



3. メニューで、**[デフォルトログインページの作成]** をクリックします。

   ログインするとこのアプリケーションが表示されるようになります。

デフォルトのアプリケーションを削除する

デフォルトのアプリケーションを削除する方法

1. Tenable にログインします。

   [ワークスペース] ページが表示されます。

2. 削除するアプリケーションの右上にある ⋮ ボタンをクリックします。

   メニューが表示されます。

3. **[デフォルトログインページの削除]** をクリックします。

   ログインすると **[ワークスペース]** ページが表示されるようになります。

ユーザー環境設定

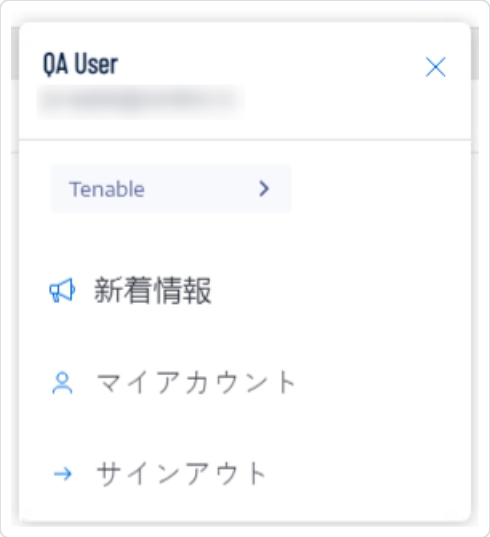
Tenable Identity Exposure のユーザー環境を設定できます。

- 言語を選択するには
- プロファイルを選択するには
- パスワードを変更するには
- プロファイルを選択するには

環境設定を行うには

1. Tenable Identity Exposure で、右上隅のユーザープロファイルアイコンをクリックします。

   サブメニューが表示されます。



2. **[マイアカウント]** を選択します。

   [環境設定] ページが表示されます。

言語を選択するには

a. **[言語]** で、ドロップダウンリストの矢印をクリックして、使用する言語を選択します。

b. **[保存]** をクリックします。

Tenable Identity Exposure が環境設定を更新したことを確認するメッセージが表示されます。ユーザーインターフェースに選択した言語が表示されます。

プロファイルを選択するには

あるセキュリティプロファイルから別のセキュリティプロファイルに切り替えると、Tenable Identity Exposure がインジケーターの設定を表示するには、およびダッシュボード、ウィジェット、イベント情報でデータ表現を表示するにはが変わります。

a. **[環境設定]** で、**[プロファイル]** をクリックします。

b. Tenable Identity Exposure に接続した後、**[優先するプロファイル]** のドロップダウン矢印をクリックしてデフォルトのプロファイルを選択します。

c. **[保存]** をクリックします。

Tenable Identity Exposure が環境設定を更新したことを確認するメッセージが表示されます。

詳細は、セキュリティプロファイルを参照してください。

パスワードを変更するには

注意: Tenable One のライセンスがある場合、パスワード情報を利用できません。この場合、Tenable Vulnerability Management がすべての認証設定を管理します。詳細については、Tenable Vulnerability Management ユーザーガイドのアクセス制御を参照してください。

a. **[環境設定]** で、**[認証情報]** をクリックします。

b. 以下の情報を入力します。

- 古いパスワード
- 新しいパスワード

c. **[新しいパスワードの確認]** ボックスに新しいパスワードを再入力します。

d. **[保存]** をクリックします。

Tenable Identity Exposure がパスワードを変更したことを確認するメッセージが表示されます。

注意: Tenable Identity Exposure では、LDAP や SAMLなどの外部プロバイダーを通じて接続されているアカウントのパスワードは変更できません。

API キーを管理するには

a. **[環境設定]** で **[API キー]** をクリックします。

   [現在の API キー] ボックスにアクセストークンが表示されます。

b. 以下を実行できます。

c. 📋 アイコンをクリックして、API キーをクリップボードにコピーし、必要に応じて使用します。

d. **[API キーの更新]** をクリックすると、新しいアクセストークンが生成されます。

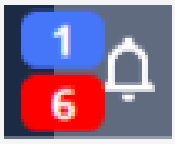
   確認を求めるメッセージが表示されます。

   > **注意**: API キーを更新すると、Tenable Identity Exposure は現在のトークンを無効にします。

詳細については、公開 API の使用をご覧ください。

通知

Tenable Identity Exposure のホームページの右上隅に、確認待ちの攻撃アラートや露出アラートがベルのアイコンとバッジのカウントで通知されます。Tenable Identity Exposure は新しいアラートを受信すると、通知バッジの数を増やします。

	**青**	露出アラート
	赤	攻撃アラート

アラートを表示するには

1. Tenable Identity Exposure でベルのアイコンをクリックします。

   [アラート] ペインが開きます。

2. 次のいずれかを実行します。
   - 露出アラートを表示するには **[露出アラート]** タブをクリックします。
   - 攻撃アラートを表示するには **[攻撃アラート]** タブをクリックします。

     関連するアラートのリストが表示されます。

アラートに関連するイベントを表示するには

1. リストからアラートを選択し、**[アクション]** > **[逸脱を表示]** をクリックします。

   イベントの詳細ペインが開き、次の情報が表示されます。
   - ソース (イベントコレクター)
   - オブジェクトタイプ
   - ファイル
   - パス
   - 影響を受けているドメイン
   - 日付
   - イベント発生時の値と現在の値を含む属性のリスト

2. **[逸脱]** タブをクリックします。

   [逸脱] ペインが開き、イベントに関連する逸脱のリストが表示されます。

3. **[n/n 個のインジケーター]** をクリックして、アラートをトリガーした露出インジケーターのペインを表示します。
4. **[n/n 個の理由]** をクリックして、アラートの理由を表示します。
5. 矢印をクリックして、アラートの情報を展開または折りたたみます。
6. インジケーター名をクリックして、インジケーターの詳細ページを表示します。

アラートをアーカイブするには

アラートを表示した後にアーカイブできます。

1. **[アラート]** ペインのアラートのリストで、アーカイブするアラートのチェックボックスを選択します。
   - オプションで、ペインの下部の **[n/n 個のオブジェクトを選択済み]** チェックボックスをクリックして、すべてのアラートをまとめて選択できます。
2. ペインの下部の **[アクションの選択]** > **[アーカイブ]** をクリックします。
3. **[OK]** をクリックします。

ダッシュボード

ダッシュボードを使用すると、Active Directory のセキュリティに影響を与えるデータや傾向を視覚化できます。ウィジェットを使用してカスタマイズし、要件に応じてチャートやカウンターを表示できます。

Tenable Identity Exposure が提供しているダッシュボードテンプレートを使用すると、所属組織が懸念する優先度の高い問題に集中することができます。たとえば、次のようなテンプレートがあります。

- **AD コンプライアンスおよびトップリスク** - コンプライアンススコア、変化、リスク重大度コンプライアンス
- **AD リスク 360** – 露出インジケーターの深刻度レベル別の逸脱の変化と問題
- **パスワード管理リスク** - パスワード関連の問題
- **ユーザーの監視** - AD ユーザーの変化、ユーザーカテゴリカウント
- **ネイティブ管理者の監視** - 管理アカウントのメトリクス

テンプレートを使用して新しいダッシュボードを作成するには

1. Tenable Identity Exposure で、  か **[ダッシュボード]** をクリックします。(このページは、Tenable Identity Exposure でもデフォルトで開きます。)
2. 次のいずれかを実行できます。
    - ペインが空の場合、**[ダッシュボードの追加]** をクリックします。
    - ペインにすでに 1 つ以上のダッシュボードがある場合、右上隅にある  > **[新しいダッシュボードの追加]** をクリックします。

      [ダッシュボードテンプレートの設定] ペインが開きます。
3. 追加するダッシュボードを選択します。
4. **[ダッシュボードの追加]** をクリックします。
5. Tenable Identity Exposure がダッシュボードとウィジェットを作成したことを確認するメッセージが表示されます。**[ダッシュボード]** ペインのタブの下に新しいダッシュボードが表示されます。

カスタムダッシュボードを追加するには

1. Tenable Identity Exposure で、  か **[ダッシュボード]** をクリックします。(このページは、Tenable Identity Exposure でもデフォルトで開きます。)
2. 右上隅の  > **[新しいダッシュボードの追加]** をクリックします。

   [ダッシュボードテンプレートの設定] ペインが開きます。
3. 下にある **[カスタムダッシュボード]** テンプレートを選択します。
4. ダッシュボードの名前を入力します。
5. **[ダッシュボードの追加]** をクリックします。

   Tenable Identity Exposure がダッシュボードを作成したことを確認するメッセージが表示されます。**[ダッシュボード]** ペインのタブの下に新しいダッシュボードが表示されます。
6. ウィジェットをダッシュボードに追加する方法については、ウィジェットを参照してください。

ダッシュボードの名前を変更するには

1. **[ダッシュボード]** ペインで、名前を変更するダッシュボードのタブを選択します。
2. 右上隅の > **[名前の編集]** をクリックします。

   [ダッシュボードの設定] ペインが開きます。
3. **[名前]** ボックスにダッシュボードの名前を入力します。
4. **[編集]** をクリックします。

   Tenable Identity Exposure がダッシュボードを更新したことを確認するメッセージが表示されます。

ダッシュボードを削除するには

1. **[ダッシュボード]** ペインで、削除するダッシュボードのタブを選択します。
2. 右上隅の > **[ダッシュボードの削除]** をクリックします。

   [ダッシュボードの削除] ペインが開き、削除の確認を求められます。
3. **[削除]** をクリックします。

   Tenable Identity Exposure がダッシュボードを削除したことを確認するメッセージが表示されます。

ウィジェット

ダッシュボードのウィジェットを使用して、棒グラフ、折れ線グラフ、カウンターの形式で Active Directory に関するデータを視覚化できます。ウィジェットをカスタマイズして詳細情報を表示したり、ウィジェットをドラッグしてダッシュボード上で位置を変更したりできます。

新しく作成したダッシュボードや既存のダッシュボードにウィジェットを追加できます。

ウィジェットをダッシュボードに追加するには

1. Tenable Identity Exposure で、  か **[ダッシュボード]** をクリックします。(このページは、Tenable Identity Exposure でもデフォルトで開きます。)
2. ダッシュボードペインで、ダッシュボードタブを選択します。
3. 次のいずれかを実行します。
    - ダッシュボードが空の場合、**[ウィジェットの追加]** をクリックします。
    - ダッシュボードにすでにウィジェットが含まれている場合、右上隅の  > **[現在のダッシュボードにウィジェットを追加]** をクリックします。

      [ウィジェットの追加] ペインが開きます。
4. タイルをクリックして次のいずれかを選択します。
    - 棒グラフ
    - 折れ線グラフ
    - カウンター
5. **[ウィジェットの名前]** ボックスにウィジェットの名前を入力します。
6. **[ウィジェットの設定]** の **[データのタイプ]** ボックスでドロップダウンリストの矢印をクリックして、次のいずれかを選択します。
    - ユーザー数: ドメインのアクティブユーザーの数。
    - 逸脱数: 検出された逸脱またはセキュリティ違反の数。

- コンプライアンススコア: 0 ～ 100 の値で示されるスコア。検出された逸脱の数とその深刻度を計算して、Tenable Identity Exposure により算出されます。
- 期間 (折れ線グラフの場合): ドロップダウンリストの矢印をクリックして、表示する期間を選択します。

7. **[データセットの設定]** で、次を行います。

データセットの設定	
ステータス (ユーザー数)	アクティブ、非アクティブ、すべてのいずれかを選択します。
インジケーター	a. **[インジケーター]** をクリックして、1 つ以上のインジケーターを選択します。 **[露出インジケーター]** ペインが開きます。 b. リストから 1 つまたは複数のインジケーターを選択します。オプションで、以下のように行うこともできます。 ■ 検索ボックスにインジケーター名を入力する。 ■ すべてのインジケーターを選択する。 ■ 特定の深刻度レベル (重大、高、中、低) のすべてのインジケーターを選択する。 c. **[選択内容でフィルター]** をクリックします。
ドメイン	a. **[ドメイン]** をクリックして、1 つ以上のドメインを選択します。 **[フォレストとドメイン]** ペインが開きます。 b. リストからドメインを選択します。オプションで、以下のように行うこともできます。 ■ 検索ボックスにドメイン名を入力する。 ■ すべてのドメインを選択する。 c. **[選択内容でフィルター]** をクリックします。

8. **[データセットの名前]** にデータセットの名前を入力します。

9. ウィジェットのドメインを選択します。

   オプションで、検索ボックスにドメイン名を入力することができます。

10. **[選択内容でフィルター]** をクリックします。

11. オプションで、**[新しいデータセットの追加]** をクリックして、ウィジェットのオプションが異なる別のデータセットを追加することができます。

12. **[追加]** をクリックします。

    Tenable Identity Exposure がウィジェットを追加したことを確認するメッセージが表示されます。

ウィジェットを変更するには

1. Tenable Identity Exposure で、**[ダッシュボード]** をクリックします。
2. 変更するウィジェットが含まれているダッシュボードを選択します。
3. ウィジェットを選択します。
4. ウィジェットの右上隅の アイコンをクリックします。

   [ウィジェットの変更] ペインが開きます。

5. 必要に応じて変更します。
6. **[編集]** をクリックします。

   Tenable Identity Exposure がウィジェットをアップデートしたことを確認するメッセージが表示されます。

ウィジェットをリフレッシュするには

1. ウィジェットを選択します。
2. ウィジェットの右上隅の アイコンをクリックします。

   ウィジェットがリフレッシュされます。

ウィジェットを削除するには

1. Tenable Identity Exposure で、**[ダッシュボード]** をクリックします。
2. 削除するウィジェットが含まれているダッシュボードを選択します。
3. ウィジェットを選択します。
4. 🗑 アイコンをクリックします。

   [ウィジェットの削除] ペインが開きます。削除の確認を求めるメッセージが表示されます。
5. **[OK]** をクリックします。

   Tenable Identity Exposure がダッシュボードからウィジェットを削除したことを確認するメッセージが表示されます。

関連項目

- ダッシュボード

アイデンティティエクスプローラー

アクセス許可: Microsoft Entra ID の設定とデータ視覚化にアクセスするには、ユーザーロールに適切なアクセス許可が必要です。詳細は、ロールのアクセス許可の設定 を参照してください。

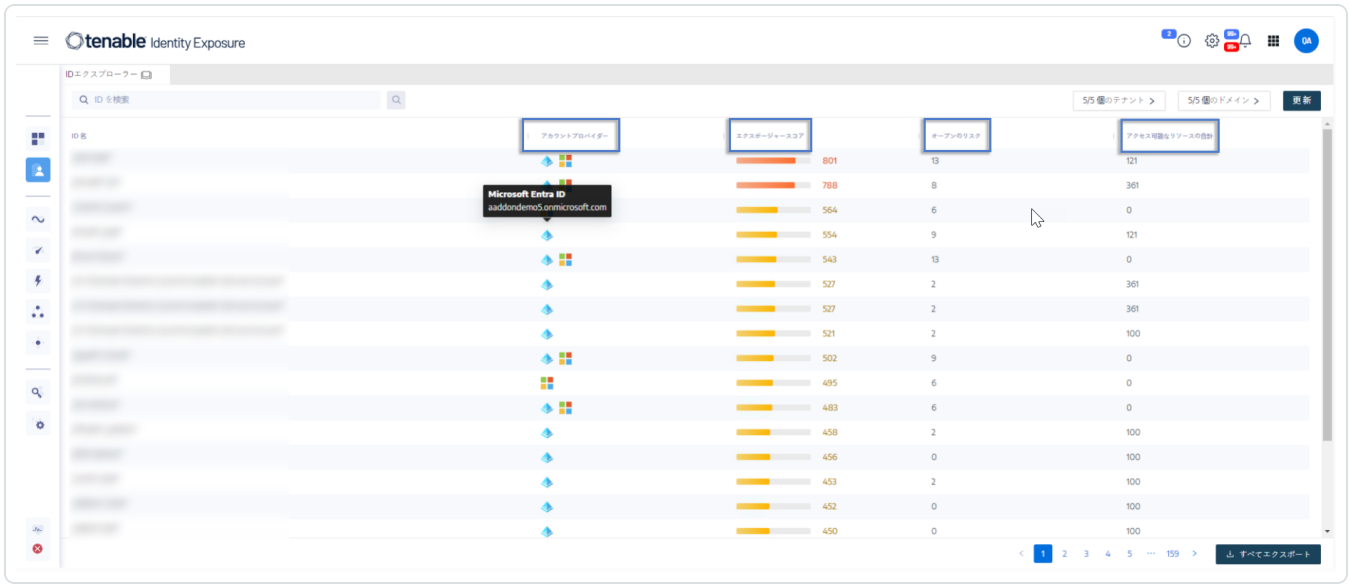
Tenable Identity Exposure のアイデンティティエクスプローラービューは、Active Directory と Microsoft Entra ID 両方の ID を統合します。このビューには、リストされている各資産のアイデンティティリスクスコア(ベータ版)と、侵害されたアイデンティティの考えられる影響範囲が表示されます。

Identity Explorer にアクセスするには

注意: アイデンティティエクスプローラーは、Microsoft Entra ID 機能を使用する場合にのみ表示されます。詳細は、Microsoft Entra ID のサポート を参照してください。

- Tenable Identity Exposure で、左側のナビゲーションバーの Identity Explorer アイコン をクリックします。

  [Identity Explorer] ペインが開きます。



[Identity Explorer] ペインには、アクセス可能なリソース全体の以下の情報が表示されます。

- **ID 名** - 当該 ID プロバイダーのユーザーアカウントの名前。
- **アカウントプロバイダー** - ID プロバイダー。

- **エクスポージャースコア** - Tenable Identity Exposure は、資産の重大度、または各 ID プロバイダーの ID とその脆弱性を評価することでこのメトリクスを算出し、メトリクスを集計して、特定の ID の総合的なエクスポージャースコアを出します。

  > **注意**: Tenable Identity Exposure は Tenable One ライセンスがある場合にのみエクスポージャースコアを表示します。

- **オープンのリスク** - Microsoft Entra ID の露出インジケーターが資産をスキャンした時に検出した検出結果の数。詳細は、Microsoft Entra ID 関連の露出インジケーター を参照してください。
- **アクセス可能なリソースの合計** - この資産がアクセス(読み取り、書き込みなど) できるタイプのリソースの数。

ID を検索するには

1. **[Identity Explorer]** ペインの **[検索]** ボックスに、ユーザー名かアカウント名を入力します。
2. アイコンをクリックします。

   Tenable Identity Exposure は一致する結果を表示します。

ID をエクスポートするには

1. **[Identity Explorer]** ペインの下部で、**[すべてエクスポート]** をクリックします。

   [ID のエクスポート] ペインが開きます。
2. **[すべてエクスポート]** をクリックします。

   Tenable Identity Exposure によりファイルがローカルマシンにダウンロードされます。

イベント情報

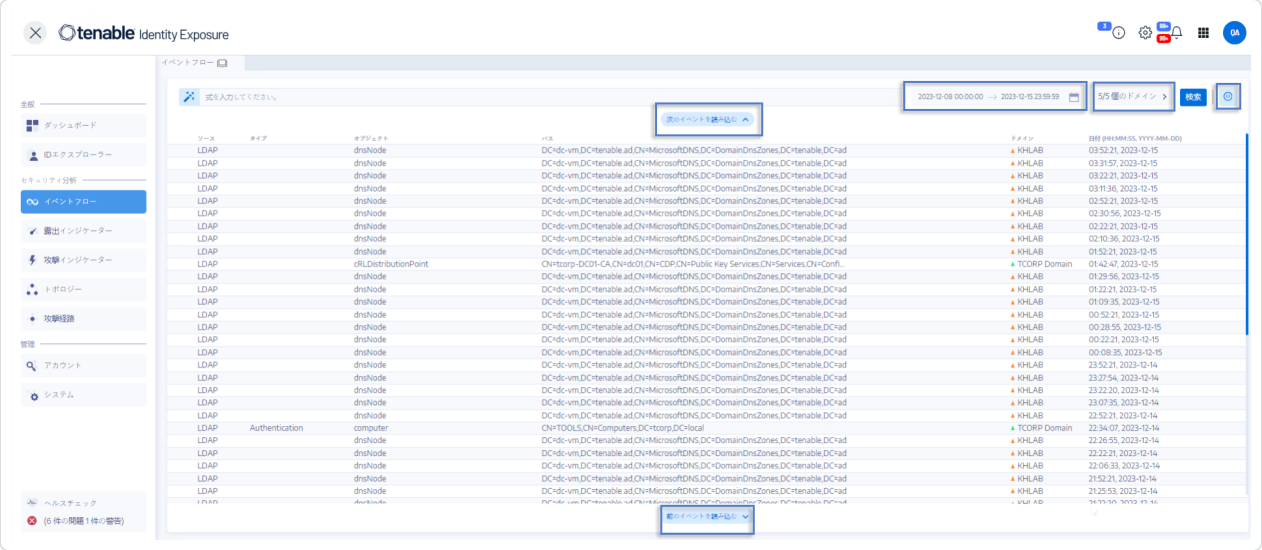
Tenable Identity Exposure のイベント情報は、AD インフラに影響を与えるイベントをリアルタイムで監視し分析した結果を表示します。イベント情報を使用して、重大な脆弱性と推奨される修正方法を特定できます。

[イベント情報] ページを使用して、時間を遡って以前のイベントをロードしたり、特定のイベントを検索したりできます。ページの上部にある検索ボックスを使用して、脅威を検索したり悪質なパターンを検出したりすることもできます。

イベント情報にアクセスするには

- Tenable Identity Exposure で、左側のナビゲーションバーの **[イベント情報]** をクリックします。

  [イベント情報] ページが開き、イベントのリストが表示されます。詳細は、イベントの詳細テーブルを参照してください。



タイムフレームを選択するには

1. **[イベント情報]** ページの上部で、カレンダーボックスをクリックします。
2. 開始日と終了日を選択します。
3. **[検索]** をクリックします。

   Tenable Identity Exposure は、選択されたタイムフレームでイベント情報テーブルをアップデートします。

ドメインを選択するには

1. **[イベント情報]** ページの上部で、**[n/n 個のドメイン >]** をクリックします。

   [フォレストとドメイン] ペインが開きます。

2. フォレストとドメインを選択します。

3. **[選択内容でフィルター]** をクリックします。

   Tenable Identity Exposure は、選択したフォレストとドメインの情報でイベント情報テーブルをアップデートします。

イベントを表示するには

- イベント情報テーブルで、調査するイベントが含まれている行をクリックします。

  イベントの詳細ペインが表示されます。詳細は、イベントの詳細 を参照してください。

イベント情報を一時停止して再開するには

- 次のいずれかを実行します。
  - ⏸ アイコンをクリックして、イベント情報を一時停止します。

    イベント情報を一時停止すると、最新イベントの自動の縦スクロールが停止しますが、分析はバックグラウンドで引き続き実行され、イベントの検索は実行できます。
  - ⏵ アイコンをクリックして、イベント情報を再開します。

次のイベントまたは前のイベントを読み込むには

- [イベントの詳細]ページで、次のいずれかを行います。
  - [次のイベントを読み込む]をクリックします。
  - [前のイベントを読み込む]をクリックします。

イベントの詳細テーブル

Tenable Identity Exposure は、Active Directory のイベントが発生次第、それらをイベントの詳細テーブルに継続的に一覧表示します。イベントの詳細テーブルには以下の情報が含まれています。

情報	説明
ソース	AD インフラで起きたセキュリティ関連の変更の発生源を示しています。 可能性のある発生源は 2 種類あります。 • AD インフラとの通信に使用されている Lightweight Directory Access Protocol (LDAP) • ファイルやプリンターなどの共有に使用されている Server Message Block (SMB) プロトコル **Tenable Identity Exposure** はネットワーク上の LDAP と SMB のトラフィックを徹底的に分析し、異常や潜在的な脅威を検出します。 **注意**: Active Directory (AD) の管理者は、ユーザーアカウントやマシンアカウントにデプロイされた設定を制御するグループポリシーを作成できます。グループポリシーオブジェクト (GPO)は、こうした制御設定を保存します。Sysvol フォルダーは、ドメインコントローラー (DC) の GPO ファイルを保存します。各ドメインメンバーは高レベルの権限を使って GPO を適用したり実行したりできるため、AD のセキュリティのために GPO の内容を監視することは重要です。
タイプ	以下のようなイベントの特徴的な要素を表示します。 • ACL の変更 • SPN の変更 • メンバーの削除 • 新しいメンバー • 新しい信頼 • 不明な種類のファイルの追加 • 新しいオブジェクト • オブジェクトの削除

	• パスワードの変更 • UAC の変更 • 新しい GPO のリンク • GPO のリンクの削除 • 所有者の変更 • ファイル名の変更 • SPN の作成 • 認証リセットの失敗 • 認証の失敗
オブジェクト	AD オブジェクトに関連付けられたクラスまたはファイル拡張子を示します。ディレクトリオブジェクト (ユーザー、コンピューターなど) や、ファイル名に特定の拡張子 (ini、XML、csv) が含まれるファイルを検索できます。
パス	AD オブジェクトへのフルパスを示し、そのオブジェクトの AD 内の一意の場所を特定できるようにします。
ディレクトリ	AD インフラに対する変更元となったディレクトリを示します。
日付	イベントが発生した時間を示します。

ウィザードを使用してイベント情報を検索

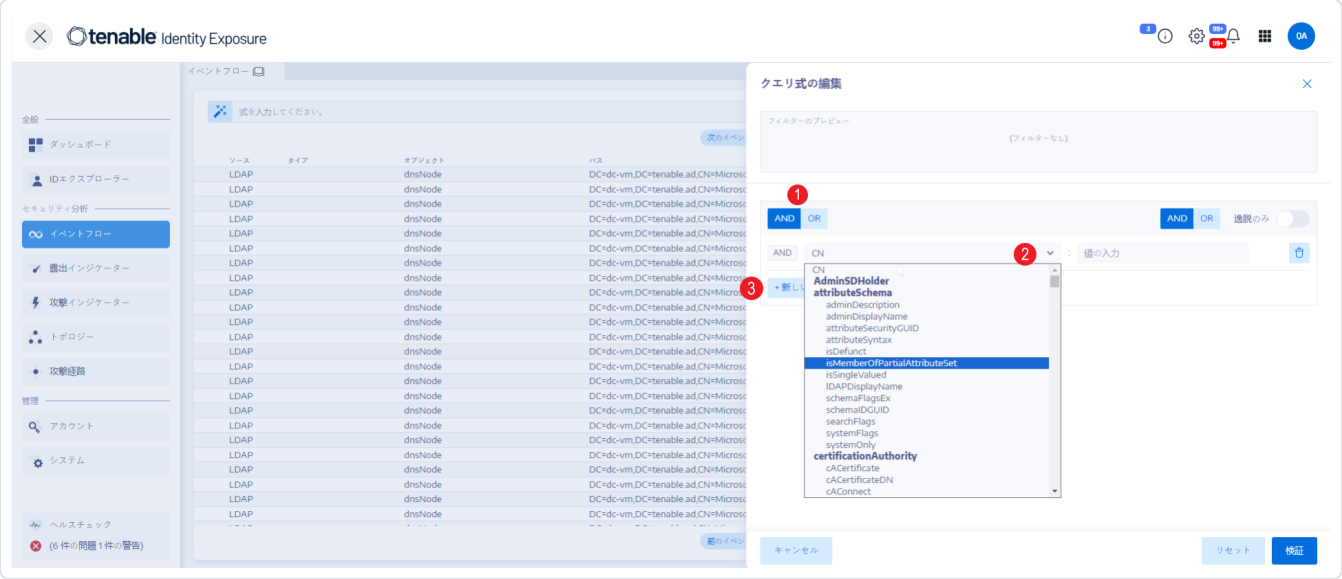
検索ウィザードでは、クエリ式を作成して組み合わせることができます。

- 検索ボックスで頻繁に使用する式をブックマークのリストに追加して、後で使用することができます。
- 検索ボックスに式を入力すると、Tenable Identity Exposure はこの式を[履歴]ペインに保存し、再利用できるようにします。

ウィザードを使用して検索するには

1. Tenable Identity Exposure で、**[イベント情報]**をクリックして[イベント情報]ページを開きます。
2. アイコンをクリックします。

   [クエリ式の編集]ペインが開きます。詳細は、イベント情報のクエリをカスタマイズするを参照してください。



3. パネルでクエリ式を定義するには、**AND** または **OR** 演算子ボタン(1)をクリックして、最初の条件に適用します。
4. 属性をドロップダウンメニューから選択し、値を入力します(2)。
5. 次のいずれかを行います。

- 属性を追加するには、**[+ 新しいルールの追加]**(3)をクリックします。
- 別の条件を追加するには、**[新しい条件の追加]**の**+ AND**または**+ OR**演算子をクリックします。属性をドロップダウンメニューから選択し、値を入力します。
- 逸脱オブジェクトだけを検索するには、**[逸脱のみ]**のトグルをクリックして許可します。**+ AND**または**+ OR**演算子を選択して、条件をクエリに追加します。
- 条件またはルールを削除するには、🗑アイコンをクリックします。

6. **[検証]**をクリックして検索を実行するか、**[リセット]**をクリックしてクエリ式を変更します。

関連項目

- イベント情報を手動で検索
- ウィザードを使用してイベント情報を検索
- イベント情報のクエリをカスタマイズする
- ブックマーククエリ
- クエリ履歴

イベント情報を手動で検索

特定の文字列またはパターンに一致するイベントをフィルタリングするには、検索ボックスに式を入力し、ブール演算子 *****、**AND**、**OR** を使用して結果を絞り込みます。検索の優先順位を変更したい場合は、括弧を使用して **OR** ステートメントをカプセル化できます。検索では、Active Directory 属性の特定の値が検索されます。

イベント情報を手動で検索するには

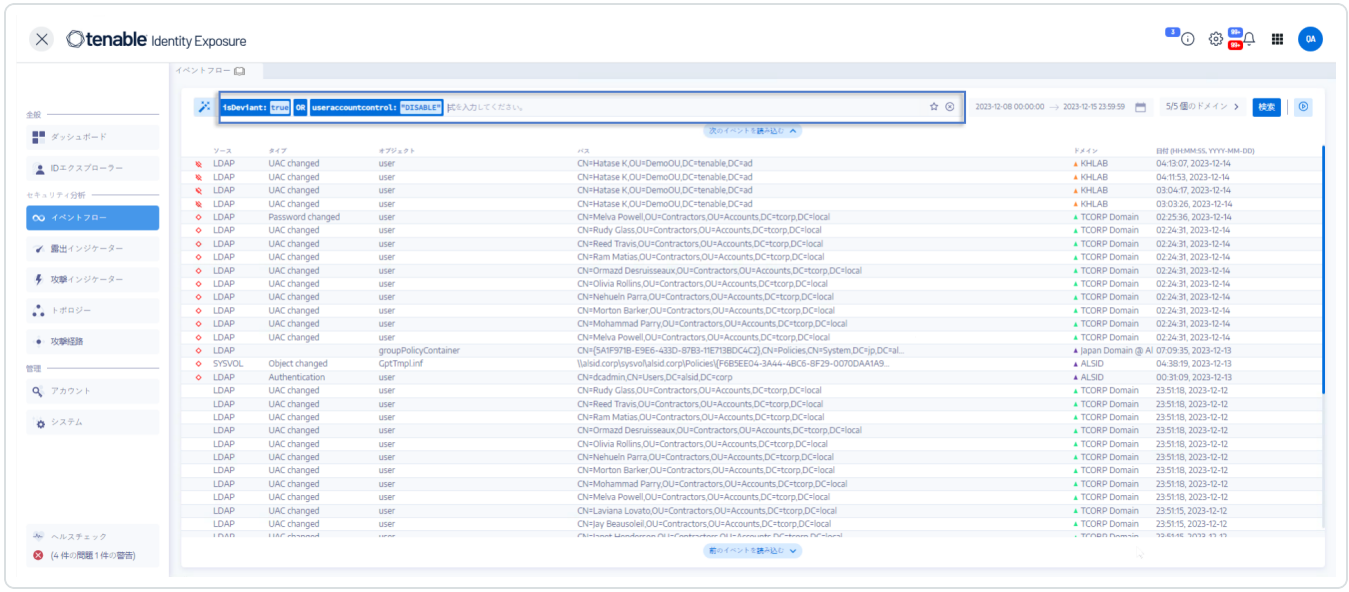
1. Tenable Identity Exposure で、**[イベント情報]** をクリックして [イベント情報] ページを開きます。
2. 検索ボックスに、クエリ式を入力します。
3. 次のように検索結果をフィルタリングできます。
    - **[カレンダー]** ボックスをクリックして、開始日と終了日を選択します。
    - **[n/n 個のドメイン]** をクリックして、フォレストとドメインを選択します。
4. **[検索]** をクリックします。

    Tenable Identity Exposure は、検索条件に一致する結果でリストを更新します。

例

以下の例では、次のイベント情報を検索します。

- 監視対象の AD インフラを危険にさらす可能性のある、非アクティブのユーザーアカウント
- 不審なアクティビティおよびアカウントの異常な使用



文法と構文

手動クエリ式は、次の文法と構文を使用します。

- 文法: `EXPRESSION [OPERATOR EXPRESSION]*`
- 構文: `__KEY__ __SELECTOR__ __VALUE__`

  各部の説明

  - `__KEY__`: 検索する AD オブジェクト属性を表します (`CN`、`userAccountControl`、`members` など)。
  - `__SELECTOR__`: 演算子 (`:`、`>`、`<`、`>=`、`<=`) を表します。
  - `__VALUE__`: 検索する値を表します。

    特定のコンテンツを検索する場合は、さらに多くのキーを使用できます。
  - `isDeviant`: 逸脱を引き起こしたイベントを検索します。

AND と **OR** 演算子を使用して、イベント情報のクエリ式を複数組み合わせることができます。

例

- 共通の名前属性で文字列 alice を含むすべてのオブジェクトを検索: `cn:"alice"`
- 共通の名前属性で文字列 alice を含み、かつ特定の逸脱を引き起こしたすべてのオブジェクトを検索: `isDeviant: "true" AND cn: "alice"`
- Default Domain Policy という名前の GPO を検索: `objectClass:"groupPolicyContainer" AND displayname:"Default Domain Policy"`
- S-1-5-21 を含む SID を持つすべての非アクティブ化されたアカウントを検索: `userAccountControl:"DISABLE" AND objectSid:"S-1-5-21"`
- Sysvol 内のすべての `script.ini` ファイルを検索: `globalpath:"sysvol" AND types:"SCRIPTSini"`

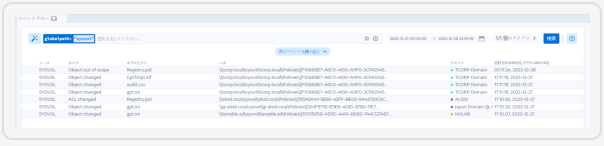
> **注意**: ここの types は列ヘッダーではなくオブジェクト属性のことです。

イベント情報のクエリをカスタマイズする

イベント情報を使用すると、デフォルトの露出インジケーターと攻撃インジケーターの監視に加えて、Tenable Identity Exposure 機能を拡張することができます。カスタムクエリを作成してデータをすばやく取得し、そのクエリを Tenable Identity Exposure が Security Information and Event Management (SIEM) に送信できるカスタムアラートとして使用することもできます。

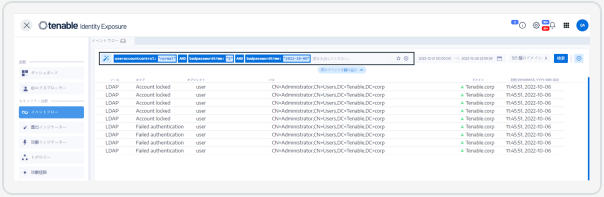
次の例は、Tenable Identity Exposure で実際に使用できるカスタムクエリを示しています。

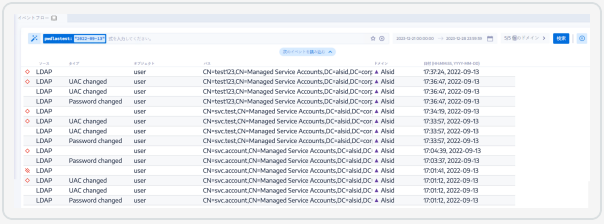
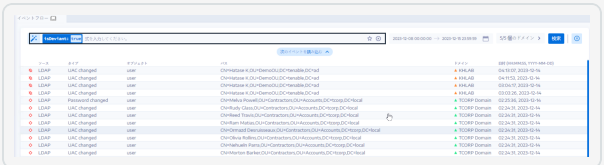
ユースケース	説明

GPO の起動と停止バイナリとグローバル SYSVOL パスの監視	起動パスまたはグローバル SYSVOL レプリケーションパスのスクリプトを監視します。攻撃者はしばしば、これらのスクリプトを使用してネイティブ AD サービスを悪用し、環境全体にランサムウェアをすばやく増殖させます。
	• **起動パスのスクリプトのクエリ:**
	`globalpath: "sysvol" AND types: "Scriptsini"`
	注意: ここでは、types は列ヘッダーではなくオブジェクト属性のことです。
	• **SYSVOL 監視クエリ:**
	`globalpath:"sysvol" AND (globalpath:".ps1" OR globalpath:".msi" OR globalpath:".bat" OR globalpath:".exe")`
	 

GPO 設定の変更	GPO 設定に対する変更を監視します。攻撃者はしばしば、このメソッドを使用してセキュリティ設定をダウングレードし、執拗な不正アクセスやアカウント乗っ取りを助長します。

	• **GPO 監視クエリ:** `gptini-displayname:"New Group Policy Object" AND changetype:"Changed"` 

認証の失敗とパスワードのリセット	ロックアウトにつながる認証試行の複数回の失敗を監視します。これは、ブルートフォース攻撃の早期警告フラグとして機能します。
	
	注意: ロックアウトポリシーと日付/時刻変数を設定する必要があります。詳細は、Tenable Identity Exposure アカウントを使用した認証 を参照してください。
	
	• **認証失敗クエリ**
	
	`useraccountcontrol:"Normal" AND badpwdcount:"<ACCOUNT_LOCKOUT_THRESHOLD>" AND badpasswordtime:"<DATE_TIME_STAMP>"`
	
	 
	
	• **パスワードリセットクエリ**
	
	`pwdlastset: "<DATE_TIME_STAMP"`

	
追加、削除、または変更されたオブジェクトのアクセス許可	ACL 権限および関連するオブジェクトのアクセス許可セットに対する不正な変更を監視します。攻撃者はこのメソッドを悪用してアクセス許可を昇格します。 **注意**: 日付/時刻変数を指定する必要があります。 • **オブジェクトのアクセス許可クエリ** `ntsecuritydescriptor:0 AND whenchanged:"DATE_TIME_STAMP"` 
逸脱を引き起こす管理者への変更	ビルトイン管理グループおよびカスタムグループは機密性の高いグループであり、リスクが発生する可能性がある逸脱や設定変更を厳重に監視する必要があります。このクエリを使用すると、管理者グループ内のセキュリティ設定に悪影響を与えた可能性のある最近の変更をすばやく確認できます。 • **管理者への変更クエリ** `isDeviant:true AND cn:"admins"` 

関連項目

- イベント情報を手動で検索
- ウィザードを使用してイベント情報を検索
- ブックマーククエリ
- クエリ履歴
- イベント情報のユースケース

ブックマーククエリ

クエリ式を頻繁に使用する場合、その式をカスタマイズしたブックマークのリストに追加して、再度使用することができます。

クエリ式をブックマークするには

1. Tenable Identity Exposure で、**[イベント情報]** をクリックして [イベント情報] ページを開きます。
2. 検索ボックスの横にある アイコンをクリックします。

   [クエリ式の編集] ペインが開きます。
3. 検索ボックスに、クエリ式を入力します。
4. 検索ボックスの右にある ☆ アイコンをクリックします。

   [ブックマークに追加] ボックスが表示されます。
5. **[フォルダーを選択]** ボックスでドロップダウン矢印をクリックして、リストからフォルダーを選択します。
6. (オプション) **[新規フォルダーの作成]** のトグルをクリックして、**[はい]** に切り替えます。**[フォルダーの名前]** ボックスに、ブックマークフォルダーの名前を入力します。
7. **[ブックマークの名前]** ボックスに、ブックマークの名前を入力します。
8. **[追加]** をクリックします。

   Tenable Identity Exposure がリストにブックマークを追加したことを確認するメッセージが表示されます。

ブックマークしたクエリ式を使用するには

1. Tenable Identity Exposure で、**[イベント情報]** をクリックして [イベント情報] ページを開きます。
2. 検索ボックス内をクリックします。

   検索ボックスの下に **[履歴]** タブと **[ブックマーク]** タブが表示されます。
3. **[ブックマーク]** タブをクリックします。

   ブックマークのリストが表示されます。

4. ブックマークをクリックして選択します。

   Tenable Identity Exposure がクエリ式を読み込み、検索を実行します。

ブックマークを管理するには

1. Tenable Identity Exposure で、**[イベント情報]** をクリックして [イベント情報] ページを開きます。
2. 検索ボックス内をクリックします。

   検索ボックスの下に **[履歴]** タブと **[ブックマーク]** タブが表示されます。
3. **[ブックマーク]** タブをクリックします。

   ブックマークのリストが表示されます。
4. **[ブックマークの管理]** をクリックします。

   [ブックマーク] ペインが開きます。
5. 次のいずれかを行います。
   - ブックマークを検索する
     a. 検索ボックスにブックマーク名を入力します。
     b. ドロップダウンリストからフォルダーを選択します。
   - ブックマークまたはブックマークフォルダーの名前を編集する
     a. ブックマークまたはブックマークフォルダーの アイコンをクリックします。
     b. **[ブックマークの名前]** または **[フォルダーの名前]** ボックスに、ブックマークまたはブックマークフォルダーの新しい名前を入力します。
     c. **[編集]** をクリックします。

        Tenable Identity Exposure がブックマークまたはブックマークフォルダー名を更新したことを確認するメッセージが表示されます。
   - ブックマークフォルダーのブックマークを削除する
     - ブックマークまたはブックマークフォルダーの アイコンをクリックします。

関連項目

- イベント情報を手動で検索
- ウィザードを使用してイベント情報を検索
- イベント情報のクエリをカスタマイズする
- クエリ履歴
- イベント情報のユースケース

クエリ履歴

検索ボックスに式を入力すると、Tenable Identity Exposure はこの式を [履歴] ペインに保存し、再利用できるようにします。

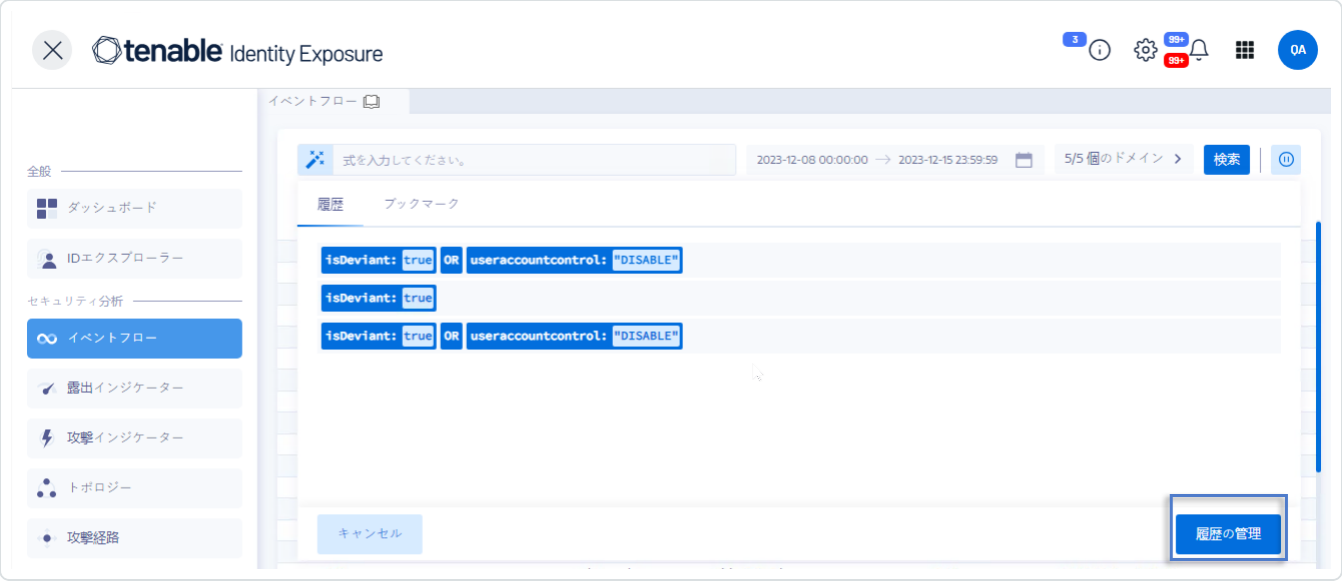
履歴にあるクエリ式を使用するには

1. Tenable Identity Exposure で、**[イベント情報]** をクリックして [イベント情報] ページを開きます。
2. 検索ボックス内をクリックします。

   検索ボックスの下に **[履歴]** タブと **[ブックマーク]** タブが表示されます。
3. **[履歴]** タブをクリックします。

   クエリ式のリストが表示されます。
4. 使用するクエリ式をクリックして、選択します。

   Tenable Identity Exposure がクエリ式を読み込み、検索を実行します。



クエリ式の履歴を管理するには

1. Tenable Identity Exposure で、**[イベント情報]** をクリックして [イベント情報] ページを開きます。
2. 検索ボックス内をクリックします。

   検索ボックスの下に **[履歴]** タブと **[ブックマーク]** タブが表示されます。

3. **[履歴]** タブをクリックします。

   クエリ式のリストが表示されます。

4. **[履歴の管理]** をクリックします。

   [履歴] ペインが開きます。

5. 次のいずれかを行います。

- クエリ式を検索する

  a. 検索ボックスに、クエリ式を入力します。

  b. カレンダーボックスをクリックして、開始日と終了日を選択します。

  c. **[検索]** をクリックします。

- 履歴からクエリ式を削除する

  - 🗑 アイコンをクリックします。

- 履歴からすべてのクエリ式を消去する

  a. **[選択内容のクリア]** をクリックします。

     削除の確認を求めるメッセージが表示されます。

  b. **[確認]** をクリックします。

関連項目

- イベント情報を手動で検索
- ウィザードを使用してイベント情報を検索
- イベント情報のクエリをカスタマイズする
- ブックマーククエリ
- イベント情報のユースケース

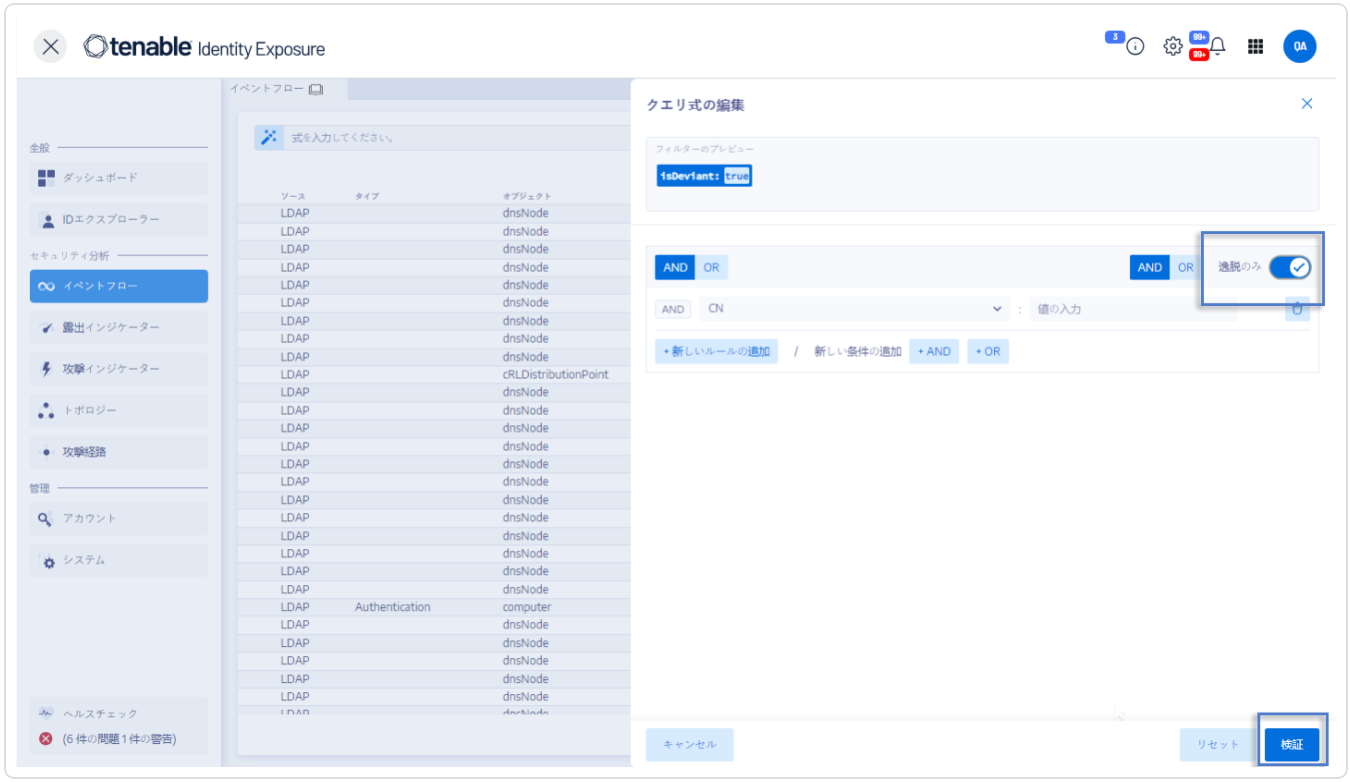
逸脱イベントを表示

イベント情報テーブルに逸脱イベントだけを表示することができます。

逸脱イベントのみを表示するには

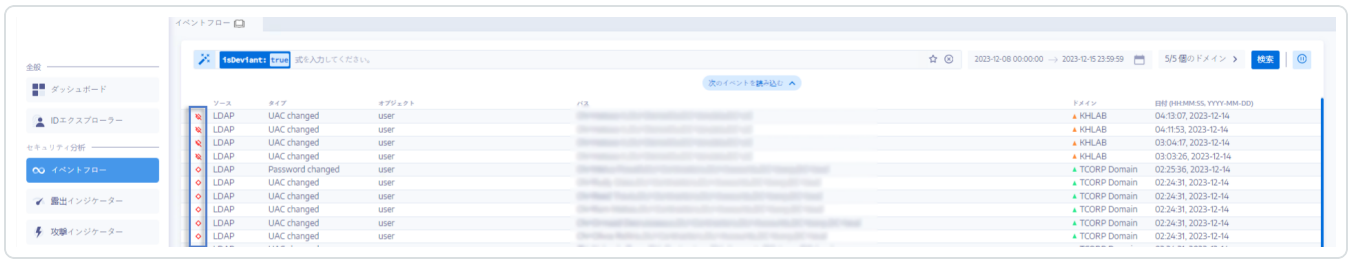
1. Tenable Identity Exposure で、**[イベント情報]** をクリックして [イベント情報] ページを開きます。
2. 検索ボックスの横にある アイコンをクリックします。

   [クエリ式の編集] ペインが開きます。



3. **[逸脱のみ]** トグルをクリックして [許可] に切り替えます。
4. **[検証]** をクリックします。

   Tenable Identity Exposure は、イベント情報テーブルの [ソース] の横に赤いひし形マークを付けてイベントのリストを更新します。



各部の説明

- イベント情報が、Tenable Identity Exposure セキュリティプロファイルの逸脱を検出しました。
- イベント情報が、他のセキュリティプロファイルの逸脱を検出しました。
- 変更によって逸脱が解決されたことを示します。

イベントの詳細

Tenable Identity Exposure のイベント情報には、Active Directory (AD) に影響する各イベントの詳細情報が表示されます。特定のイベントに関する詳細情報が得られるため、ユーザーは技術的な情報を確認し、露出インジケーターの深刻度レベル (重大、高、中、低) に応じて必要であれば対策措置を講じることができます。

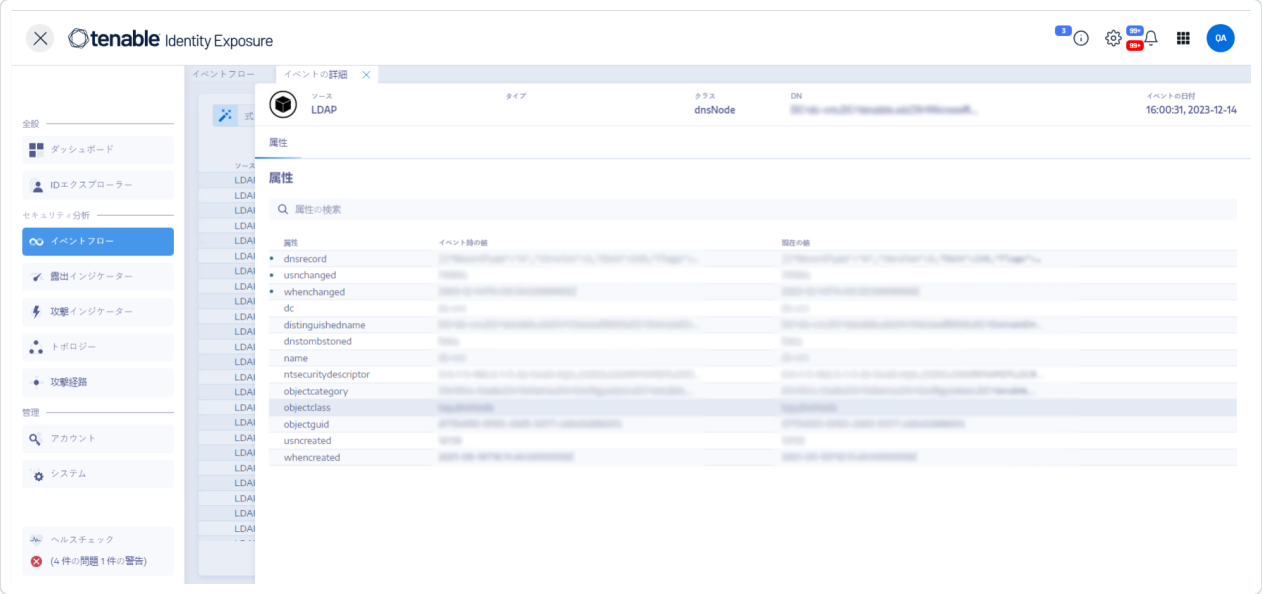
イベントの詳細を表示するには

1. Tenable Identity Exposure で、**[イベント情報]** をクリックして [イベント情報] ページを開きます。
2. [イベント情報] テーブルのエントリをクリックして選択します。

   [イベントの詳細] ペインが開きます。

IoE、イベント、逸脱オブジェクト

- **露出インジケーター** (IoE) は、AD に影響を与えている脅威について説明します。Tenable Identity Exposure の IoE は、イベントをリアルタイムで受信してセキュリティレベルを評価します。IoE にいくつかの技術的な脆弱性が含まれる場合もあります。IoE は、検出された脆弱性に関する情報、関連する逸脱オブジェクト、推奨対策措置を提供します。
- **イベント** は、AD で発生する可能性があるセキュリティ関連の変更を示します。これには、パスワードの変更やユーザーの作成、新しい GPO や変更された GPO、新しく委任された権限などが含まれます。イベントにより、IoE のコンプライアンスステータスが準拠から非準拠に変わる可能性があります。
- **逸脱オブジェクト** は技術的な要素です。それ単体で、または別の逸脱オブジェクトと関連付けられて、IoE の攻撃手法の特定が機能するようになります。



属性テーブル

属性テーブルには、次の列が含まれています。

列	説明
属性	イベント情報テーブルで選択したイベントに関連する AD オブジェクトの属性を示します。属性はオブジェクトの特徴を説明します。複数の属性で 1つの AD オブジェクトを説明することができます。
イベント時の値	イベント発生時の属性の値を示します。
現在の値	表示している時点における AD の属性の値を示します。

ヒント: イベントが発生する前の属性の値を表示するには、左側にある青い点の上にカーソルを合わせます (存在する場合)。

属性を検索するには

- **[イベントの詳細]** ペインで、検索ボックスに文字列を入力します。

  Tenable Identity Exposure は、検索文字列に一致する属性に絞り込んだリストを表示します。

詳細は、属性の変化 を参照してください。

逸脱

[イベント情報]のイベントに逸脱が含まれている場合、[イベントの詳細]ペインにも表示され、問題の原因を特定することができます。

逸脱を表示するには

1. Tenable Identity Exposure で、**[イベント情報]**をクリックして[イベント情報]ページを開きます。
2. [イベント情報]テーブルのエントリをクリックして選択します。

   [イベントの詳細]ペインが開きます。
3. **[逸脱]**タブを選択します。

   Tenable Identity Exposure は、逸脱のリストと、逸脱をトリガーした IoE を表示します。

IoE の詳細をドリルダウンするには

1. **[逸脱]**タブで、逸脱の理由の下にある IoE タイルをクリックします。

   [インジケーターの詳細]ペインが開き、逸脱オブジェクトのリストと次の情報が表示されます。

   - IoE の名前
   - IoE の深刻度(重大、高、中、低)
   - IoE のステータス
   - 直近の検出のタイムスタンプ

2. 次のいずれかのタブをクリックします。
    - **情報** – IoE に関する内部と外部のリソースが含まれています。
    - **脆弱性の詳細** – AD で検出された弱点に関する説明が表示されます。
    - **逸脱オブジェクト** – 技術的な詳細と、オブジェクトをフィルターする検索ボックスが含まれています。
    - **推奨事項** – 問題の解決方法に関するヒントが含まれています。

属性の変化

属性の値が変わると、イベント情報の**[属性]**列の前に青い点が表示されます。

属性の変化を表示するには

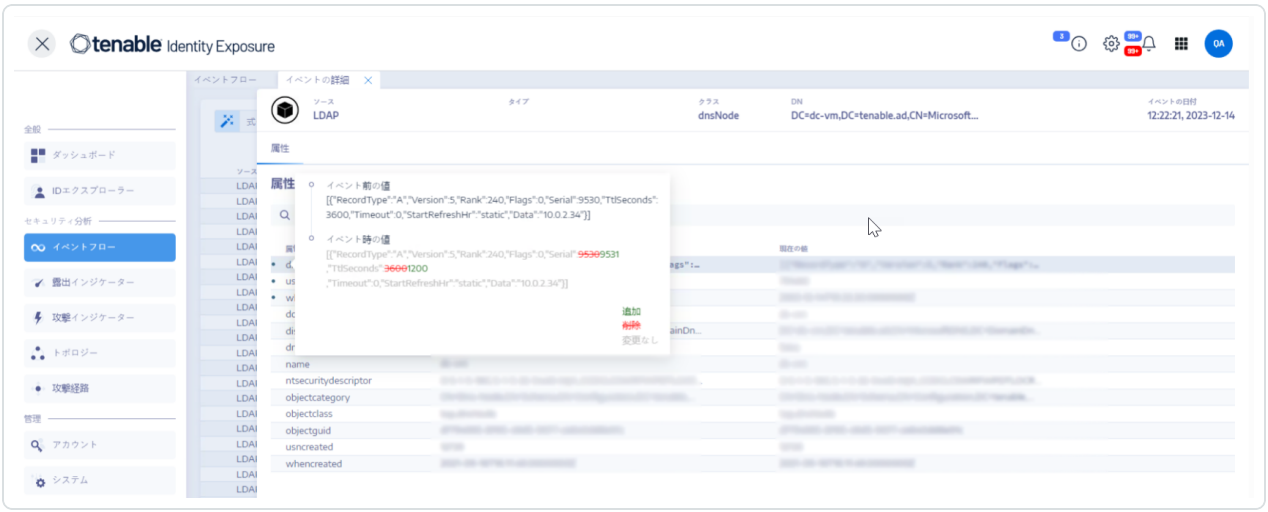
1. Tenable Identity Exposure で、左側のナビゲーションバーの**[イベント情報]**をクリックします。

   [イベント情報]ページが開き、イベントのリストが表示されます。

2. 変更内容を表示するには、イベント行の前にある青い点にカーソルを合わせます。

   [イベント時の値]ラベルの色は、属性に適用された変更に応じて異なります。

   - 緑 – **追加**
   - 赤 – **削除**
   - 灰色 – **変更なし**



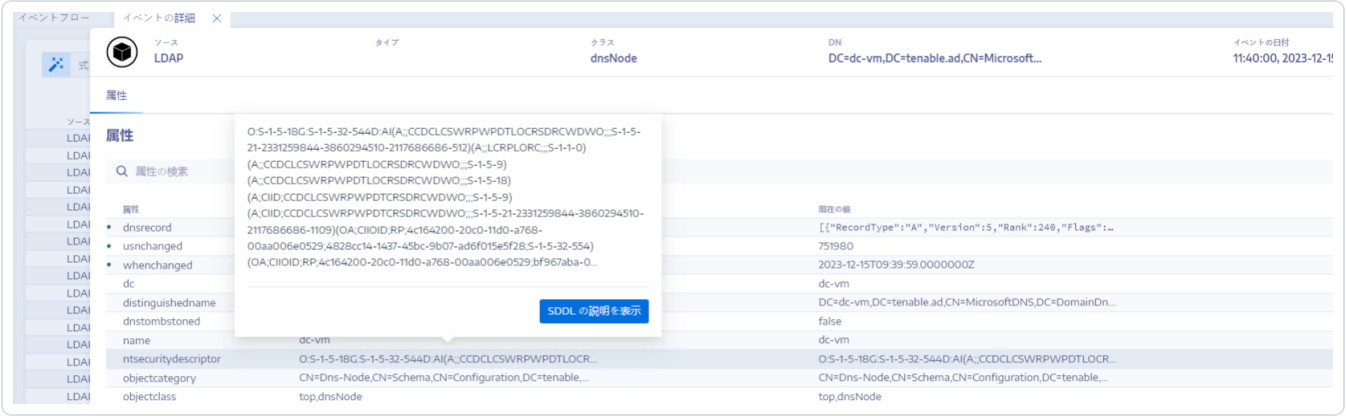
属性「ntsecuritydescriptor」

セキュリティ記述子は、所有者やアクセス許可といった、AD オブジェクトに関するセキュリティ情報を格納しているデータ構造です。詳細は、Microsoft のオンラインドキュメントをご覧ください。

オブジェクトのセキュリティ記述子の詳細を表示するには

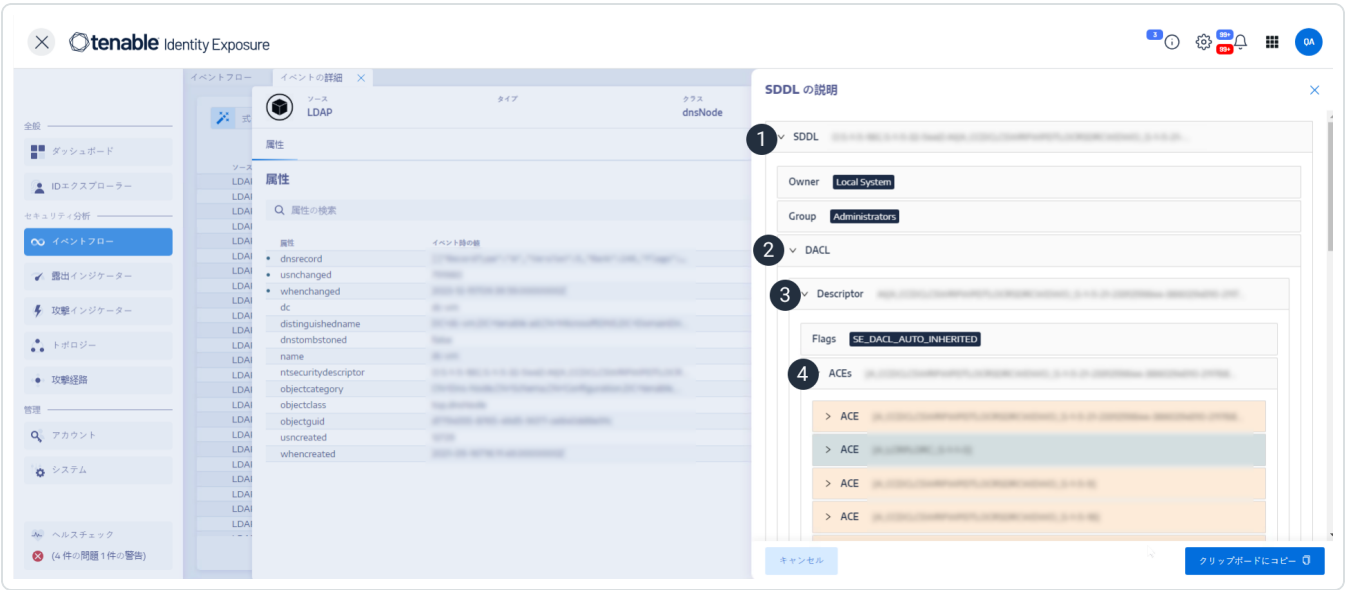
1. Tenable Identity Exposure で、**[イベント情報]** をクリックして [イベント情報] ページを開きます。
2. [イベント情報] テーブルのエントリをクリックして選択します。

   [イベントの詳細] ペインが開きます。
3. `ntsecuritydescriptor` 属性エントリにカーソルを合わせます([イベント時の値] 列または [現在の値] 列)**。



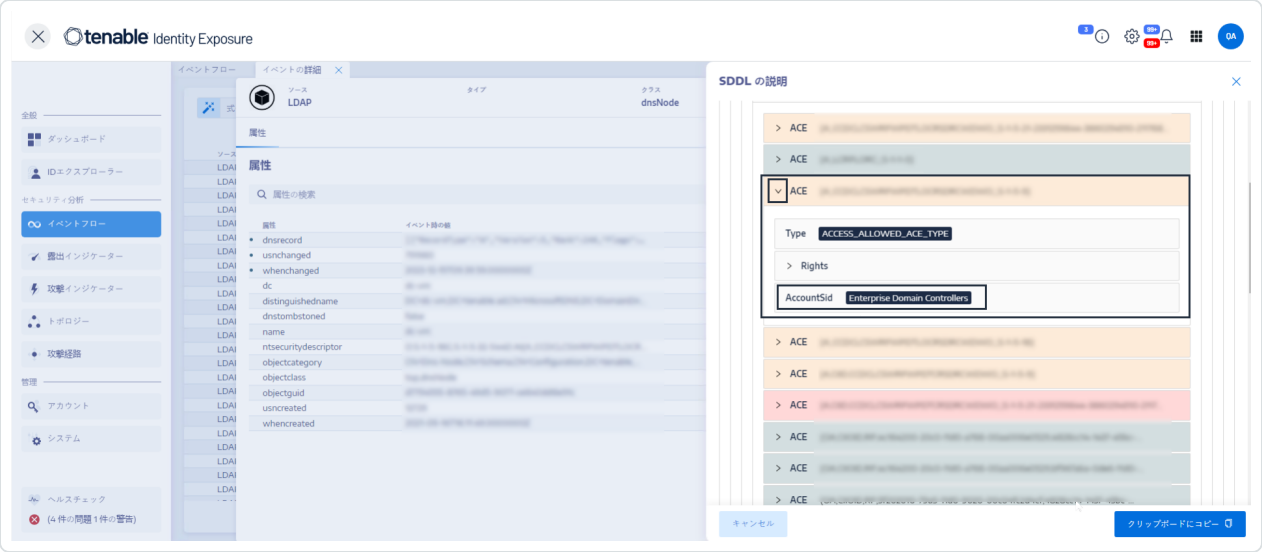
4. **[SDDL の説明を表示]** をクリックします。

   [SDDLの説明] ペインが開きます。
5. SDDL (1)、DACL (2)、記述子 (3) の左側にある矢印をクリックして、説明を展開します。



6. 色付きでハイライトされたアクセス制御エントリ(ACE)(4)を参照して、オブジェクトのアクセス権を表示します。カラーコードは以下を表しています。

   - **赤** – オブジェクトへのアクセス権があってはならないユーザーに危険な権限が割り当てられています。
   - **オレンジ** – 特権ユーザーに危険な権限が割り当てられています。ただし、特権ユーザーは通常この種の権限(ドメイン管理者など)を持っています 。
   - **緑** – 危険な権限はありません。



7. SDDL の説明をコピーするには、**[クリップボードにコピー]** をクリックします。

イベント情報のユースケース

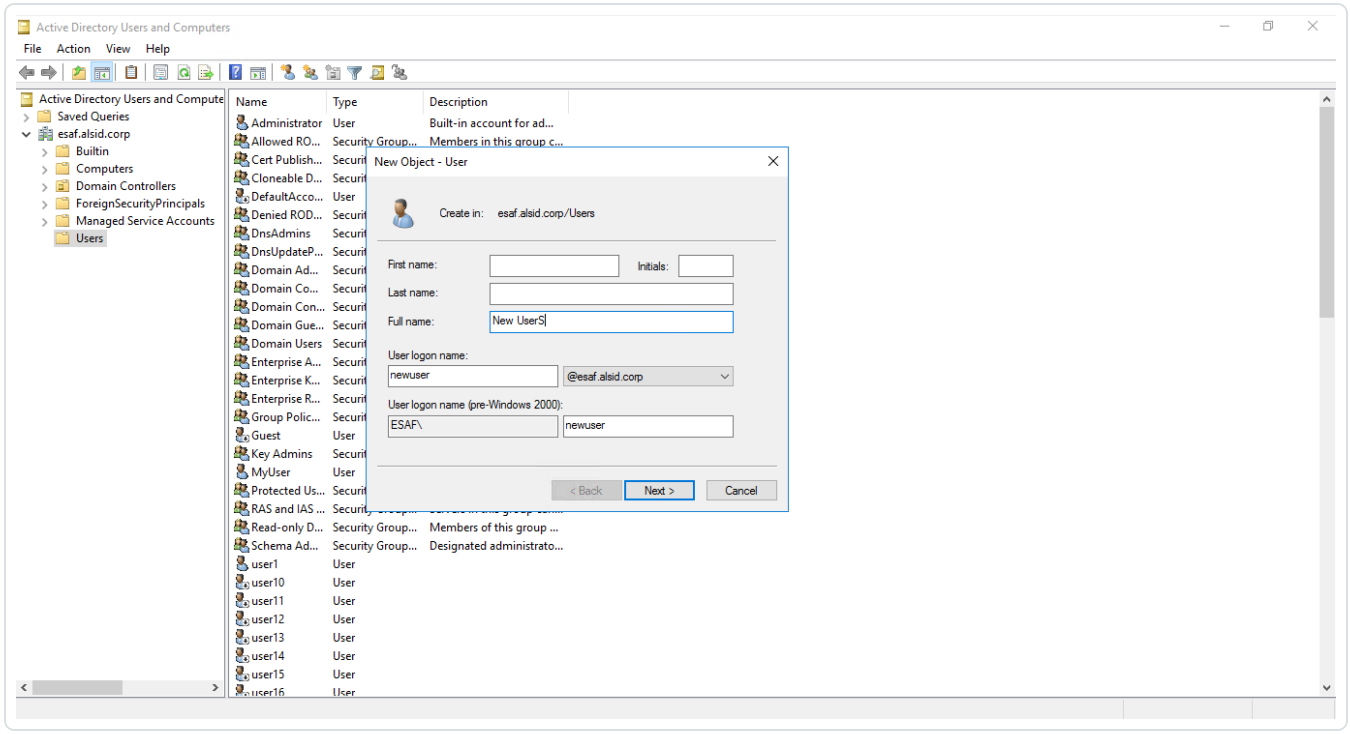
イベント情報の動作を理解するために、Active Directory (AD)インターフェースでの操作がどのようにイベント情報ページに反映されるのかを示す 2 つの例を考察します。

それぞれの例で、管理者側からのデータ (AD インターフェース) と、エンドユーザー側からのデータ (Tenable Identity Exposure) を比較します。アプリケーション、API、サービスのどれから AD の操作を実行しても、イベント情報での結果は同じです。

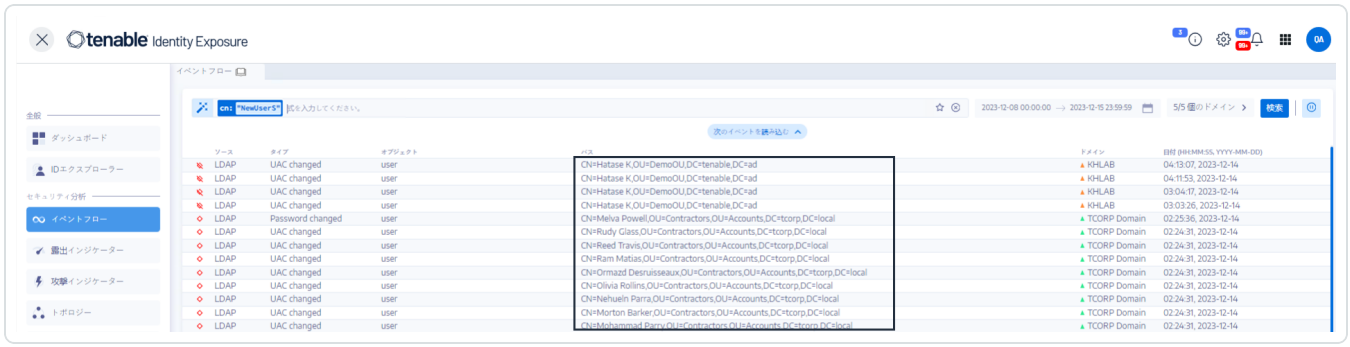
注意: ここで紹介するユースケースは例であって、起こり得るすべての状況には対応していません。

新しい AD ユーザーアカウントを作成したときのイベント情報の動作

- 管理者の側では、新しいユーザーアカウントに関するさまざまな情報を入力します。

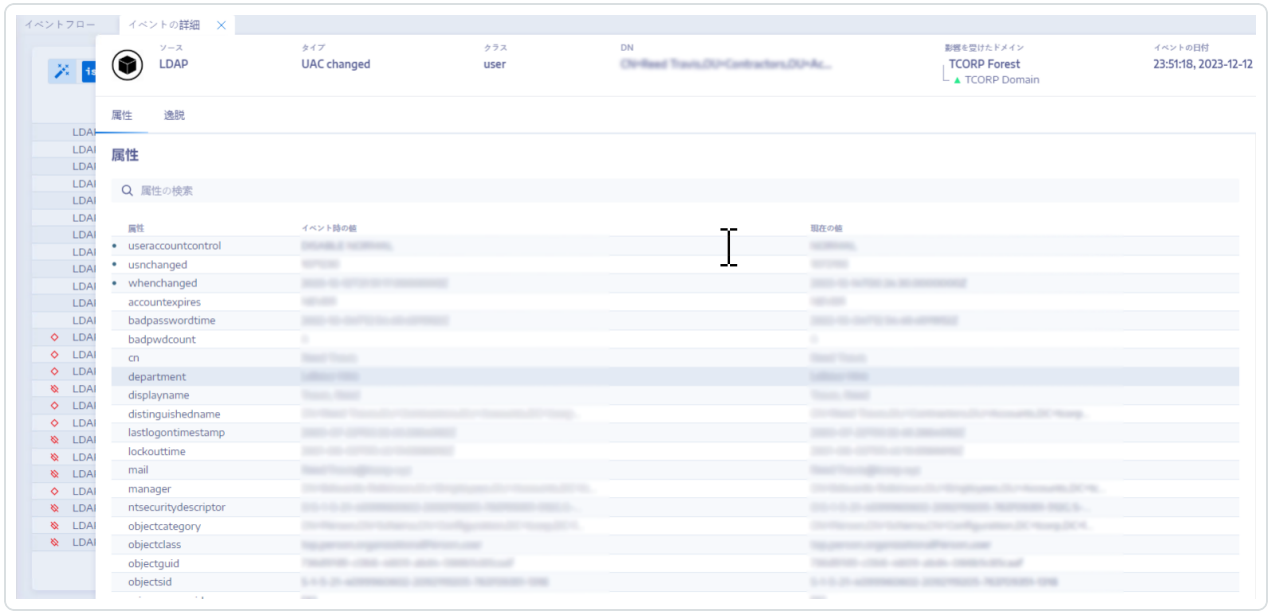


- エンドユーザーの側では、Tenable Identity Exposure が **[イベント情報]** ページを更新します。**[タイプ]** 列に、*[新しいオブジェクト]* と表示されています。



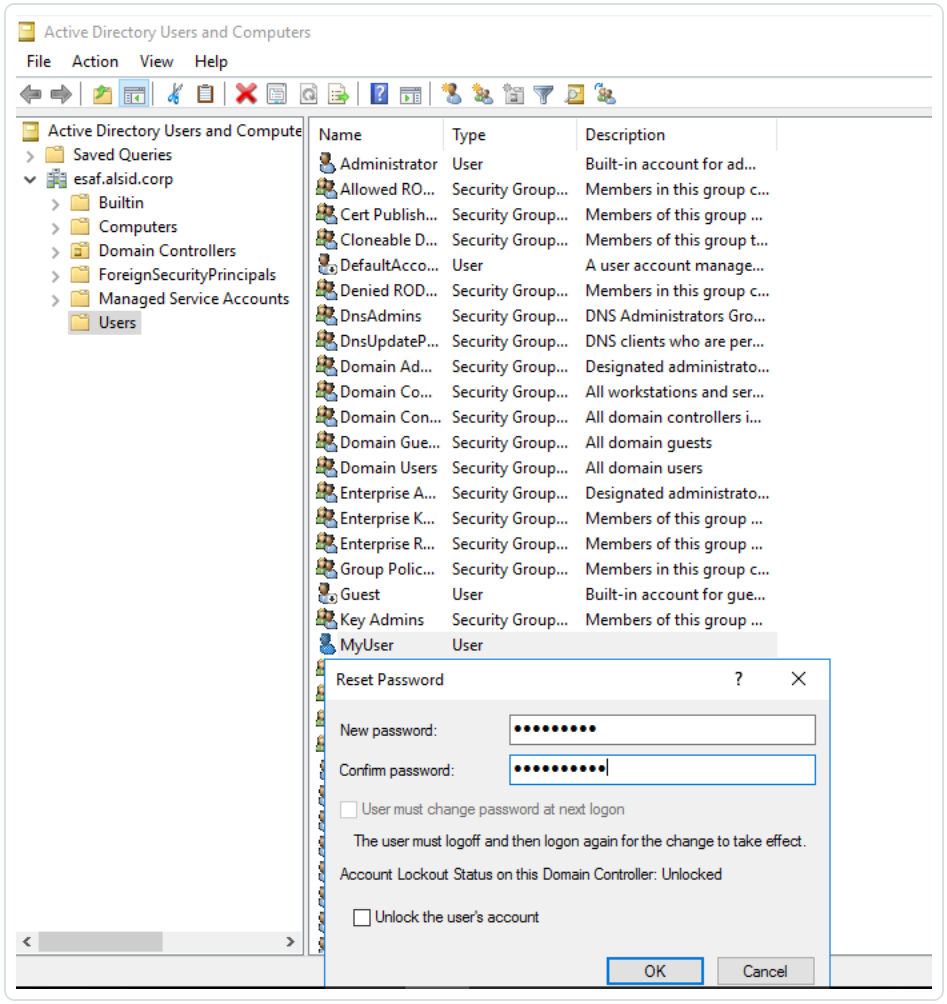
- **[イベントの詳細]** ページにもこの変更が反映されます。属性名の左側にある青い点は、更新が発生したことを示します。

  属性に関する詳細については、イベントの詳細の表示をご覧ください。



AD ユーザーのパスワードを変更したときのイベント情報の動作

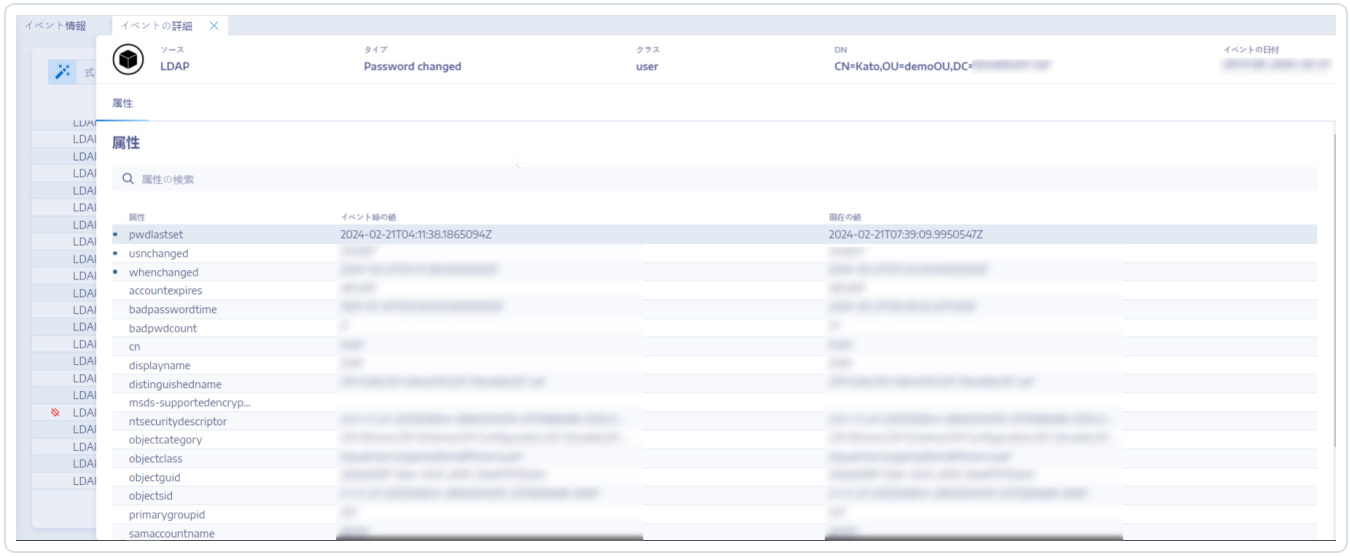
- 管理者の側では、ユーザーのパスワードをリセットするためのさまざまな情報を入力します。



- エンドユーザーの側では、Tenable Identity Exposure が**[イベント情報]**ページを更新します。**[タイプ]**列に、[パスワードが変更されました]と表示されます。

- この変更は**[イベントの詳細]**ページにも反映され、whenchanged 属性の左側に青い点が表示されます。

属性の詳細については、イベントの詳細を参照してください。



関連項目

- イベント情報を手動で検索
- ウィザードを使用してイベント情報を検索
- イベント情報のクエリをカスタマイズする
- ブックマーククエリ
- クエリ履歴

露出インジケーター

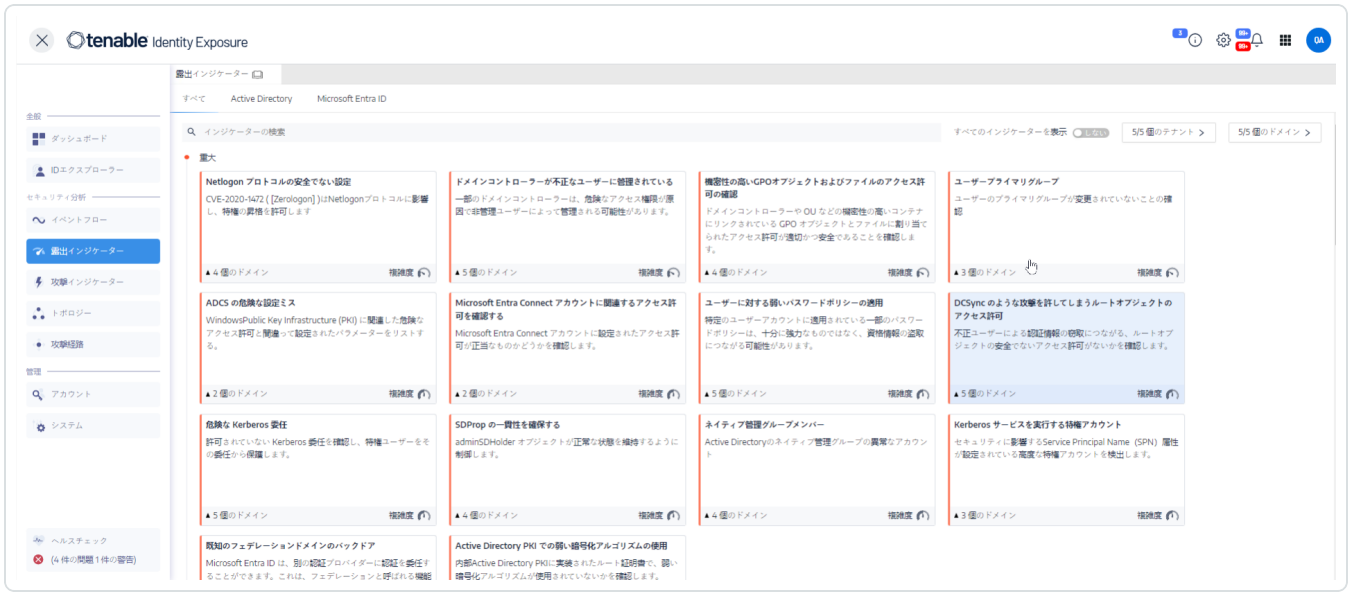
Tenable Identity Exposure は、AD インフラのセキュリティ成熟度を露出インジケーターを通じて測定し、監視および分析対象のイベントのフローに対して深刻度レベルを割り当てます。Tenable Identity Exposure は、セキュリティの悪化を検出するとアラートを送信します。

IoE を表示するには

1. Tenable Identity Exposure で、ナビゲーションペインの **[露出インジケーター]** をクリックします。

   [露出インジケーター] ペインが開きます。デフォルトでは、Tenable Identity Exposure は逸脱を含む IoE だけを表示します。

2. (オプション) すべての IoE を表示するには、**[すべてのインジケーターを表示]** トグルをクリックして **[はい]** に切り替えます。



IoE を検索するには

1. **[露出インジケーター]** ページの上部にある検索ボックスに文字列を入力します。文字列は、パスワード、ユーザー、ログオンなど、IoE に関連する任意の用語を使用できます。

2. Enter を押します。

   IoE ページが、入力した検索用語に関連するインジケーターで更新されます。

特定のフォレストやドメインの IoE を表示するようフィルタリングするには

1. **[n/n 個のドメイン]** をクリックします。

   [フォレストとドメイン] ペインが開きます。

2. フォレストまたはドメインを選択します。
3. **[選択内容でフィルター]** をクリックします。

深刻度レベル

深刻度レベルにより、検出された脆弱性の深刻度を評価し、修正アクションに優先順位を付けることが可能になります。

[露出インジケーター] ペインに IoE が次のように表示されます。

- カラーコードを使用した深刻度レベル。
- 垂直方向 – 深刻度の高い順 (赤が最も優先順位が高く、青が最も低い)。
- 水平方向 – 複雑度の高い順。Tenable Identity Exposure は複雑度の指標を動的に計算して、逸脱した IoE の修正の難易度を示します。

深刻度	説明
重大 – 赤	特定の非特権ユーザーによる Active Directory の攻撃や侵害を防止するにはを示します。
高 – オレンジ	認証情報の盗取やセキュリティ機能のバイパスにつながる侵入後のテクニック、または危険な状態へと連鎖的につながる可能性のある手口を示します。
中 – 黄	Active Directory インフラに対する限定的なリスクを示します。
低 – 青	優れたセキュリティ対策を示します。特定のビジネス環境では、必ずしも AD のセキュリティに影響を与えるとは限らない影響度の低い逸脱が許容される場合もあります。これらの逸脱は、管理者が非アクティブなアカウントをアクティブ化するなどのミスをした場合にのみ、ADに影響を与えます。

関連項目

- 露出インジケーターの詳細
- 逸脱オブジェクト
- 逸脱オブジェクトを検索
- 逸脱オブジェクトの無視
- 危険の原因となっている属性

露出インジケーターの詳細

特定の露出インジケーターの詳細では、検出された脆弱性、関連する逸脱オブジェクト、および修正の推奨事項に関する技術情報を確認できます。

露出インジケーターの詳細を表示するには

1. Tenable Identity Exposure で、ナビゲーションペインの**[露出インジケーター]**をクリックします。

   [露出インジケーター]ペインが開きます。デフォルトでは、Tenable Identity Exposure は逸脱を含む IoE だけを表示します。

2. (オプション) すべての IoE を表示するには、**[すべてのインジケーターを表示]**トグルをクリックして**[はい]**に切り替えます。

3. ページにある任意の**[露出インジケーター]**タイルをクリックします。

   [インジケーターの詳細]ペインが開きます。

[インジケーターの詳細]ペインの上部に、イベント情報テーブルですでに提供されている情報の要約が表示されます。

- IoE の**名前**
- IoE の**深刻度**レベル(重大、高、中、低)
- 前回 Tenable Identity Exposure が行った分析結果に基づいたコンプライアンスの**ステータス**
- Tenable Identity Exposure が最後に分析を実行した時刻を示す**最新の検出**

4. 次のいずれかのタブをクリックすると、IoE の詳細が表示されます。

タブ	説明
情報	IoE に関する以下のような内部と外部のリソースが含まれています。 • エグゼクティブサマリー – 問題の概要が記載されており、適切な意思決定を行うのに役立ちます。 • ドキュメント – 当該 IoE に関する外部リソースへのリンク。 • 攻撃者の既知のツール – ハッキングツールの名前。 • 影響を受けたドメインのツリー構造。
脆弱性の詳細	AD で検出された脆弱性の説明、および修正措置をしない場合に Active Directory (AD) に及ぶリスクが表示されます。
逸脱オブジェクト	逸脱オブジェクトは、AD の脆弱性や潜在的に危険な動作を明らかにします。逸脱オブジェクトにフィルターを適用して、重大な問題を正確に特定できます。 IoE のステータスが非準拠で逸脱オブジェクトが含まれる場合、修正措置を講じて Tenable Identity Exposure によって検出されたセキュリティ上の欠陥を是正することができます。詳細は、逸脱オブジェクト を参照してください。
推奨事項	セキュリティ要件へのコンプライアンスを取り戻し、AD のセキュリティを改善するには に関するヒント。 • エグゼクティブサマリーには、Tenable Identity Exposure が提案する解決策の概要が示されます。 • 詳細サブセクションには、アクションプランの実施方法に関するアドバイスが表示され、マネージャーが AD インフラに対して必要な変更を開始するのに役立ちます。 • ドキュメントサブセクションには、推奨されている解決策や脅威に関する外部リソースへのリンクがあります。

関連項目

- 露出インジケーター
- 逸脱オブジェクト
- 逸脱オブジェクトを検索
- 逸脱オブジェクトの無視
- 危険の原因となっている属性

逸脱オブジェクト

Tenable Identity Exposure の露出インジケーター(IoE)は、Active Directory(AD)の脆弱性や潜在的に危険な動作を明らかにする逸脱オブジェクトにフラグを立てることができます。これらの逸脱オブジェクトに注意を払えば、重大な問題を正確に特定して修正することができます。以下の操作が可能です。

- 逸脱オブジェクトを検索する
- 一定期間、逸脱オブジェクトを無視する
- フォレストとドメインを選択して逸脱オブジェクトを検索する
- IoE に影響を与えている、危険の原因となっている属性に関する説明を取得する
- すべての逸脱オブジェクトが記載されたレポートをダウンロードする

逸脱オブジェクトを表示するには

1. Tenable Identity Exposure で、ナビゲーションペインの **[露出インジケーター]** をクリックします。

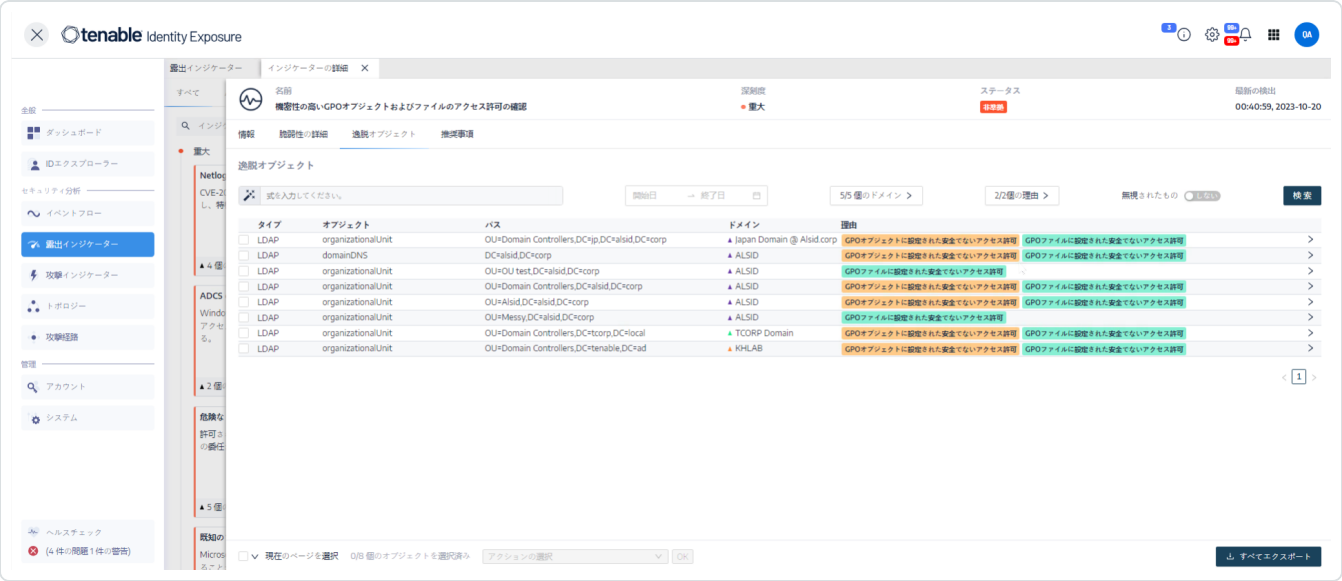
   [露出インジケーター] のページが開きます。デフォルトでは、Tenable Identity Exposure は逸脱を含む IoE だけを表示します。

2. ページにある任意の **[露出インジケーター]** タイルをクリックします。

   [インジケーターの詳細] ペインが開きます。

3. **[逸脱オブジェクト]** タブをクリックします。

   IoE に関連付けられている逸脱オブジェクトのリストが表示されます。



逸脱オブジェクトのテーブルには、以下の情報が含まれています。

- **タイプ** – AD (LDAP または SMB プロトコル) で起きたセキュリティ関連の変更の発生源を示します。
- **オブジェクト** – AD オブジェクトに関連付けられたクラスまたはファイル拡張子を示します。
- **パス** – AD オブジェクトへのフルパスを示し、そのオブジェクトの AD 内の一意の場所を特定できるようにします。
- **ドメイン** – AD の変更が発生したドメインを示します。
- **理由** – 逸脱オブジェクトに影響を与えている、危険の原因となった属性の一覧を示します。

逸脱オブジェクトのレポートをエクスポートするには

1. **[逸脱オブジェクト]** ページの下部にある **[すべてエクスポート]** をクリックします。

   [逸脱オブジェクトのエクスポート] ペインが表示されます。

2. **[エクスポート形式]** ボックスでドロップダウン矢印をクリックして、形式を選択します。
3. **[すべてエクスポート]** をクリックします。

   Tenable Identity Exposure は逸脱オブジェクトのレポートをマシンにダウンロードします。

関連項目

- 露出インジケーター
- 露出インジケーターの詳細
- 逸脱オブジェクトを検索
- 逸脱オブジェクトの無視
- 危険の原因となっている属性

逸脱オブジェクトを検索

逸脱オブジェクトを手動で、またはウィザードを使用して検索できます。

ウィザードでの検索

検索ウィザードで、クエリ式を作成できます。

- 検索ボックスで頻繁に使用する式をブックマークのリストに追加して、後で使用することができます。
- 検索ボックスに式を入力すると、Tenable Identity Exposure はこの式を[履歴]ペインに保存し、再利用できるようにします。

ウィザードを使用して逸脱オブジェクトを検索するには

1. 逸脱オブジェクトのリストを表示します。
2. アイコンをクリックします。

   [クエリ式の編集]ペインが開きます。

3. パネルでクエリ式を定義するには、**AND** または **OR** 演算子ボタン(1)をクリックして、最初の条件に適用します。
4. 属性をドロップダウンメニューから選択し、値を入力します(2)。
5. 次のいずれかを行います。

- 属性を追加するには、**[+ 新しいルールの追加]**(3)をクリックします。
- 別の条件を追加するには、**[新しい条件の追加]**の**+ AND**または**+ OR**演算子をクリックします。属性をドロップダウンメニューから選択し、値を入力します。
- 逸脱オブジェクトだけを検索するには、**[逸脱のみ]**のトグルをクリックして許可します。**+ AND**または**+ OR**演算子を選択して、条件をクエリに追加します。
- 条件またはルールを削除するには、🗑アイコンをクリックします。

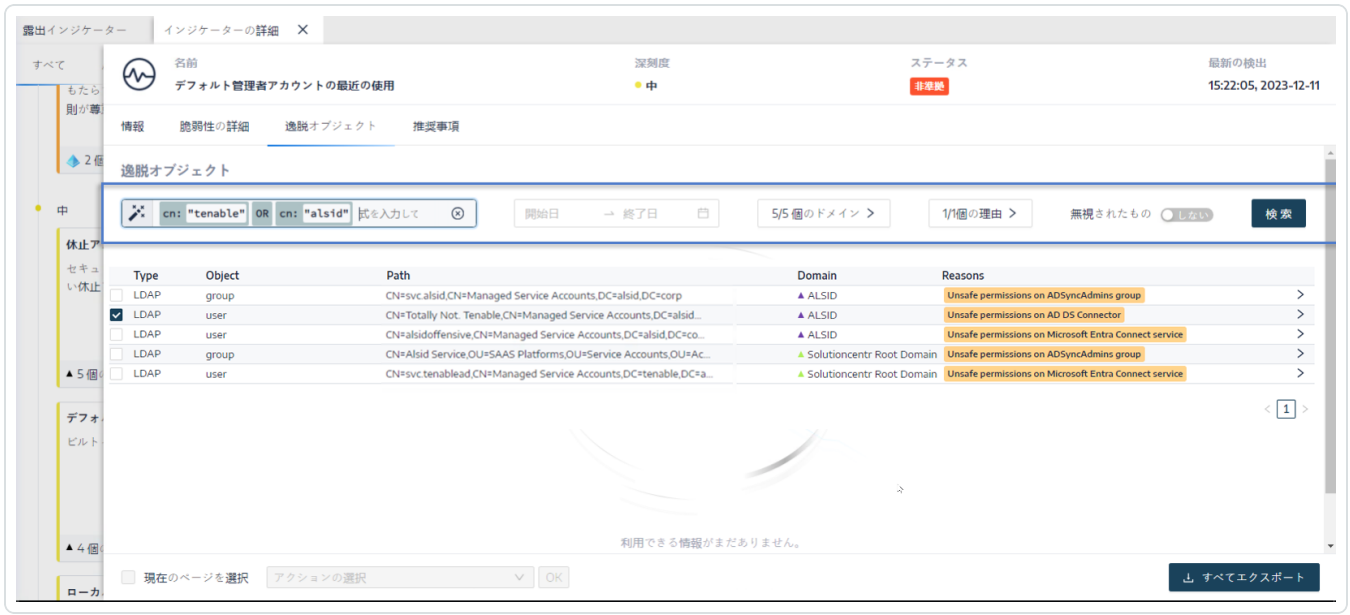
6. **[検証]**をクリックして検索を実行するか、**[リセット]**をクリックしてクエリ式を変更します。

手動の検索

特定の文字列またはパターンに一致する逸脱オブジェクトだけを表示するようフィルタリングするには、検索ボックスに式を入力し、ブール演算子 *、**AND**、**OR**を使用して結果を絞り込みます。検索の優先順位を変更したい場合は、括弧を使用して**OR**ステートメントをカプセル化できます。検索では、Active Directory属性の特定の値が検索されます。イベント情報を手動で検索するには

逸脱オブジェクトを手動で検索するには

1. 逸脱オブジェクトのリストを表示します。



2. 検索ボックスに、クエリ式を入力します。
3. 次のように検索結果をフィルタリングできます。

- **[カレンダー]** ボックスをクリックして、開始日と終了日を選択します。
- **[n/n 個のドメイン]** をクリックして、フォレストとドメインを選択します。

4. **[検索]** をクリックします。

   Tenable Identity Exposure は、検索条件に一致する結果でリストを更新します。

文法と構文

手動クエリ式は、次の文法と構文を使用します。

- 文法: `EXPRESSION [OPERATOR EXPRESSION]*`
- 構文: `__KEY__ __SELECTOR__ __VALUE__`

  各部の説明

  - `__KEY__`: 検索する AD オブジェクト属性を表します (`CN`、`userAccountControl`、`members` など)。
  - `__SELECTOR__`: 演算子 (`:`、`>`、`<`、`>=`、`<=`) を表します。
  - `__VALUE__`: 検索する値を表します。

    特定のコンテンツを検索する場合は、さらに多くのキーを使用できます。
  - `isDeviant`: 逸脱を引き起こしたイベントを検索します。

AND と **OR** 演算子を使用して、イベント情報のクエリ式を複数組み合わせることができます。

例

- 共通の名前属性で文字列 `alice` を含むすべてのオブジェクトを検索: `cn:"alice"`
- 共通の名前属性で文字列 `alice` を含み、かつ特定の逸脱を引き起こしたすべてのオブジェクトを検索: `isDeviant: "true" AND cn: "alice"`
- Default Domain Policy という名前の GPO を検索: `objectClass:"groupPolicyContainer" AND displayname:"Default Domain Policy"`
- S-1-5-21 を含む SID を持つすべての非アクティブ化されたアカウントを検索: `userAccountControl:"DISABLE" AND objectSid:"S-1-5-21"`

- Sysvol 内のすべての script.ini ファイルを検索：globalpath:"sysvol" AND types:"SCRIPTSini"

> **注意**：ここの types は列ヘッダーではなくオブジェクト属性のことです。

関連項目

- 露出インジケーター
- 露出インジケーターの詳細
- 逸脱オブジェクト
- 逸脱オブジェクトの無視
- 危険の原因となっている属性

逸脱オブジェクトの無視

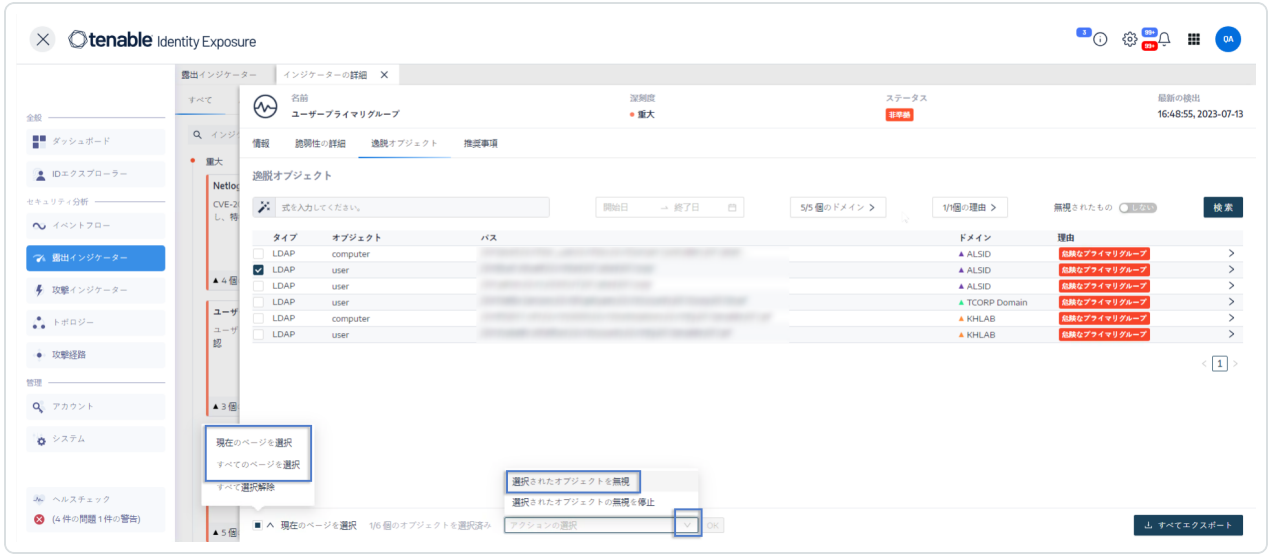
調査やレポート作成の際に画面が乱雑になるのを防ぐ目的で、Tenable Identity Exposure が選択された特定の期間を無視するようにして、一部の逸脱オブジェクトをフィルターで除外することができます。1 つまたは複数の逸脱オブジェクトを無視することもできます。カスタムフィルターを直ちに適用するか、フィルターを有効にする時間枠を指定できます。

注意: オブジェクトを無視しても、Tenable Identity Exposure で解決されるわけではありません。

逸脱オブジェクトを無視するには

1. Tenable Identity Exposure で逸脱オブジェクトのリストを表示します。
2. 無視する逸脱オブジェクトの前にあるチェックボックスを選択します。
3. オプションで、逸脱オブジェクトをフィルタリングして無視することもできます。
    - **[カレンダー]** ボックスをクリックして、開始日と終了日を選択します。
    - **[n/n 個のドメイン]** をクリックして、フォレストとドメインを選択します。

ヒント: 選択を速やかに行うには、ページの下部にある **[すべてのページを選択]** または **[現在のページを選択]** ボックスにチェックを入れます。



4. ページ下部にあるドロップダウンリストから **[選択されたオブジェクトを無視]** を選択します。
5. **[OK]** をクリックします。

[選択されたオブジェクトを無視] ペインが表示されます。

6. **[無視する期間の終了日]** ボックスをクリックしてカレンダーを表示し、Tenable Identity Exposure が逸脱オブジェクトを無視する最後の日付を選択します。
7. **[OK]** をクリックします。

   Tenable Identity Exposure は確認メッセージを表示し、残りの逸脱オブジェクトのリストを更新します。

無視した逸脱オブジェクトを表示するには

1. **[無視されたもの]** トグルをクリックして **[はい]** に切り替えます。
2. ページの下部にある **[すべてのページを選択]** をクリックします。
3. ドロップダウンリストから **[選択されたオブジェクトの無視を停止]** を選択します。
4. **[OK]** をクリックします。

   確認ペインが表示されます。
5. **[OK]** をクリックして、変更を確定します。

   Tenable Identity Exposure は無視された逸脱オブジェクトを表示します。

関連項目

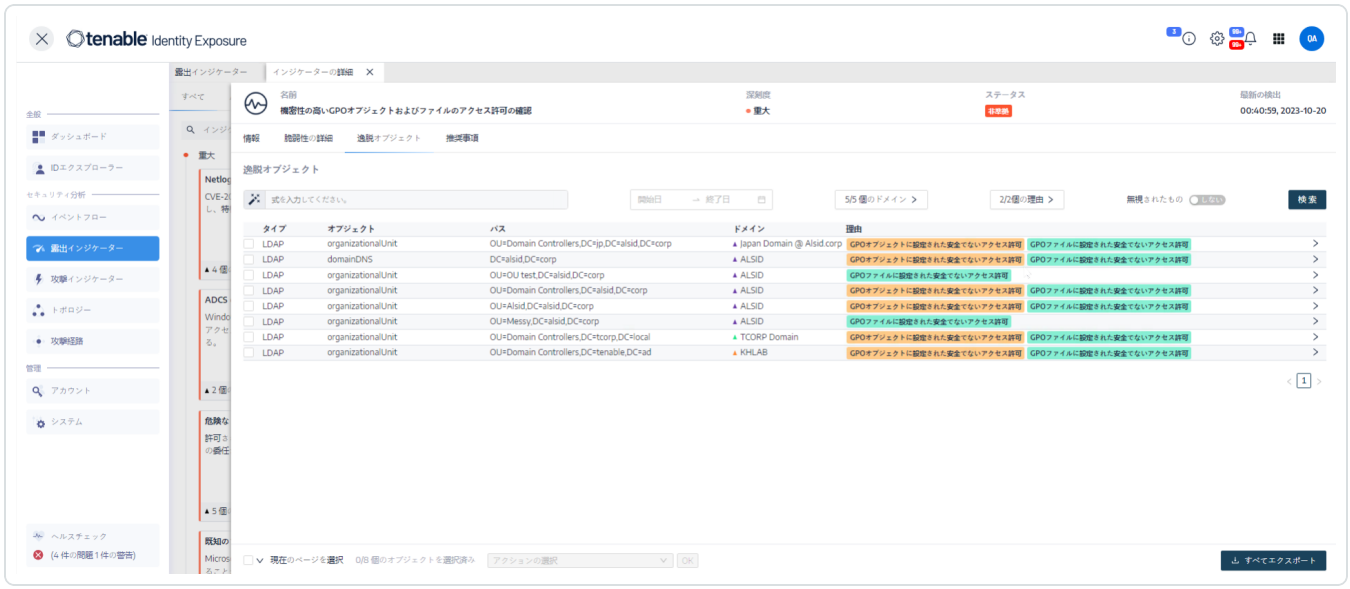
- 露出インジケーター
- 露出インジケーターの詳細
- 逸脱オブジェクト
- 逸脱オブジェクトを検索
- 危険の原因となっている属性

危険の原因となっている属性

Tenable Identity Exposure は、逸脱オブジェクトをトリガーする原因となっている属性を露出インジケーターに表示して、その理由を示し、ユーザーが逸脱を理解して修正できるようにします。

危険の原因となっている属性を表示するには

1. 逸脱オブジェクトのリストを表示します。



2. 逸脱オブジェクトのリストのエントリをクリックします。

   Tenable Identity Exposure は、その逸脱オブジェクトの原因となっている属性のリストを表示しま

す。

リストには以下の情報が含まれています。

- 理由が複数ある場合に理由を区別するための**色分けされたタグ**
- 値
  - ?: 属性値の欠落(空)。異常な動作を示します。
  - [この逸脱の利用可能な説明はありません]: この逸脱はバージョン 2.6 の時点で検出されたものであり、現在 Tenable Identity Exposure はこの属性を管理していません。

危険の原因となっている属性をコピーするには

- 属性を選択し、 アイコンをクリックします。

関連項目

- 露出インジケーター
- 露出インジケーターの詳細
- 逸脱オブジェクト
- 逸脱オブジェクトを検索
- 逸脱オブジェクトの無視

RSoP ベースの露出インジケーター

Tenable Identity Exposure は、一連の RSoP (ポリシーの結果セット) ベースの露出インジケーター (IoE) を使用して、さまざまな側面のセキュリティとコンプライアンスを評価し保証します。このセクションでは、特定の RSoP IoE の現在の動作について、およびその計算に関連するパフォーマンスの懸念事項に Tenable Identity Exposure がどのように対処しているかについて、インサイトを提供します。

次の RSoP ベースの IoE は、Tenable Identity Exposure のセキュリティフレームワークで役割を果たします。

- 特権ユーザーのログオン制限
- 機密性の高い危険な特権
- ユーザーに対する弱いパスワードポリシーの適用
- ランサムウェアに対する不十分な堅牢化
- Netlogon プロトコルの安全でない設定

これらの IoE は、必要に応じて初期化される RSoP 計算結果キャッシュに依存し、既存の値に依存せずにリクエストに応じて追加される値を計算します。以前は、`AdObjects` への変更がキャッシュ無効化を引き起こし、IoE の RSoP 実行中に頻繁に再計算が行われていました。

Tenable Identity Exposure では、RSoP 計算に関連するパフォーマンスへの影響に次のように対処しています。

1. **最新ではない可能性のあるデータを使用したライブ IoE 分析** – RSoP に依存する IoE の計算 (入出力イベント) は、処理に使用されるデータが最新のものでなくても、発生時にリアルタイムで実行されます。RSoP キャッシュを無効にする可能性のあるバッファされたイベントは、特定の条件を満たすまで保存され、予測した計算が行われるようにします。
2. **スケジュールされた RSoP 無効化** – 再計算の条件を満たすと、システムは無効化プロセス中にバッファされたイベントを考慮して、RSoP キャッシュを無効にします。
3. **最新のキャッシュを使用した IoE の再実行** – キャッシュが無効化された後、バッファされたイベントを取り込んで、キャッシュにある最新バージョンの `AdObject` で IoE が再実行されます。Tenable Identity Exposure は、バッファされたイベントごとに IoE を個別に計算します。

こうした理由により、RSoP に依存する IoE の計算時間が最適化されると、RSoP に関連する逸脱の計算に時間がかかります。

Microsoft Entra ID 関連の露出インジケーター

Microsoft Entra ID 専用の露出インジケーター

Tenable Identity Exposure には、Microsoft Entra ID の資産に存在する可能性のある脆弱性を警告する専用の露出インジケーター(IoE) があります。

Microsoft Entra ID の IoE を表示するには

1. Tenable Identity Exposure で、左側のナビゲーションバーの IoE アイコン をクリックします。

   IoE ペインが開きます。

2. **[Microsoft Entra ID]** タブをクリックします。

   Tenable Identity Exposure は、検出結果をトリガーした Microsoft Entra ID に関連する IoE を表示します。

3. 調査したい IoE のタイルをクリックします。

4. [インジケーター ID の詳細] ペインが開き、次の情報が表示されます。

   - **脆弱性情報**: どのように攻撃にさらされる可能性があるか
   - **検出結果**: ID プロバイダーのタイプに関する詳細とリスクの説明
   - **推奨事項**: 脅威を修正する手順

露出インジケーターからの逸脱を修正

Tenable Identity Exposure は、露出インジケーター(IoE)が、修正が必要な逸脱オブジェクトに遭遇したときにアラートをトリガーします。

以下は、3 つの特定の IoE に対する修正手順の実行方法を示す例です。

- 標準ユーザーに設定される AdminCount 属性
- 危険な Kerberos 委任
- SDProp の一貫性を確保する

IoE の詳細については、Tenable Identity Exposure ユーザーインターフェースで提供されるドキュメントを参照してください。

標準ユーザーに設定される AdminCount 属性

ユーザーアカウントの adminCount 属性は、管理グループにおける過去のメンバーシップを示し、アカウントがグループに含まれなくなった後でもリセットされません。その結果、古い管理アカウントにもこの属性があり、Active Directory のアクセス許可の継承がブロックされます。本来は管理者を保護することを目的としていますが、アクセス許可に関する問題が発生する可能性があります。

この中レベルの IoE は、この属性を持つアクティブなユーザーアカウントとグループのみをレポートし、adminCount 属性が 1に設定された正当なメンバーを持つ特権グループはレポートしません。

標準ユーザーに設定される AdminCount 属性 IoE からの逸脱オブジェクトを修正するには、次の手順を実行します。

1. Tenable Identity Exposure で、ナビゲーションペインの **[露出インジケーター]** をクリックして開きます。

   デフォルトでは、Tenable Identity Exposure は逸脱オブジェクトを含む IoE だけを表示します。

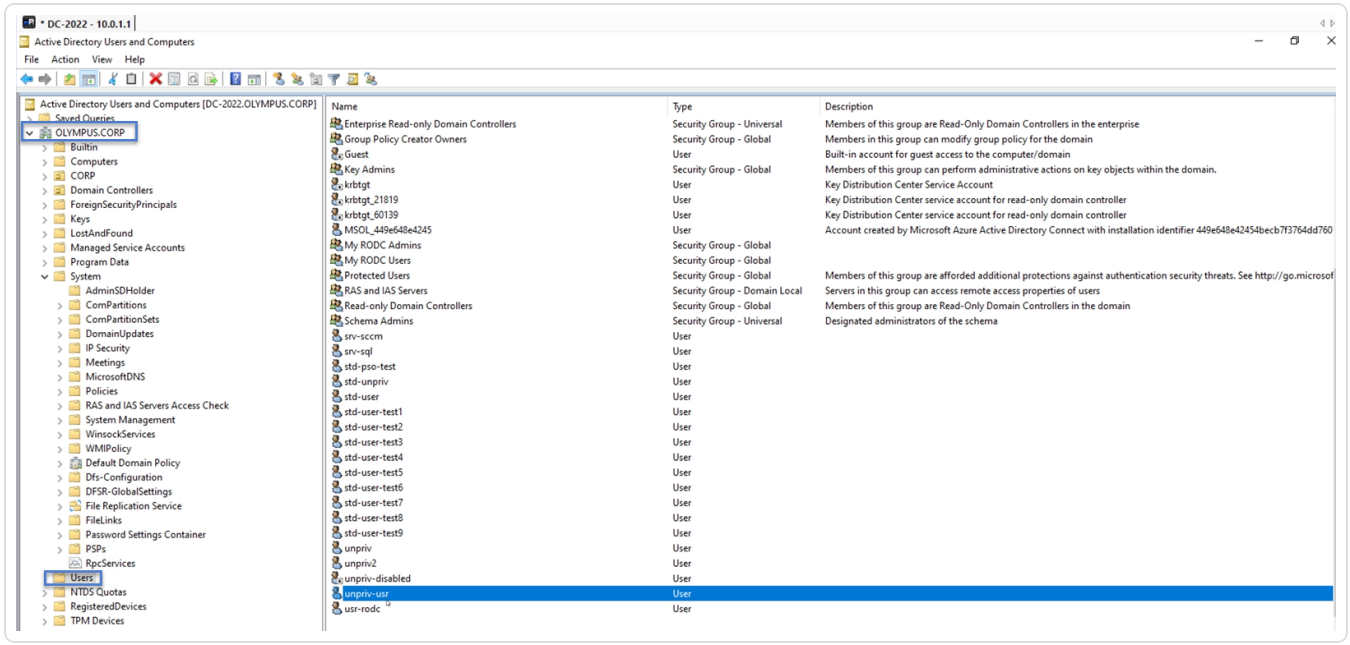
2. **標準ユーザーに設定される AdminCount 属性** IoE のタイルをクリックします。

   [インジケーターの詳細] ペインが開きます。

3. 逸脱オブジェクトにカーソルを合わせてクリックすると詳細が表示されるので、ドメイン名とアカウントを書き留めます。(この例では、ドメイン = OLYMPUS.CORP、標準アカウントは unpriv-usr)

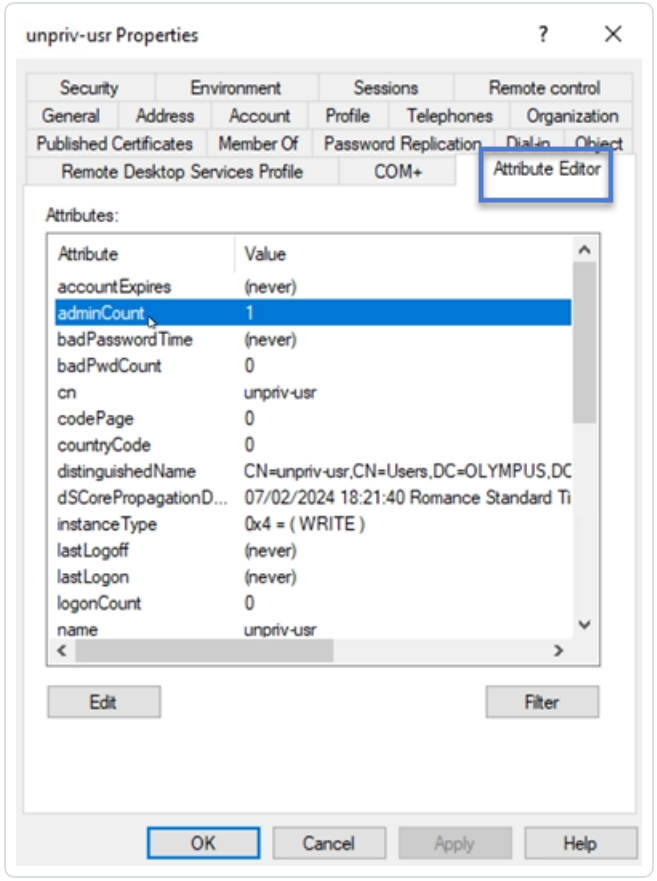
4. リモートデスクトップマネージャー(または類似のツール)で、ドメイン名を見つけて、**[ユーザー]** と Tenable Identity Exposure フラグが付けられたアカウントに移動します。

> **必要なアクセス許可**: この手順を実行するには、ドメインの管理者アカウントが必要です。

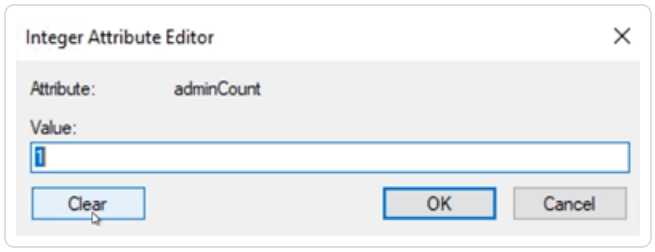


5. アカウント名をクリックして **[プロパティ]** ダイアログボックスを開き、**[属性エディター]** タブを選択します。

6. 属性のリストで、[adminCount] をクリックして **[Integer Attribute Editor]** (整数属性エディター) ダイアログボックスを開きます。



7. ダイアログボックスで、**[クリア]** および **[OK]** をクリックします。



8. Tenable Identity Exposure で、[インジケーターの詳細] ペインに戻り、ページを更新します。

   逸脱オブジェクトがリストに表示されなくなります。

危険な Kerberos 委任

Kerberos プロトコルは Active Directory のセキュリティの中核をなすもので、選択したサーバーにユーザー認証情報を再利用する許可を与えます。攻撃者がこの選択したサーバーの 1 つを侵害すると、その認証情報を盗み、他のリソースで認証を得るために使用することができます。

この重大レベルの IoE は、委任の属性を持つアカウントすべてを報告します。ただし、無効化されたアカウントは除外します。特権ユーザーは委任属性を持つべきではありません。これらのユーザーアカウントを保護するには、「保護ユーザー」グループに追加するか、「アカウントは重要なので委任できない」をマークします。

アカウントを「保護されたグループ」に追加するには

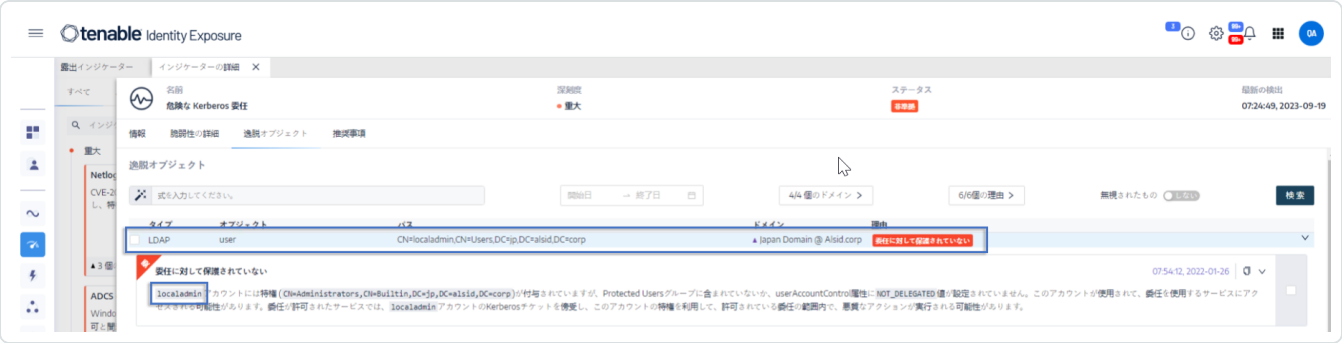
1. Tenable Identity Exposure で、ナビゲーションペインの **[露出インジケーター]** をクリックして開きます。

   デフォルトでは、Tenable Identity Exposure は逸脱オブジェクトを含む IoE だけを表示します。

2. **危険な Kerberos 委任** IoE のタイルをクリックします。

[インジケーターの詳細] ペインが開きます。

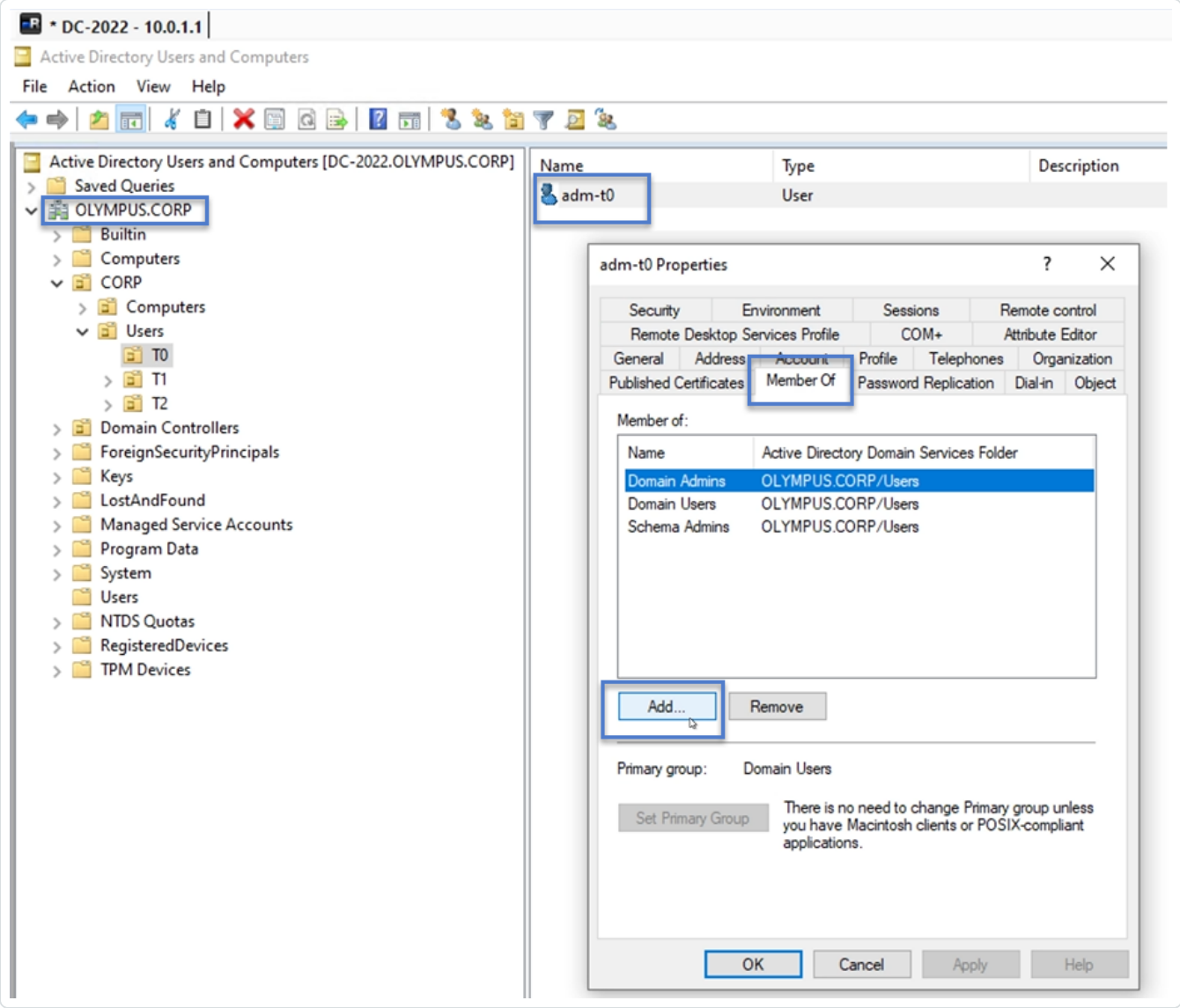
3. 逸脱オブジェクトにカーソルを合わせてクリックすると詳細が表示されるので、ドメイン名とアカウントを書き留めます。(この例では、ドメイン = OLYMPUS.CORP、アカウント = `adm-t0`)。



4. リモートデスクトップマネージャー(または類似のツール)で、ドメイン名を見つけて、ドメインと Tenable Identity Exposure フラグが付けられたアカウントに移動します。

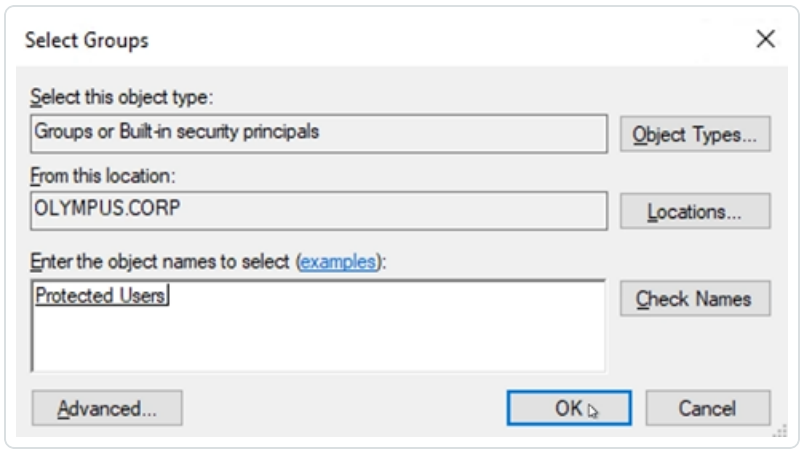
> **必要なアクセス許可**: この手順を実行するには、ドメインの管理者アカウントが必要です。

5. アカウント名をクリックして **[プロパティ]** ダイアログボックスを開き、**[所属グループ]** タブを選択します。
6. メンバーリストで、**[追加]** をクリックします。



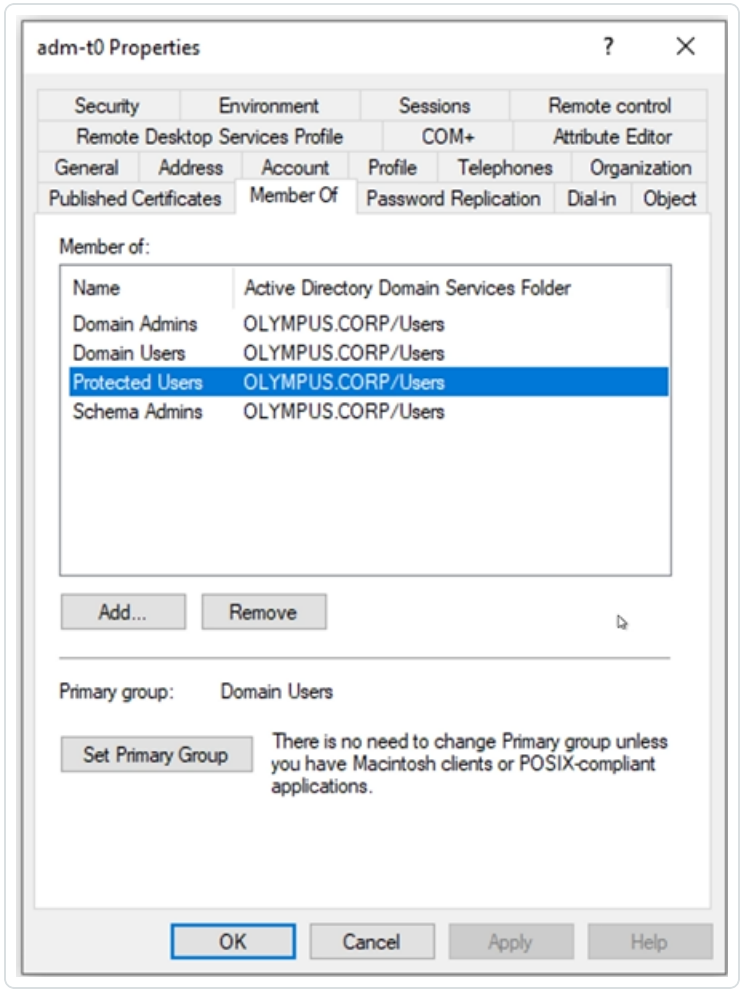
[グループの選択] ダイアログボックスが表示されます。

7. オブジェクト名に「保護ユーザー」と入力し、**[名前の確認]** をクリックします。



8. **[OK]** をクリックして、ダイアログボックスを閉じます。
9. **[プロパティ]** ダイアログボックスで、**[適用]** をクリックします。

   新しいグループがメンバーリストに表示されます。



10. **[OK]** をクリックして、ダイアログボックスを閉じます。
11. Tenable Identity Exposure で、[インジケーターの詳細] ペインに戻り、ページを更新します。

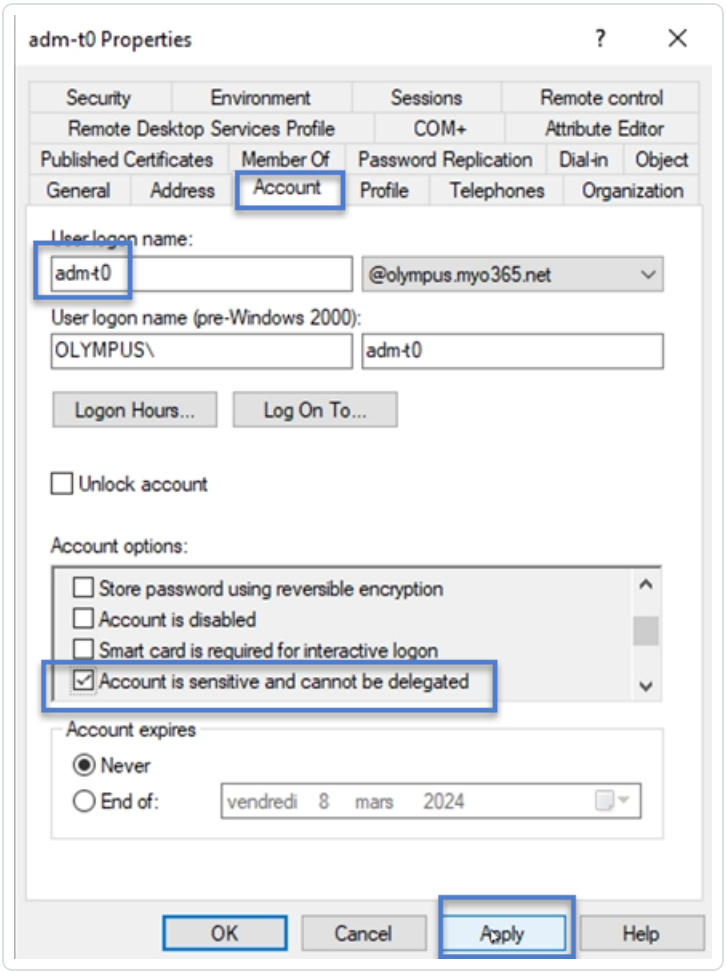
    逸脱オブジェクトがリストに表示されなくなります。

アカウントを「委任できない」に設定するには

1. リモートデスクトップマネージャーで、ドメイン名を見つけて、ドメインと Tenable Identity Exposure フラグが付けられたアカウントに移動します。

   必要なアクセス許可: この手順を実行するには、ドメインの管理者アカウントが必要です。

2. アカウント名をクリックして **[プロパティ]** ダイアログボックスを開き、**[アカウント]** タブを選択します。
3. アカウントオプションのリストから、[アカウントは重要なので委任できない] を選択し、**[適用]** をクリックします。



4. **[OK]** をクリックして、ダイアログボックスを閉じます。
5. Tenable Identity Exposure で、[インジケーターの詳細] ペインに戻り、ページを更新します。

   逸脱オブジェクトがリストに表示されなくなります。

SDProp の一貫性を確保する

Active Directoryドメインを侵害する攻撃者は通常、adminSDHolder オブジェクトの ACL を変更し、攻撃者が ACL に追加するアクセス許可は特権ユーザーにコピーされるため、バックドアが簡単に設置されてしまいます。

この重大レベルの IoE は、adminSDHolder オブジェクトに設定されているアクセス許可が管理者アカウントへの特権アクセスのみを許可していることをチェックします。

SDProp の一貫性を確保する IoE から逸脱オブジェクトを修正するには

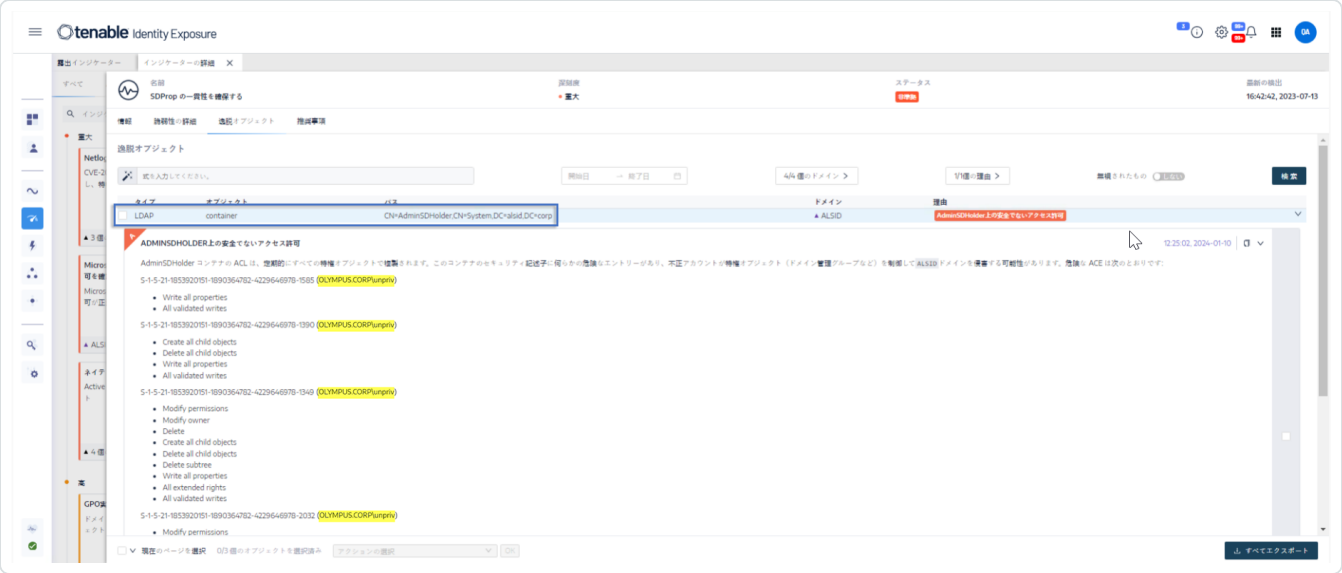
1. Tenable Identity Exposure で、ナビゲーションペインの **[露出インジケーター]** をクリックして開きます。

   デフォルトでは、Tenable Identity Exposure は逸脱オブジェクトを含む IoE だけを表示します。

2. **SDProp の一貫性を確保する** IoE のタイルをクリックします。

[インジケーターの詳細] ペインが開きます。

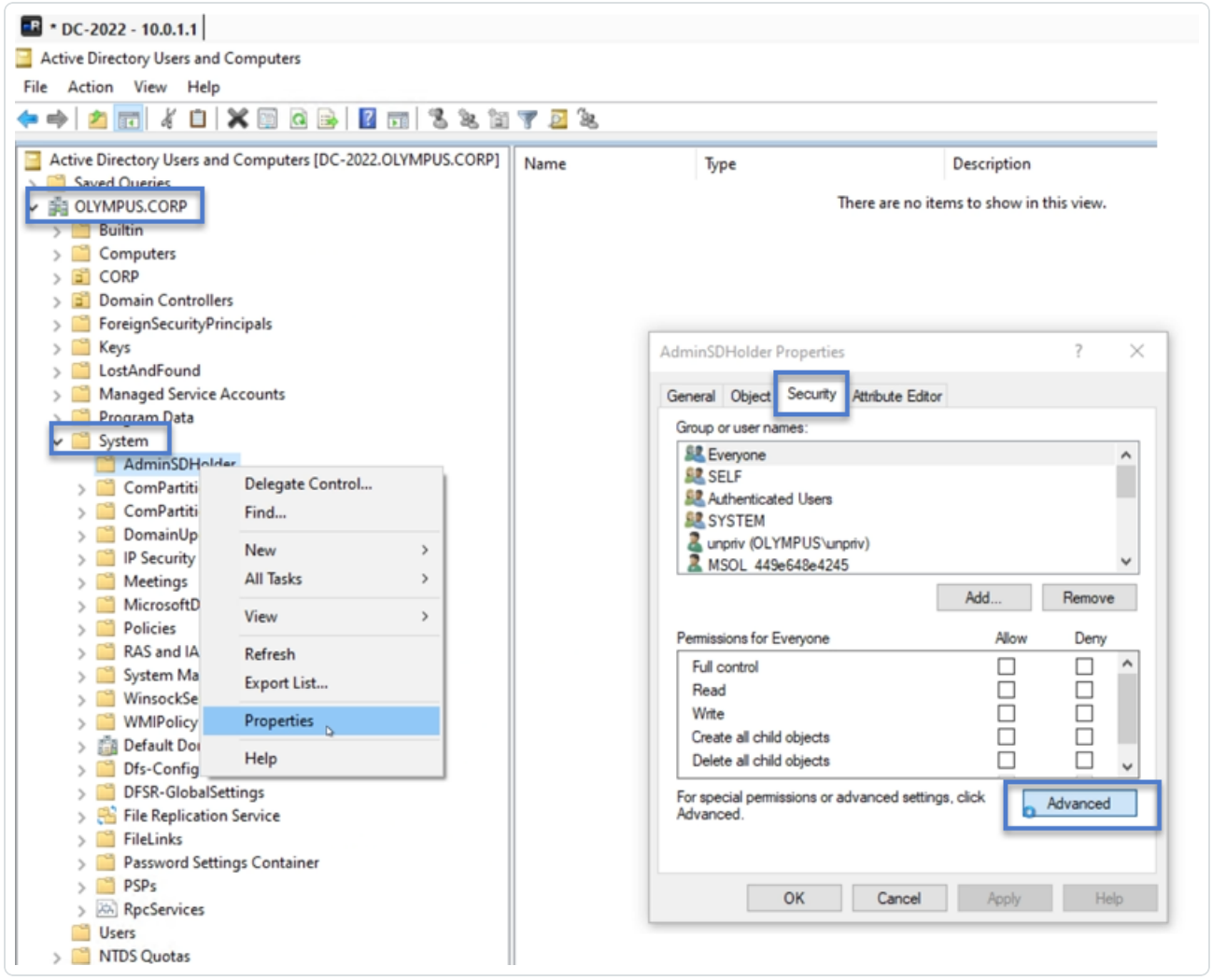
3. 逸脱オブジェクトにカーソルを合わせてクリックすると詳細が表示されます。Tenable Identity Exposure がフラグを立てたドメイン名と関連するアクセス許可を書き留めます。(この例では、`OLYMPUS.CORP .\unpriv`)。



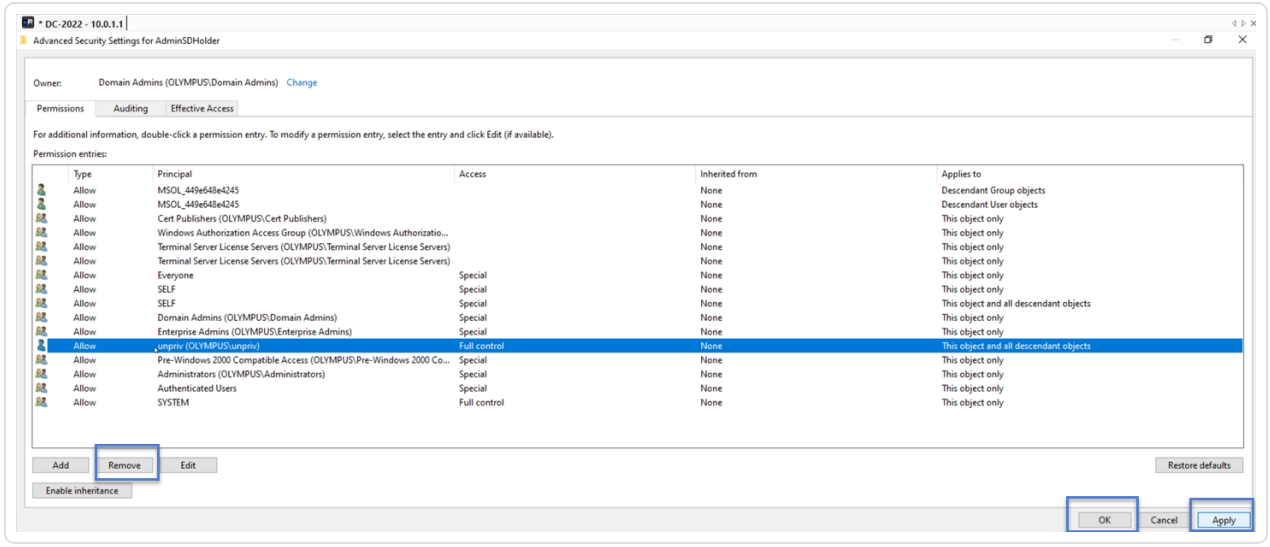
4. リモートデスクトップマネージャー（または類似のツール）で、ドメイン名を見つけて、**[システム]** > **[AdminSDHolder]** に移動します。

> **必要なアクセス許可**：この手順を実行するには、ドメインの管理者アカウントが必要です。

5. **[AdminSDHolder]** を右クリックし、コンテキストメニューから **[プロパティ]** を選択します。



6. **[プロパティ]** ダイアログ ボックスで、**[セキュリティ]** タブを選択し、**[詳細]** をクリックします。
7. **[セキュリティの詳細設定]** ウィンドウの **[アクセス許可]** タブで、アクセス許可エントリのリストからアラートが発生したアクセス許可を選択します。
8. **[削除]** をクリックします。
9. **[適用]**、**[OK]** の順にクリックして、設定ウィンドウを閉じます。
10. **[OK]** をクリックして、**[プロパティ]** ウィンドウを閉じます。



11. Tenable Identity Exposure で、[インジケーターの詳細] ペインに戻り、ページを更新します。

    逸脱オブジェクトがリストに表示されなくなります。

攻撃インジケーター

必要なライセンス: 攻撃インジケーター

Tenable Identity Exposure の **攻撃インジケーター**(IoA) により、Active Directory (AD) に対する攻撃を検出することができます。

攻撃インジケーターの統合ビューには、タイムライン、リアルタイムで AD に影響を与えたトップ 3 のインシデント、および攻撃の分布が 1 つのペインにまとめて表示されます。以下を実行できます。

- 正確な攻撃タイムラインによってすべての脅威を視覚化
- AD への攻撃の詳細な情報を分析
- 検出されたインシデントから、直接 MITRE ATT&CK の説明を確認

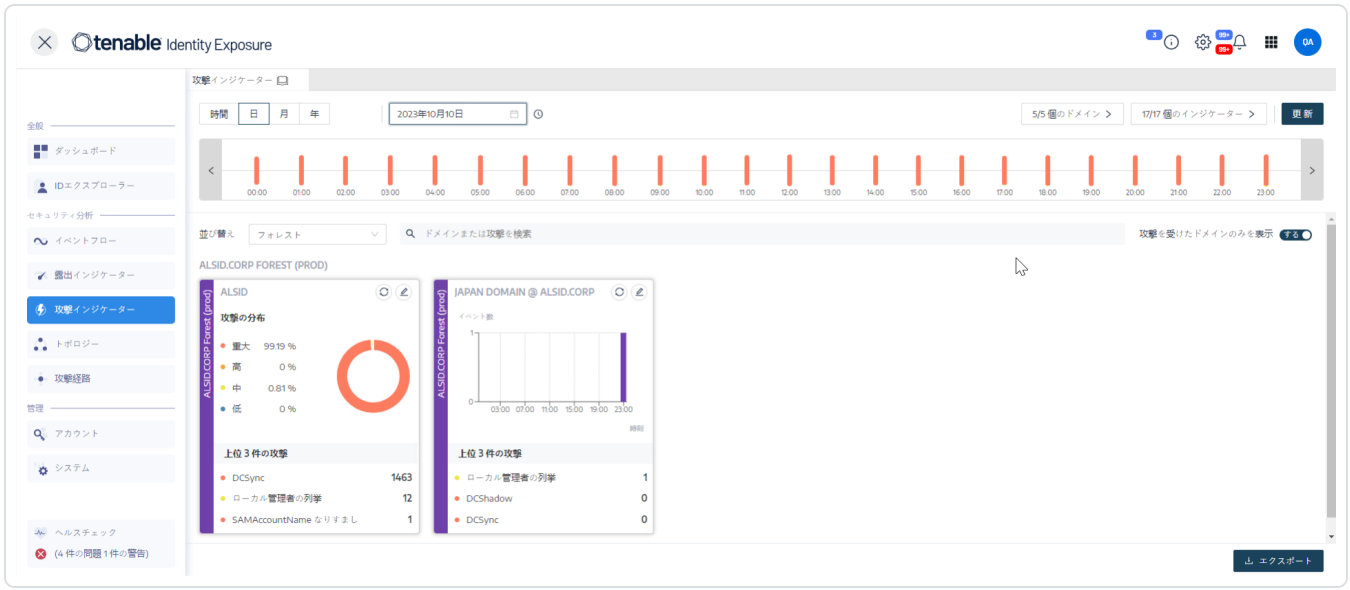
特定の IoA の詳細については、Indicators of Attack and the Active Directoryを参照してください。

注意: 検出された攻撃の数が多い場合は、管理者がさまざまな攻撃インジケーターのオプションに推奨値を適用して IoA を正しく調整していることを確認してください。詳しくは、IoA を調整するにはを参照してください。

攻撃インジケーターを表示するには

1. Tenable Identity Exposure で、ナビゲーションペインの **[攻撃インジケーター]** をクリックします。

   [攻撃インジケーター] ペインが開きます。



2. デフォルトでは、Tenable Identity Exposure はすべての AD フォレストとドメインを表示します。この表示を調整するには、次のいずれかを実行します。

   - 表示する期間を選択 - **時間**、**日** (デフォルト)、**月**、または**年**をクリックします。
   - タイムラインに沿って移動 - 左または右の矢印をクリックして、タイムラインを前後に移動します。
   - 特定の時間を選択 - 日付の選択コントロールをクリックして、時間、日、月、年を選択します。
   - 現在の日付と時刻に戻る - 日付の選択コントロールの横にある アイコンをクリックします。
   - ドメインを選択 - **[n/n 個ドメイン]** をクリックします。

     a. **[フォレストとドメイン]** ペインで、ドメインを選択します。

     b. **[選択内容でフィルター]** をクリックします。

     Tenable Identity Exposure がビューを更新します。
   - IoA を選択 - **[n/n 個のインジケーター]** をクリックします。

     a. 攻撃インジケーターペインで、IoA を選択します。

     b. **[選択内容でフィルター]** をクリックします。

     Tenable Identity Exposure がビューを更新します。
   - IoA タイルを並べ替え – **[並び順]** ボックスの矢印をクリックして、**ドメイン**、**重大度**、**フォレスト** の選択肢がある選択ドロップダウンリストを表示します。
   - ドメインまたは攻撃の検索 – **[検索]** ボックスに、ドメイン名または攻撃を入力します。
   - 攻撃されているドメインのみを表示 – **[攻撃を受けたドメインのみを表示]** トグルをクリックして、**[はい]** に切り替えます。
   - 攻撃レポートをエクスポート - **[エクスポート]** をクリックします。

   [カードのエクスポート] ペインが表示されます。

a. **[エクスポート形式]** ボックスで、ドロップダウン矢印をクリックして、**PDF**、**CSV**、**PPTX** から形式を選択します。

b. **[エクスポート]** をクリックします。

Tenable Identity Exposure はレポートをローカルマシンにダウンロードします。

深刻度レベル

Tenable Identity Exposure は、攻撃を検出し、以下の深刻度レベルを割り当てます。

レベル	説明
重大 – 赤	前提条件としてドメインの支配が必要な、実証済みの悪用後の攻撃を検出しました。
高 – オレンジ	攻撃者がドメインの支配を可能にする重大な攻撃を検出しました。
中 – 黄	IoA は、危険な権限昇格や、機密性の高いリソースへのアクセスの許可につながる可能性のある攻撃と関連しています。
低 – 青	偵察活動や影響度の低いインシデントに関連する疑わしい動作について警告しています。

関連項目

- 攻撃インジケーターの詳細
- 攻撃インジケーターインシデント

攻撃インジケーターの詳細

Tenable Identity Exposure の攻撃インジゲーターペインには、Active Directory で発生した攻撃に関する情報が表示されます。

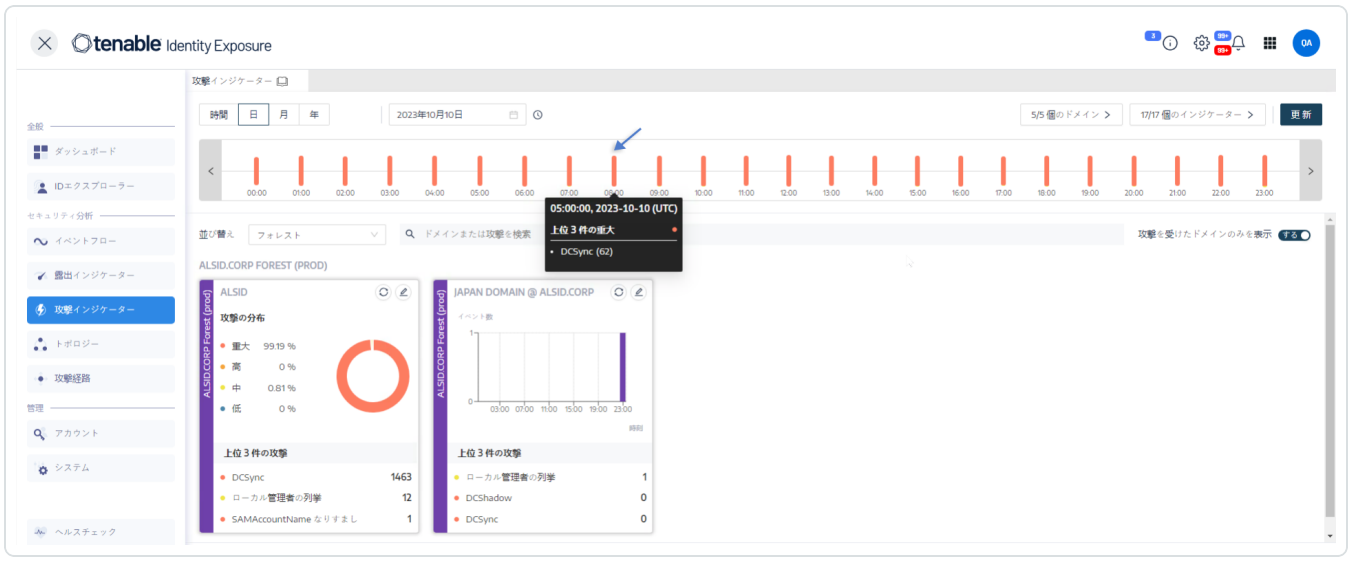
攻撃インジケーターを表示するには

- Tenable Identity Exposure で、ナビゲーションペインの **[攻撃インジケーター]** をクリックします。

  [攻撃インジケーター] ペインが開きます。

タイムラインの攻撃情報を表示するには

- タイムラインに沿って並んでいるイベントをクリックすると、以下が表示されます。
  - インシデントが検出された日時
  - トップ 3 の攻撃の深刻度レベル
  - この日時に検出された攻撃の総数



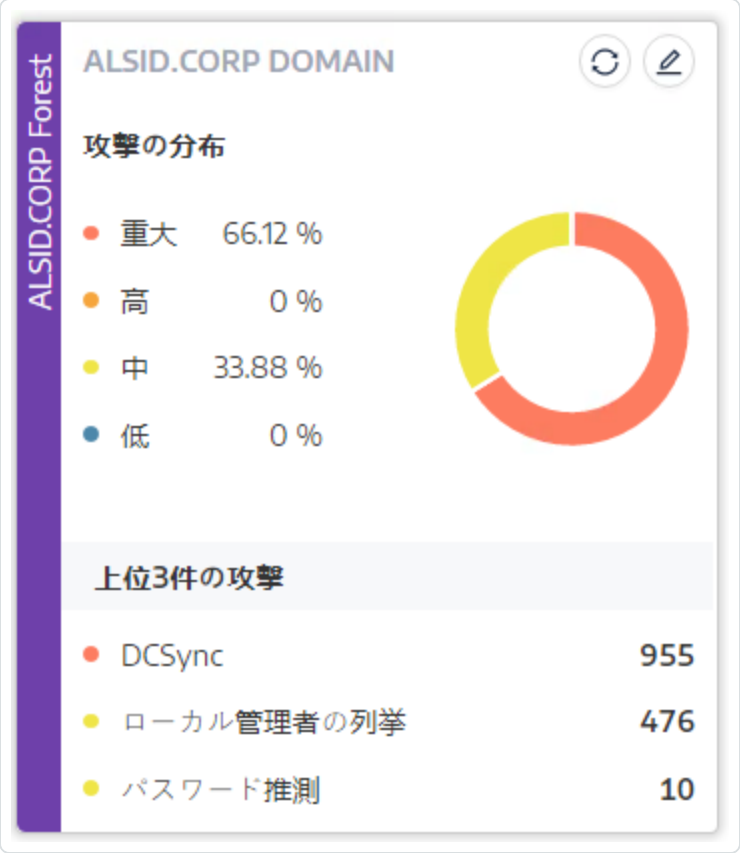
グラフの種類を変更するには

1. アイコンをクリックして、ドメインタイルを編集します。

   [カード情報の編集] ペインが表示されます。

2. グラフのタイプを選択します。

- **攻撃の分布**: 攻撃の深刻度の分布を表示します。



- **イベント数:** トップ 3 の攻撃とその発生回数を表示します。

3. **[保存]**をクリックします。

   Tenable Identity Exposure がグラフを更新します。

関連項目

- 攻撃インジケーター
- 攻撃インジケーターインシデント

攻撃インジケーターインシデント

インシデントの攻撃インジケーター(IoA)リストは、Active Directory(AD)に対する特定の攻撃の詳細情報を提供します。これにより、IoAの深刻度レベルに応じて必要なアクションを実行できます。

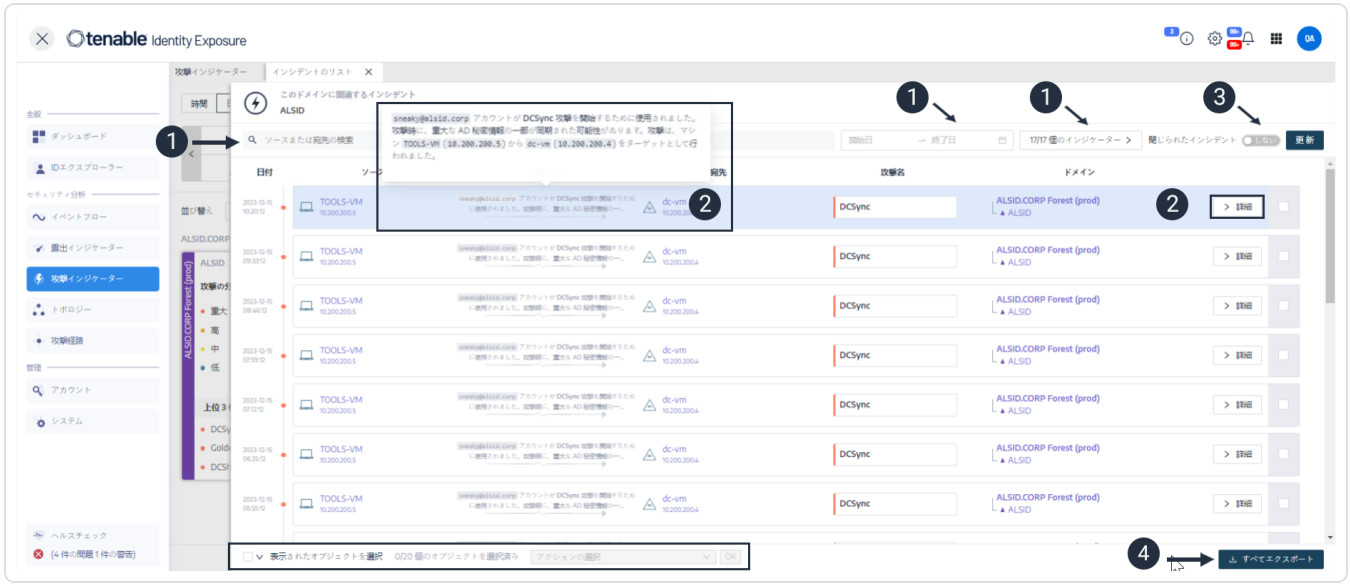
攻撃インシデントを表示するには

1. Tenable Identity Exposureで、ナビゲーションペインの**[攻撃インジケーター]**をクリックします。

   [攻撃インジケーター]ペインが開きます。

2. 任意のドメインタイルをクリックします。

   [インシデントのリスト]ペインが、ドメインで発生したインシデントのリストとともに表示されます。



3. このリストから、次のいずれかを実行できます。

   - 特定のインシデントを検索するための検索条件を定義する❶
   - ADに影響を与えている攻撃に関する詳しい説明にアクセスする❷
   - インシデントを閉じる/再度開く❸
   - すべてのインシデントが表示されたレポートをダウンロードする❹

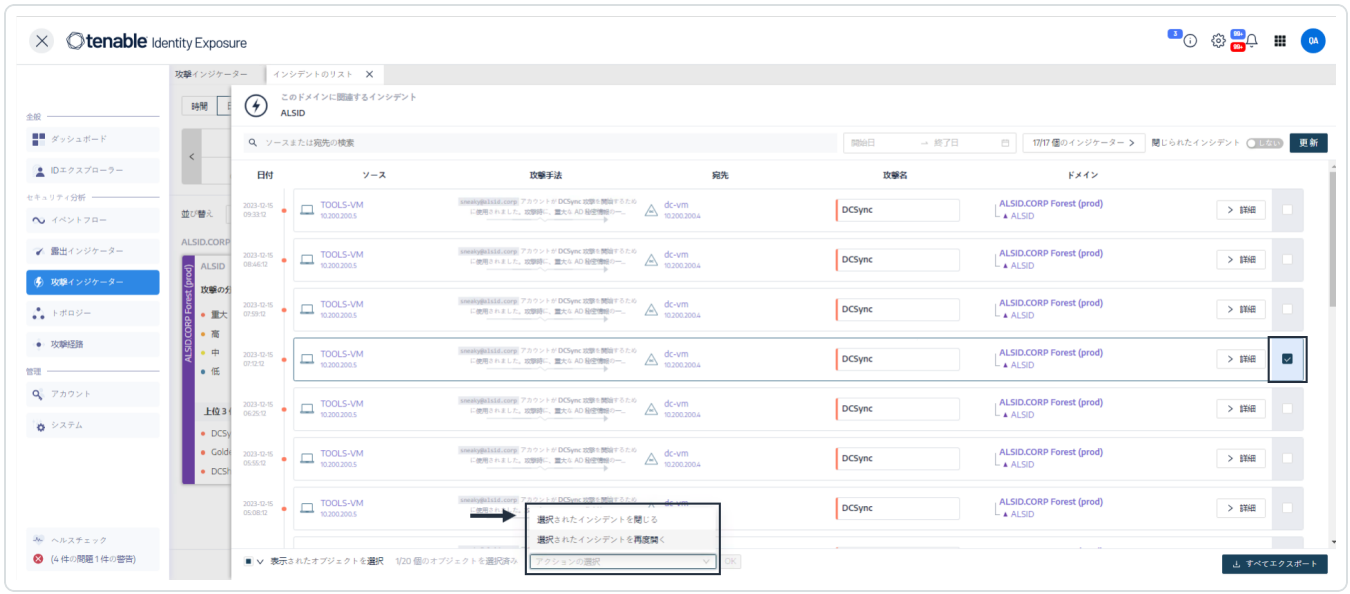
インシデントを検索するには

1. **[検索]**ボックスで、ソースまたは宛先の名前を入力します。
2. 日付の選択コントロールをクリックして、インシデントの開始日と終了日を選択します。
3. **[n/n 個のインジケーター]** をクリックして、関連するインジケーターを選択します。
4. **[閉じられたインシデント]** トグルをクリックして **[はい]** に切り替え、検索を閉じられたインシデントに限定します。
5. **[更新]** をクリックします。

   Tenable Identity Exposure は、一致するインシデントでリストを更新します。

インシデントを閉じる方法

1. インシデントのリストから、閉じるまたは再オープンするインシデントを選択します。



2. ペインの下部で、ドロップダウンメニューをクリックし、**[選択されたインシデントを閉じる]** を選択します。

3. **[OK]** をクリックします。

   クローズの確認を求めるメッセージが表示されます。

4. **[確認]** をクリックします。

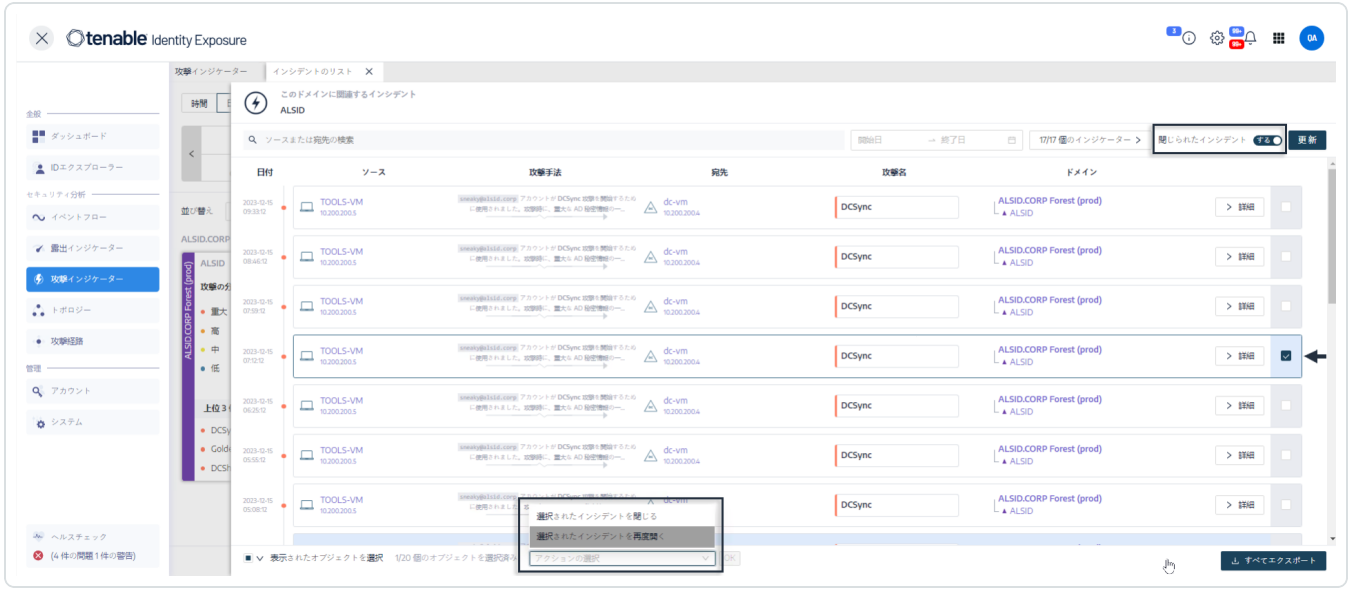
   Tenable Identity Exposure がインシデントを閉じて、今後表示しないことを確認するメッセージが表示されます。

インシデントを再度開く方法

1. **[インシデントのリスト]** ペインで、**[閉じられたインシデント]** トグルを **[はい]** に切り替えます。

   Tenable Identity Exposure は、閉じられたインシデントでリストを更新します。

2. 再度開くインシデントを選択します。



3. ペインの下部で、ドロップダウンメニューをクリックし、**[選択されたインシデントを再度開く]** を選択します。

4. **[OK]** をクリックします。

   Tenable Identity Exposureがインシデントを再度開いたことを確認するメッセージが表示されます。

ヒント：インシデントをまとめて閉めるまたは再度開くには、画面の下部で、**[表示されたオブジェクトを選択]** をクリックします。

インシデントの詳細

インシデントのリストの各エントリには、次の情報が表示されます。

- **日付** - IoA をトリガーしているインシデントが発生した日付。Tenable Identity Exposure は、タイムラインの一番上に最新のインシデントを表示します。
- **ソース** - 攻撃元とその IP アドレス。
- **攻撃手法** - 攻撃中に何が起きたかについての説明。

  ヒント: IoA の詳細情報を表示するには、攻撃手法にカーソルを合わせます。

- **宛先** - 攻撃先とその IP アドレス。
- **攻撃名** - 攻撃の技術的な名前。
- **ドメイン** - 攻撃が影響を与えたドメイン。

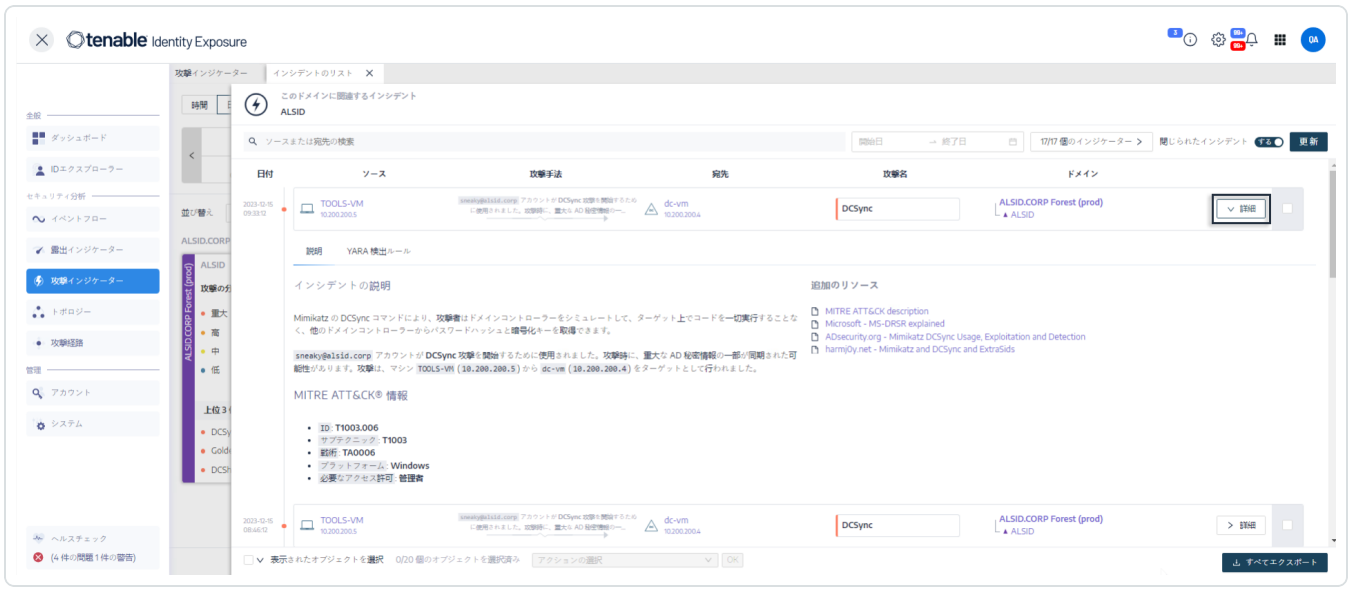
  ヒント: **[インシデントのリスト]** でインタラクティブな要素 (リンク、アクションボタンなど) をいくつかクリックすると、Tenable Identity Exposure に最大 5 つのペインを表示することができます。すべてのペインを同時に閉じるには、ページ内の任意の場所をクリックします。

攻撃の詳細

インシデントのリストから、特定の攻撃をドリルダウンし、必要なアクションを実行して修正できます。

攻撃の詳細を表示するには

1. インシデントのリストから、詳細をドリルダウンするインシデントを選択します。
2. **[詳細]** をクリックします。



Tenable Identity Exposure は、その攻撃に関連する詳細を表示します。

説明

[説明] タブには、以下のセクションがあります。

- **インシデントの説明** - 攻撃に関する簡単な説明が表示されます。
- **MITRE ATT&CK 情報** - Mitre Att&ck (Adversarial Tactics, Techniques, and Common Knowledge) ナレッジベースから取得された技術的な情報が表示されます。Mitre Att&ck とは、攻撃者による攻撃を分類し、攻撃者がネットワークを侵害した後に行った操作を解説するフレームワークのことです。サイバーセキュリティのコミュニティによる共通認識を可能にする、セキュリティの脆弱性に対する標準識別子も提供されています。
- **追加のリソース** - 攻撃に関するさらに詳しい情報を掲載したウェブサイトや記事、ホワイトペーパーへのリンクが記載されています。

YARA 検出ルール

[YARA 検出ルール] タブは YARA ルールについて説明しています。Tenable Identity Exposure はこれらのルールを使用して、ネットワークレベルで AD 攻撃を検出し、Tenable Identity Exposure の検出チェーンを強化します。

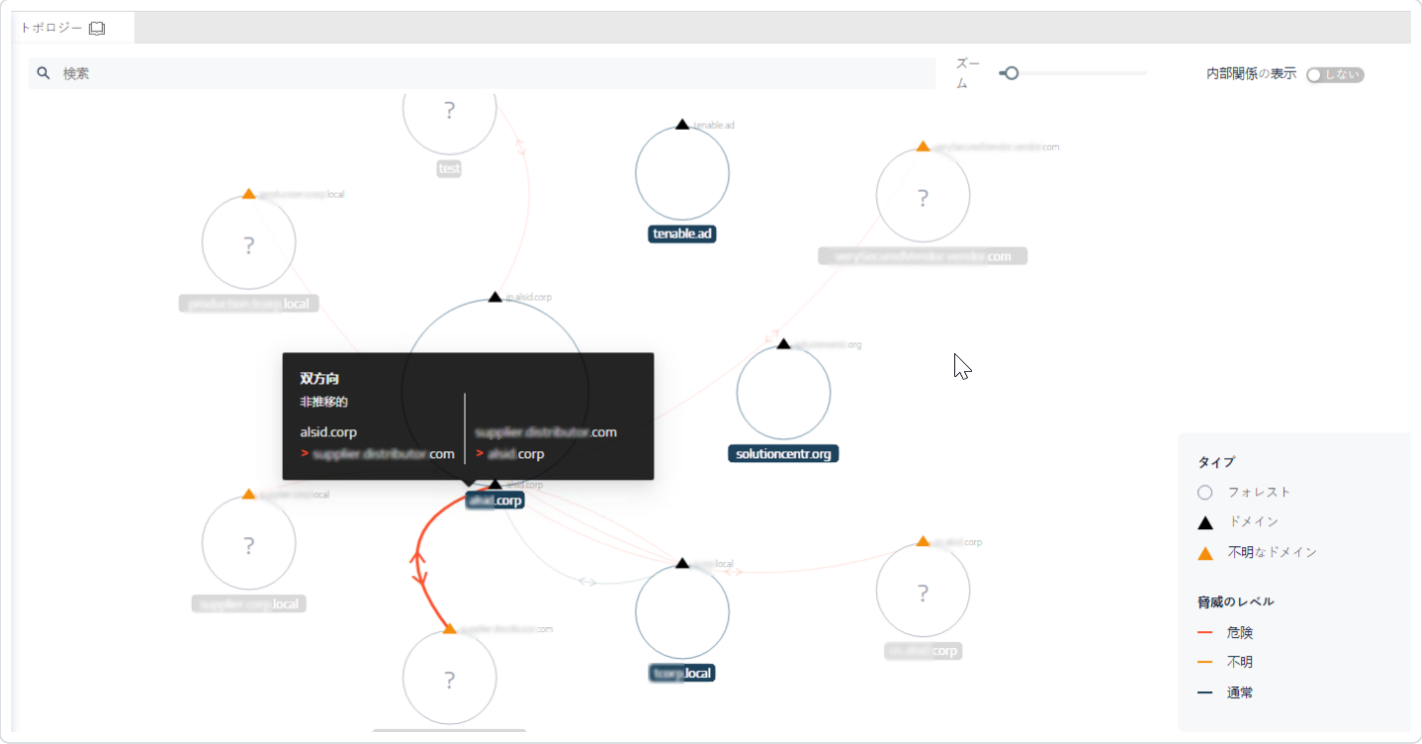
注意: YARA とは、主にマルウェアの研究や検出に使用されるツールの名前です。このツールは、テキストまたはバイナリのパターンに基づいてマルウェアファミリーの記述を作成する、ルールベースのアプローチを提供します。説明が実質的に YARA のルール名となります。このルールは、一連の文字列とブール式で構成されています (出典: wikipedia.org)。

関連項目

- 攻撃インジケーター
- 攻撃インジケーターの詳細

トポロジー

トポロジーページは、Active Directory をインタラクティブなグラフで表示します。**トポロジーグラフ**には、フォレストやドメイン、そしてそれらの間に存在する信頼関係が表示されます。



トポロジーページを開くには

- Tenable Identity Exposure で、左側のナビゲーションメニューの **[トポロジー]** をクリックします。

  トポロジーペインが開き、AD がグラフィック表示されます。

ドメインを検索するには

- **[トポロジー]** ペインの **[検索]** ボックスにドメイン名を入力します。

  Tenable Identity Exposure がドメインをハイライトします。

グラフを拡大するには

- **[トポロジー]** ペインで、**[ズーム]** スライダーをクリックして、グラフのサイズを調整します

2 つのドメイン間のリンクを表示するには

- **[トポロジー]** ペインで **[内部関係の表示]** をクリックして、**[はい]** に切り替えます。

ドメインの詳細を表示するには

- **[トポロジー]** ペインで、ドメイン名の ▲ をクリックします。

  [ドメインの詳細] ペインが開き、検出された露出インジケーター、およびドメインのコンプライアンススコアが表示されます。IoE のタイルをクリックすると、詳細情報を表示できます。

関連項目

- 信頼関係
- 危険な信頼

信頼関係

トポロジーグラフのドメイン間の曲線矢印は、信頼関係を表しています。

信頼関係を表示するには

- トポロジーグラフで、曲線矢印にカーソルを合わせます。

  Tenable Identity Exposure は 2 つのエンティティ間の特定の属性を示す信頼関係を表示します。

信頼関係の色は、異なる脅威レベルを表しています。

- **赤**は危険な信頼
- **オレンジ**は通常の信頼
- **青**は未知の信頼

詳細は、危険な信頼 を参照してください。

信頼属性の情報は、信頼の方向を**一方向**または**双方向**(入力/出力)で示し、次のいずれかの値を表示します。

値	説明
非推移的	フォレスト内の信頼は、推移的な信頼がデフォルトです。Tenable Identity Exposure はこのフラグを使用して、推移的な信頼を非推移的な信頼に変換します。それに対して、フォレスト間の信頼は、非推移的な信頼がデフォルトです。そのため、フォレスト推移的のフラグが存在します。Tenable Identity Exposure は、フォレスト内でドメイン間の信頼

	が存在する場合にこの値を表示します。この信頼によって、フォレストを超えて相互に接続されたドメインにアクセス権が付与されることはなく、認証が委任されることもありません。
フォレスト推移的	2 つのフォレスト間に推移的信頼が存在することを示します。別のドメインに付与された信頼は、信頼されたフォレストに渡すことができます。
フォレスト内	同じフォレスト内にドメイン間の信頼が存在することを示します。`WITHIN_FOREST` と `QUARANTINED_DOMAIN` の両方が存在する場合、信頼は **QuarantinedWithinForest** と表記されます。
アップレベルのみ	Windows 2000 以降のオペレーティングシステムで動作しているクライアントのみがこの信頼を利用できることを示します。
外部として扱う	(`FOREST_TRANSITIVE` が適用される場合にのみ) 外部タイプの信頼を示します。Tenable Identity Exposure は、外部信頼に適用されるセキュリティ識別子 (SID) フィルターを調整して、相対識別子 (RID) が 1,000 以上である SID を認証してフォレスト間を通過させます。
検疫済み	Tenable Identity Exposure が、その信頼で RID が 1,000 以上である SID のフィルタリングを有効にしたことを示します。デフォルトでは、Tenable Identity Exposure は外部の信頼に対してのみ有効にしますが、親/子の信頼またはフォレストの信頼にも適用できます。
組織をまたがる認証	Tenable Identity Exposure が選択的認証を有効にしており、ドメインやフォレストの信頼で使用できることを示します。
選択的認証	上の行にある「組織をまたがる認証」を参照してください。
TGT 委任なしで組織をまたがる	信頼されたドメインへの委任が完全に無効化されている場合に表示されます (発行されるサービスチケットに ok-as-delegate オプションは決して設定されません)。

RC4 暗号化	信頼が Kerberos 交換で RC4 暗号化キーをサポートすることを示します。このフラグが表示されるのは、trustType が TRUST_TYPE_MIT に適用されている場合のみです。
AES キー	信頼が Kerberos 交換で AES 暗号化キーをサポートすることを示します。
PIM 信頼	FOREST_TRANSITIVE フラグと TREAT_AS_EXTERNAL フラグが適用されていて、QUARANTINED_DOMAIN フラグがオンでない場合、この PIM 信頼のフラグは、信頼されたフォレストが SID フィルタリングに関して特権 ID を管理している(特権アイデンティティ管理)ことを示します(ローカルの SID はこの信頼を通過できます)。PIM 信頼は、要塞フォレストを実装するために機能します。
属性なし	外部の信頼に特定の属性がないことを示します。

危険な信頼

信頼関係の色は、異なる脅威レベルを表しています。

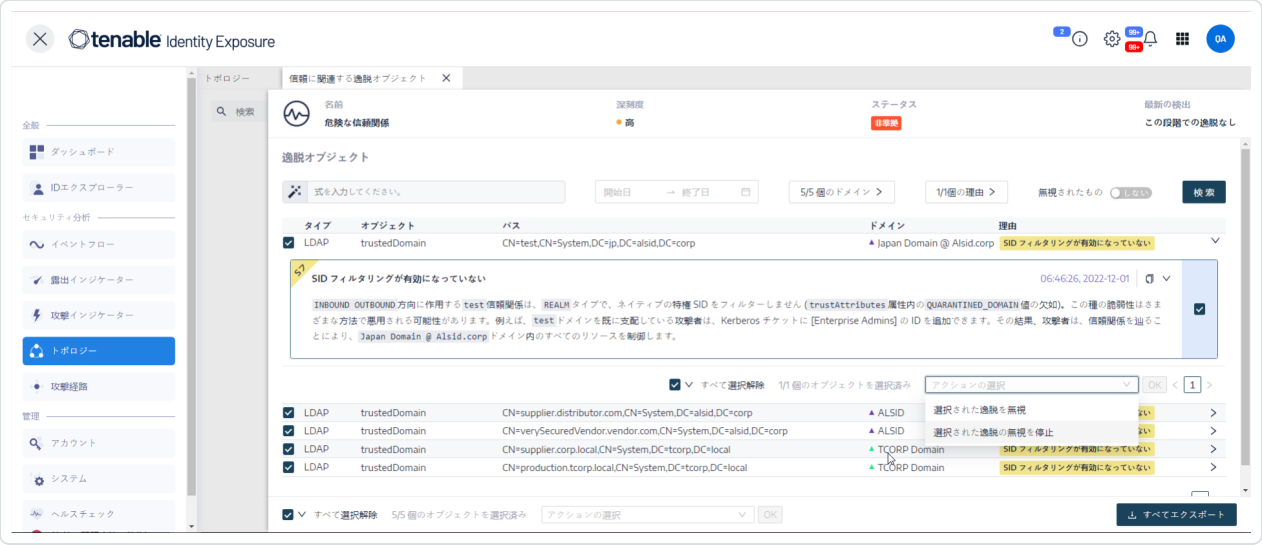
- **赤**は危険な信頼
- **オレンジ**は通常の信頼
- **青**は未知の信頼

危険な信頼を調査するには

1. トポロジーグラフで、曲線矢印をクリックします。

   [信頼に関連する逸脱オブジェクト] ペインが開きます。

   > **ヒント**: この危険な信頼関係ペインに表示されるイベントの詳細はすべて、**危険な信頼関係**の露出インジケーターに関連付けられています。これは、**[露出インジケーター]**ナビゲーションメニューからもアクセスできます。



2. 逸脱オブジェクトにカーソルを合わせてクリックし、詳細を表示します。

逸脱オブジェクトをエクスポートするには

1. トポロジーグラフで、曲線矢印をクリックします。

   [信頼に関連する逸脱オブジェクト] ペインが開きます。

2. **[すべてエクスポート]** をクリックします。

[逸脱オブジェクトのエクスポート] ペインが開きます。

3. **[エクスポート形式]** ボックスでドロップダウン矢印をクリックして、形式を選択します。
4. **[すべてエクスポート]** をクリックします。

   Tenable Identity Exposure は、選択された形式でファイルをコンピューターにダウンロードします。
5. **[X]** をクリックして、ペインを閉じます。

攻撃経路

Tenable Identity Exposure は、グラフィック表示を通じて、ビジネス資産の潜在的な脆弱性を視覚化するにはを複数提供しています。

- **攻撃経路**: 攻撃者がエントリポイントから資産を侵害する可能性のある経路を示します。
- **影響範囲**: 任意の資産から Active Directory に入る可能性のあるラテラルムーブメントを示します。
- **露出資産**: 資産をコントロールする可能性のあるすべての経路を示します。

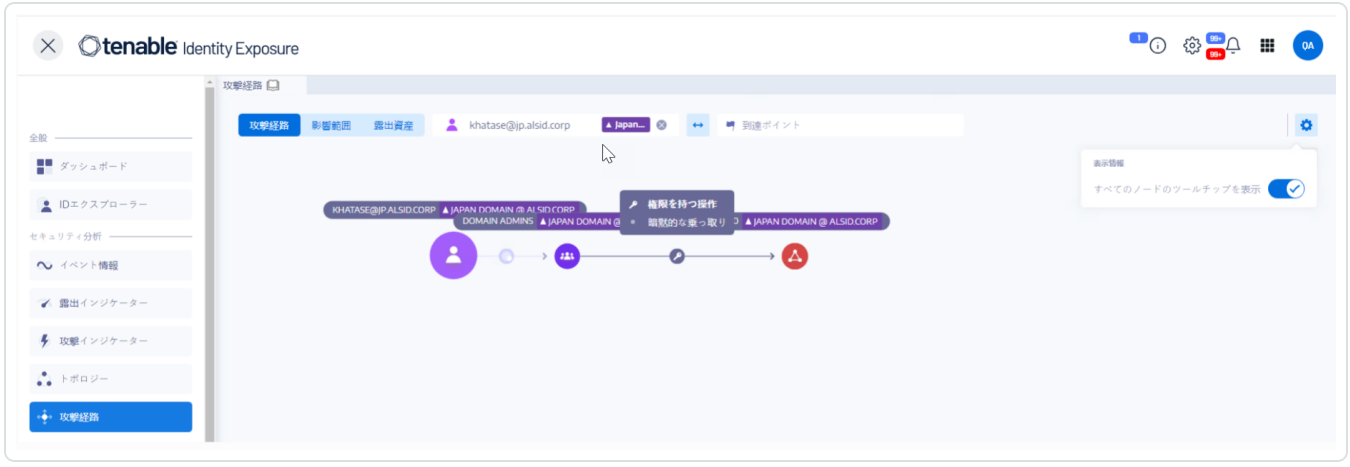
攻撃経路を表示するには

1. Tenable Identity Exposure で、サイドバーメニューの**[攻撃経路]**をクリックします。

   [攻撃経路]ペインが表示されます。

2. バナーの**[攻撃経路]**をクリックします。
3. **[開始ポイント]**ボックスに、エントリポイントとなる資産を入力します。
4. **[到着ポイント]**ボックスに、経路の最終ポイントとなる資産を入力します。
5.  アイコンをクリックします。

   Tenable Identity Exposure が 2 つの資産間の攻撃経路を表示します。



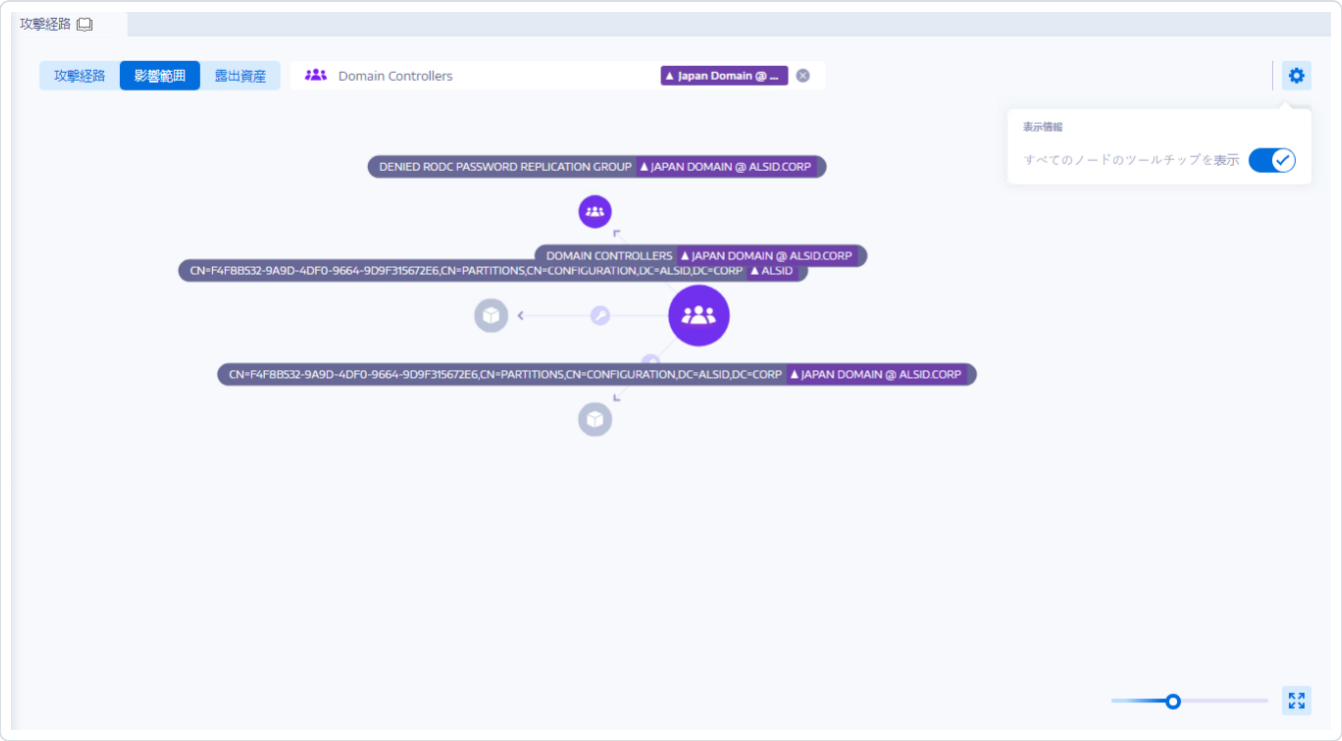
6. オプションで、  アイコンをクリックして以下を実行できます。
   - **[ズーム]** スライダーをクリックして、グラフの縮尺を調整します。
   - **[すべてのノードツールチップを表示]** トグルをクリックして、資産に関する情報を表示します。

影響範囲を表示するには

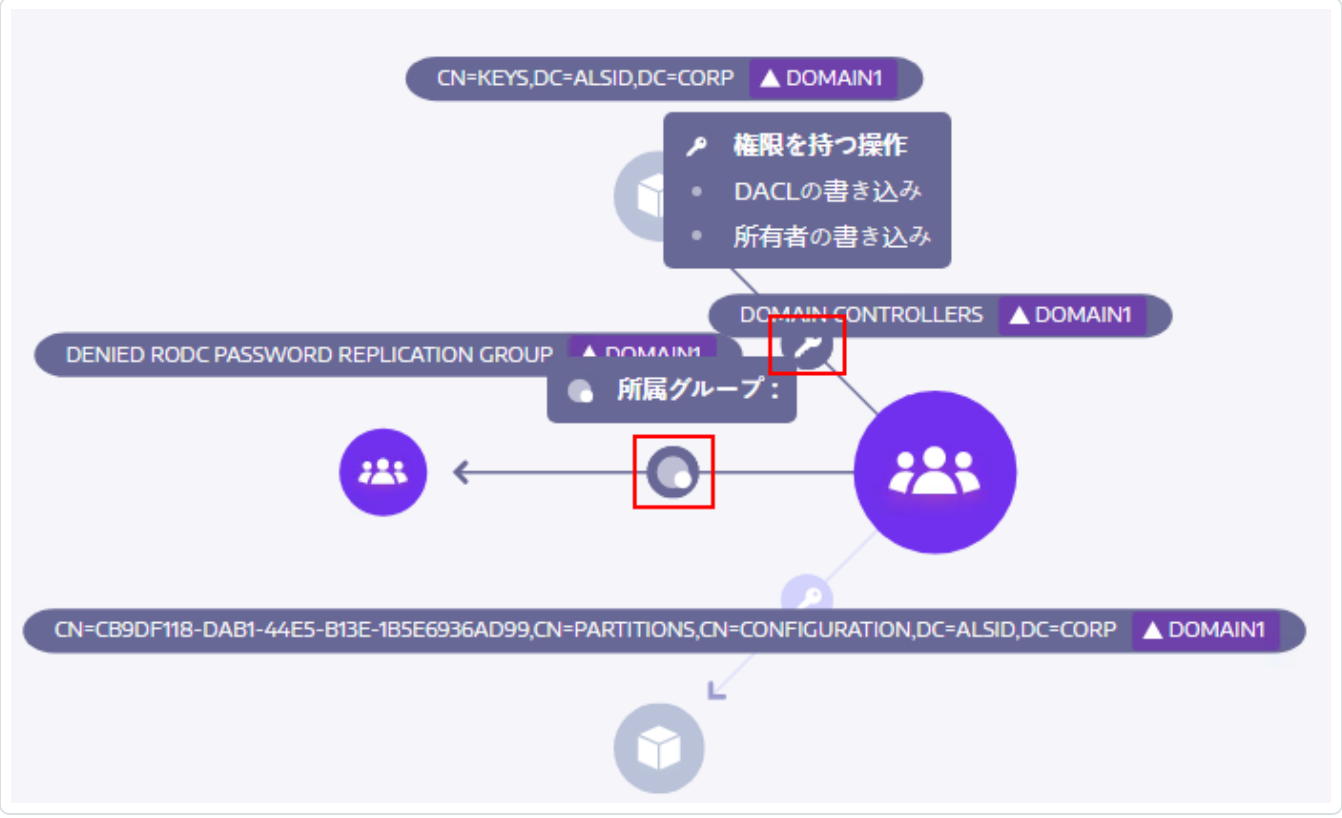
1. Tenable Identity Exposure で、サイドバーメニューの **[攻撃経路]** をクリックします。

   [攻撃経路] ペインが表示されます。
2. バナーの **[影響範囲]** をクリックします。
3. **[オブジェクトを検索]** ボックスに、資産の名前を入力します。
4.  アイコンをクリックします。

   Tenable Identity Exposure がその資産から放射状に広がる横方向の接続を表示します。



5. 資産と資産をつなぐ矢印アイコンをクリックして、資産相互の関係を表示します。



露出資産を表示するには

1. 影響範囲を表示するには
2. Tenable Identity Exposure で、サイドバーメニューの**[攻撃経路]**をクリックします。

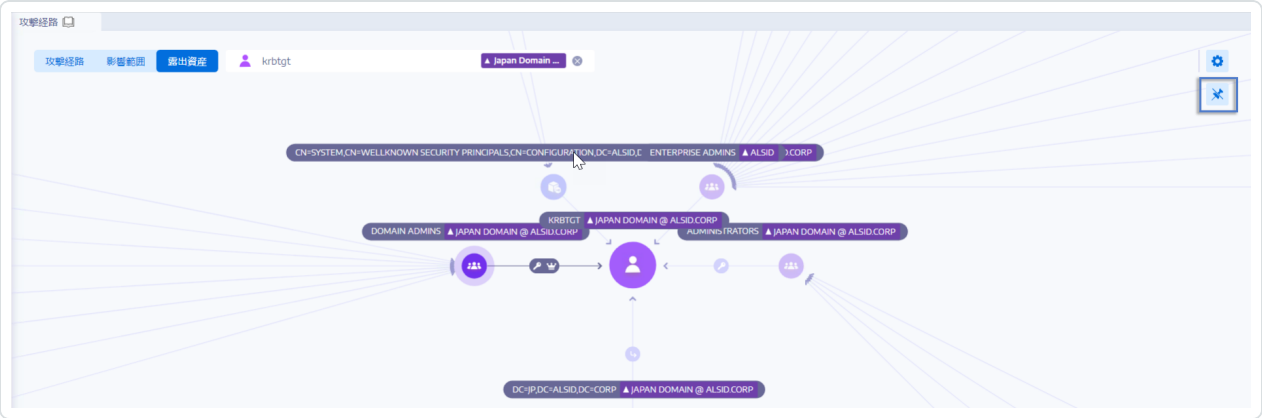
   [攻撃経路]ペインが表示されます。
3. バナーの**[露出資産]**をクリックします。
4. **[オブジェクトを検索]**ボックスに、資産の名前を入力します。
5. アイコンをクリックします。

   Tenable Identity Exposure が資産につながる経路と資産同士の関係を表示します。
6. 資産と資産をつなぐ矢印アイコンをクリックして、資産相互の関係を表示します。

攻撃経路の表示を固定するには

1. 強調表示する攻撃経路のノードをクリックします。

   Tenable Identity Exposure の画面上でその攻撃経路の表示が固定されます。
2. 攻撃経路の固定表示を解除するには、アイコンをクリックするか別の攻撃経路の別のノードをクリックします。

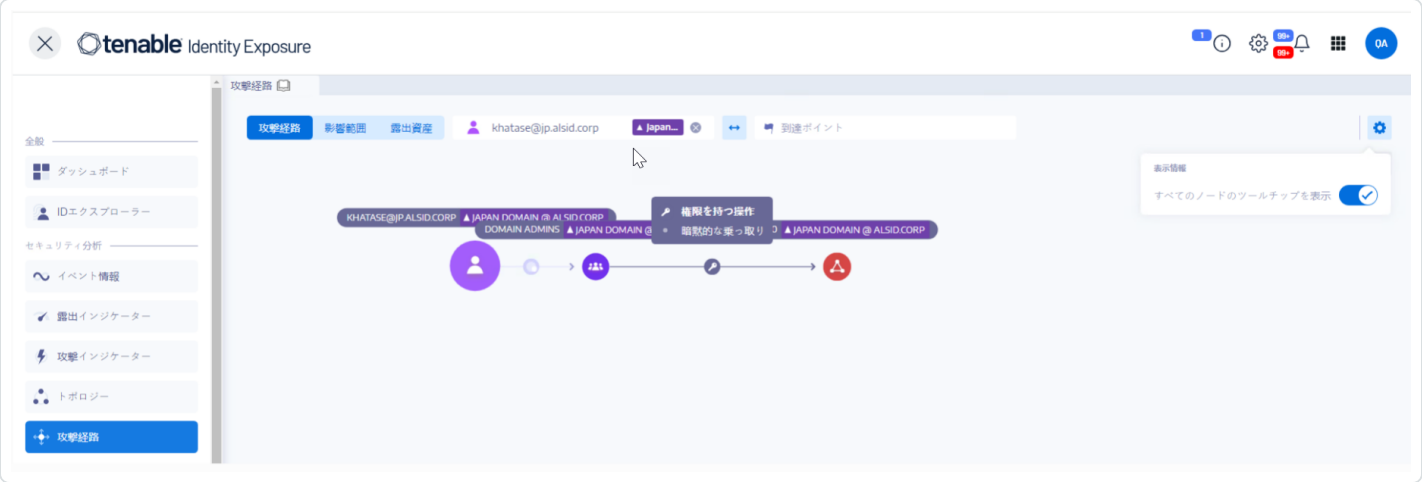

攻撃経路
攻撃経路
影響範囲
露出資産
krbtgt
Japan Domain ...
CN=SYSTEM,CN=WELLKNOWN SECURITY PRINCIPALS,CN=CONFIGURATION,DC=ALSID,[
ENTERPRISE ADMINS
ALSID
.CORP
KRBTGT
JAPAN DOMAIN @ ALSID.CORP
DOMAIN ADMINS
JAPAN DOMAIN @ ALSID.CORP
ADMINISTRATORS
JAPAN DOMAIN @ ALSID.CORP
DC=JP,DC=ALSID,DC=CORP
JAPAN DOMAIN @ ALSID.CORP

関連項目

- 攻撃関係

攻撃関係

攻撃関係は、ソースノードからターゲットノードへの一方向のものです。関係は推移的であるため、攻撃者はそれらを連鎖させて「攻撃経路」を作成することが可能です。



Tenable Identity Exposure に次の攻撃関係があります。

- キー認証情報の追加
- メンバーの追加
- 操作が許可されている
- 委任が許可されている
- GPO に属している
- DCSync
- 操作の許可を付与できる
- SID 履歴あり
- 暗黙的な乗っ取り
- GPO を継承
- リンクされている GPO
- グループのメンバー
- 所有

- パスワードのリセット
- RODC 管理
- DACL の書き込み
- 所有者の書き込み

キー認証情報の追加

説明

ソースのセキュリティプリンシパルは、キー認証情報または「シャドー認証情報」としても知られるキー信頼アカウントマッピングを悪用することで、ターゲットになりすます可能性があります。

なりすましが可能なのは、ソースがターゲットの `msDS-KeyCredentialLink` 属性を編集するアクセス許可を持っているためです。

通常、Windows Hello for Business (WHfB) がこの機能を使用しますが、使用されていない場合でも攻撃者はこれを悪用することができます。

悪用

ソースのセキュリティプリンシパルを侵害した攻撃者は、Whisker や DSInternals などの特殊なハッカーツールを使用して、ターゲットコンピューターの `msDS-KeyCredentialLink` 属性を編集しなければなりません。

攻撃者の目標は、このターゲットの属性に、自分たちがプライベートキーを持っている新しい証明書を追加することです。その後、Kerberos PKINIT プロトコルを使用し、持っているプライベートキーを使ってターゲットとして認証し、TGT を取得できます。このプロトコルは、攻撃者がターゲットの NTLM ハッシュをフェッチすることも許可してしまいます。

修正方法

ネイティブで特権を持ついくつかのセキュリティプリンシパル(アカウントオペレーター、管理者、ドメイン管理者、エンタープライズ管理者、エンタープライズキー管理者、キー管理者、システムなど) には、デフォルトでこのアクセス許可があります。これらの正当なセキュリティプリンシパルには、修正は必要ありません。

この属性を変更する正当な理由のないソースセキュリティプリンシパルの場合は、上記のアクセス許可を削除する必要があります。「すべてのプロパティの書き込み」、「msDS-AllowedToActOnBehalfOfOtherIdentity の書き込み」、「フルコントロール」などのアクセス許可を検索します。

関連項目

- メンバーの追加
- 操作が許可されている
- 委任が許可されている
- GPO に属している
- DCSync
- 操作の許可を付与できる
- SID 履歴あり
- 暗黙的な乗っ取り
- GPO を継承
- リンクされている GPO
- グループのメンバー
- 所有
- パスワードのリセット
- RODC 管理
- DACL の書き込み
- 所有者の書き込み

メンバーの追加

説明

ソースのセキュリティプリンシパルは、自分（検証された書き込み権限）または任意のユーザー（プロパティの書き込み権限）をターゲットグループのメンバーに追加でき、そのグループに与えられたアクセス権の恩恵を受けることができます。

悪意のあるセキュリティプリンシパルがこの操作を実行すると、「グループのメンバー」攻撃関係が作成されます。

悪用

ソースのセキュリティプリンシパルを侵害した攻撃者は、Windows のネイティブコマンド（例：net group/domain）、PowerShell（例：Add-ADGroupMember）、管理ツール（例：Active Directory ユーザーとコンピューター）、専用のハッカーツール（例：PowerSploit）を使用して、ターゲットグループの「メンバー」属性を編集するだけで悪用することができます。

修正方法

ソースセキュリティプリンシパルがターゲットグループにメンバーを追加するアクセス許可を必要としない場合は、そのアクセス許可を削除する必要があります。

ターゲットグループのセキュリティ記述子を変更するには

1. 「Active Directory ユーザーとコンピューター」で、右クリックで **[プロパティ]** > **[セキュリティ]** の順に選択します。
2. 「メンバーの書き込み」、「すべてのプロパティの書き込み」、「フルコントロール」、「検証されたすべての書き込み」、「メンバーとしての自身の追加/削除」などのアクセス許可を削除します。

> **注意**：グループは、Active Directory ツリーの上位にあるオブジェクトからアクセス許可を継承できます。

関連項目

- キー認証情報の追加
- 操作が許可されている

- 委任が許可されている
- GPO に属している
- DCSync
- 操作の許可を付与できる
- SID 履歴あり
- 暗黙的な乗っ取り
- GPO を継承
- リンクされている GPO
- グループのメンバー
- 所有
- パスワードのリセット
- RODC 管理
- DACL の書き込み
- 所有者の書き込み

操作が許可されている

説明

ソースのセキュリティプリンシパルは、ターゲットコンピューターで Kerberos リソースベースの制約付き委任を実行することが許可されています。これは、ターゲットコンピューターで実行されている任意のサービスに Kerberos で認証するときに、任意のユーザーになりすます可能性があることを意味します。

したがって、多くの場合、ターゲットコンピューターが完全に侵害される恐れがあります。

この攻撃は、リソースベースの制約付き委任 (RBCD)、Kerberos リソースベースの制約付き委任 (KRBCD)、リソースベースの Kerberos 制約付き委任 (RBKCD)、および「他の ID の代わりに操作が許可されている」などと呼ばれています。

悪用

ソースのセキュリティプリンシパルを侵害した攻撃者は、Rubeus などの専用のハッカーツールを使用して正当な Kerberos プロトコル拡張 (S4U2self と S4U2proxy) を悪用し、Kerberos サービスチケットを偽造し、ターゲットユーザーになりすます可能性があります。攻撃者は、たいてい特権ユーザーになりすまして特権アクセスを取得します。

攻撃者がサービスチケットを偽造すると、Kerberos と互換性のある任意のネイティブ管理ツールや特殊なハッカーツールを使用して、リモートで任意のコマンドを実行できるようになります。

悪用は、次の制約が満たされている場合に成功します。

- ソースおよびターゲットのセキュリティプリンシパルに ServicePrincipalName が設定されていること。設定されていない場合、Tenable Identity Exposure はこの攻撃関係を作成しません。
- なりすましの標的となるのは、「機密であり委任できない」(UserAccountControl の ADS_UF_NOT_DELEGATED) とマークされておらず、「保護されたユーザー」グループのメンバーでもないアカウントです。なぜなら、Active Directory が委任攻撃からこのようなアカウントを保護しているからです。

修正方法

ソースセキュリティプリンシパルにターゲットコンピューターで Kerberos リソースベースの制約付き委任を実行するアクセス許可が必要ない場合は、そのアクセス許可を削除する必要があります。「委任が許可されている」委任攻撃の関係の場合とは逆に、ターゲット側で変更を行う必要があります。

「Active Directory ユーザーとコンピューター」などの既存のグラフ管理ツールでは、RBCD を管理できません。代わりに PowerShell を使用して、msDS-AllowedToActOnBehalfOfOtherIdentity 属性の中身を変更する必要があります。

次のコマンドを使用して、ターゲットでの操作が許可されているソースセキュリティプリンシパルをリスト表示します(「アクセス」セクション)。

```
Get-ADComputer target -Properties msDS-AllowedToActOnBehalfOfOtherIdentity | Select-Object -
ExpandProperty msDS-AllowedToActOnBehalfOfOtherIdentity | Format-List
```

リスト内のセキュリティプリンシパルのいずれも必要でない場合は、次のコマンドですべて消去できます。

```
Set-ADComputer target -Clear "msDS-AllowedToActOnBehalfOfOtherIdentity"
```

1 つのセキュリティプリンシパルをリストから削除するだけでよい場合は、残念ながら Microsoft はダイレクトコマンドを提供しておらず、削除する 1 つのセキュリティプリンシパルを除いた同じリストで属性を上書きする必要があります。たとえば、「sourceA」、「sourceB」、「sourceC」がすべて許可されており、「sourceB」のみを削除したい場合は、次のコマンドを実行します。

```
Set-ADComputer target -PrincipalsAllowedToDelegateToAccount (Get-ADUser sourceA),(Get-ADUser sourceC)
```

最後に、一般的な推奨事項として、機密の特権アカウントがそのような攻撃にさらされるのを制限するために、Tenable Identity Exposure は「機密であり委任できない」(ADS_UF_NOT_DELEGATED)としてマークするか、関連する運用上の影響を注意深く検証したうえで「保護されたユーザー」グループに追加することを推奨します。

関連項目

- キー認証情報の追加
- メンバーの追加
- 委任が許可されている
- GPO に属している
- DCSync
- 操作の許可を付与できる

- SID 履歴あり
- 暗黙的な乗っ取り
- GPO を継承
- リンクされている GPO
- グループのメンバー
- 所有
- パスワードのリセット
- RODC 管理
- DACL の書き込み
- 所有者の書き込み

委任が許可されている

説明

ソースセキュリティプリンシパルは、ターゲットコンピューターでプロトコル遷移を使用して Kerberos 制約付き委任 (KCD) を実行できます。これは、ターゲットコンピューターで実行されている任意のサービスに Kerberos で認証するときに、任意のユーザーになりすます可能性があることを意味します。

したがって、多くの場合、ターゲットコンピューターが完全に侵害される恐れがあります。

悪用

ソースのセキュリティプリンシパルを侵害した攻撃者は、Rubeus などの専用のハッカーツールを使用して正当な Kerberos プロトコル拡張 (S4U2self と S4U2proxy) を悪用し、Kerberos サービスチケットを偽造し、ターゲットユーザーになりすます可能性があります。攻撃者は、たいてい特権ユーザーになりすまして特権アクセスを取得します。

攻撃者がサービスチケットを偽造すると、Kerberos と互換性のある任意のネイティブ管理ツールや特殊なハッカーツールを使用して、リモートで任意のコマンドを実行できるようになります。

悪用は、次の制約が満たされている場合に成功します。

- ソースのセキュリティプリンシパルに対してプロトコル遷移が有効になっていること (UserAccountControl の ADS_UF_TRUSTED_TO_AUTHENTICATE_FOR_DELEGATION/委任 GUI の「Use any authentication protocol」)。厳密に言えば、攻撃はプロトコル遷移がなくても (委任 GUI の「Use Kerberos only」) 可能ですが、その場合、攻撃者はまずターゲットユーザーからソースセキュリティプリンシパルへの Kerberos 認証を強制する必要があるため、攻撃しにくくなります。したがって、このケースでは Tenable Identity Exposure は攻撃関係を作成しません。
- ソースおよびターゲットのセキュリティプリンシパルに ServicePrincipalName が設定されていること。設定されていない場合、Tenable Identity Exposure はこの攻撃関係を作成しません。
- なりすましの標的となるのは、「機密であり委任できない」(UserAccountControl の ADS_UF_NOT_DELEGATED) とマークされておらず、「保護されたユーザー」グループのメンバーでもないアカウントです。なぜなら、Active Directory がこのようなアカウントを委任攻撃から保護しているからです。

逆に、委任が許可されているターゲットコンピューターは、サービスプリンシパル名 (SPN) で指定されているため、「cifs/host.example.net」の SMB、「http/host.example.net」の HTTP などの特定のサービスを含んでいます。ただし、現実には攻撃者は「名前置換攻撃」を使用して、同じターゲットアカウントで実行され

ている他の SPN やサービスを標的にすることができます。したがって、これは悪用を制限するものとはみなされません。

修正方法

ソースセキュリティプリンシパルに、ターゲットコンピューターで Kerberos 制約付き委任 (KCD) を実行するアクセス許可が必要ない場合は、そのアクセス許可を削除する必要があります。「操作が許可されている」委任攻撃の関係とは逆に、ソース側で変更を行う必要があります。

ソースセキュリティプリンシパルを削除するには

1. 「Active Directory ユーザーとコンピューター」の管理 GUI で、ソースオブジェクトの **[プロパティ]** > **[委任]** タブに移動します。
2. ターゲットに対応するサービスプリンシパル名を削除します。
3. このソースからの委任を一切望まない場合は、すべての SPN を削除し、「委任に関してこのコンピューターを信頼しない」を選択します。

あるいは、PowerShell を使用して、ソースの「msDS-AllowedToDelegateTo」属性のコンテンツを変更することもできます。

- たとえば、Powershell で次のコマンドを実行して、すべての値を置き換えます。

```
Set-ADObject -Identity "CN=Source,OU=corp,DC=example,DC=net" -Replace @{ "msDS-
AllowedToDelegateTo" = @("cifs/desiredTarget.example.net") }
```

- このソースからの委任を一切望まない場合は、次のコマンドを実行して属性を消去します。

```
Set-ADObject -Identity "CN=Source,OU=corp,DC=example,DC=net" -Clear "msDS-
AllowedToDelegateTo"
```

プロトコル遷移を無効にすることで、この攻撃経路を完全に閉じることなくリスクを軽減することも可能です。そのためには、すべてのセキュリティプリンシパルは NTLM ではなく Kerberos のみを使用してソースに接続する必要があります。

プロトコル遷移を無効にするには

1. 「Active Directory ユーザーとコンピューター」の管理 GUI で、ソースオブジェクトの **[プロパティ]** > **[委任]** タブに移動します。
2. [Use any authentication protocol] の代わりに [Use Kerberos only] を選択します。

または、PowerShell で次のコマンドを実行して、プロトコル遷移を無効にすることもできます。

```
Set-ADAccountControl -Identity "CN=Source,OU=corp,DC=example,DC=net" -TrustedToAuthForDelegation
$false
```

最後に、一般的な推奨事項として、機密の特権アカウントがそのような攻撃にさらされるのを制限するために、Tenable Identity Exposure は「機密であり委任できない」(ADS_UF_NOT_DELEGATED) としてマークするか、関連する運用上の影響を注意深く検証したうえで「保護されたユーザー」グループに追加することを推奨します。

関連項目

- キー認証情報の追加
- メンバーの追加
- 操作が許可されている
- GPO に属している
- DCSync
- 操作の許可を付与できる
- SID 履歴あり
- 暗黙的な乗っ取り
- GPO を継承
- リンクされている GPO
- グループのメンバー
- 所有
- パスワードのリセット
- RODC 管理

- DACL の書き込み
- 所有者の書き込み

GPO に属している

説明

SYSVOL 共有のソース GPO ファイルやフォルダーは、ターゲット GPC (GPO) に属しています。つまり、GPO が適用する設定やプログラムまたはスクリプトはターゲット GPC によって定義されています。

悪用

これは、攻撃者が個別に使用できる攻撃関係ではありません。ただし、例えば、GPO に属する GPO ファイルや GPO フォルダーを制御できる攻撃者が、任意の設定を強制したり、攻撃経路の最終ポイントにあるユーザーまたはコンピューターでスクリプトを起動したりできる場合、完全な攻撃経路を示すことがあります。

修正方法

この関係は、SYSVOL にある GPO ファイルとフォルダーが、対応する GPC (GPO) オブジェクトとどのように関係しているかを示します。これは正常であり、設計によるものです。

したがって、修正の必要はありません。

関連項目

- キー認証情報の追加
- メンバーの追加
- 操作が許可されている
- 委任が許可されている
- DCSync
- 操作の許可を付与できる
- SID 履歴あり
- 暗黙的な乗っ取り
- GPO を継承

- リンクされている GPO
- グループのメンバー
- 所有
- パスワードのリセット
- RODC 管理
- DACL の書き込み
- 所有者の書き込み

DCSync

説明

DCSync は、ドメインコントローラーが変更を複製するためだけに使用する正当な Active Directory 機能ですが、不正なセキュリティプリンシパルもこれを使用できます。

ソースセキュリティプリンシパルは、DCSync 機能を使用してターゲットドメインから機密性の高いシークレット (パスワードハッシュ、Kerberos キーなど) をリクエストすることができ、最終的にドメインの完全な侵害につながりかねません。

シークレットをフェッチするには、「ディレクトリ変更の複製」(`DS-Replication-Get-Changes`) と「ディレクトリ変更のすべてを複製」(`DS-Replication-Get-Changes-All`) の 2 つのセキュリティアクセス許可が必要です。この関係が発生するのは、直接またはネスト化されたグループメンバーシップを使用して、これらのアクセス許可の両方をソースに付与した場合のみです。

悪用

ソースのセキュリティプリンシパルを侵害した攻撃者は、*mimikatz* や *impacket*などの専用のハッカーツールを使用してシークレットをフェッチできます。

- **ゴールデンチケット**:「krbtgt」アカウントのパスワードハッシュを取得した結果、Kerberos TGT の偽造が可能になり、任意のコンピューター/サービス上の任意の人になりすますことができます。なりしましにより、特にドメイン内の任意のコンピューターに対する管理者権限が付与されます。
- **シルバーチケット**: コンピューター/サービスアカウントのパスワードハッシュを取得した結果、Kerberos サービスチケットの偽造が可能になり、特定のコンピューター/サービス上の任意の人になりすますことができます。

修正方法

デフォルトで DCSync を利用できる正当なセキュリティプリンシパルは以下のとおりです。

- 管理者
- ドメイン管理者
- エンタープライズ管理者
- システム

さらに、Microsoft Entra ID Connect 設定では、パスワードハッシュ同期サービスアカウント (MSOL _...) が DCSync を利用することを許可しています。

また、特定のセキュリティツール、特にパスワード監査ソリューションのサービスアカウントが見つかる場合もあります。担当者と共にそれらの正当性を検証してください。

DCSync を実行する正当な理由のないソースセキュリティプリンシパルの場合は、このアクセス許可を削除する必要があります。

ターゲットドメインのセキュリティ記述子を変更するには

1. 「Active Directory ユーザーとコンピューター」で、ドメイン名を右クリックして [プロパティ] > [セキュリティ] の順に選択します。
2. 正当性のないセキュリティプリンシパルの「ディレクトリ変更の複製」および「ディレクトリ変更のすべてを複製」のアクセス許可を削除します。

注意: DCSync 関係は、ネストされたグループメンバーシップで継承されたアクセス許可によって発生する可能性があります。したがって、特定の状況では、グループ自体を削除するか、一部のメンバーのみを削除する必要があります。

関連項目

- キー認証情報の追加
- メンバーの追加
- 操作が許可されている
- 委任が許可されている
- GPO に属している
- 操作の許可を付与できる
- SID 履歴あり
- 暗黙的な乗っ取り
- GPO を継承
- リンクされている GPO

- グループのメンバー
- 所有
- パスワードのリセット
- RODC 管理
- DACL の書き込み
- 所有者の書き込み

操作の許可を付与できる

説明

ソースセキュリティプリンシパルは、自分または任意のユーザーに、ターゲットコンピューターとの操作が許可されている関係を与えることができます。多くの場合、Kerberos RBCD 委任攻撃によりターゲットコンピューターが完全に侵害される恐れがあります。

悪用が可能なのは、ソースがターゲットの「msDS-AllowedToActOnBehalfOfOtherIdentity」属性を編集するアクセス許可を持っているためです。

悪意のあるセキュリティプリンシパルがこの操作を実行すると、「操作が許可されている」攻撃関係が作成される場合があります。

悪用

ソースのセキュリティプリンシパルを侵害した攻撃者が、PowerShell (例:「Set-ADComputer <target> -PrincipalsAllowedToDelegateToAccount ...」)を使用して、ターゲットコンピューターの `msDS-AllowedToActOnBehalfOfOtherIdentity` 属性を編集する必要があります。

修正方法

ネイティブで特権を持ついくつかのセキュリティプリンシパル(アカウントオペレーター、管理者、ドメイン管理者、エンタープライズ管理者、システムなど) には、デフォルトでこのアクセス許可が付与されています。これらのセキュリティプリンシパルは正当なので、修正は必要ありません。

Kerberos RBCD の仕様により、コンピューターの管理者は、そのコンピューターで委任を実行する権利を、必要とする任意のユーザーに与えることができるようになっています。これは、ドメイン管理者レベルのアクセス許可を必要とする Kerberos 委任の他のモードとは異なります。この結果、下位レベルの管理者がこれらのセキュリティ設定を自分で管理できるようになります。この原則は委任とも呼ばれます。この場合、関係は正当なものです。

ただし、ソースセキュリティプリンシパルがターゲットコンピューターの正当な管理者でない場合、関係は正当ではないため、このアクセス許可を削除する必要があります。

ターゲットコンピューターのセキュリティ記述子を変更するには

1. 「Active Directory ユーザーとコンピューター」で、右クリックで **[プロパティ]** > **[セキュリティ]** の順に選択します。
2. ソースセキュリティプリンシパルに与えられたアクセス許可を削除します。「msDS-AllowedToActOnBehalfOfOtherIdentity の書き込み」、「すべてのプロパティの書き込み」、「アカウント制限の書き込み」、「フルコントロール」などのアカウント許可を検索します。

注意: ソースセキュリティプリンシパルは、Active Directory ツリーの上位にあるオブジェクトからアクセス許可を継承できます。

関連項目

- キー認証情報の追加
- メンバーの追加
- 操作が許可されている
- 委任が許可されている
- GPO に属している
- DCSync
- SID 履歴あり
- 暗黙的な乗っ取り
- GPO を継承
- リンクされている GPO
- グループのメンバー
- 所有
- パスワードのリセット
- RODC 管理
- DACL の書き込み
- 所有者の書き込み

SID 履歴あり

説明

ソースセキュリティプリンシパルの SIDHistory 属性にターゲットセキュリティプリンシパルの SID がある場合、それはソースがターゲットと同じ権限を持っていることを意味します。

SID 履歴は、ドメイン間でセキュリティプリンシパルを移行して、過去の SID 機能を参照するすべての権限を保持するために使用される正当なメカニズムです。

ただし、これは攻撃者が使用する永続的なメカニズムともなります。これを使うことによって、目立たないバックドアアカウントに、管理者アカウントなど任意のターゲットと同じ権限を与えることが可能になるからです。

悪用

ターゲットの SID は Active Directory 認証メカニズムが生成するトークン (NTLM および Kerberos) に透過的に追加されるため、ソースのセキュリティプリンシパルを侵害した攻撃者は、ターゲットのセキュリティプリンシパルとして直接認証を受けられます。

修正方法

ソースとターゲットのセキュリティプリンシパルが承認されたドメイン移行に関連している場合、その関係は正当なものであり、アクションは一切実行されません。この関係は、潜在的な攻撃経路を示すものとして表示されたままになります。

元のドメインが移行後に削除されたか Tenable Identity Exposure で設定されていない場合、ターゲットセキュリティプリンシパルは未解決としてマークされます。リスクはターゲットにありますが、そのターゲットが存在しないため、リスクはなく、修正は必要ありません。

逆に、ネイティブの特権ユーザーまたは特権グループに関係する SID 履歴が存在する場合は、Active Directory がその作成を阻止しているので、悪質なものである可能性が非常に高いです。それらの関係がおそらく「DCShadow」攻撃などのハッカー技術を使用して作成されたことを意味します。これらのケースは、「SID 履歴」に関連する IoE にも表示されます。

その場合、Tenable Identity Exposure は Active Directory フォレスト全体のフォレンジック検査を提案します。なぜなら、ソースの SID 履歴が編集できるということは、攻撃者がドメイン管理者または同等の高い権限を取得していることを表しているからです。フォレンジック検査は、対応する修正ガイダンスを使うなどして攻撃を分析するのに役立ち、削除するべき潜在的なバックドアを特定します。

最後に、Microsoft は、すべてのサービス(SMB 共有、Exchange など)のすべてのアクセス権を変更して新しい SID を使用し、この移行の完了後に不要な SIDHistory 値を削除することを推奨しています。すべての ACL を徹底的に特定して修正することは非常に困難ですが、これはハウスキーピングとしてベストプラクティスです。

ソースオブジェクト自体の SIDHistory 属性を編集する権限を持つユーザーは、SIDHistory 値を削除できます。作成とは違い、この操作にはドメイン管理者権限は必要ありません。

Active Directory ユーザーとコンピューターなどのグラフツールでは失敗するため、この操作を行うには PowerShell が必要です。例

```
Set-ADUser -Identity <user> -Remove @{sidhistory="S-1-..."}
```

注意: SIDHistory 値を削除することは簡単ですが、この操作を元に戻すのは非常に複雑です。廃止になっているかもしれない他のドメインの存在を必要とする SIDHistory 値を再作成しなければならないからです。そのため、Microsoft はスナップショットやバックアップを準備することも推奨しています。

関連項目

- キー認証情報の追加
- メンバーの追加
- 操作が許可されている
- 委任が許可されている
- GPO に属している
- DCSync
- 操作の許可を付与できる
- 暗黙的な乗っ取り
- GPO を継承
- リンクされている GPO
- グループのメンバー
- 所有

- パスワードのリセット
- RODC 管理
- DACL の書き込み
- 所有者の書き込み

暗黙的な乗っ取り

説明

ソースは Tier0 セキュリティプリンシパルです。Tier0 とは、ドメインで最高の権限を持つ Active Directory オブジェクトのセットです。ドメイン管理者グループやドメインコントローラーグループのメンバーがこれにあたります。すべての Tier0 資産は、明示的な他の関係がない場合でも、ドメイン内の他のオブジェクトを暗黙的に侵害する可能性があります。

この関係により、Active Directory に組み込まれた暗黙的な権限のモデル化が可能になります。これらの権限は設計によるものであり、文書化されているため、攻撃者に知られています。ただし、Tenable Identity Exposure は標準的な手段でこれらの権限を収集することはできません。さらに、攻撃者が Tier0 ノードを侵害するとすぐに、他の明示的な関係を介さずに他のオブジェクトを直接攻撃できるため、攻撃経路グラフはシンプルになります。

つまり、ソース Tier0 資産はすべて、グラフ内の任意のターゲットノードに対して「暗黙的な乗っ取り」関係があると見なされます。

悪用

実際の悪用方法は、標的にされるソース Tier0 資産のタイプによって異なりますが、これらの手法は十分に文書化され、攻撃者が効率的に習得できるようになっています。

修正方法

この関係は設計によるものであり、修正できません。Tier0 資産に到達した攻撃者を阻止して、さらなる攻撃を行えないようにすることはほぼ不可能です。

攻撃経路の上流の関係を重点的に修正するようにします。

関連項目

- キー認証情報の追加
- メンバーの追加
- 操作が許可されている
- 委任が許可されている

- GPO に属している
- DCSync
- 操作の許可を付与できる
- SID 履歴あり
- GPO を継承
- リンクされている GPO
- グループのメンバー
- 所有
- パスワードのリセット
- RODC 管理
- DACL の書き込み
- 所有者の書き込み

GPO を継承

説明

LDAP ツリーでは、組織単位 (OU) やドメインなど(サイトは除く)、ソースのリンク可能なコンテナには、ターゲット OU、ユーザー、デバイス、ドメインコントローラー(DC)、読み取り専用ドメインコントローラー(RODC)が含まれています。これは、リンク可能なコンテナの子オブジェクトが、リンクされている GPO を継承するためです(「リンクされている GPO」関係を参照)。

Tenable Identity Exposure は、OU による継承のブロックを必ず考慮に含めます。

悪用

攻撃者が攻撃経路の GPO 上流を侵害することができる限り、攻撃者はこの関係を悪用するために何もする必要はありません。GPO 関係の継承に示されているように、関係は、設計上、リンク可能なコンテナとその下のオブジェクトに適用されます。

修正方法

ほとんどの場合、GPO が親コンテナからリンク可能な子コンテナに適用されるのは正常かつ正当なことです。ただし、このリンクがその他の攻撃経路を露出してしまいます。

したがって、リスクを軽減するために可能なら GPO を組織単位階層の最下位レベルにリンクしてください。

さらに GPO が他の攻撃関係にさらされないように、攻撃者による不正な変更から保護する必要があります。

最後に、OU は「継承のブロック」オプションを使用して、より高いレベルからの GPO 継承を無効にできます。ただし、このオプションではすべての GPO (最高のドメインレベルで定義された潜在的なセキュリティ強化 GPO も含む) がブロックされるため、最後の手段としてのみ使用してください。ブロックすると、適用されている GPO の正当性を判断することもより困難になります。

関連項目

- キー認証情報の追加
- メンバーの追加
- 操作が許可されている

- 委任が許可されている
- GPO に属している
- DCSync
- 操作の許可を付与できる
- SID 履歴あり
- 暗黙的な乗っ取り
- リンクされている GPO
- グループのメンバー
- 所有
- パスワードのリセット
- RODC 管理
- DACL の書き込み
- 所有者の書き込み

リンクされている GPO

説明

ソース GPO は、ドメインや組織単位 (OU) など、ターゲットのリンク可能なコンテナにリンクされています。これは、ソース GPO が設定を割り当てて、ターゲットに含まれるデバイスとユーザーに対してプログラムを実行できることを意味します。ソース GPO は、「GPO を継承」関係を通じて、その下のコンテナ内のオブジェクトにも適用されます。

結果として、GPO は GPO が適用されているデバイスとユーザーを侵害することが可能です。

悪用

攻撃者は、最初に別の攻撃関係を通してソース GPO を侵害する必要があります。

そこから、いくつかの手法を使用して、ターゲットとその下に含まれるデバイスやユーザーに対して悪質なアクションを実行します。次にいくつかの例を示します。

- 正当な「すぐに実行されるようにスケジュールされたタスク」を悪用し、デバイスで任意のスクリプトを実行する
- すべてのデバイスで管理権限を持つ新しいローカルユーザーを追加する
- MSI プログラムをインストールする
- ファイヤーウォールまたはウイルス対策を無効化する
- その他の権利を付与する
- -

攻撃者は、「グループポリシー管理」などの管理ツールや PowerSploit などの専用ハッカーツールを使用して GPO コンテンツを手動で編集し、GPO を変更する可能性があります。

修正方法

ほとんどの場合、GPO をリンク可能なコンテナにリンクすることは正常で正当なことです。ただし、このリンクによりアタックサーフェスが拡大し、その下のコンテナ内のアタックサーフェスも拡大します。

したがって、リスクを軽減するために可能なら GPO を組織単位階層の最下位レベルにリンクしてください。

さらに GPO が他の攻撃関係にさらされないように、攻撃者による不正な変更から保護する必要があります。

関連項目

- キー認証情報の追加
- メンバーの追加
- 操作が許可されている
- 委任が許可されている
- GPO に属している
- DCSync
- 操作の許可を付与できる
- SID 履歴あり
- 暗黙的な乗っ取り
- GPO を継承
- グループのメンバー
- 所有
- パスワードのリセット
- RODC 管理
- DACL の書き込み
- 所有者の書き込み

グループのメンバー

説明

ソースセキュリティプリンシパルはターゲットグループのメンバーです。したがって、ファイル共有へのアクセス、ビジネスアプリケーションでのロールの引き受けなど、グループが保持するすべてのアクセス権の恩恵を受けます。

悪用

攻撃者は、この攻撃関係を悪用するために何もする必要はありません。ローカルまたはリモートのセキュリティトークンでターゲットグループを取得したり、Kerberos チケットを取得したりすることは、ソースセキュリティプリンシパルとして認証するだけで実行できます。

修正方法

ソースセキュリティプリンシパルがターゲットグループの不正なメンバーである場合は、削除する必要があります。

「Active Directoryユーザーとコンピューター」などの標準の Active Directory 管理ツールや、Remove-ADGroupMember などの PowerShell を使用できます。

関連項目

- キー認証情報の追加
- メンバーの追加
- 操作が許可されている
- 委任が許可されている
- GPO に属している
- DCSync
- 操作の許可を付与できる
- SID 履歴あり
- 暗黙的な乗っ取り

- GPO を継承
- リンクされている GPO
- 所有
- パスワードのリセット
- RODC 管理
- DACL の書き込み
- 所有者の書き込み

所有

説明

通常ソースセキュリティプリンシパルは、ターゲットオブジェクトを作成しているため、ターゲットオブジェクトの宣言された所有者になります。所有者には「コントロールの読み取り」および「DACL の書き込み」の黙示的な権利があるため、所有者自身または他のユーザーのために追加の権利を取得し、最終的にターゲットオブジェクトを侵害することができます。

悪用

ソースのセキュリティプリンシパルを侵害した攻撃者は、Windows のネイティブコマンド (dsacls)、PowerShell (Set-ACL)、管理ツール(「Active Directory ユーザーとコンピューター」)、専用ハッカーツール (PowerSploit) を使用して、ターゲットオブジェクトのセキュリティ記述子を編集するだけで悪用できます。

下位の特権ユーザーがオブジェクトを作成して所有し (標準のヘルプデスクの技術者など)、その後オブジェクトが管理者などのより高位の特権に昇格されると、権限昇格のリスクがあります。元の所有者がそのまま存続し、新しい特権オブジェクトを侵害してその特権を悪用する可能性があります。

修正方法

ソースセキュリティプリンシパルがターゲットオブジェクトの正当な所有者でない場合は、変更する必要があります。

ターゲットオブジェクトの所有者を変更するには

1. 「Active Directory ユーザーとコンピューター」で、右クリックで **[プロパティ]** > **[セキュリティ]** > **[詳細]** を選択します。
2. 上部の **[所有者]** 行で、**[変更]** をクリックします。

ほとんどの機密性の高い Active Directory オブジェクトに対してデフォルトで使用される安全なターゲットオブジェクトの所有者は次のとおりです。

- ドメインパーティションのオブジェクト:「管理者」または「ドメイン管理者」
- 設定パーティションのオブジェクト:「エンタープライズ管理者」
- スキーマパーティションのオブジェクト:「スキーマ管理者」

関連項目

- キー認証情報の追加
- メンバーの追加
- 操作が許可されている
- 委任が許可されている
- GPO に属している
- DCSync
- 操作の許可を付与できる
- SID 履歴あり
- 暗黙的な乗っ取り
- GPO を継承
- リンクされている GPO
- グループのメンバー
- パスワードのリセット
- RODC 管理
- DACL の書き込み
- 所有者の書き込み

パスワードのリセット

説明

ソースセキュリティプリンシパルは、ターゲットのパスワードをリセットできるため、新しい属性のパスワードを使用してターゲットとして認証され、ターゲットの特権を利用できます。

パスワードのリセットはパスワードの変更と同じではありません。変更は現在のパスワードを知っている誰もが行うことができます。通常、パスワードの変更はスワードの有効期限が切れたときに発生します。

悪用

ソースのセキュリティプリンシパルを侵害した攻撃者は、Windows のネイティブコマンド (例: net group/domain)、PowerShell (例: Set-ADAccountPassword -Reset)、管理ツール (例: Active Directory ユーザーとコンピューター)、専用ハッカーツール (例: PowerSploit) を使用して、ターゲットのパスワードをリセットすることができます。

その後、攻撃者は新しく選択したパスワードを使用して正当な認証方法で、Active Directory または標的のリソースに認証されるだけで、ターゲットに完全になりすませます。

ただし、攻撃者は通常、以前のパスワードを知らないので、攻撃後に元のパスワードに戻すことができません。したがって、攻撃はターゲットの背後にいる正当なユーザーが経験する結果になることが多く、サービスアカウントの場合は特にサービス拒否を引き起こす可能性さえあります。

修正方法

IT 管理者およびヘルプデスクスタッフは、パスワードをリセットすることが正当に許可されています。ただし、適切な委任を実装して、許可された範囲内でのみこのアクションを実行できるようにする必要があります。

また、ティアモデルに従い、通常のユーザー向けのヘルプデスクなど、下位レベルのスタッフが、ドメイン管理者などの上位レベルのアカウントのパスワードをリセットできないようにする必要があります。権限昇格の機会となることを防ぐためです。

ターゲットのセキュリティ記述子を変更し、不正なアクセス許可を削除するには

1. 「Active Directory ユーザーとコンピューター」で、右クリックして[プロパティ]>[セキュリティ]の順に選択します。
2. ソースセキュリティプリンシパルの「パスワードのリセット」のアクセス許可を削除します。

   注意: このアクセス許可を「パスワードの変更」と混同しないでください。

関連項目

- キー認証情報の追加
- メンバーの追加
- 操作が許可されている
- 委任が許可されている
- GPO に属している
- DCSync
- 操作の許可を付与できる
- SID 履歴あり
- 暗黙的な乗っ取り
- GPO を継承
- リンクされている GPO
- グループのメンバー
- 所有
- RODC 管理
- DACL の書き込み
- 所有者の書き込み

RODC 管理

説明

ターゲットの読み取り専用ドメインコントローラー(RODC)の「ManagedBy」属性に、ソースセキュリティプリンシパルが指定されています。これは、ソースがターゲットの RODC に対して管理者権限を持っていることを意味します。

> **注意**: 他の Active Directory オブジェクトタイプは、情報提供のためだけに同じ「ManagedBy」属性を使用していますが、宣言されたマネージャーにいかなる管理権限も付与しません。したがって、この関係は RODC タイプのターゲットノードの場合にのみ存在します。

RODC は、より一般的な書き込み可能のドメインコントローラーと比べて機密性は低いですが、RODC から認証情報を盗み、他のシステムにさらにピボットできるため、攻撃者にとって依然として重要な標的になります。これは、RODC がシークレットを持つオブジェクトをいくつ同期できるかなど、RODC の設定の強化レベルにより異なります。

悪用

悪用の方法は、「AdminTo」関係の場合と同じです。

ソースのセキュリティプリンシパルを侵害した攻撃者は、そのアクセス認証を使用してリモートで接続し、管理者権限でターゲットの RODC に対しコマンドを実行することができます。管理共有のある Server Message Block (SMB)、Remote Desktop Protocol (RDP)、Windows Management Instrumentation (WMI)、Remote Procedure Call (RPC)、Windows Remote Management (WinRM) など、利用可能なネイティブプロトコルを悪用する可能性があります。

攻撃者は、ネイティブのリモート管理ツール(PsExec、サービス、スケジュールされたタスク、Invoke-Command)、または特殊なハッカーツール(wmiexec、smbexec、Invoke-DCOM、SharpRDP)を使用する場合があります。

攻撃の最終目標は、ターゲットの RODC を侵害すること、または mimikatz などの認証情報ダンプツールを使用して、より多くの認証情報とシークレットを取得し、他のマシンの侵害に悪用することです。

修正方法

ソースセキュリティプリンシパルがターゲットの読み取り専用ドメインコントローラー(RODC)の正当な管理者でない場合は、適切な管理者に置き換える必要があります。

ドメイン管理者は通常 RODC を管理しないため、専用の「managed by」設定があります。これは、高い特権を持つドメイン管理者が、信頼レベルが低い RODC に認証を実行して、自分の認証情報を露呈しないようにするためです。

したがって、Active Directory RODC ルールに従って、RODC に対して適切な「中間レベル」の管理者を選択する必要があります (RODC が配置されている企業のローカル支社の IT 管理者など)。

「ManagedBy」属性を変更するには

1. 「Active Directory ユーザーとコンピューター」で、[RODC] > **[プロパティ]** > **[ManagedBy]** タブを選択します。
2. **[変更]** をクリックします。

PowerShell で次のコマンドを実行することもできます。

```
Set-ADComputer <rodc> -ManagedBy (Get-ADUser <rodc_admin>)
```

関連項目

- キー認証情報の追加
- メンバーの追加
- 操作が許可されている
- 委任が許可されている
- GPO に属している
- DCSync
- 操作の許可を付与できる
- SID 履歴あり
- 暗黙的な乗っ取り
- GPO を継承
- リンクされている GPO
- グループのメンバー

- 所有
- パスワードのリセット
- DACL の書き込み
- 所有者の書き込み

DACL の書き込み

説明

ソースセキュリティプリンシパルは、任意アクセス制御リスト (DACL) のターゲットオブジェクトのアクセス許可を変更する権限を持っています。このため、ソースは追加のアクセス許可を自分自身のために取得したり、他の誰かに与えたりして、最終的にターゲットオブジェクトを侵害することができます。

悪用

ソースのセキュリティプリンシパルを侵害した攻撃者は、Windows のネイティブコマンド (dsacls)、PowerShell (Set-ACL)、管理ツール (「Active Directory ユーザーとコンピューター」)、専用ハッカーツール (PowerSploit) を使用して、ターゲットオブジェクトのセキュリティ記述子を編集するだけで悪用できます。

修正方法

ソースセキュリティプリンシパルがターゲットオブジェクトのアクセス許可を変更する正当なアクセス許可を持っていない場合は、このアクセス許可を削除する必要があります。

ターゲットオブジェクトのセキュリティ記述子を変更するには

1. 「Active Directory ユーザーとコンピューター」で、オブジェクトを右クリックし、**[プロパティ]** > **[セキュリティ]** > **[詳細]** を選択します。
2. ソースセキュリティプリンシパルの「アクセス許可の変更」のアクセス許可を削除します。

> **注意**: オブジェクトは、Active Directory ツリーの上位にあるオブジェクトからこのアクセス許可を継承できます。

関連項目

- キー認証情報の追加
- メンバーの追加
- 操作が許可されている
- 委任が許可されている
- GPO に属している

- DCSync
- 操作の許可を付与できる
- SID 履歴あり
- 暗黙的な乗っ取り
- GPO を継承
- リンクされている GPO
- グループのメンバー
- 所有
- パスワードのリセット
- RODC 管理
- 所有者の書き込み

所有者の書き込み

説明

ソースセキュリティプリンシパルは、自身を所有者として割り当てることを含め、ターゲットオブジェクトの所有者を変更するアクセス許可を持っています。所有者には「コントロールの読み取り」および「DACLの書き込み」の黙示的な権利があるため、所有者自身または他のユーザーのために追加の権利を取得し、最終的にターゲットオブジェクトを侵害することができます。

詳細は、所有関係を参照してください。

悪用

ソースのセキュリティプリンシパルを侵害した攻撃者は、Windows のネイティブコマンド (例: dsacls/takeownership)、PowerShell (例: Set-ACL)、管理ツール (例: Active Directory ユーザーとコンピューター)、専用ハッカーツール (例: PowerSploit) を使用して、自分をターゲットの所有者に割り当てることができます。

その後、同様の方法を使用して、ターゲットオブジェクトのセキュリティ記述子を編集できます。

修正方法

ソースセキュリティプリンシパルがターゲットオブジェクトの所有者を変更する正当なアクセス許可を持っていない場合は、このアクセス許可を削除する必要があります。

ターゲットオブジェクトのセキュリティ記述子を変更するには

1. 「Active Directory ユーザーとコンピューター」で、オブジェクトを右クリックし、**[プロパティ]** > **[セキュリティ]** > **[詳細]** を選択します。
2. ソースセキュリティプリンシパルの「所有者の変更」のアクセス許可を削除します。

注意: オブジェクトは、Active Directory ツリーの上位にあるオブジェクトからこのアクセス許可を継承できます。

関連項目

- キー認証情報の追加
- メンバーの追加

- 操作が許可されている
- 委任が許可されている
- GPO に属している
- DCSync
- 操作の許可を付与できる
- SID 履歴あり
- 暗黙的な乗っ取り
- GPO を継承
- リンクされている GPO
- グループのメンバー
- 所有
- パスワードのリセット
- RODC 管理
- DACL の書き込み

ティア 0 資産の特定

ティア 0 資産には、Active Directory のフォレストとドメインを直接または間接的に管理できるアカウント、グループ、その他の資産が含まれます。

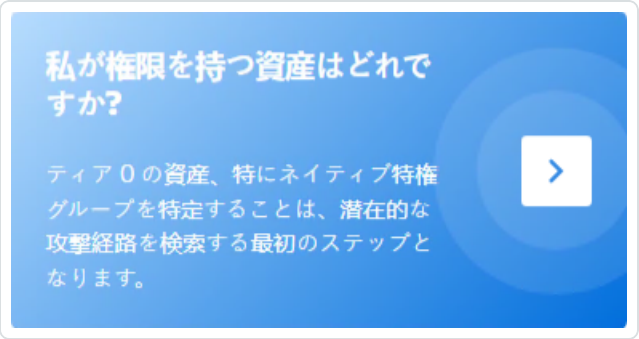
Tenable Identity Exposure は、ティア 0 資産とその資産につながる潜在的な攻撃経路があるアカウントを一覧表示します。

ティア 0 資産をリストするには

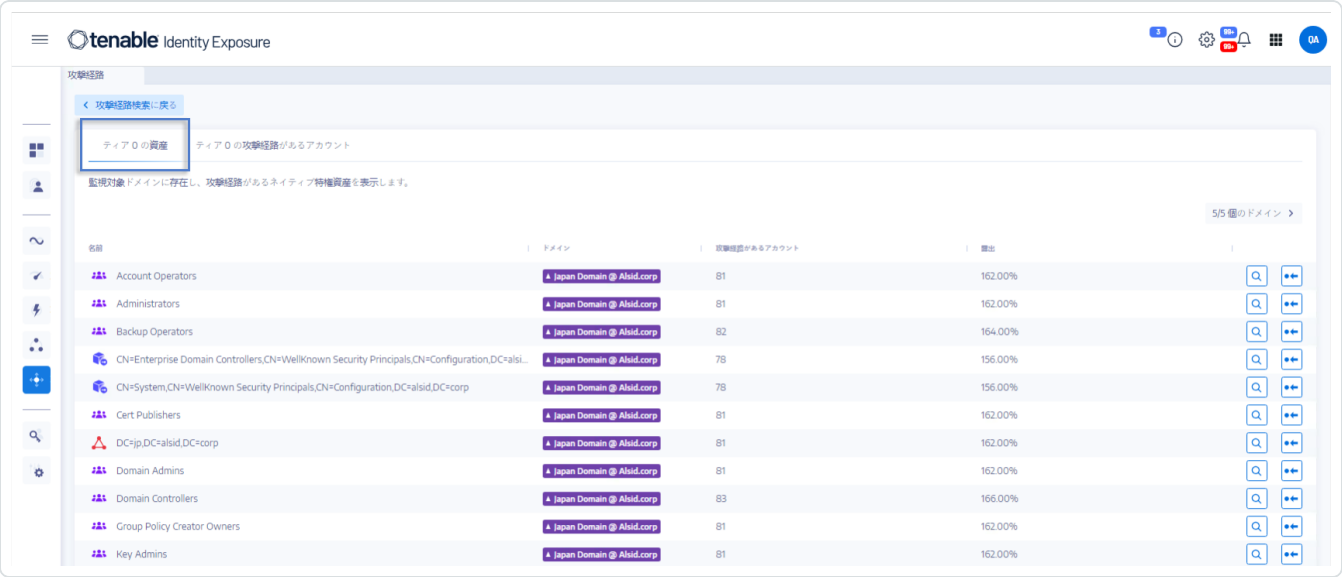
1. Tenable Identity Exposure で、左側のナビゲーションバーの攻撃経路アイコン をクリックします。

   [攻撃経路] ペインが開きます。

2. 「**私が権限を持つ資産はどれですか**」というタイルをクリックします。



Tenable Identity Exposure は AD のティア 0 資産のリストを表示します。



各行には、**資産名**、その**ドメイン**、および次の情報が表示されます。

- **攻撃経路のあるアカウント**: ティア 0 資産に至る攻撃経路を持つ資産の数
- **露出**: ドメイン内のアカウントの合計数に対する、ティア 0 資産に至る攻撃経路のあるアカウント数の比率

特定のドメインの資産をフィルターするには

1. **n/n** ボタンをクリックします。

   [フォレストとドメイン] ペインが開きます。次のいずれかを実行できます。

   - **[検索]** ボックスにフォレストまたはドメインの名前を入力します。
   - **[すべて展開]** ボックスを選択し、必要なフォレストまたはドメインを選択します。

2. **[選択内容でフィルター]** をクリックします。

   Tenable Identity Exposure が資産のリストを更新します。

ティア 0 資産に至る攻撃経路のあるアカウントをリストするには

- ティア 0 資産名の行末にある アイコンをクリックします。

  Tenable Identity Exposure は、そのティア 0 資産につながる攻撃経路のあるアカウントのリストを表示します。

ティア 0 資産の露出資産を確認するには

- ティア 0 資産名の行末にある アイコンをクリックします。

  Tenable Identity Exposure は、ティア 0 資産の露出資産ページを開きます。詳細は、攻撃関係を参照してください。

攻撃経路のあるアカウント

Tenable Identity Exposure は、ティア 0 資産に至る攻撃経路を持つアカウントを表示します。ここから潜在的なセキュリティの脅威の全体像を把握することができます。なぜなら、ユーザーおよびコンピューターのアカウントはさまざまな攻撃関係を通じて特権を持つようになる場合があるからです。

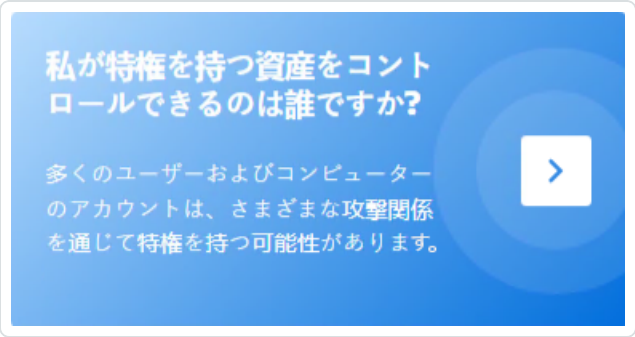
詳細は、ティア 0 資産の特定 を参照してください。

攻撃経路のある資産を表示するには

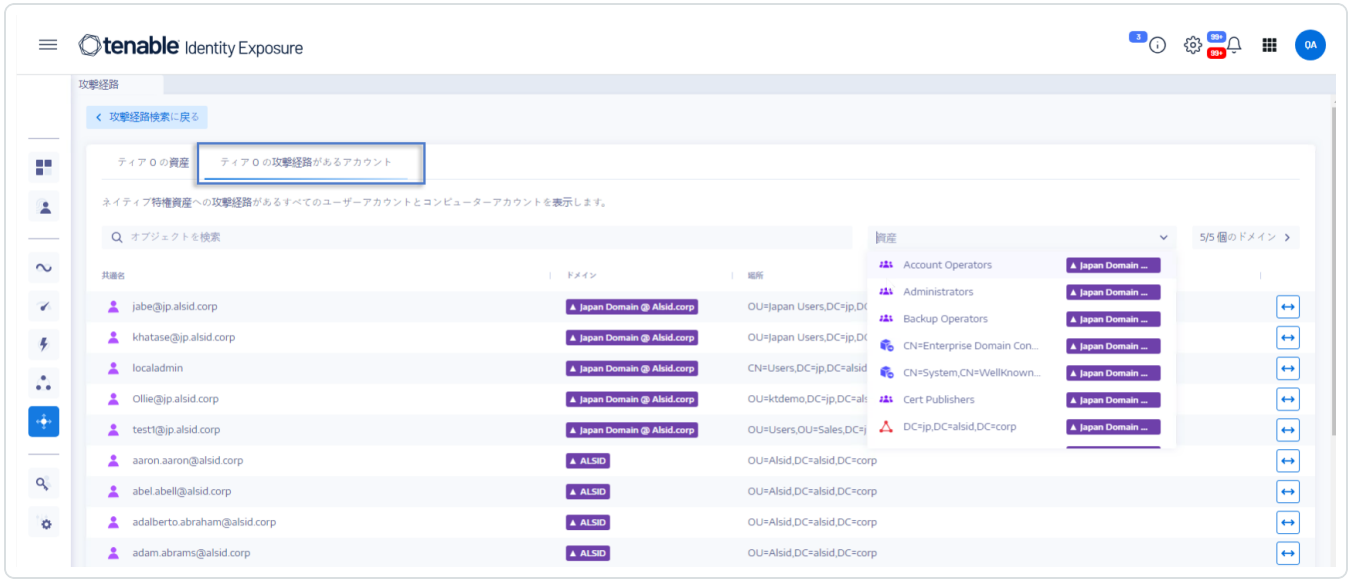
1. Tenable Identity Exposure で、左側のナビゲーションバーの攻撃経路アイコン をクリックします。

   [攻撃経路] ペインが開きます。

2. **私が特権を持つ資産をコントロールできるのは誰ですか**というタイルをクリックします。



Tenable Identity Exposure は、ティア 0 資産に至る攻撃経路を持つすべてのユーザーとコンピューターのアカウントを表示します。



特定の資産を検索するには

1. **[検索]** ボックスに資産の名前を入力します。
2. **[資産]** ボックスの矢印 **>** をクリックして、ティア 0 資産のドロップダウンリストを表示して、その中から 1 つ選択します。

   Tenable Identity Exposure は一致する結果でリストを更新します。

特定のドメインの資産をフィルターするには

1. **n/n** ボタンをクリックします。

   [フォレストとドメイン] ペインが開きます。次のいずれかを実行できます。

   - **[検索]** ボックスにフォレストまたはドメインの名前を入力します。
   - **[すべて展開]** ボックスを選択し、必要なフォレストまたはドメインを選択します。

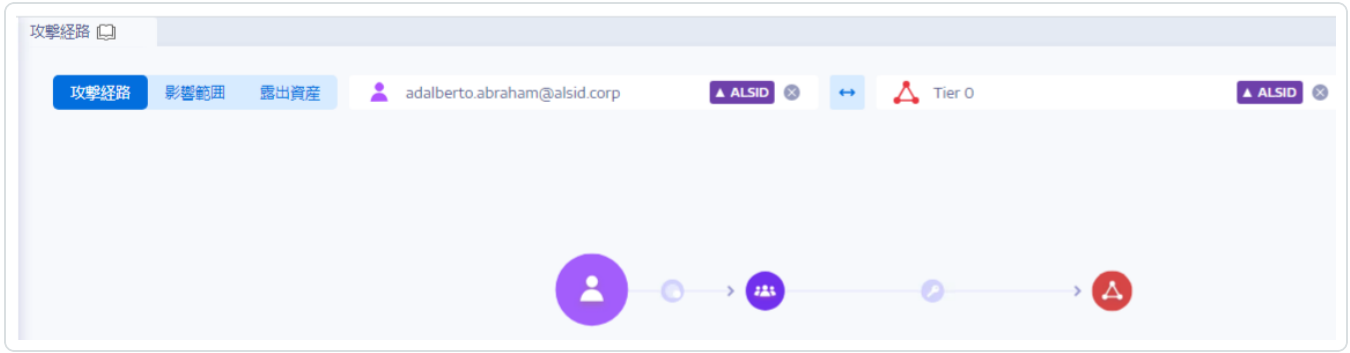
2. **[選択内容でフィルター]** をクリックします。

   Tenable Identity Exposure が資産のリストを更新します。

攻撃経路を探索するには

- 資産名の行末にある  アイコンをクリックします。

  Tenable Identity Exposure が攻撃経路ページを開きます。その資産からすべてのティア 0 資産までの経路が示されています。詳細は、攻撃経路と攻撃関係を参照してください。



攻撃経路のノードタイプ

Tenable Identity Exposure の攻撃経路機能は、Active Directory 環境内で攻撃者が利用可能な攻撃経路をビジュアル化したグラフを表示します。このグラフは、攻撃関係を表す**エッジ**と、Active Directory (LDAP/SYSVOL) オブジェクトを表す**ノード**で構成されています。

次のリストは、攻撃経路グラフで表示される可能性のあるすべてのノードタイプを示しています。

ノードタイプ	場所	アイコン	説明
ユーザー	LDAP		`user` クラスを含むが `computer` は含まない `objectClass` 属性を持つ LDAP オブジェクト。
グループ	LDAP		`class` グループを含む `objectClass` 属性を持つ LDAP オブジェクト。
デバイス	LDAP		`computer` クラスを含むが `msDS-GroupManagedServiceAccount` は含まない `objectClass` 属性を持つ LDAP オブジェクト。 その `primaryGroupID` 属性が 516 (DC) または 521 (RODC) と等しくない。 **注意**: Tenable 製品を区別するために、このカテゴリは「コンピューター」ではなく、より一般的な「デバイス」と呼ばれています。
組織単位 (OU)	LDAP		クラス `organizationalUnit` を含む `objectClass` 属性を持つ LDAP オブジェクト。`container` クラスのオブジェクトと、任意の Active Directory (AD) オブジェクトがコンテナとして機能することがある (つまり、他のオブジェクトを含めることができる) という事実を混同しないようにしてください。
ドメイン	LDAP		クラス `domainDNS` と特定の属性を含む `objectClass` 属性を持つ LDAP オブジェクト。
ドメインコントローラー	LDAP		`objectClass` 属性にクラス `computer` を含み、その `primaryGroupID` が 516 と等しい LDAP オブジェクト (し

ラー(DC)			たがって、RODC ではない)。
読み取り専用ドメインコントローラー(RODC)	LDAP		objectClass 属性にクラス computer を含み、その primaryGroupID が 521 と等しい LDAP オブジェクト(したがって、ノーマル DC ではない)。
グループポリシー(GPC)	LDAP		groupPolicyContainer を含む objectClass 属性を持つ LDAP オブジェクト。
GPO ファイル	SYSVOL		特定の GPO の SYSVOL 共有で見つかったファイル(例: "\example.net\sysvol\example.net\Policies\{A8370D7F-8AC0-452E-A875-2A6A52E9D392}\{Machine,User}\Preferences\ScheduledTasks\ScheduledTasks.xml"。)
GPO フォルダー	SYSVOL		特定の GPO の SYSVOL 共有で見つかったフォルダー。GPO ごとに 1 つ存在します(例: "\example.net\sysvol\example.net\Policies\{A8370D7F-8AC0-452E-A875-2A6A52E9D392}\Machine\Scripts\Startup"。)
グループ管理サービスアカウント(gMSA)	LDAP		msDS-GroupManagedServiceAccount を含む objectClass 属性を持つ LDAP オブジェクト。
エンタープライズ NtAuth ストア	LDAP		certificationAuthority を含む objectClass 属性を持つ LDAP オブジェクト。
PKI 証明書テンプレート	LDAP		pKICertificateTemplate を含む objectClass 属性を持つ LDAP オブジェクト。

未解決のセキュリティプリンシパル	LDAP		関係を構築する際のある時点で objectSid または DistinguishedName 属性が使用されるが、それに対応する LDAP セキュリティプリンシパルオブジェクトが不明である LDAP オブジェクト (「未解決の SID」の典型的なケース)。 また、それらに関連付けられている特定のセキュリティプリンシパルの種類 (ユーザー、コンピューター、グループなど) に関する情報もなく、SID/DN のみが判明している。
特殊 ID	LDAP		Windows と Active Directory は、内部的に既知となっている ID を使用します。これらの ID はグループと似たように働きをしますが、AD はそれらをグループとして宣言しません。詳細は、特殊 ID グループを参照してください。
その他			現在、上記のカテゴリに分類されないすべての AD/SYSVOL オブジェクト。

アクティビティログ

Tenable Identity Exposure のアクティビティログにより、特定の IP アドレス、ユーザー、アクションに関連する、Tenable Identity Exposure プラットフォームで発生したすべてのアクティビティの痕跡を確認することができます。

注意: 技術的な制限により、テナント管理などの特定のビューに関するアクティビティログ(追加、編集、削除を含む)は現在表示されません。

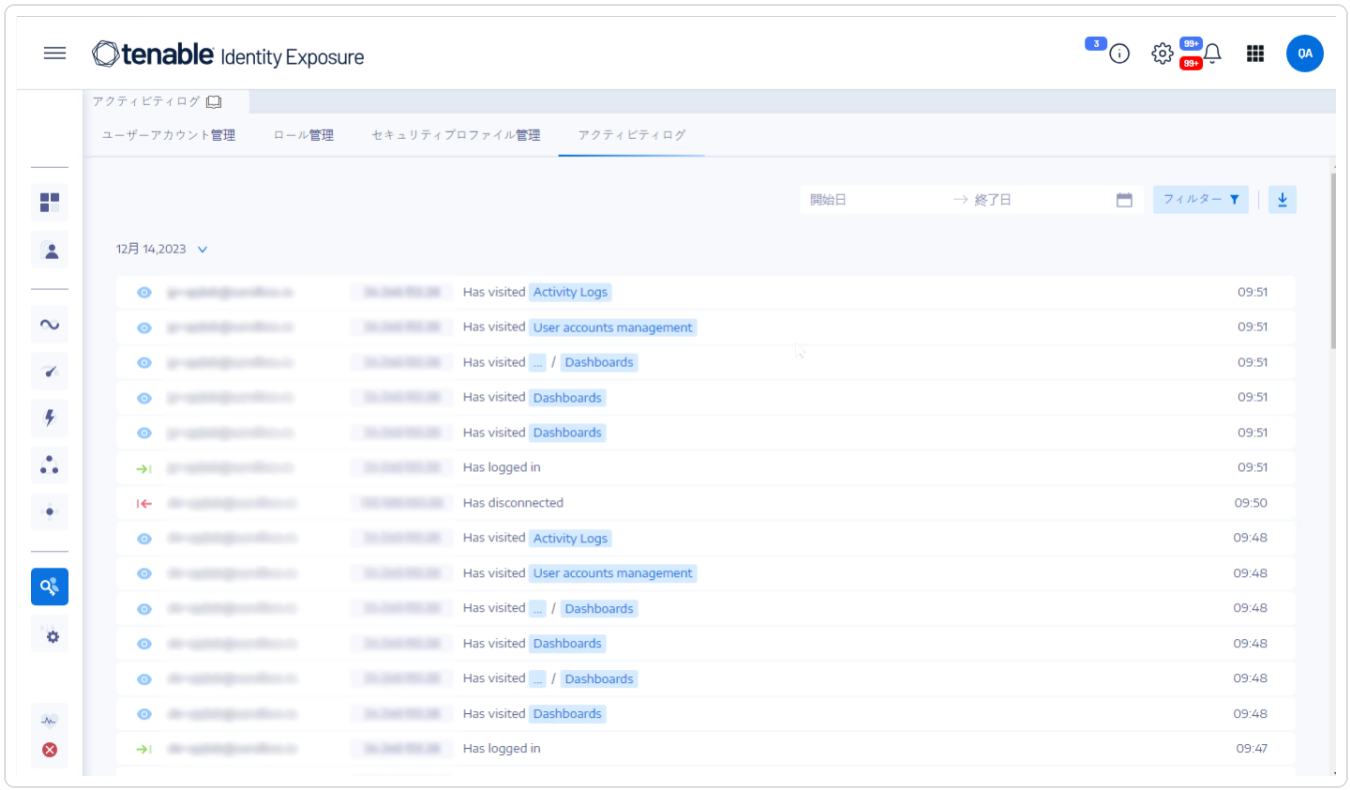
アクティビティログを表示するには

1. Tenable Identity Exposure で、左側のナビゲーションメニューの**[アカウント]** アイコンをクリックします。

   [ユーザーアカウント管理]ペインが表示されます。

2. **[アクティビティログ]** タブを選択します。

   [アクティビティログ] ペインが開きます。



特定の時間フレームのアクティビティログを表示するには

1. [アクティビティログ] ペインの上部で、日付の選択コントロールをクリックします。
2. 表示する期間の開始日と終了日を選択します。
3. (オプション) スクロールバーを使用して時刻を選択します (デフォルト: 現在時刻)。
4. **[OK]** をクリックします。

   Tenable Identity Exposure は、その期間のアクティビティログを表示します。

アクティビティログをフィルタリングするには

1. [アクティビティログ] ペインの上部で、Filters ボタンをクリックします。

   [フィルター] ペインが表示されます。
2. 次のボックスで > をクリックします。
   - IP アドレス
   - ユーザー
   - アクション
3. **[検証]** をクリックします。

   Tenable Identity Exposure は、定義されたフィルターのアクティビティログを表示します。

フィルターをクリアするには

- **[フィルター]** ペインの下部で、**[フィルターを消去]** をクリックします。

  Tenable Identity Exposure は、フィルタリングされていないアクティビティログを表示します。

アクティビティログをエクスポートするには

- [アクティビティログ] ペインの上部で、アイコンをクリックします。

  Tenable Identity Exposure は、アクティビティログを CSV 形式でコンピューターにダウンロードします。

Tenable Identity Exposure 管理者ガイド

最終更新日: 4月 30, 2024

本管理者ガイドには、Tenable Identity Exposure (旧 Tenable.ad) の管理タスクに関する情報が記載されています。

Tenable は、Tenable Identity Exposure で管理者として作業を始めるにあたり、次のいくつかを実行することを推奨します。

- 準備とインストール
- プロファイルとユーザーの設定
- 検出と監視

ヒント: Tenable Identity Exposure の詳細は、次のカスタマー向け説明資料で確認してください。

- Tenable Identity Exposure Self Help Guide
- Tenable Identity Exposure はじめに (Tenable University)

準備とインストール

Tenable Identity Exposure のインストールを準備して実行するには

- *Tenable Identity Exposure インストールガイド*の説明に従ってTenable Identity Exposure をインストールします。
- Tenable Identity Exposure に接続してサインインします。

プロファイルとユーザーの設定

続いて、次のアクションを実行して Tenable Identity Exposure インターフェースを設定しナビゲートすることを推奨します。

- プロファイルの環境設定します。デフォルト言語の設定、パスワードの変更、およびプロファイルの他の環境設定を行います。
- ユーザーを作成して Tenable Identity Exposure インスタンスに追加します。

- ロールベースのアクセス制御 (RBAC) を設定して、所属組織内のデータや機能に安全にアクセスします。

検出と監視

ビジネスニーズに合わせて Tenable Identity Exposure を設定および調整したら、データの操作を開始できます。

- 攻撃インジケーターモジュールをデプロイします。
- Tenable Identity Exposure ポータルを使用して、監視対象のインフラのセキュリティ状態に関する関連情報を管理および受信します。
- Tenable Identity Exposure が特定のドメインで監視する攻撃のタイプを選択して、攻撃シナリオを定義します。

注意: Tenable Identity Exposure は、単独で、または Tenable One パッケージの一部として購入できます。詳細は、Tenable One を参照してください。

Tenable One サイバーエクスポージャー管理プラットフォーム

Tenable One は、サイバーエクスポージャー管理プラットフォームです。DX 時代のアタックサーフェス全体の可視化、起こり得る攻撃を防ぐための取り組みへのフォーカス、サイバーリスクの正確な伝達を支援することで、最大限のビジネスパフォーマンスを発揮できるようにします。

このプラットフォームは、Tenable Research による高速で広範な脆弱性カバレッジを基盤に構築されており、IT 資産、クラウドリソース、コンテナ、ウェブアプリケーション、認証システムを合わせて網羅する、業界で最大の脆弱性カバレッジを提供します。包括的な分析機能も、対応措置の優先順位を付け、サイバーリスクを伝達してくれます。Tenable One を使用する企業は以下のことができます。

- DX 時代のアタックサーフェス全体を把握できる可視性を得る
- 起こり得る脅威に先駆けた攻撃防止対策の優先順位付け
- より適切な判断を可能にするサイバーリスクの伝達

Tenable Identity Exposure はスタンドアロン製品として存在しますが、Tenable One サイバーエクスポージャー管理プラットフォームの一部としても購入できます。

ヒント: Tenable One 製品の使用開始の詳細については、Tenable One デプロイメントガイドを参照してください。

詳細については、次を参照してください。

Active Directory の設定

Tenable Identity Exposure は、特定の機能を動作させるために、監視対象の Active Directory でいくつかの設定が必要です。

- AD オブジェクトまたはコンテナへのアクセス
- 特権分析のアクセス
- 攻撃インジケーターのデプロイメント

AD オブジェクトまたはコンテナへのアクセス

注意: このセクションは、露出インジケーターモジュールの Tenable Identity Exposure ライセンスにのみ適用されます。

Tenable Identity Exposure は、セキュリティ監視を達成するために管理者権限を必要としません。

このアプローチは、ドメインに保存されているすべての Active Directory オブジェクト (ユーザーアカウント、組織単位、グループなど) を読み取るために Tenable Identity Exposure が使用するユーザーアカウントの機能に依存しています。

ほとんどのオブジェクトはデフォルトで、Tenable Identity Exposure サービスアカウントが使用するグループドメインユーザーに対する読み取りアクセス権を持っています。ただし、一部のコンテナは、Tenable Identity Exposure ユーザーアカウントに対する読み取りアクセスを許可するために、手動で設定する必要があります。

Tenable Identity Exposure が監視する各ドメインで読み取りアクセス権を持たせるために、手動設定が必要な Active Directory オブジェクトとコンテナの詳細を次の表に示します。

コンテナの場所	説明
`CN=Deleted Objects,DC=<DOMAIN>,DC=<TLD>`	削除されたオブジェクトをホストするコンテナ
`CN=Password Settings Container,CN=System, DC=<DOMAIN>,DC=<TLD>`	(オプション) パスワード設定オブジェクトをホストするコンテナ

AD オブジェクトまたはコンテナへのアクセスを許可するには

- ドメインコントローラーのコマンドラインインターフェースで、次のコマンドを実行して、Active Directory オブジェクトまたはコンテナへのアクセスを許可します。

  注意: Tenable Identity Exposure が監視する各ドメインでこのコマンドを実行する必要があります。

  ```
  dsacls "<__CONTAINER__>" /takeownership
  dsacls "<__CONTAINER__>" /g <__SERVICE_ACCOUNT__>:LCRP /I:T
  ```

各部の説明

- <__CONTAINER__> は、アクセスを必要とするコンテナを表します。
- <__SERVICE_ACCOUNT__> は、Tenable Identity Exposure が使用するサービスアカウントを表します。

特権分析のアクセス

オプションの特権分析機能には、管理者権限が必要です。Tenable Identity Exposure が使用するサービスアカウントにアクセス許可を割り当てる必要があります。

詳細は、特権分析 を参照してください。

注意: 特権分析を有効にする各ドメインでアクセス許可を割り当てる必要があります。

コマンドラインを使用してアクセス許可を割り当てるには

要件: アクセス許可を割り当てるには、ドメイン管理者の権限または同等の権限を持つアカウントが必要です。

- ドメインコントローラーのコマンドラインインターフェースで次のコマンドを実行して、両方のアクセス許可を追加できます。

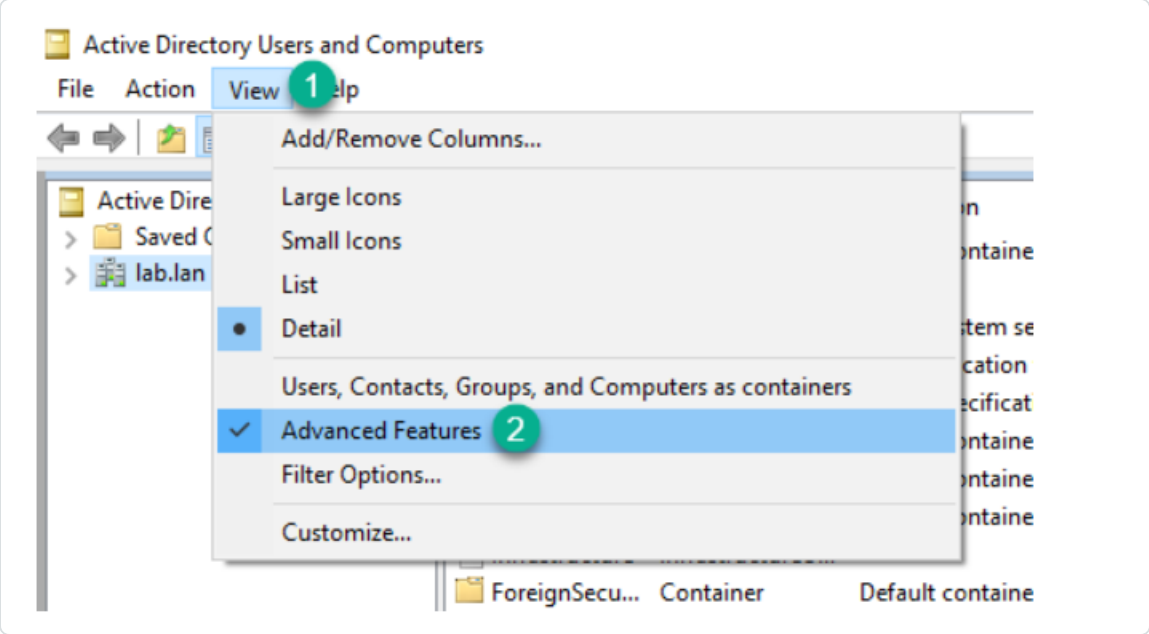
```
dsacls "<__DOMAIN_ROOT__>"  /g "<__SERVICE_ACCOUNT__>:CA;Replicating Directory Changes" "<__
SERVICE_ACCOUNT__>:CA;Replicating Directory Changes All"
```

  各部の説明

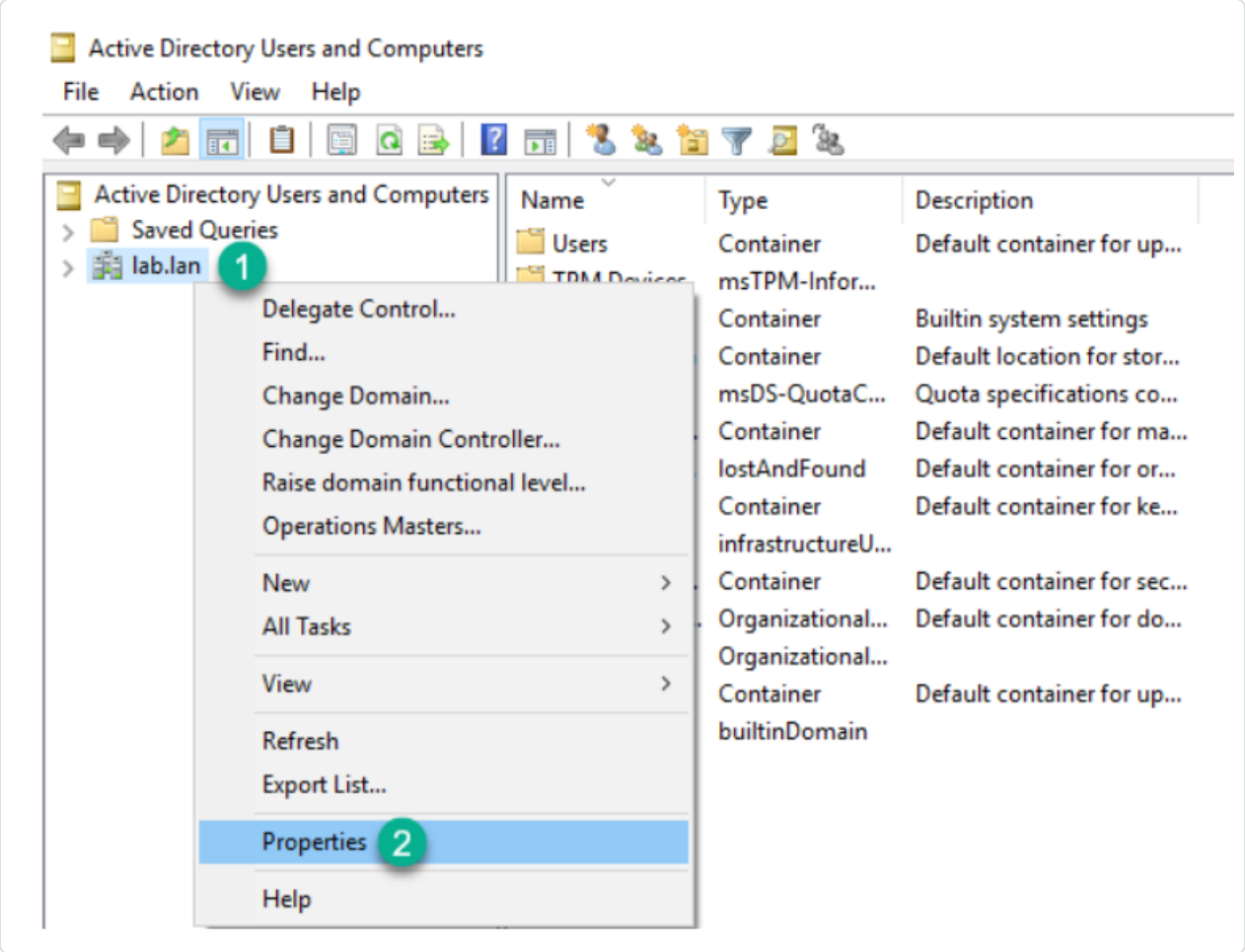
  - <__DOMAIN_ROOT__> は、ドメインのルートの識別名を表します。例:「DC=<DOMAIN>,DC=<TLD>」
  - <__SERVICE_ACCOUNT__> は、Tenable Identity Exposure が使用するサービスアカウントを表します。例:「DOMAIN\tenablead」

グラフィカルユーザーインターフェースを使用してアクセス許可を割り当てるには

1. Windows の **[スタート]** メニューから、**[Active Directory ユーザーとコンピューター]** を開きます。
2. **[表示]** メニューから **[拡張機能]** を選択します。

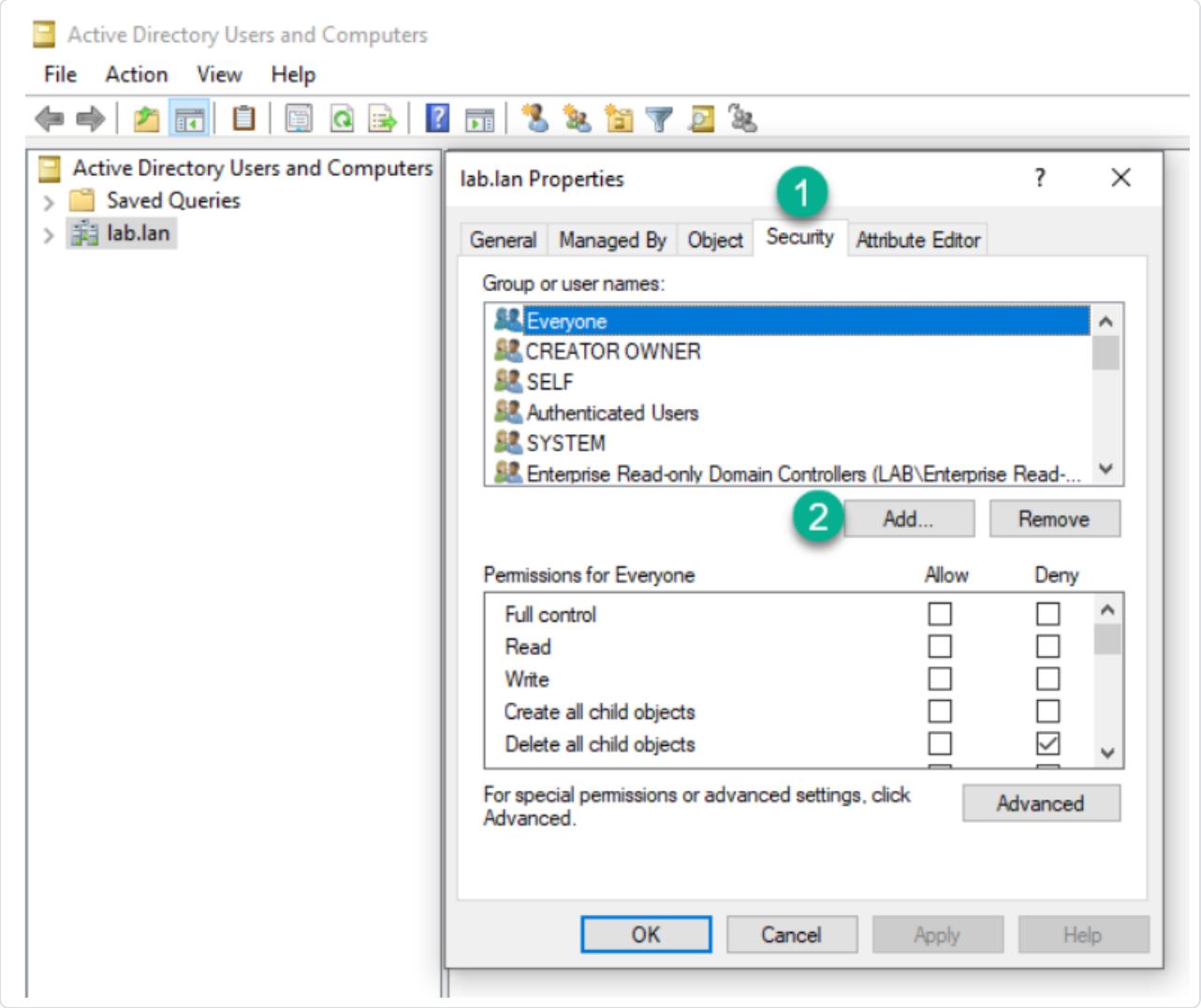


3. ドメインルートを右 クリックし、**[プロパティ]** を選 択します。



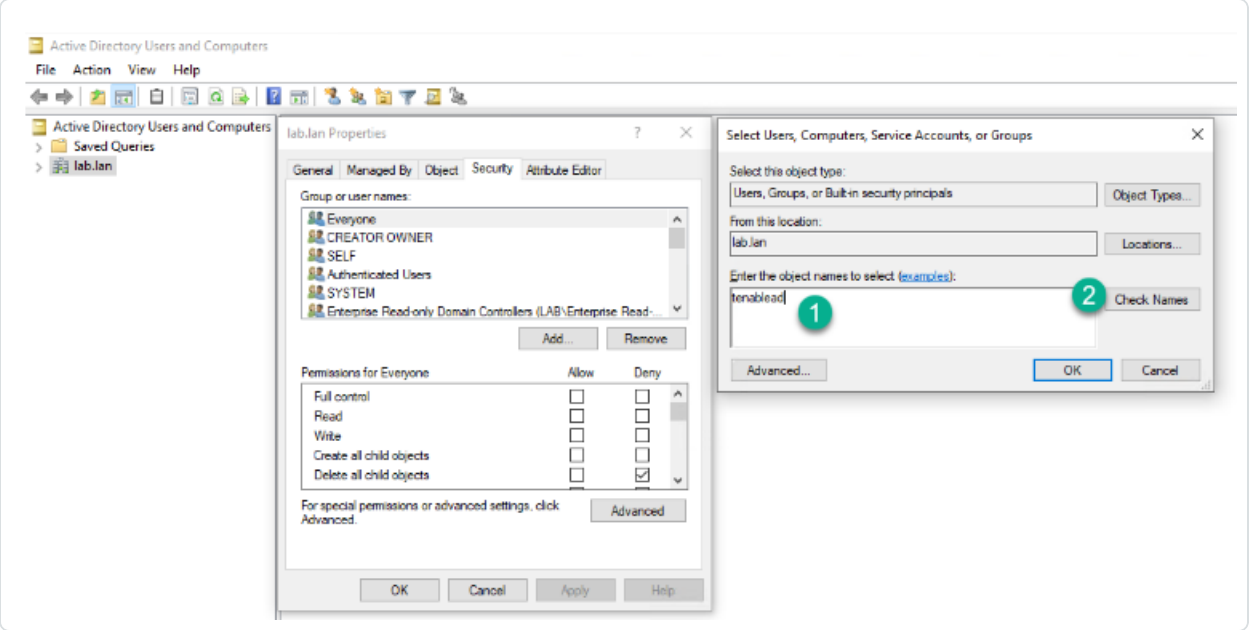
ドメインルートのプロパティペインが開きます。

4. **[セキュリティ]** タブをクリックし、**[追加]** をクリックします。



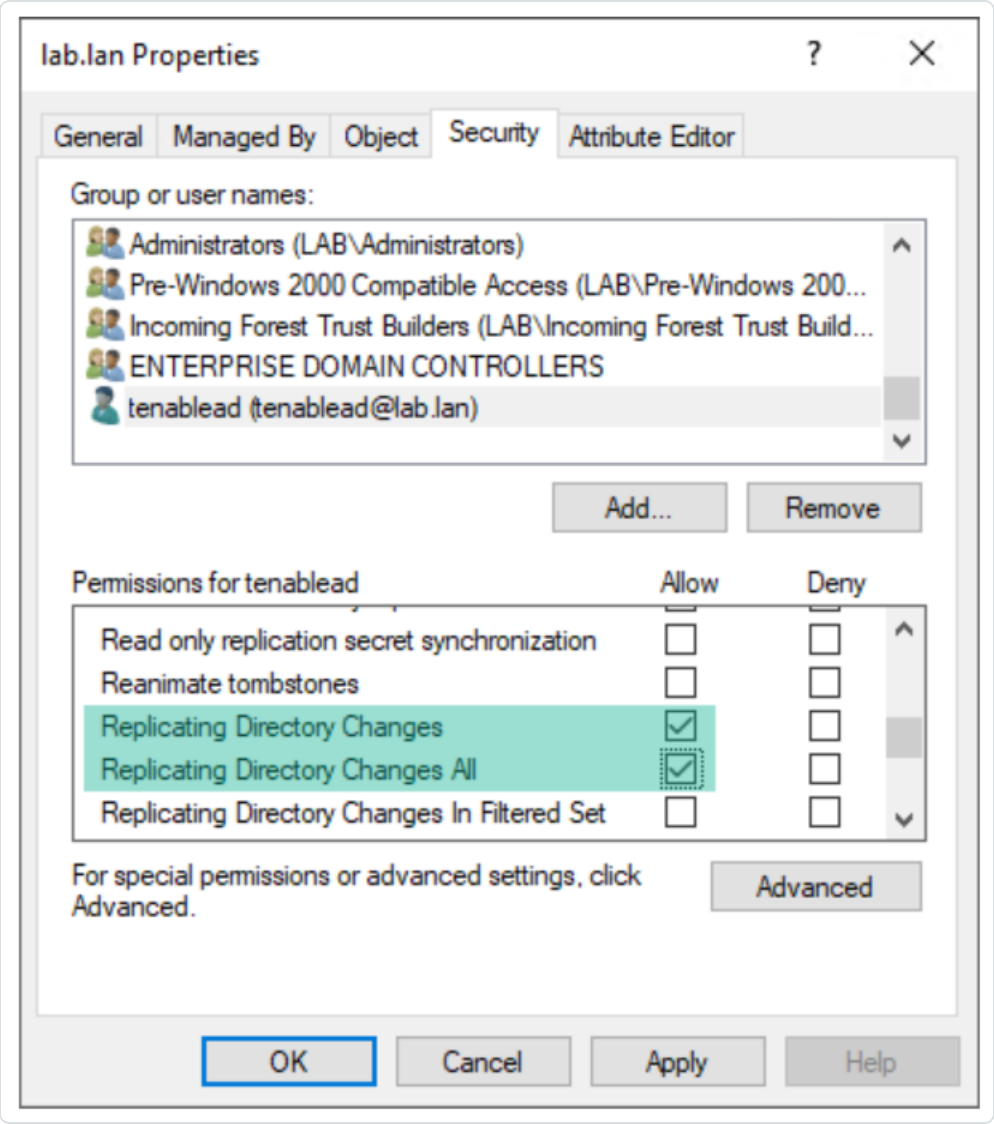
5. Tenable Identity Exposure サービスアカウントを見つけます。

注意: 複数のドメイン環境があるフォレストでは、サービスアカウントが別の Active Directory ドメインにある可能性があります。



6. リストを下にスクロールし、デフォルトで設定されているすべてのアクセス許可を選択解除します。

7. **[許可]** 列で、*[ディレクトリ変更の複製]* と *[すべてのディレクトリ変更の複製]* の両方のアクセス許可を選択します。



8. **[OK]** をクリックします。

重要事項

Tenable Identity Exposure に必要なサービスアカウントはフォレストごとに 1 つだけです。そのため、ドメインでアクセス許可を割り当てる際に、**別のドメインのサービスアカウントを検索**する必要がある場合があります。

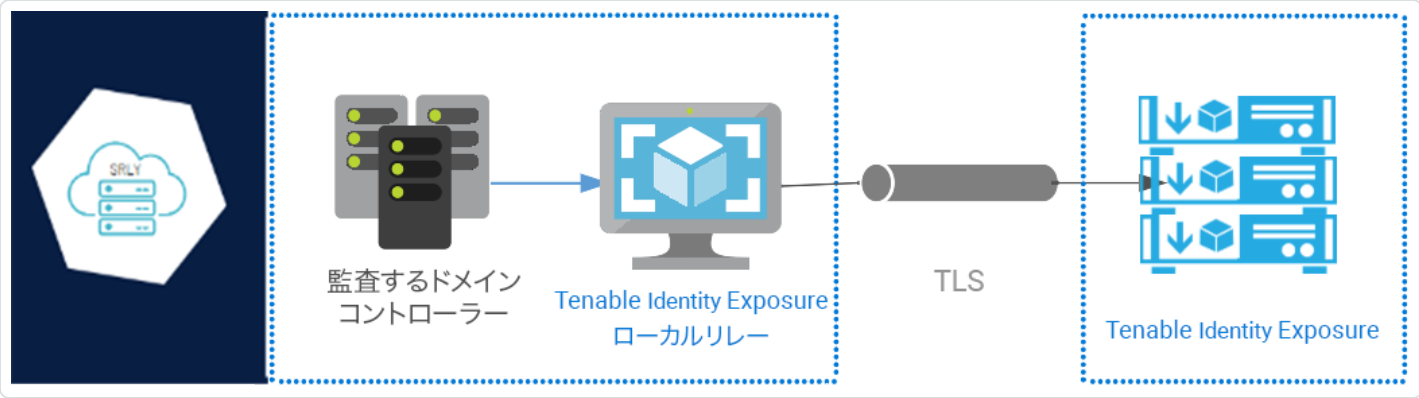
追加のアクセス許可は**ドメインルートレベルで**割り当てる必要があります。Active Directory は、組織単位または特定のユーザーに割り当てられるアクセス許可 (たとえば、特権分析を組織単位 (OU) またはユーザーに制限するアクセス許可) をサポートしていないため、何の影響も及ぼしません。

これらのアクセス許可により、Tenable Identity Exposure サービスアカウントに、Active Directory ドメインに対してより強い権限が付与されます。その後、これを**特権アカウント (Tier 0)** と見なし、ドメイン管理者アカウントと同様に保護する必要があります。全手順については、サービスアカウントの保護を参照してください。

セキュアリレー

セキュアリレーとは、この図に示すように、VPN の代わりに Transport Layer Security (TLS) を使用して、ネットワークから Tenable Identity Exposure に Active Directory データを転送する転送モードのことです。ネットワークがインターネットに到達するためにプロキシサーバーを必要とする場合、リレー機能は認証のあるまたはない HTTP プロキシもサポートします。

Tenable Identity Exposure は、お客様のニーズに応じてドメインにマッピングできる複数のセキュアリレーをサポートすることができます。

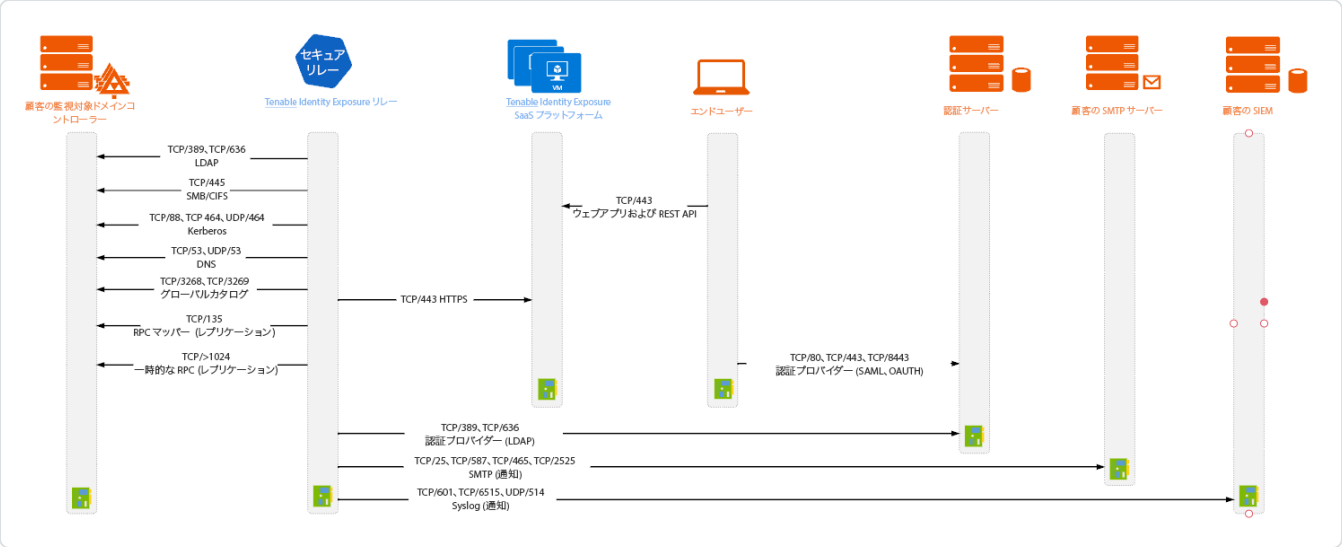


注意: 現在、セキュアリレー機能は、Tenable Identity Exposure がセキュアリレーを使用するようにプラットフォームをプロビジョニングしている場合にのみ適用されます。プロビジョニングを VPN からセキュアリレーに手動で切り替えることはできません。VPN からセキュアリレーにプラットフォームを移行する際に支援が必要な場合は、Tenable Identity Exposure カスタマーサポート担当者にご連絡ください。

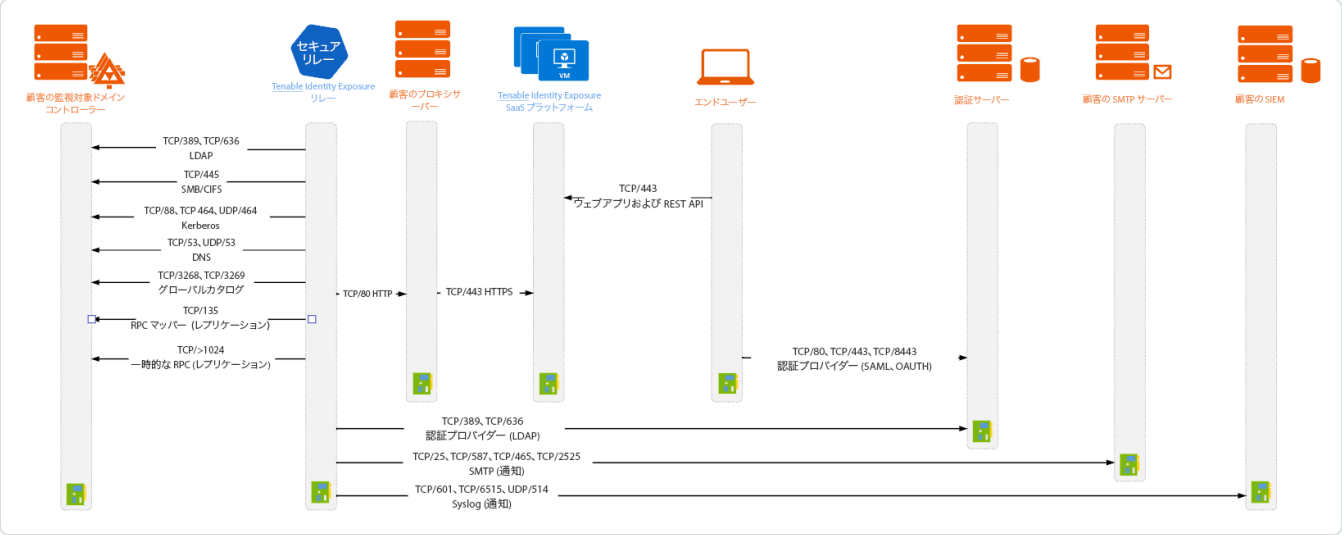
ネットワークフロー

セキュアリレーに必要なポート

- **プロキシサーバーのない**従来のセットアップの場合、リレーには次のポートが必要です。



- **プロキシサーバーを使用した**セットアップの場合、リレーには次のポートが必要です。



TLS 要件

TLS 1.2 を使用するには、2024 年 1 月 24 日の時点で、リレーサーバーが次の暗号化パッケージのうち少なくとも 1 つをサポートしている必要があります。

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

また、リレー機能との互換性のために、Windows の設定が、指定された暗号化パッケージと一致していることを確認してください。

暗号化スイートを確認するには

1. PowerShell で次のコマンドを実行します。

```
@("TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256", "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384", "TLS_ECDHE_
RSA_WITH_CHACHA20_POLY1305_SHA256") | % { Get-TlsCipherSuite -Name $_ }
```

2. 出力 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 を確認します。

```
PS C:\Users> @("TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256", "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384"
, "TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256") | % { Get-TlsCipherSuite -Name $_ }


KeyType               : 0
Certificate           : RSA
MaximumExchangeLength : 65536
MinimumExchangeLength : 0
Exchange              : ECDH
HashLength            : 0
Hash                  :
CipherBlockLength     : 16
CipherLength          : 128
BaseCipherSuite       : 49199
CipherSuite           : 49199
Cipher                : AES
Name                  : TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
Protocols             : {771, 65277}

KeyType               : 0
Certificate           : RSA
MaximumExchangeLength : 65536
MinimumExchangeLength : 0
Exchange              : ECDH
HashLength            : 0
Hash                  :
CipherBlockLength     : 16
CipherLength          : 256
BaseCipherSuite       : 49200
CipherSuite           : 49200
Cipher                : AES
Name                  : TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Protocols             : {771, 65277}
```

3. 出力が空白の場合、リレーの TLS 接続が機能するために必要な暗号化パッケージがどれも有効になっていないことを示します。少なくとも 1 つの暗号化パッケージを有効にします。

4. リレーサーバーの楕円曲線暗号 (ECC) 曲線を検証します。この検証は、ECDHE (Elliptic Curve Diffie-Hellman Ephemeral) 暗号化スイートを使用する場合に必須です。PowerShell で次のコマンドを実行します。

```
Get-TlsEccCurve
```

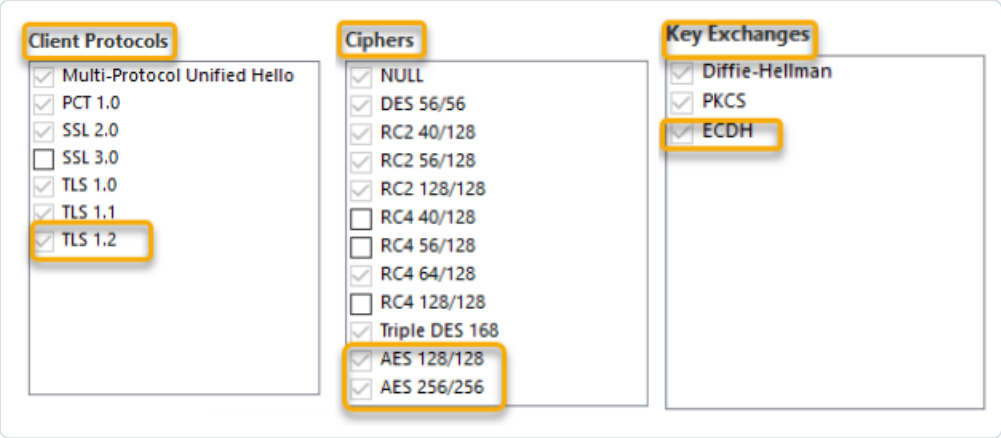
5. 曲線 **25519** があることを確認します。有効になっていない場合は有効にします。

```
PS C:\Users> Get-TlsEccCurve
curve25519
NistP256
NistP384
```

Windows の暗号化設定を検証するには

1. IIS Crypto ツールで、次のオプションが有効になっていることを確認します。

   - クライアントプロトコル: **TLS 1.2**
   - 暗号: **AES 128/128** および **AES 256/256**
   - 鍵交換: **ECDH**



2. 暗号化設定を変更した後、マシンを再起動します。

> **注意**: Windows の暗号化設定を変更すると、マシン上で実行され、「Schannel」として知られる Windows TLS ライブラリを使用するすべてのアプリケーションに影響します。したがって、調整によって意図しない問題が発生しないようにしてください。選択した設定が、組織の全体的な強化目標またはコンプライアンス要件に適合していることを確認します。

始める前に

前提条件

仮想マシン

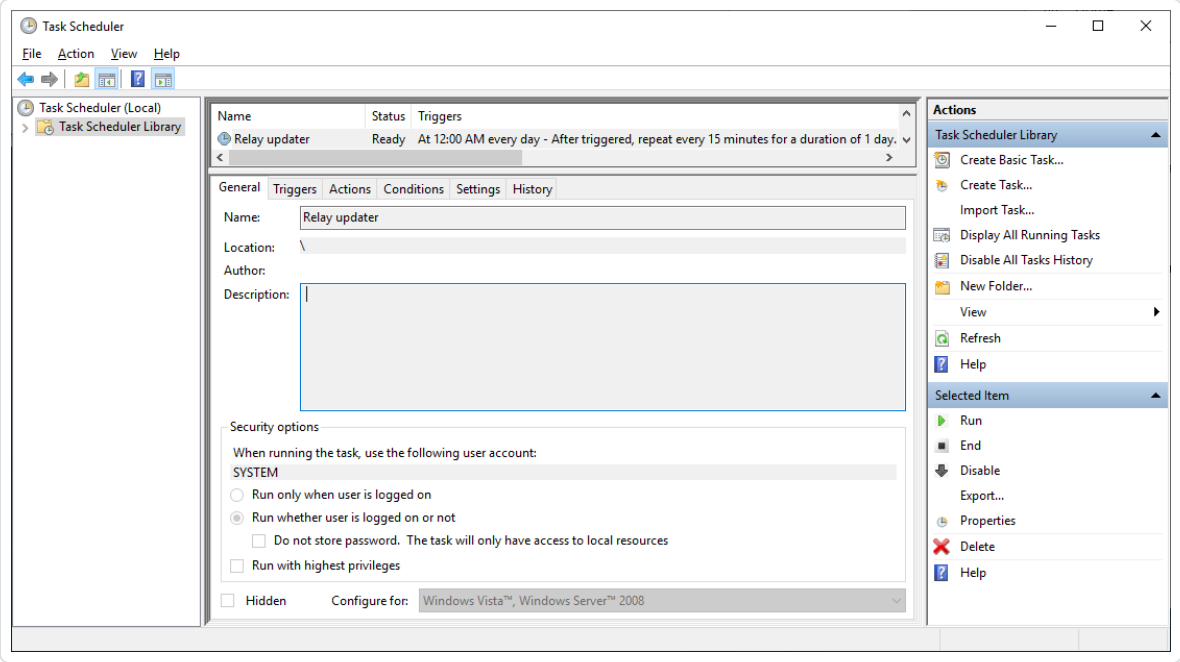
セキュアリレーをホストする仮想マシン(VM)の要件は次のとおりです。

顧客の規模	Tenable Identity Exposure サービス	必要なインスタンス	メモリ(インスタンスごと)	vCPU(インスタンスごと)	ディスクトポロジ	利用可能なディスク容量(インスタンスごと)
任意のサイズ	• Tenable_Relay • tenable_envoy	1	8 GB の RAM	2 vCPU	システムパーティションとは別のログ用パーティション	30 GB

VM には次のものも必要です。

- Windows Server 2016 以降のオペレーティングシステム(Linux 以外)
- 解決済みのインターネットに接続した DNS のクエリと、少なくとも `cloud.tenable.com` および `*.tenable.ad` に対するインターネットアクセス(TLS 1.2)
- ローカル管理者権限
- EDR、ウイルス対策、GPO 設定
    - VM に十分な CPU が残っている – たとえば、Windows Defender のリアルタイム保護機能は、CPU 使用率がかなり高く、マシンを飽和させる可能性があります。
    - 自動更新
        - `*.tenable.ad` への呼び出しを許可し、自動更新機能がリレー実行可能ファイルをダウンロードできるようにします。

- 自動更新機能をブロックしているグループポリシーオブジェクト (GPO) がないことを確認します。
- 「リレーアップデーター」のスケジュールタスクを削除したり変更したりしないでください。



ロールのアクセス許可

リレーを設定するには、ロールベースのアクセス許可を持つユーザーである必要があります。必要なアクセス許可は次のとおりです。

- **データエンティティ**: エンティティリレー
- **インターフェースエンティティ**
  - [管理] > [システム] > [設定] > [アプリケーションサービス] > [リレー]
  - [管理] > [システム] > [リレー管理]

詳細は、ロールのアクセス許可の設定 を参照してください。

許可されたファイルとプロセス

リレーをスムーズに動作させるには、特定のファイルとプロセスをアンチウイルスや EDR (エンドポイント検知・対応)、XDR (拡張検知・対応) などのサードパーティセキュリティツールに許可します。

次のファイルとプロセスを許可します。

注意: C:\ パスをリレーのインストールドライブに合わせて変更してください。

Windows
ファイル
C:\Tenable*
C:\tools*
C:\ProgramData\Tenable*
プロセス
nssm.exe --> **パス**: C:\tools\nssm.exe
Tenable.Relay.exe --> **パス**: C:\Tenable\Tenable.ad\SecureRelay\Tenable.Relay.exe
envoy.exe --> **パス**: C:\Tenable\Tenable.ad\SecureRelay\envoy.exe
updater.exe --> **パス**: C:\Tenable\Tenable.ad\updater.exe
powershell.exe --> **パス**: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe (OS のバージョンによって異なる場合があります)
スケジュールされたタスク
C:\Windows\System32\Tasks\Relay updater
C:\Windows\System32\Tasks\Manual Renew Apikey
C:\Windows\System32\Tasks\Tenable\Tenable.ad\SecureRelay\CompressLogsSecureRelay
C:\Windows\System32\Tasks\Tenable\Tenable.ad\SecureRelay\RemoveLogsSecureRelay
レジストリキー

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Tenable\Tenable.ad Secure Relay

リンクキー

セキュアリレーのインストールには、ネットワークのアドレスと認証トークンを含む使い捨てのリンクキーが必要です。Tenable Identity Exposure は、セキュアリレーのインストールが成功するたびに新しいキーを再生成します。

リンクキーを取得するには

1. Tenable Identity Exposure で、左側のメニューバーの **[システム]** をクリックし、**[設定]** タブ > **[リレー]** の順に選択します。

2. をクリックしてリンクキーをコピーします。

インストール

セキュアリレーをインストールするには

- インストール方法を選択してください。
  - セキュアリレーのインストール(GUI)
  - セキュアリレーのインストール(Tenable Nessus Agent)

アンインストール

セキュアリレーをアンインストールするには

1. Windows で、**[設定]** > **[アプリと機能]** > **[Tenable Identity Exposure セキュアリレー]** の順に移動します。
2. **[アンインストール]** をクリックします。

   アンインストールが完了すると、Tenable Identity Exposure セキュアリレーサービスと環境変数がシステムに表示されなくなります。
3. Tenable Identity Exposure で、左側のメニューバーの **[システム]** をクリックし、**[リレー管理]** タブを選択します。
4. アンインストールしたばかりのリレーを選択し、  をクリックして使用可能なリレーのリストから削除します。

自動更新

セキュアリレーをインストールすると、Tenable Identity Exposure は新しいバージョンを定期的にチェックするようになります。このプロセスは完全に自動化されており、ドメインへの HTTPS アクセス (TCP/443) が必要です。ネットワークトレイのアイコンは、Tenable Identity Exposure がセキュアリレーを更新していることを示します。プロセスが完了すると、Tenable Identity Exposure サービスが再起動しデータ収集が再開されます。

関連項目

セキュアリレーの詳細については、Tenable Identity Exposure 管理者ガイドのセキュアリレーを参照してください。

セキュアリレーのインストール(GUI)

次の手順では、Windows インストーラーを使用してセキュアリレーをインストールします。始める前に、セキュアリレーで説明されているように、必要な前提条件を満たしており、**必須のリンクキー**があることを確認してください。

セキュアリレーをインストールするには

1. Tenable Identity Exposure ダウンロードポータルから仮想マシンにインストーラーをダウンロードします。
2. ファイル `tenable.ad_SecureRelay_v3.xx.x` をダブルクリックして、インストールウィザードを開始します。

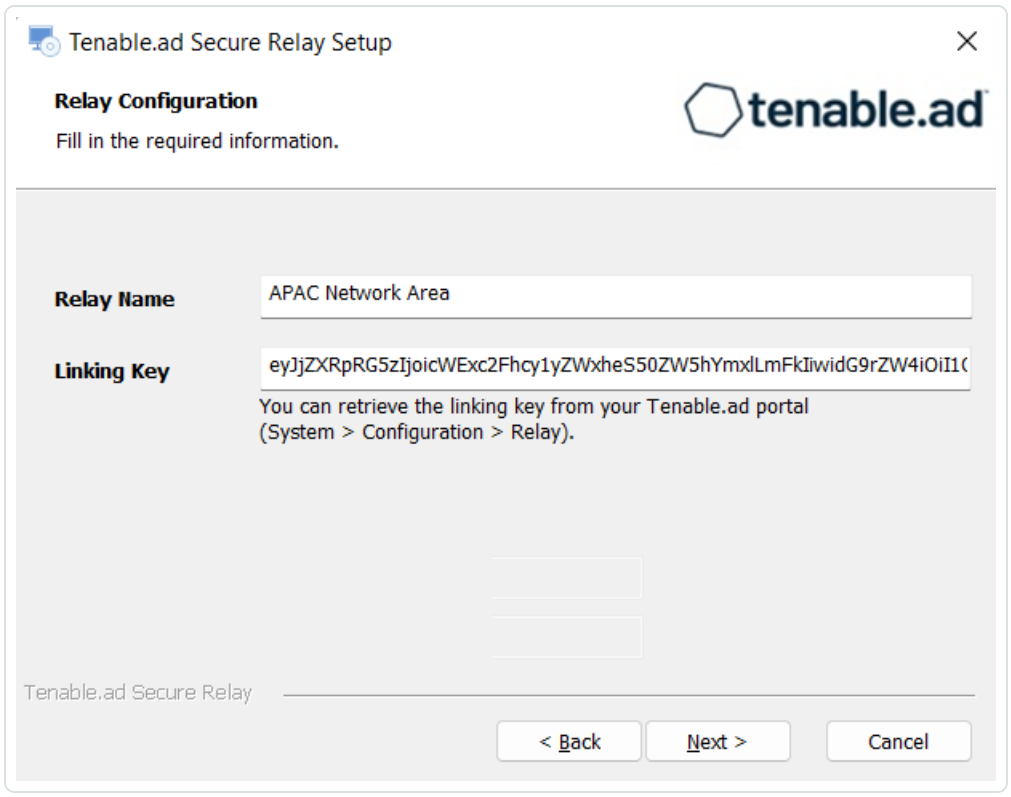
   [ようこそ] 画面が表示されます。

3. **[次へ]** をクリックします。

   [カスタムセットアップ] ウィンドウが表示されます。

4. **[参照]**をクリックして、セキュアリレー用に予約した(システムパーティションとは別の)ディスクパーティションを選択します。
5. **[次へ]**をクリックします。

   [リレー設定]ウィンドウが表示されます。



6. 以下の情報を入力します。

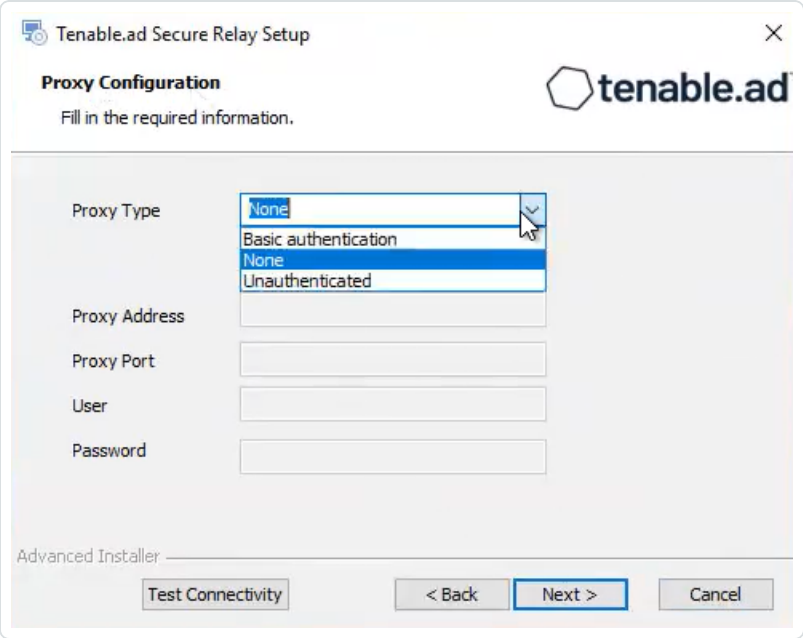
   a. **[リレー名]** ボックスに、セキュアリレーの名前を入力します。

   b. **[リンクキー]** ボックスに、Tenable Identity Exposure ポータルから取得したリンクキーを貼り付けます。

   c. プロキシサーバーを使用する場合は、**[リレー呼び出しに HTTP プロキシを使用する]** オプションを選択し、プロキシアドレスとポート番号を入力します。

7. **[次へ]** をクリックします。

   プロキシ設定ウィンドウが表示されます。



8. 次のいずれかのオプションを選択します。

    a. **なし**: プロキシサーバーを使用しません。

    b. **非認証**: プロキシサーバーのアドレスとポートを入力します。

    c. **基本認証**: アドレスとポートに加えて、プロキシサーバーのユーザーとパスワードを入力します。

    注意:「非認証」または「基本認証」を使用してプロキシを設定するために、リレーは IPv4 アドレス (`192.168.0.1` など) または `http://` や `https://` のないプロキシ URI (`myproxy.mycompany.com` など) のみをサポートし、IPv6 アドレス (`2001:0db8:85a3:0000:0000:8a2e:0370:7334` など) はサポートしません。

9. **[接続をテストする]** をクリックします。次のいずれかが発生します。

    - **緑色のライト** - 接続に成功しました。
    - **無効なリンクキー** - Tenable Identity Exposure ポータルからリンクキーを取得してください。
    - **無効なリレー名** - このボックスは空のままにできません。リレーの名前を入力します。
    - **接続に失敗しました** - インターネットアクセスを確認してください。

10. **[次へ]** をクリックします。

    [インストールの準備完了] ウィンドウが表示されます。

11. **[インストール]**をクリックします。
12. インストールが完了したら、**[終了]**をクリックします。

次の手順

- インストール後のチェック

関連項目

- セキュアリレー
- セキュアリレーのインストール(Tenable Nessus Agent)
- インストール後のチェック
- リレーを設定する

セキュアリレーのインストール(Tenable Nessus Agent)

次の手順では、Tenable Nessus Agent を使用してセキュアリレーをインストールします。

始める前に

- Tenable Nessus Agent がダウンロードされてインストールされていることを確認します。

  注意: Tenable Nessus Agent インストールプログラムは、エージェントキーを要求します。このキーはセキュアリレー機能には**必要ありません**。

- セキュアリレーの説明に従って、必要な前提条件を満たし、**必要なリンクキー**を用意してください。

セキュアリレーをインストールするには

1. Tenable Nessus Agent をホストして、リレーとして機能するマシンの Tenable Nessus Agent ディレクトリ(`c:\Program Files\Tenable\Nessus Agent`)で管理者コマンドプロンプトウィンドウを開き、次のコマンドを入力します。

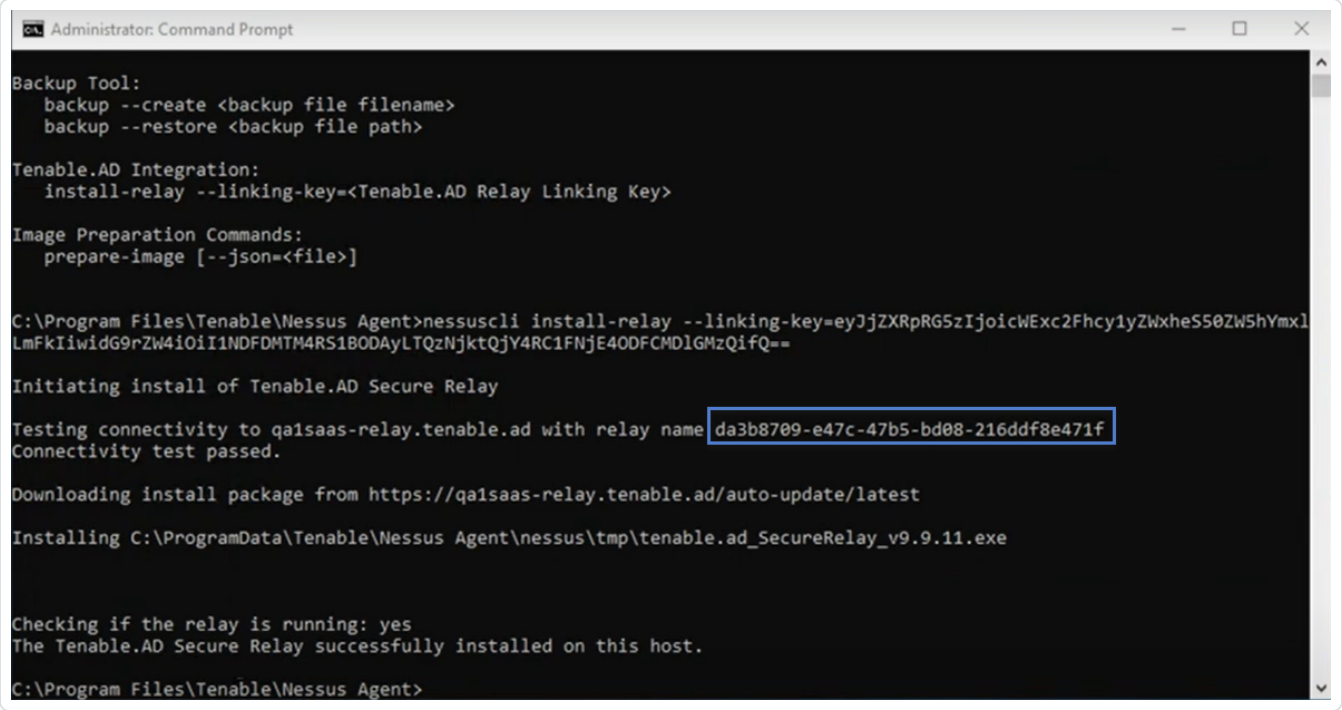
   セキュアリレーのインストール

   ```
   nessuscli install-relay --linking-key=<Relay Linking Key> --proxy-host=<Customer Proxy IP or DNS> --proxy-port=<Customer Proxy Port>
   ```

2. <Tenable Identity Exposure Relay Linking Key>を Tenable Identity Exposure インスタンスからあらかじめコピーしてあった値に置き換えます。プロキシサーバーを使用する場合は、プロキシアドレスとポート番号を指定します。

   インストールが開始されます。数分かけて接続性チェックとインストールプロセスが実行されます。

   インストールが正常に完了すると、リレーがホストマシンで実行されていることを示すメッセージが表示されます。



3. Tenable Identity Exposure で、**[システム]** > **[リレー管理]** をクリックします。新しくインストールされたリレーが、インストールウィンドウに表示された識別子とともにリレーのリストに表示されます。

次の手順

- インストール後のチェック

関連項目

- セキュアリレー
- セキュアリレーのインストール(GUI)
- インストール後のチェック
- リレーを設定する

インストール後のチェック

セキュアリレーのインストールが完了したら、次の点を確認してください。

Tenable Identity Exposure にインストールされているリレーのリスト

インストールされているリレーのリストを表示するには

- Tenable Identity Exposure で、左側のメニューバーの **[システム]** をクリックし、**[リレー管理]** タブを選択します。

  このペインには、セキュアリレーとそのリンクされたドメインのリストが表示されます。

サービス

インストールが成功すると、次のサービスが実行されます。

- `Tenable_Relay`
- `tenable_envoy`

  > **注意**: Envoy ライセンスは、Tenable Identity Exposureの**[システム]** > **[法的情報]** > **[Envoy ライセンス]** にあります。

環境変数

インストールの際には、名前が「ALSID」で始まるセキュアリレーに関連する 4 つの新しい環境変数も追加されます。プロキシサーバーの使用を選択した場合、プロキシ IP およびポートに関連する 2 つの追加の変数が存在します。

トラブルシューティング用のログ

ログは次の場所にあります。

- **インストールログ**: `C:\Users\<your user>\AppData\Local\Temp`
- **リレーログ**: インストール時に指定されたフォルダー内のセキュアリレーをホストしている VM 上

次の手順

- リレーを設定する

関連項目

- セキュアリレー
- セキュアリレーのインストール(GUI)
- セキュアリレーのインストール(Tenable Nessus Agent)

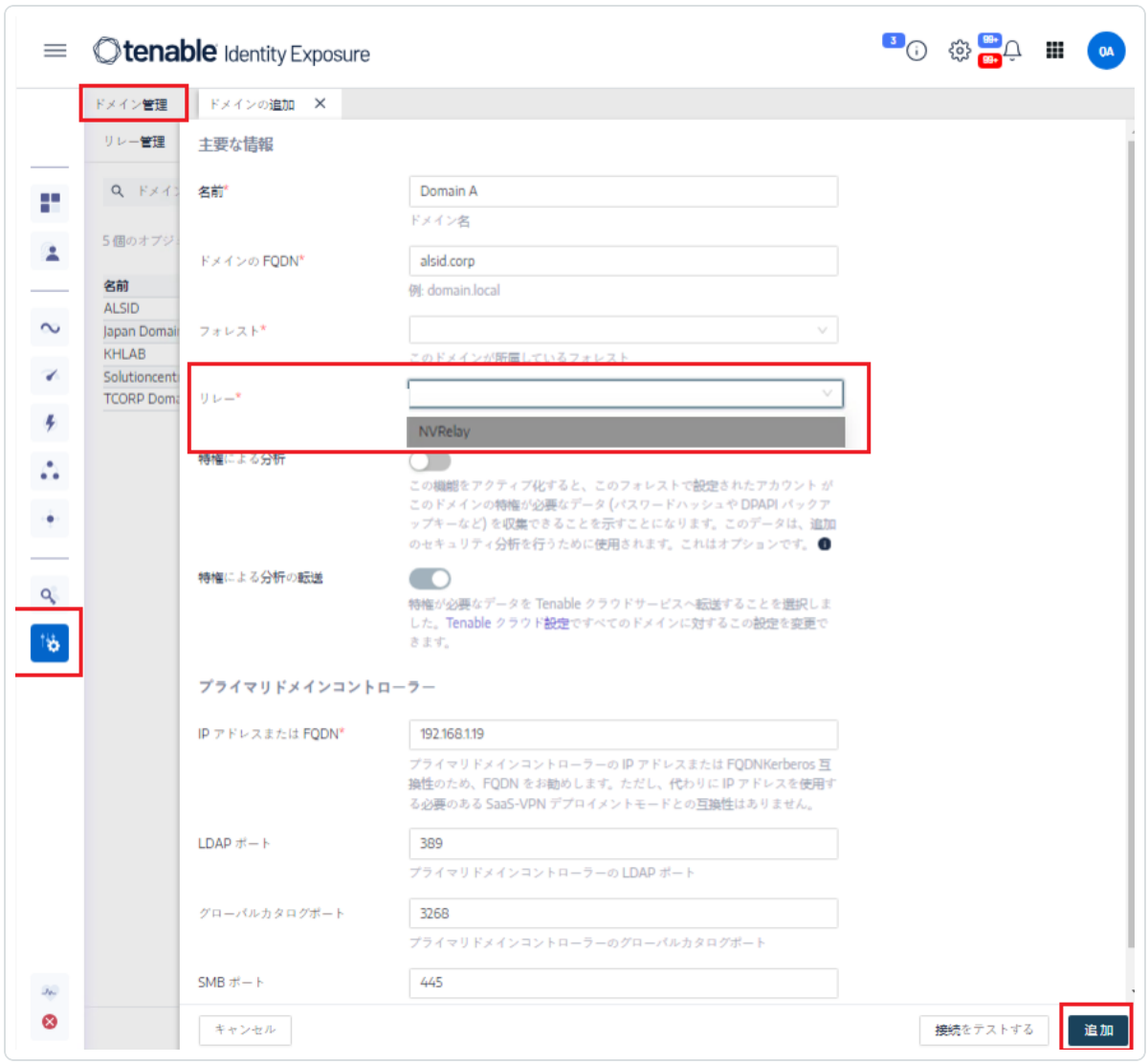
リレーを設定する

インストール時およびインストール後のチェックの後、Tenable Identity Exposure でリレーを設定してドメインにリンクし、アラートを設定します。

ドメインをセキュアリレーにリンクするには

1. Tenable Identity Exposure で、左側のメニューバーの **[システム]** をクリックし、**[ドメイン管理]** タブを選択します。
2. ドメインのリストで、リンクするドメインを選択し、行の末尾にある をクリックします。

   [ドメインの編集] ペインが開きます。
3. **[リレー]** ボックスの矢印をクリックして、インストールされているリレーのドロップダウンリストを表示し、ドメインにリンクするリレーを選択します。



4. **[編集]**をクリックします。

   Tenable Identity Exposure がドメインを更新したことを確認するメッセージが表示されます。Sysvol と LDAP が同期し、変更が含められます。イベント情報が新しいイベントの受信を開始します。

関連項目

- セキュアリレー
- セキュアリレーのインストール(GUI)
- セキュアリレーのインストール(Tenable Nessus Agent)
- インストール後のチェック

攻撃インジケーターのデプロイメント

注意: この情報は、攻撃インジケーターモジュールの恩恵を受けるライセンスにのみ適用されます。

Tenable Identity Exposure の **攻撃インジケーター** (IoA) により、Active Directory (AD) に対する攻撃を検出することができます。各 IoA には、インストールスクリプトによって自動的に有効にされる特定の監査ポリシーが必要です。Tenable Identity Exposure の IoA とその実装の完全なリストについては、Tenable ダウンロードポータルの Tenable Identity Exposure の攻撃インジケーターリファレンスガイドを参照してください。

攻撃インジケーターと Active Directory

Tenable Identity Exposure は、エージェントをデプロイすることなく環境内の設定変更を最小限にして、Active Directory インフラを監視する非侵入型ソリューションとして機能します。

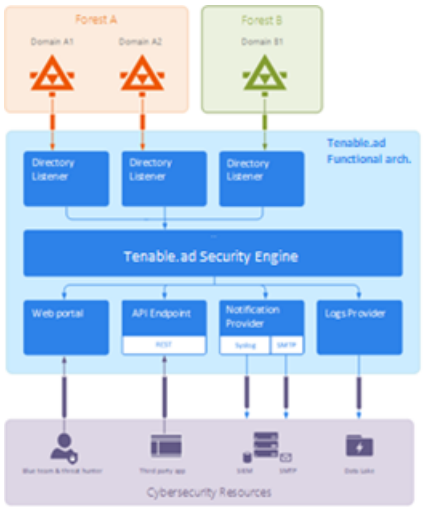
Tenable Identity Exposure は、管理アクセス許可のない通常のユーザーアカウントを使用して標準 API に接続し、そのセキュリティ監視機能を使用します。

Tenable Identity Exposure は、Active Directory レプリケーションメカニズムを利用して関連情報を取得しています。これにより、各ドメインの PDC と Tenable Identity Exposure のディレクトリリスナーの間で必要になる帯域幅コストは限定的なものになります。

Tenable Identity Exposure は、攻撃インジケーターを使用してセキュリティインシデントを効率的に検出するために、Event Tracing for Windows (ETW) の情報と各ドメインコントローラーで利用可能なレプリケーションメカニズムを使用します。この一連の情報を収集するには、攻撃インジケーターのインストールで説明されているように、Tenable Identity Exposure のスクリプトを使用して専用のグループポリシーオブジェクト (GPO) をデプロイします。

この GPO は、システムボリューム (SYSVOL) に書き込むすべてのドメインコントローラーで Windows EvtSubscribe API を使用してイベントログリスナーをアクティブにし、AD のレプリケーションエンジンと Tenable Identity Exposure の SYSVOL イベントをリッスンする機能を利用します。GPO は各ドメインコントローラーの SYSVOL にファイルを作成し、そのコンテンツを定期的にフラッシュします。

セキュリティ監視を開始するために、Tenable Identity Exposure は Microsoft の標準ディレクトリ API とやり取りする必要があります。



ドメインコントローラー

Tenable Identity Exposure が必要とするのは、Network Flow Matrix (ネットワークフローマトリクス) で説明されているネットワークプロトコルを使用するプライマリドメインコントローラーエミュレーター (PDCe) との通信のみです。

複数のドメインまたはフォレストが監視対象となている場合、Tenable Identity Exposure は各ドメインの PDCe に到達する必要があります。最高のパフォーマンスを得るために、Tenable は監視する PDCe に近い物理ネットワークで Tenable Identity Exposure をホストすることを推奨します。

ユーザーアカウント

Tenable Identity Exposure は、非管理者ユーザーアカウントを使用して監視対象のインフラに認証し、レプリケーションフローにアクセスします。

単純な Tenable Identity Exposure ユーザーは、収集されたすべてのデータにアクセスできます。Tenable Identity Exposure は、認証情報、パスワードハッシュ、Kerberos キーなどのシークレット属性にはアクセスしません。

Tenable は、次のようなサービスアカウントを作成し、それを「ドメインユーザー」グループのメンバーにすることを推奨しています。

- サービスアカウントはメインの監視対象ドメインにある。
- サービスアカウントは、任意の組織単位 (OU)にある。できれば、ほかのセキュリティサービスアカウントもそこで作成する。

- サービスアカウントは、標準のユーザーグループメンバーである(例:ドメインユーザー AD デフォルトグループのメンバー)。

始める前に

- 技術的な変更と潜在的な影響 の説明に従って、IoA のインストールに関する制限と潜在的な影響を確認します。
- DC に Active Directory とグループポリシーの PowerShell モジュールがインストールされ、利用可能であることを確認します。
- DC が分散ファイルシステムツール機能 RSAT-DFS-Mgmt-Con を有効にしていることを確認します。有効にすると、DC のレプリケーション中は GPO を作成できないため、デプロイメントスクリプトがレプリケーションステータスをチェックできるようになります。
- Tenable Identity Exposure では、プラットフォームの中断を制限するために、オフピーク時に IoA をインストール/アップグレードすることを推奨しています。
- アクセス許可を確認する – IoA をインストールするには、次のアクセス許可のあるユーザーロールが必要です。
    - **[データエンティティ]** で、以下に対する「読み取り」アクセス権
        - すべての攻撃インジケーター
        - すべてのドメイン
    - **[インターフェースエンティティ]** で、以下に対するアクセス権
        - 管理 > システム > 設定
        - 管理 > システム > 設定 > アプリケーションサービス > 攻撃インジケーター
        - 管理 > システム > 設定 > アプリケーションサービス > 攻撃インジケーター > インストールファイルのダウンロード

  ロールベースのアクセス許可についての詳細は、ロールのアクセス許可の設定を参照してください。

関連項目

- 攻撃インジケーターのインストール
- 攻撃インジケーターインストールスクリプト
- 技術的な変更と潜在的な影響
- Microsoft Sysmon のインストール。これは、関連するシステムデータを取得するために Tenable Identity Exposure の一部の攻撃インジケーターが必要とする Windows システムツールです。
- 攻撃インジケーターのトラブルシューティング

攻撃インジケーターのインストール

必要なユーザーロール: Tenable Identity Exposure の攻撃インジケーター設定を変更するアクセス許可を持つ組織のユーザー詳細は、ロールのアクセス許可の設定 を参照してください。

Tenable Identity Exposure の攻撃インジケーター(IoA)モジュールでは、新しいグループポリシーオブジェクト(GPO)を作成し、組織単位(OU)にリンクできる管理者アカウントで PowerShell インストールスクリプトを実行する必要があります。Tenable Identity Exposure の監視対象である Active Directory ドメインに参加していて、ネットワーク経由でドメインコントローラーに到達できる任意のマシンから、このスクリプトを実行できます。

このインストールスクリプトは、各 AD ドメインに1回実行するだけで済みます。これは、作成された GPO が、イベントリスナーを既存および新規のすべてのドメインコントローラー(DC)に自動的にデプロイするからです。

さらに、「自動更新」オプションを有効にすると、IoA 設定を変更した場合でも、インストールスクリプトを再実行する必要がなくなります。

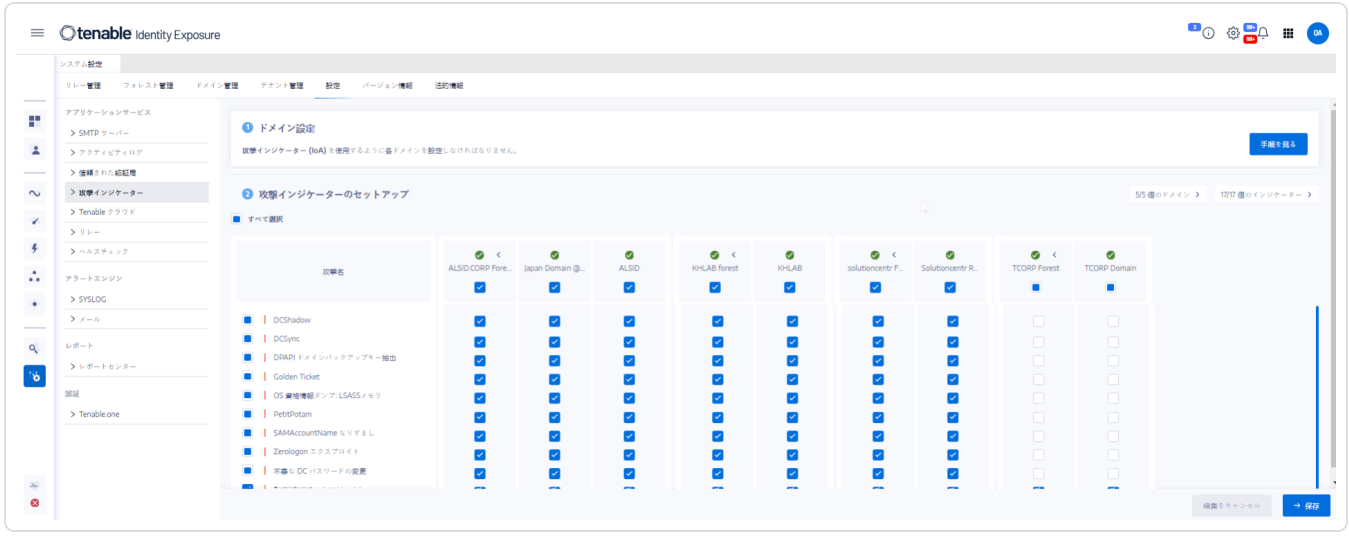
IoA のドメインを設定するには

1. Tenable Identity Exposure で、左側のメニューバーの **[システム]**をクリックして、**[設定]** タブをクリックします。

   [設定] ペインが表示されます。

2. **[攻撃インジケーター]** をクリックします。

   IoA 設定ペインが表示されます。



3. **[(1)ドメイン設定]** で、**[手順を見る]** をクリックします。

   手順ウィンドウが開きます。

4. **[今後は自動更新しますか?]** で以下を行います。

   - デフォルトオプションの **[有効]** を使用すると、今後 Tenable Identity Exposure で IoA 設定が変更されるたびに、Tenable Identity Exposure が IoA 設定を自動的に更新するようになりま

す。これにより、継続的なセキュリティ分析を確実に行うことができます。

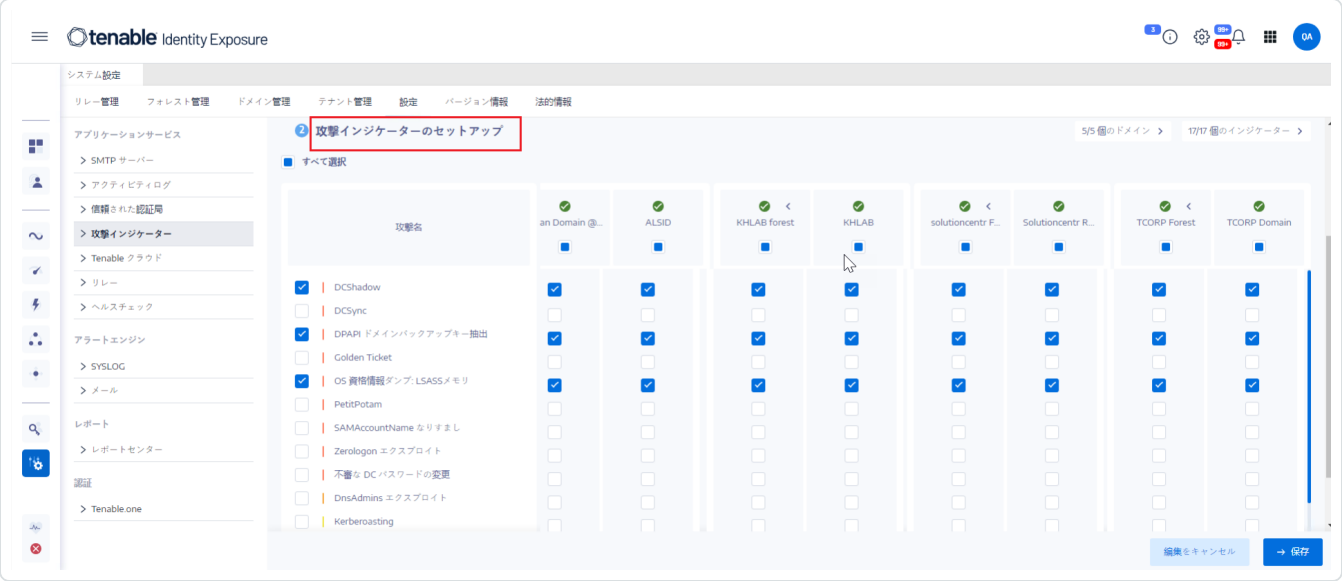
- このオプションをオフにすると、今後の自動更新を取得するためにオンにするように求めるメッセージが表示されます。**[手順を見る]** をクリックし、**[有効]** に切り替えます。

5. **[ダウンロード]** をクリックして、各ドメインに対して実行するスクリプト (`Register-TenableIOA.ps1`) をダウンロードします。
6. **[ダウンロード]** をクリックして、ドメインの設定ファイル (`TadIoaConfig-AllDomains.json`) をダウンロードします。
7. をクリックして Powershell コマンドをコピーし、ドメインを設定します。
8. 手順ウィンドウの外側をクリックして閉じます。
9. 管理者権限で PowerShell ターミナルを開き、コマンドを実行して IoA のドメインコントローラーを設定します。

> **注意**: IoA のインストールとドメインのクエリに使用するサービスアカウントには、Tenable Identity Exposure (旧 Tenable.ad) GPO フォルダーへの書き込みのアクセス許可が必要です。このアクセス許可はインストールスクリプトによって自動的に追加されます。このアクセス許可を削除すると、Tenable Identity Exposure にエラーメッセージが表示され、自動更新が機能しなくなります。詳細は、攻撃インジケーターインストールスクリプト を参照してください。

IoA をセットアップするには

1. IoA 設定ペインの**[攻撃インジケーターのセットアップ]**で、設定に含める IoA を選択します。

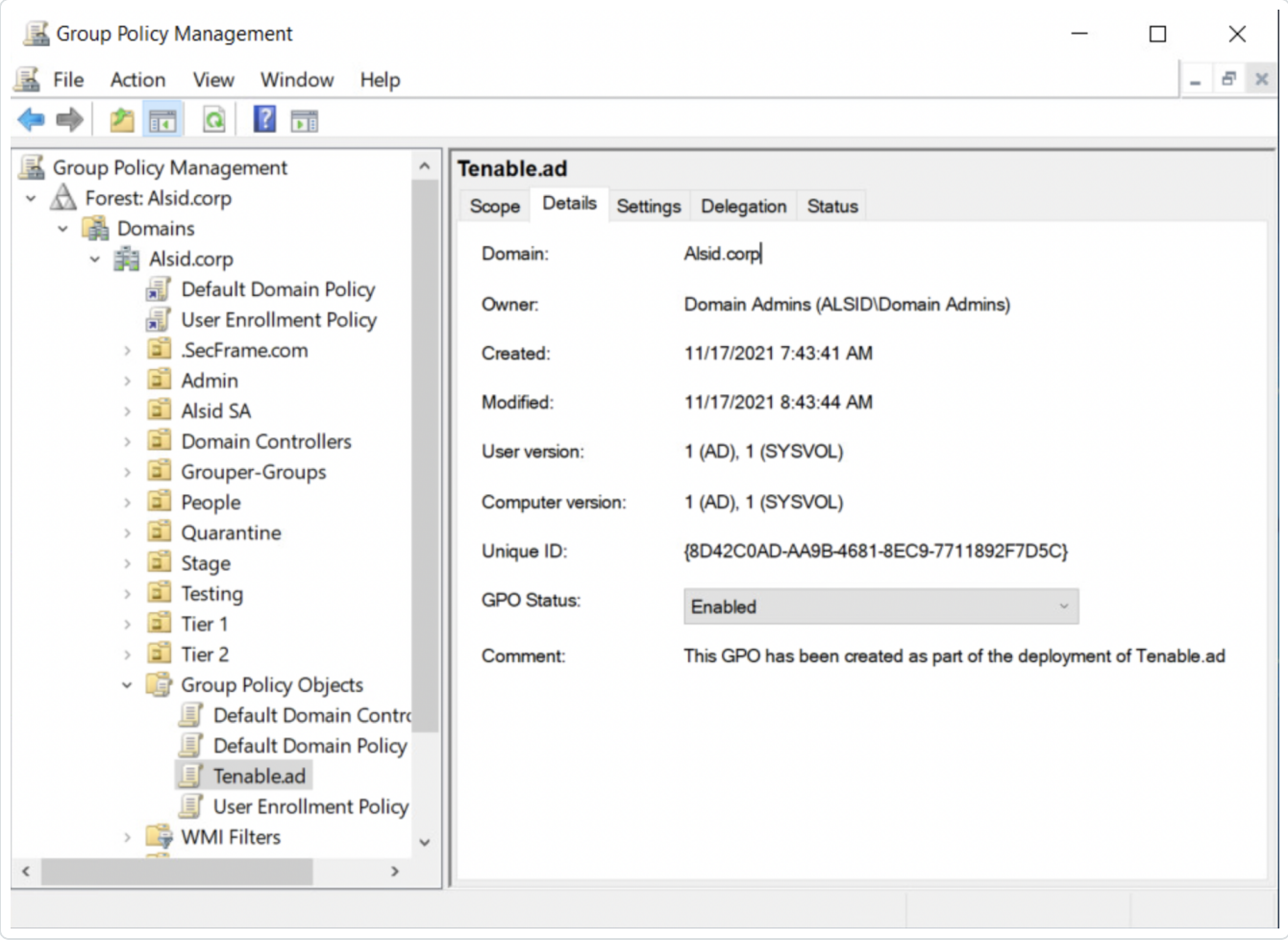


ヒント：**Zerologon の悪用**の攻撃インジケーター(IoA)の日付は 2020 年以降です。すべてのドメインコントローラー(DC)が過去 3 年以内に更新プログラムを受け取っている場合は、この脆弱性から保護されています。この脆弱性に対して DC を保護するために必要なパッチを判断するには、Microsoft の Netlogon の権限の昇格の脆弱性にある情報を参照してください。DC のセキュリティを確認したら、この IoA を安全に無効化して、不要なアラートを回避できます。

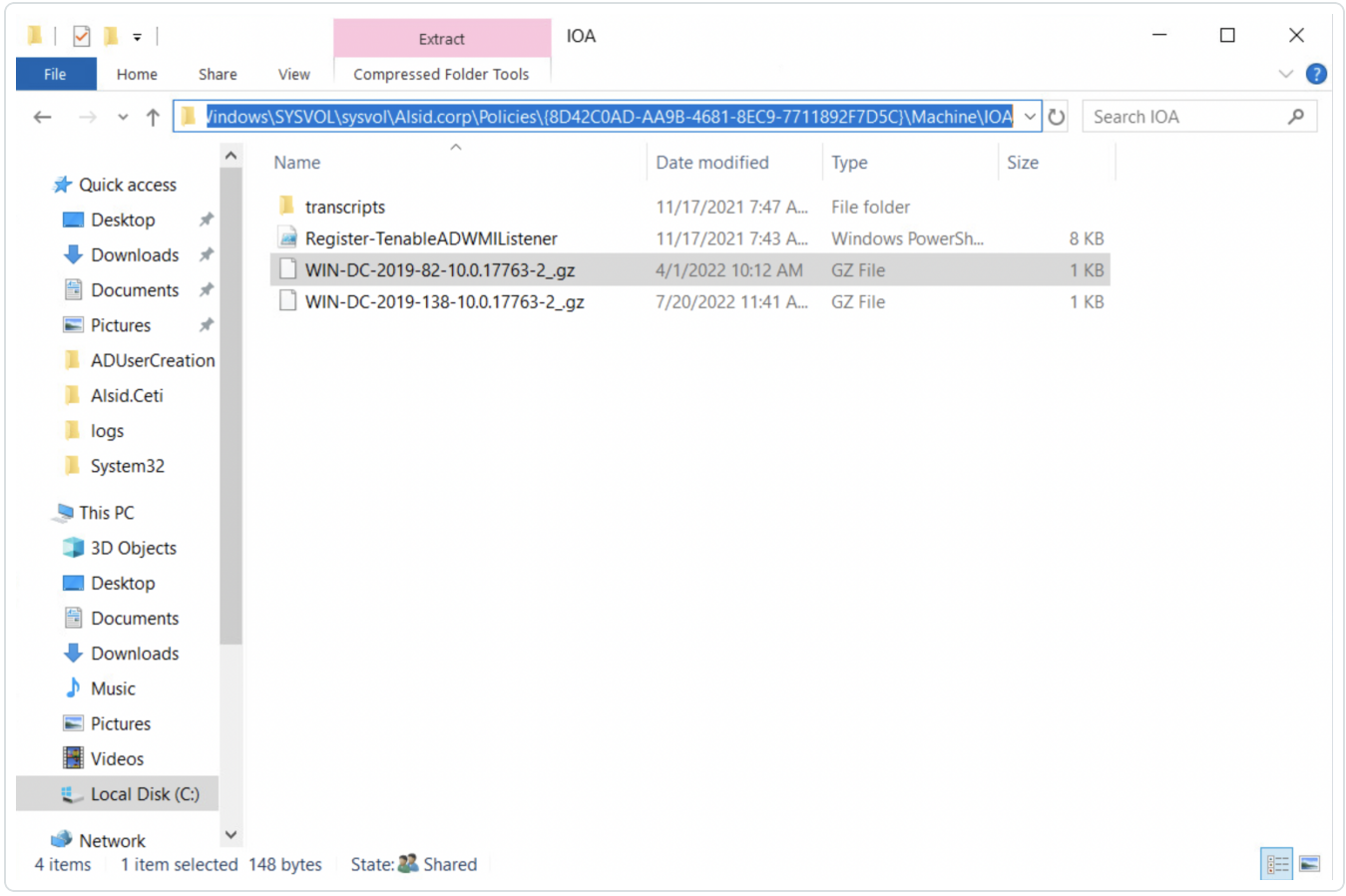
2. **[保存]**をクリックします。
   - **[今後は自動更新しますか?]**を有効にしてある場合、Tenable Identity Exposure は新しい設定を保存し、自動的に更新します。この更新が有効になるまで数分かかります。
   - **[今後は自動更新しますか?]**を有効にしていなかった場合は、手順ウィンドウが表示され、IoA のドメインを設定するにはに案内されます。

IoA のインストールをチェックするには

1. グループポリシー管理で、新しい Tenable Identity Exposure GPO が存在し、この GPO がドメインコントローラー OU にリンクしていることを確認します。



2. パス `C:\Windows\SYSVOL\sysvol\alsid.corp\Policies\{GUID}\Machine\IOA` に移動し、IoA をテストする前に、**すべてのドメインコントローラー**に `.gz` ファイルが存在することを確認します。



Tenable Identity Exposure サービスアカウントの「書き込み」アクセス許可をチェックするには

1. ファイルマネージャーで、\\<DNS-NAME>\sysvol\<DNS-NAME>\Policies\{<GPO-ID>}\Machine\ に移動します。
2. 「IOA」フォルダーを右クリックし、**[プロパティ]** を選択します。
3. **[セキュリティ]** タブを選択し、**[詳細]** をクリックします。
4. **[有効なアクセス]** タブをクリックします。
5. **[ユーザーを選択]** をクリックします。
6. <TENABLE-SERVICE-ACCOUNT-NAME> と入力し **[OK]** をクリックします。
7. **[有効なアクセスを表示]** をクリックします。
8. 「書き込み」アクセス許可が有効になっていることを確認します。

または、Powershell を使用することもできます。

- 次のコマンドを実行してください。

```
Install-Module -Name NTFSSecurity -RequiredVersion 4.2.3
```

```
Get-NTFSEffectiveAccess -Path \\<DNS-NAME>\sysvol\<DNS-NAME>\Policies\{<GPO-ID>}\IOA\ -
Account <TENABLE-SERVICE-ACCOUNT-NAME>
```

IoA を調整するには

攻撃の誤検出を回避しかつ正当な攻撃が検出されないことを回避するには、IoA を Active Directory のサイズに適合させ、既知のツールをホワイトリストに登録するなどして、環境に応じて IoA を調整する必要があります。

1. 選択するオプションおよび推奨値については、Tenable Identity Exposure の攻撃インジケーターリファレンスガイドを参照してください。
2. インジケーターのカスタマイズ で説明されているように、セキュリティプロファイルの各 IoA にオプションと値を適用します。

トラブルシューティング

デプロイメント中に次のエラーメッセージが表示される場合があります。

メッセージ	修正方法
「ターゲットフォルダー <targetFolder> が存在しないため、Tenable Identity Exposure は設定ファイルに書き込めません。IoA モジュールのデプロイメントが失敗した可能性があります。」	スクリプトをアンインストールし、[手順を表示する] をクリックして、スクリプトを再インストールする手順を確認します。
「Tenable Identity Exposure は <targetFile> にある設定ファイルに書き込んで更新することができませんでした。ファイルをロックしている別のプロセスまたはアクセス許可の変更が原因である可能性があります。」	• IoA モジュール以外のプロセスが設定ファイルを使用していないことを確認します。 • サービスアカウントにファイルの内容を変更するアクセス許可があることを確認します。

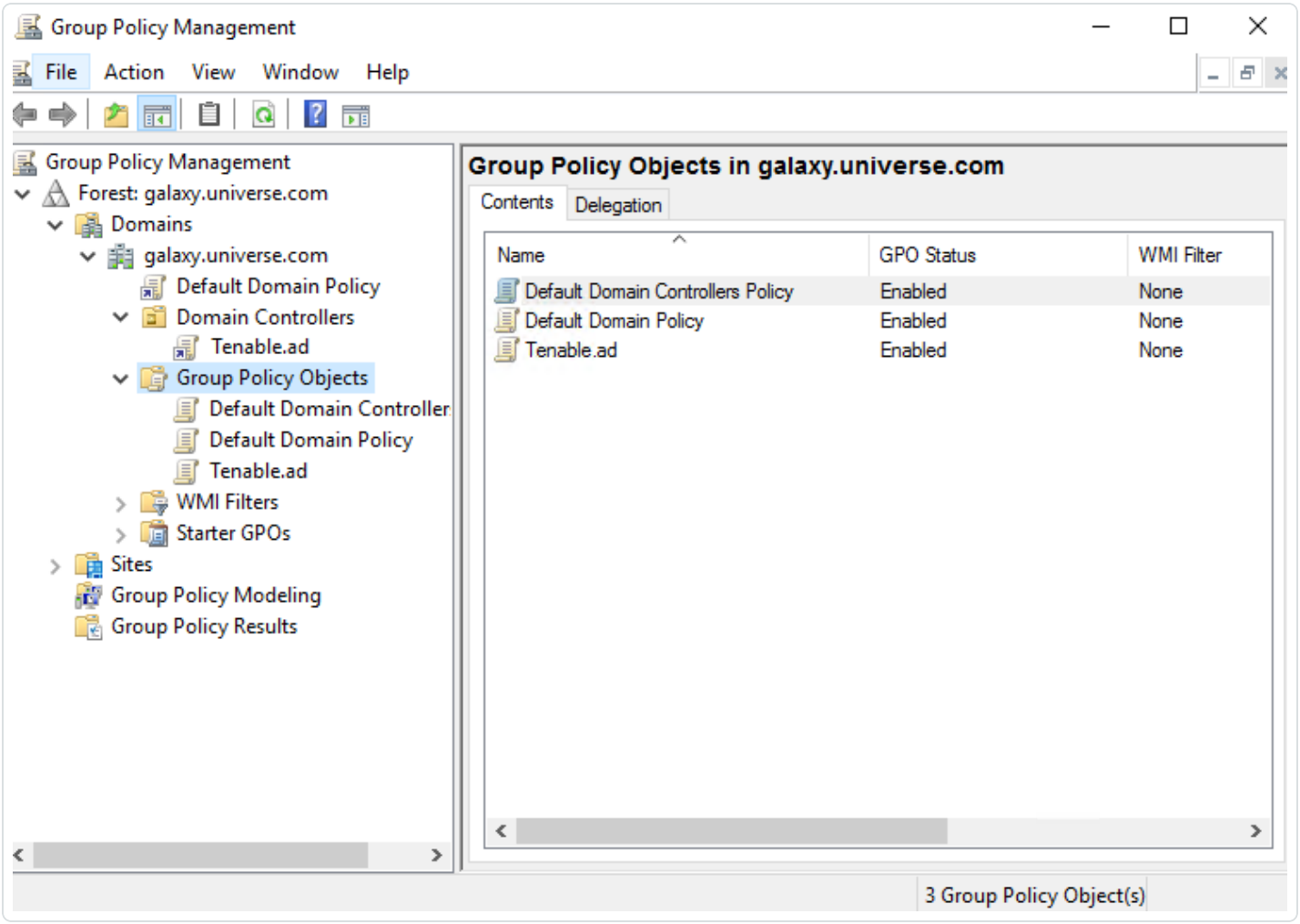
	• サービスアカウントにアクセス許可を付与したくない場合は、「自動更新」トグルを無効にし、[手順を表示する]をクリックして、IoA 設定を変更するたびに手動で更新するにはを確認します。
「ターゲットフォルダー <targetFolder> に自動更新を実行できないバージョンの Tenable Identity Exposure が含まれています。」	現在インストールされているスクリプトが、WMI を使用している古いバージョンです。現在のバージョンをアンインストールし、新しいインストールスクリプトをダウンロードして、このスクリプトを実行します。
「設定ファイルのデプロイメント中に予期しないエラーが発生しました。」	スクリプトをアンインストールし、[手順を表示する]をクリックして、スクリプトを再インストールする手順を確認します。解決しない場合は、カスタマーサポート担当者に連絡してください。

詳細については、次を参照してください。

- 攻撃インジケーターインストールスクリプト
- 技術的な変更と潜在的な影響
- アンチウイルス検出
- 監査ポリシーの詳細設定の優先順位

攻撃インジケーターインストールスクリプト

攻撃インジケーター(IoA)インストールファイルをダウンロードして実行すると、IoA スクリプトにより、デフォルトで Tenable.ad という名前の新しいグループポリシーオブジェクト (GPO) が Active Directory (AD) データベースに作成されます。システムは、その Tenable Identity Exposure GPO を、すべてのドメインコントローラー(DC)を含んでいるドメインコントローラーの組織単位 (OU) にのみリンクします。この GPO の仕組みを使用して、新しいポリシーはすべての DC 間で自動的に複製されます。



インストールスクリプト (Tenable Identity Exposure v. 3.29)

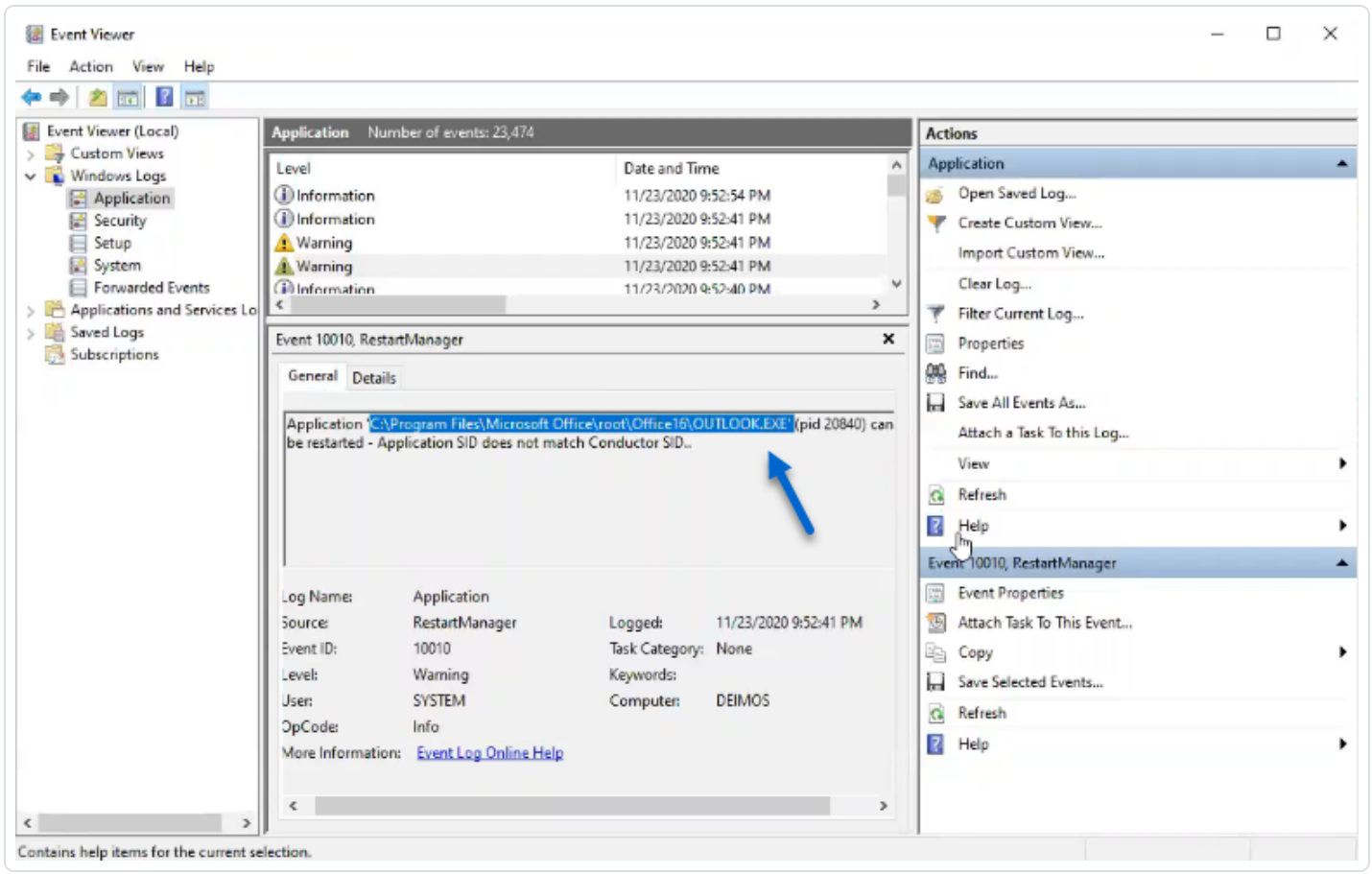
GPO に含まれている PowerShell スクリプトを、すべての DC がローカルで次のように実行して、対象データを収集します。

- このスクリプトは、Windows EvtSubscribe API を使用して、各ドメインコントローラーでイベントログリスナーを設定します。スクリプトは、一致する各イベントログに対してリクエストと EvtSubscribe によってトリガーされるコールバックを送信して、`TenableADEventsListenerConfiguration.json` 設定ファイルで指定されているように、必要なイベントログチャネルごとにサブスクリプションを作成します。
- イベントリスナーはイベントログを受信してバッファリングしてから、定期的に Sysvol と呼ばれるネットワーク共有に保存されるファイルにフラッシュします。各 DC は、収集されたイベントを単一の Sysvol ファイルにフラッシュしてファイル内に保存し、それを他のドメインコントローラーに複製します。
- このスクリプトは、DC の再起動時にイベントサブスクライバーを再登録して、このメカニズムが永続的であることを保証する WMI コンシューマーも作成します。WMI は、DC が再起動するたびにコンシューマーに通知し、コンシューマーがイベントリスナーを再登録できるようにします。
- この時点で分散ファイルシステム(DFS)レプリケーションが発生し、ドメインコントローラー間でファイルを自動的に同期します。DFS の受信レプリケーショントラフィックをリッスンしている Tenable Identity Exposure のプラットフォームは、このデータを使用してイベントを収集し、セキュリティ分析を実行してから、IoA アラートを生成します。

ローカルデータの取得

Windows イベントログには、オペレーティングシステムとアプリケーションで発生したすべてのイベントが記録されます。イベントログは、Windows に統合されたコンポーネントのフレームワークに依存しています。

Tenable Identity Exposure IoA イベントログリスナーは、EvtSubscribe API を使用して、有用なイベントログのデータセグメントのみを、イベントログから抽出する挿入文字列の形式で収集します。Tenable Identity Exposure は、これらの挿入文字列を Sysvol フォルダーに保存されたファイルに書き込み、DFS エンジンでそれを複製します。これにより、Tenable Identity Exposure はセキュリティ分析を実行して攻撃を検出するのに適正な量のセキュリティ関連データをイベントログから収集します。



IoA スクリプトのサマリー

次の表は、Tenable Identity Exposure スクリプトのデプロイメントの概要を示しています。

手順	説明	関連するコンポーネント	技術的なアクション
1	Tenable Identity Exposure の IoA デプロイメントを登	GPO 管理	`Tenable.ad` (デフォルト名) GPO が作成され、ドメインコントローラー OU にリンクされます。

	録する		
2	DC への Tenable Identity Exposure の IoA デプロイメントを始める	DC ローカルシステム	各 DC で適用する新しい GPO が検出されます (AD のレプリケーションとグループポリシーの更新間隔に応じて異なる)。
3	高度なログ記録ポリシーの状態を制御する	DC ローカルシステム	システムは、レジストリキー HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy を設定することにより、高度なログ記録ポリシーを有効にします。
4	ローカルログ記録ポリシーを更新する	DC ローカルシステム	検出する IoA に応じて、Tenable Identity Exposure は特定の監査ポリシーを動的に生成して有効にします。このポリシーによって既存のログ記録ポリシーが無効になることはなく、必要に応じて強化のみを行います。競合が検出されると、GPO インストールスクリプトが停止し、[Tenable Identity Exposure は監査ポリシー「...」が必要ですが、現在の AD 設定では使用できません] というメッセージが表示されます。
5	イベントリスナーと WMI プロデューサーを登録する	DC ローカルシステム	システムは、GPO に含まれるスクリプトを登録して実行します。このスクリプトは、PowerShell プロセスを実行し、EvtSubscribe API を使用してイベントログをサブスクライブし、永続化するために ActiveScriptEventConsumer のインスタンスを作成します。Tenable Identity Exposure は、これらのオブジェクトを使用して、イベントログを受信して内容を保存します。

6	イベントログメッセージを収集する	DC ローカルシステム	Tenable Identity Exposure は、関連するイベントログメッセージを取得し、一定期間バッファリングした後、Tenable Identity Exposure GPO に関連付けられた Sysvol フォルダー(`...{GPO_GUID}\Machine\IOA<DC_name>`)に格納されているファイル(DC ごとに 1 つ)に保存します。
7	宣言された DC SYSVOL フォルダーにファイルを複製する	Active Directory	DFS を使用して、AD はドメイン全体、特に宣言された DC でファイルを複製します。Tenable Identity Exposure プラットフォームは各ファイルの通知を受け取り、その内容を読み取ります。
8	これらのファイルを上書きする	Active Directory	各 DC は、定期的にバッファリングされたイベントを自動的かつ継続的に同じファイルに書き込みます。

インストールスクリプト (Tenable Identity Exposure v. 3.19.11 以前)

GPO に含まれている PowerShell スクリプトを、すべての DC がローカルで次のように実行して、対象データを収集します。

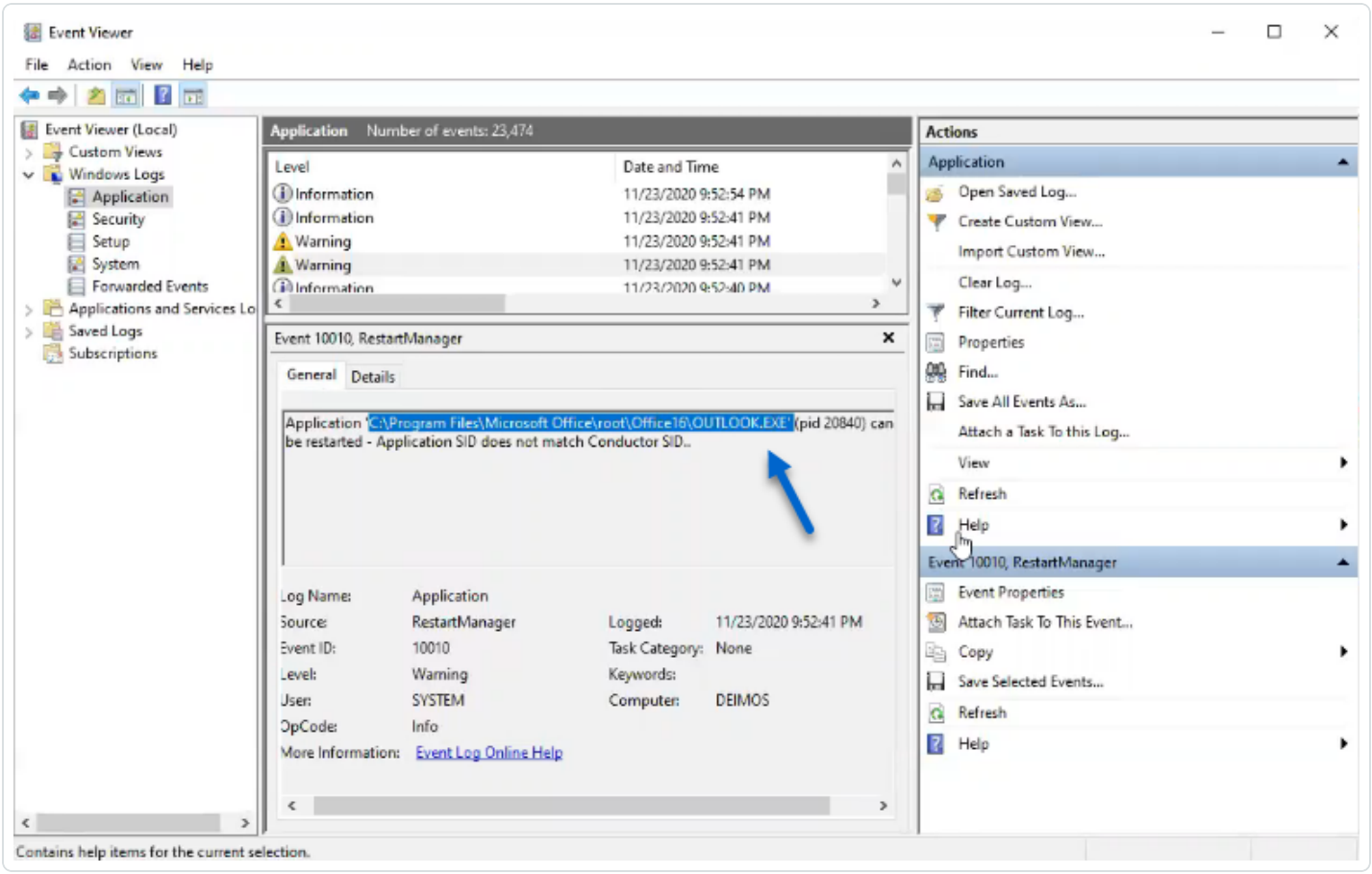
- スクリプトは、マシンのメモリでイベントウォッチャーおよび Windows Management Instrumentation (WMI) プロデューサー/コンシューマーを設定します。WMI は Windows コンポーネントの一種で、ローカルやリモートのコンピューターシステムのステータス情報を知らせます。
- イベントウォッチャーはイベントログを受信してバッファリングしてから、定期的に Sysvol と呼ばれるネットワーク共有に保存されているファイルにフラッシュします。各 DC は、収集されたイベントを単一の Sysvol ファイルにフラッシュしてファイル内に保存し、それを他のドメインコントローラーに複製します。
- WMI コンシューマーは、DC の再起動時にイベントウォッチャーを再登録することにより、この仕組みを永続化します。プロデューサーは DC が再起動するたびにウェイクアップし、コンシューマーに通知します。その結果、コンシューマーはイベントウォッチャーを再登録します。

- この時点で分散ファイルシステム(DFS)のレプリケーションが発生し、ドメインコントローラー間でファイルを自動的に同期します。DFS の受信レプリケーショントラフィックをリッスンしている Tenable Identity Exposure のプラットフォームは、このデータを使用してイベントを収集し、セキュリティ分析を実行してから、IoA アラートを生成します。

ローカルデータの取得

Windows イベントログには、オペレーティングシステムとアプリケーションで発生したすべてのイベントが記録されます。Event Tracing for Windows (ETW) と呼ばれるイベントログは、Windows に統合されたコンポーネントのフレームワークに依存しています。ETW はカーネル内にあり、DC のローカルに保存されて AD プロトコルによって複製されないデータを生成します。

Tenable Identity Exposure は、WMI エンジンを使用して、有用な ETW データセグメントのみを、イベントログから抽出する挿入文字列の形式で収集します。Tenable Identity Exposure は、これらの挿入文字列を Sysvol フォルダーに保存されたファイルに書き込み、DFS エンジンでそれを複製します。これにより、Tenable Identity Exposure はセキュリティ分析を実行して攻撃を検出するのに適正な量のセキュリティ関連データを ETW から収集します。



IoA スクリプトのサマリー

次の表は、Tenable Identity Exposure スクリプトのデプロイメントの概要を示しています。

手順	説明	関連するコンポーネント	技術的なアクション
1	Tenable Identity Exposure の IoA デプロイメントを登録する	GPO 管理	`Tenable.ad`(デフォルト名)GPO が作成され、ドメインコントローラー OU にリンクされます。
2	DC への Tenable Identity Exposure の IoA デプロイメントを始める	DC ローカルシステム	各 DC で適用する新しい GPO が検出されます(AD のレプリケーションとグループポリシーの更新間隔に応じて異なる)。
3	イベントウォッチャーと WMI プロデューサー/コンシューマーを	DC ローカルシステム	システムは、即時タスクを登録して、実行します。このタスクによって PowerShell プロセスが実行され、`ManagementEventWatcher` と `ActiveScriptEventConsumer` のクラスのインスタンスが作成されます。Tenable Identity Exposure は、これらのオブジェクトを使用して、ETW メッセージを受信して保存します。

	登録する		
4	高度なログ記録ポリシーの状態を制御する	DC ローカルシステム	システムは、レジストリキー HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy を設定することにより、高度なログ記録ポリシーを有効にします。
5	ローカルログ記録ポリシーを更新する	DC ローカルシステム	検出する IoA に応じて、Tenable Identity Exposure は高度なログ記録ポリシーを動的に生成して有効にします。このポリシーによって既存のログ記録ポリシーが無効になることはなく、必要に応じて強化のみを行います。競合が検出されると、GPO インストールスクリプトが停止し、[Tenable Identity Exposure は監査ポリシー「...」が必要ですが、現在の AD 設定では使用できません] というメッセージが表示されます。
6	ETW メッセージを収集する	DC ローカルシステム	Tenable Identity Exposure は、関連する ETW メッセージを取得し、一定期間バッファリングした後、Tenable Identity Exposure GPO に関連付けられた Sysvol フォルダー(...{GPO_GUID}\Machine\IOA<DC_name>) に格納されたファイル(DC ごとに 1 つ) に保存します。
7	ファイルを Tenable Identity Exposure プラットフォームに複製する	Active Directory	DFS を使用して、AD はドメイン全体でファイルを複製します。Tenable Identity Exposure プラットフォームもファイルを受信します。
8	これらの	Active	各 DC は、定期的にバッファリングされたイベントを自動的かつ継続

	ファイルを上書きする	Directory	的に同じファイルに書き込みます。

関連項目

- Indicators of Attack and the Active Directory
- 攻撃インジケーターのインストール
- 技術的な変更と潜在的な影響

技術的な変更と潜在的な影響

攻撃インジケーター(IoA)モジュールのインストールスクリプトは、監視対象の DC に透過的に以下の変更を適用する GPO を作成します。

- デフォルトで「Tenable.ad」という名前の新しい GPO が追加され、デフォルトでドメインコントローラーの組織単位 (OU) にリンクされる
- Microsoft Advanced ログ記録ポリシーをアクティブにするためのレジストリキーを変更する
- ドメインコントローラーに IoA が必要とする ETW 情報を強制的に生成させる、新しいイベントログポリシーをアクティブ化する

  > **注意**: ETW エンジンが Tenable Identity Exposure が必要とする挿入文字列を生成できるようにするために、イベントログポリシーは必須です。このポリシーによって既存のログ記録ポリシーが無効になることはなく、追加のみを行います。競合がある場合、デプロイメントスクリプトはエラーメッセージを表示して停止します。

- GPO フォルダーに保存されている IoA 設定の「自動更新」を可能にする Tenable Identity Exposure サービスアカウントへの書き込みのアクセス許可の追加

制限と潜在的な影響

攻撃インジケーター(IoA)モジュールは、次の制限を課す可能性があります。

- IoA モジュールは ETW データに依存し、Microsoft が定義する制限内で動作します。
- インストールされた GPO は、ドメイン全体にレプリケートされる必要があります。また、インストールプロセスを完了するには、GPO の更新間隔が経過する必要もあります。このレプリケーション期間中、Tenable Identity Exposure は攻撃インジケーターエンジンでのチェックをすぐに開始しないことにより、誤検出や検出漏れを最小限にしていますが、全く発生しないというわけではありません。
- Tenable は SYSVOL ファイル共有を使用して、ドメインコントローラーからの ETW 情報を取得します。SYSVOL がドメイン内のすべてのドメインコントローラーに複製されるため、Active Directory アクティビティのピークが高いときに、レプリケーションアクティビティが大幅に増加します。
- ドメインコントローラーと Tenable Identity Exposure の間でファイルを複製すると、ネットワーク帯域幅も消費されます。Tenable Identity Exposure は、収集したファイルを自動的に削除することでこれらの影響を制御し、各ファイルのサイズも制限しています(デフォルトで最大 500 MB)。

- 分散ファイルシステム(DFS)レプリケーションの遅延または破損に関する問題。詳細は、DFS レプリケーションの問題の緩和 を参照してください。

関連項目

- Indicators of Attack and the Active Directory
- 攻撃インジケーターのインストール
- 攻撃インジケーターインストールスクリプト
- 攻撃インジケーターのトラブルシューティング

攻撃シナリオ(v. 3.36 以前)

注意: 攻撃インジケーターのこの設定更新機能は、Tenable Identity Exposure バージョン 3.36 以降には適用されなくなりました。

必要なユーザーロール: 攻撃インジケーター設定を変更するアクセス許可を持つ組織のユーザー

Tenable Identity Exposure が特定のドメインで監視する攻撃のタイプを選択して、攻撃シナリオとして定義します。

始める前に

攻撃シナリオを変更するには、以下のアクセス許可を持つユーザーロールが必要です。

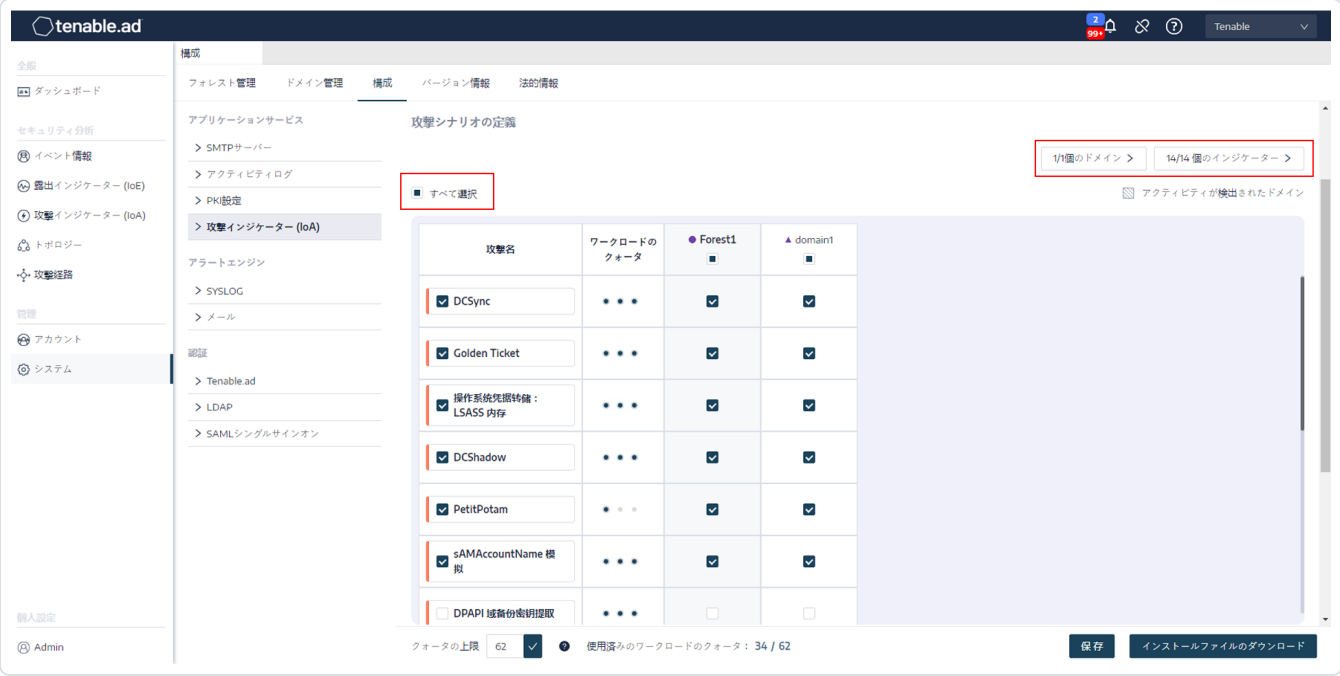
- **[データエンティティ]** で、以下に対する「読み取り」アクセス権
  - すべての攻撃インジケーター
  - すべてのドメイン
- **[インターフェースエンティティ]** で、以下に対するアクセス権
  - 管理 > システム > 設定
  - 管理 > システム > 設定 > アプリケーションサービス > 攻撃インジケーター
  - 管理 > システム > 設定 > アプリケーションサービス > 攻撃インジケーター > インストールファイルのダウンロード

ロールベースのアクセス許可についての詳細は、ロールのアクセス許可の設定を参照してください。

攻撃シナリオを定義するには

1. Tenable Identity Exposure で、**[システム]** > **[設定]** > **[攻撃インジケーター]** をクリックします。

   [攻撃シナリオの定義] ペインが開きます。



2. **[攻撃名]** で、監視する攻撃を選択します。
3. 選択した攻撃を監視するドメインを選択します。
4. オプションで、次のいずれかを実行できます。
   - **[すべて選択]** をクリックして、すべてのドメインですべての攻撃を監視します。
   - 特定のドメインをフィルタリングして特定の攻撃を監視するには、**[n/n 個のドメイン]** または **[n/n 個のインジケーター]** をクリックします。
5. **[保存]** をクリックします。

   設定の保存後に Tenable Identity Exposure により各攻撃のアクティビティステータスが消去されることを通知する確認メッセージが表示されます。
6. **[確認]** をクリックします。

   Tenable Identity Exposure が攻撃インジケーター設定を更新したことを確認するメッセージが表示されます。
7. **[インストールファイルのダウンロード]** をクリックします。
8. 新しい攻撃設定を有効にするには、次のようにインストールファイルを実行します。

a. ダウンロードしたインストールファイルをコピーし、監視対象ドメインの DC に貼り付けます。

b. 管理者権限で PowerShell ターミナルを開きます。

c. Tenable Identity Exposure で、ウィンドウの下部にある攻撃インジケーターセクションのコマンドをコピーします。

d. PowerShell ウィンドウにそのコマンドを貼り付けて、スクリプトを実行します。

ワークロードクォータ

警告: ワークロードクォータ機能は、Tenable Identity Exposure バージョン 3.36 以降には適用されなくなりました。

必要なユーザーロール: ワークロードクォータを編集するアクセス許可を持つ組織のユーザー

Tenable Identity Exposure の各攻撃インジケーター (IoA) には、攻撃のデータを分析するために必要なリソースを考慮したワークロードクォータが割り当てられています。

Tenable Identity Exposure は、同時に実行される攻撃インジケーター (IoA) の数を制限するためにワークロードクォータを計算します。同時実行は、ドメインコントローラーのイベント生成の帯域幅と CPU 使用率に影響を与えます。

ワークロードクォータの制限を変更した後、次の操作を行います。

- 増加した場合: 増加後の統計を監視し、十分な余裕があることを確認します。
- 削減した場合: このクォータを超過しないように一部の IoA を非アクティブにします。この場合、攻撃に対するセキュリティカバレッジは狭くなります。

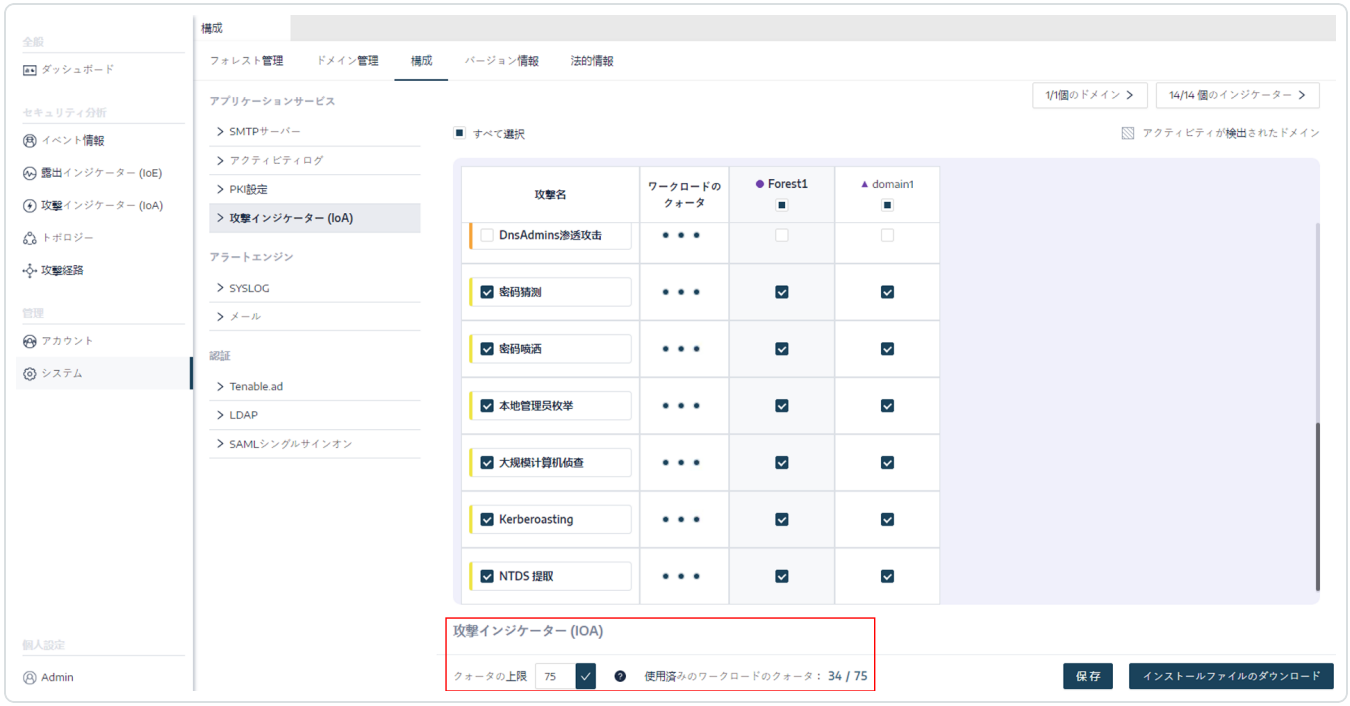
ワークロードクォータ制限を変更するには

1. Tenable Identity Exposure で、**[システム]** > **[設定]** > **[攻撃インジケーター]** をクリックします。

   [IoA 設定] ペインが開きます。

2. 設定に必要な IoA を選択します。

3. **[攻撃インジケーター]** の **[クォータの上限]** ボックスに、ワークロードクォータ制限の値を入力します。



4. 入力した値の横にあるチェックマークをクリックします。

   変更が Tenable Identity Exposure に及ぼす影響を通知するメッセージが表示されます。

   注意: クォータの上限に現在の攻撃設定で必要とされる値よりも小さい値を入力した場合は、アクティブな攻撃インジケーターの数を調整するか、または制限を引き上げる必要があります。

5. **[確認]** をクリックします。

   Tenable Identity Exposure がクォータの最大制限を更新したことを確認するメッセージが表示されます。

6. **[保存]** をクリックします。

   設定の保存後に Tenable Identity Exposure により各攻撃のアクティビティステータスが消去されることを通知する確認メッセージが表示されます。

7. **[確認]**をクリックします。

   Tenable Identity Exposure が攻撃インジケーター設定を更新したことを確認するメッセージが表示されます。

8. **[インストールファイルのダウンロード]**をクリックします。

9. 新しい攻撃設定を有効にするには、次のようにインストールファイルを実行します。

   a. ダウンロードしたインストールファイルをコピーし、監視対象ドメインの DC に貼り付けます。

   b. 管理者権限で PowerShell ターミナルを開きます。

   c. Tenable Identity Exposure で、ウィンドウの下部にある攻撃インジケーターセクションのコマンドをコピーします。

   d. PowerShell ウィンドウにそのコマンドを貼り付けて、スクリプトを実行します。

Microsoft Sysmon のインストール

一部の Tenable Identity Exposure の攻撃インジケーター(IoA) では、Microsoft System Monitor (Sysmon) サービスをアクティブにする必要があります。

Sysmon は、システムアクティビティを監視し、Windows イベントログに記録することで、Event Tracing for Windows (ETW) インフラでよりセキュリティ指向の情報を提供します。

なぜなら、他の Windows サービスやドライバーをインストールすると、AD インフラをホスティングしているドメインコントローラーのパフォーマンスに影響が出る場合があるからです。Tenable が自動的に Microsoft Sysmon を導入することはありません。手動で、または専用の GPO を使用してインストールする必要があります。

次の IoA は、Microsoft Sysmon が必要です。

名前	理由
OS 認証情報のダンプ: LSASS メモリ	プロセスインジェクションの検出

注意: Sysmon をインストールする場合、必要なイベントをすべて収集するには、PDC だけでなく、すべてのドメインコントローラーにインストールする必要があります。

注意: Tenable Identity Exposure を完全にデプロイする前に、Sysmon インストールの互換性をテストしてください。

ヒント: 潜在的な脆弱性に対処するパッチを利用するために、インストール後も Sysmon を定期的に更新するようにしてください。Tenable Identity Exposure と互換性のある最も古いバージョンは Sysmon 12.0 です。

Sysmon をインストールするには

1. Sysmon を Microsoft のウェブサイトからダウンロードします。
2. コマンドラインインターフェースで、次のコマンドを実行して Microsoft Sysmon をローカルマシンにインストールします。

```
.\Sysmon64.exe -accepteula -i C:\TenableSysmonConfigFile.xml
```

注意: 設定の説明については、Sysmon 設定ファイルのコメントを参照してください。

3. 次のコマンドを実行して、Sysmon がインストールされていることを WMI フィルターに示すレジストリキーを追加します。

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Microsoft-Windows-Sysmon/Operational"
```

Sysmon をアンインストールするには

1. PowerShell ターミナルを開きます。
2. Sysmon64.exe が含まれているフォルダーを参照します。
3. 次のコマンドを入力します。

```
PS C:\> .\Sysmon64.exe -u
```

レジストリキーを削除するには

- コマンドラインインターフェースで、Sysmon を実行しているすべてのマシンに次のコマンドを入力します。

```
reg delete "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Microsoft-Windows-Sysmon/Operational"
```

Sysmon 設定ファイル

注意:
- Sysmon 設定ファイルを使用する前に、XML ファイルとしてコピーして保存してください。エラーが発生した場合は、ここから設定ファイルを直接ダウンロードすることもできます。
- 実行する前に、ファイルのプロパティでファイルのブロックを解除します。

```
<Sysmon schemaversion="4.40">
  <EventFiltering>

    <!--SYSMON EVENT ID 1 : PROCESS CREATION [ProcessCreate]-->
    <RuleGroup name="" groupRelation="or">
      <ProcessCreate onmatch="exclude">
        <!--NOTE: Using "exclude" with no rules means everything in this section will be logged-->
      </ProcessCreate>
```

```
    </RuleGroup>

    <!--SYSMON EVENT ID 2 : FILE CREATION TIME RETROACTIVELY CHANGED IN THE FILESYSTEM
[FileCreateTime]-->
    <RuleGroup name="" groupRelation="or">
      <FileCreateTime onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileCreateTime>
    </RuleGroup>

    <!--SYSMON EVENT ID 3 : NETWORK CONNECTION INITIATED [NetworkConnect]-->
    <RuleGroup name="" groupRelation="or">
      <NetworkConnect onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </NetworkConnect>
    </RuleGroup>

    <!--SYSMON EVENT ID 4 : RESERVED FOR SYSMON SERVICE STATUS MESSAGES-->
      <!--Cannot be filtered.-->

    <!--SYSMON EVENT ID 5 : PROCESS ENDED [ProcessTerminate]-->
    <RuleGroup name="" groupRelation="or">
      <ProcessTerminate onmatch="exclude">
        <!--NOTE: Using "exclude" with no rules means everything in this section will be logged-->
      </ProcessTerminate>
    </RuleGroup>

    <!--SYSMON EVENT ID 6 : DRIVER LOADED INTO KERNEL [DriverLoad]-->
    <RuleGroup name="" groupRelation="or">
      <DriverLoad onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </DriverLoad>
    </RuleGroup>

    <!--SYSMON EVENT ID 7 : DLL (IMAGE) LOADED BY PROCESS [ImageLoad]-->
    <RuleGroup name="" groupRelation="or">
      <ImageLoad onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </ImageLoad>
    </RuleGroup>

    <!--SYSMON EVENT ID 8 : REMOTE THREAD CREATED [CreateRemoteThread]-->
    <RuleGroup name="" groupRelation="or">
      <CreateRemoteThread onmatch="include">
        <TargetImage name="lsass" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      </CreateRemoteThread>
    </RuleGroup>

    <!--SYSMON EVENT ID 9 : RAW DISK ACCESS [RawAccessRead]-->
    <RuleGroup name="" groupRelation="or">
      <RawAccessRead onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </RawAccessRead>
    </RuleGroup>

    <!--SYSMON EVENT ID 10 : INTER-PROCESS ACCESS [ProcessAccess]-->
    <RuleGroup name="" groupRelation="or">
        <ProcessAccess onmatch="include">
```

```
          <!-- Detect Access to LSASS-->
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x1FFFFF</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x1F1FFF</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x1010</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x143A</GrantedAccess>
          </Rule>

          <!-- Detect process hollowing to LSASS-->
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x0800</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x800</GrantedAccess>
          </Rule>

          <!-- Detect process process injection to LSASS-->
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1055,technique_name=Process Injection"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x0820</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1055,technique_name=Process Injection"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x820</GrantedAccess>
          </Rule>
        </ProcessAccess>
    </RuleGroup>

    <!--SYSMON EVENT ID 11 : FILE CREATED [FileCreate]-->
    <RuleGroup name="" groupRelation="or">
      <FileCreate onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileCreate>
    </RuleGroup>

    <!--SYSMON EVENT ID 12 & 13 & 14 : REGISTRY MODIFICATION [RegistryEvent]-->
    <RuleGroup name="" groupRelation="or">
      <RegistryEvent onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
```

```
      </RegistryEvent>
    </RuleGroup>

    <!--SYSMON EVENT ID 15 : ALTERNATE DATA STREAM CREATED [FileCreateStreamHash]-->
    <RuleGroup name="" groupRelation="or">
      <FileCreateStreamHash onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileCreateStreamHash>
    </RuleGroup>

    <!--SYSMON EVENT ID 16 : SYSMON CONFIGURATION CHANGE-->
      <!--Cannot be filtered.-->

    <!--SYSMON EVENT ID 17 & 18 : PIPE CREATED / PIPE CONNECTED [PipeEvent]-->
    <RuleGroup name="" groupRelation="or">
      <PipeEvent onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </PipeEvent>
    </RuleGroup>

    <!--SYSMON EVENT ID 19 & 20 & 21 : WMI EVENT MONITORING [WmiEvent]-->
    <RuleGroup name="" groupRelation="or">
      <WmiEvent onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </WmiEvent>
    </RuleGroup>

    <!--SYSMON EVENT ID 22 : DNS QUERY [DnsQuery]-->
    <RuleGroup name="" groupRelation="or">
      <DnsQuery onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </DnsQuery>
    </RuleGroup>

    <!--SYSMON EVENT ID 23 : FILE DELETED [FileDelete]-->
    <RuleGroup name="" groupRelation="or">
      <FileDelete onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileDelete>
    </RuleGroup>

  </EventFiltering>
</Sysmon>
```

攻撃インジケーターのアンインストール

必要なロール: ローカルマシンの管理者

攻撃インジケーター(IoA)モジュールをアンインストールするには、Tenable Identity Exposure クリーニングと呼ばれる新しいグループポリシーオブジェクト(GPO)を作成するコマンドを実行します。

アンインストールプロセスはこの新しい GPO を使用して、デフォルトで、以前インストールされた GPO とその SYSVOL ファイル、レジストリ設定、詳細なロギングポリシー、WMI フィルターを消去します。

注意: 初期 GPO の名前を変更した場合は、変更した名前をアンインストーラーに渡して、アンインストールする GPO を認識させる必要があります。新しい GPO 名を渡すには、パラメーター `-GpoDisplayName` を使用します。

IoA モジュールをアンインストールするには

1. コマンドラインインターフェースで、次のコマンドを実行して IoA モジュールをアンインストールします。

```
Register-TenableIOA.ps1 -Uninstall
```

2. この新しい GPO をドメイン全体に複製します。スクリプトは、レプリケーションが完了するまでに 4 時間の遅延を強制します。

3. 次のコマンドを実行して、クリーニング GPO を削除します。

```
Remove-GPO -Guid <GUID> -Domain "<DOMAIN>"
```

4. オプション: 次のコマンドを実行して、この GPO が存在しないことを確認します。

```
(Get-ADDomainController -Filter *).Name | Foreach-Object {Get-GPO -Name "Tenable.ad cleaning"}
| Select Displayname| measure
```

攻撃インジケーターのトラブルシューティング

- 監査ポリシーの詳細設定の優先順位
- アンチウイルス検出
- Tenable Identity Exposure ログファイル
- イベントログリスナーの検証
- DFS レプリケーションの問題の緩和

アンチウイルス検出

Tenable と Microsoft は、ドメインコントローラー(または中央管理コンソールを備えたその他のツール)に、アンチウイルス、エンドポイント保護プラットフォーム(EPP)、エンドポイント検知・対応(EDR)ソフトウェアをインストールすることを推奨していません。インストールした場合は、ドメインコントローラーの攻撃インジケーター(IoA)イベントの収集に必要なアイテムを、アンチウイルス/EPP/EDR が検出し、ブロックまたは削除してしまうこともあります。

Tenable Identity Exposure の攻撃インジケーターのデプロイメントスクリプトには、悪質なコードが含まれておらず、難読化もされていません。ただし、PowerShell と WMI の使用および実装のエージェントレスの性質を考慮すると、時折の検出は異常ではありません。

次のような問題が発生した場合

- インストール中のエラーメッセージ
- 検出における誤検出または検出漏れ

インストールスクリプトのアンチウイルス検出のトラブルシューティングを行うには

1. アンチウイルス/EPP/EDR セキュリティログをレビューして、Tenable Identity Exposure コンポーネントの検出、ブロック、削除がないかをチェックします。アンチウイルス/EPP/EDRは、以下のコンポーネントに影響を与える可能性があります。
    - ドメインコントローラーに適用された Tenable Identity Exposure GPO の `ScheduledTasks.xml` ファイル
    - PowerShell.exe を起動する、ドメインコントローラーの Tenable Identity Exposure スケジュールタスク
    - ドメインコントローラーで起動される Tenable Identity Exposure `Register-TenableADEventsListener.exe` プロセス
2. 影響を受けるコンポーネントのセキュリティ例外をツールで追加します。
    - 特に、Symantec Endpoint Protection は IoA インストールプロセス中に `CL.Downloader!gen27` の検出を引き起こすことが知られています。この特定の既知のリスクを例外ポリシーに追加できます。

- タスクスケジューラを設定したら、PowerShell を実行して Register-TenableADEventsListener.exe プロセスを開始します。アンチウイルス/EPP/EDR ソフトウェアがこの PowerShell スクリプトを妨げ、攻撃インジケーターの適切な実行を妨げる可能性があります。このプロセスを詳細に追跡し、すべての監視対象ドメインコントローラーで一度だけ実行されるようにしてください。

  アンチウイルス/EPP/EDR のファイルパス除外の例

```
Register-TenableADEventsListener.exe process
 "\\"domain"\sysvol\"domain"\Policies\{"GUID_Tenable.ad}\Machine\IOA\Register-
TenableADEventsListener.exe"
```

```
ScheduledTasks.xml file
    C:\Users\<User Name>\AppData\Local\Temp\4\Tenable.ad\
{GUID}\DomainSysvol\GPO\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml
    C:\Windows\[SYSVOL]\POLICIES\
{[GUID]}\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml
    \\[DOMAIN.FQDN]\[SYSVOL]\POLICIES\
{[GUID]}\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml
```

監査ポリシーの詳細設定の優先順位

必要なイベントログを有効にするために Tenable Identity Exposure が作成したグループポリシーオブジェクト (GPO) は、強制モードを有効にした組織単位 (OU) ドメインコントローラーにリンクされています。

これにより、GPO の優先度は高くなりますが、より高いレベル(ドメインやサイトなど) で設定された強制 GPO がそれより優先されます。

監査ポリシーの詳細設定の設定を定義する優先度の高い GPO が Tenable Identity Exposure のニーズと競合する場合、その GPO が優先され、Tenable Identity Exposure が攻撃検出に必要とするイベントは逸失してしまいます。

Windows は GPO によって定義された監査ポリシーの詳細設定をマージするため、異なる GPO では異なる設定が定義されている場合があります。

ただし、各設定レベルでは、優先度の高い GPO 定義の値のみが使用されます。たとえば、Tenable Identity Exposure には、認証情報の検証の監査の設定の成功値と失敗値が必要です。ただし、より高い優先度の GPO が認証情報の検証の監査の成功のみを定義する場合、Windows は成功イベントのみを収集し、Tenable Identity Exposure が必要とする失敗イベントは逸失してしまいます。

GPO の優先度をチェックするには

1. コマンドラインインターフェースで、ドメインコントローラーに関する次のコマンドを実行します。

   このコマンドは、すべての GPO と優先度を考慮した後、有効な監査ポリシーの詳細設定を出力します。

   ```
   auditpol.exe /get /category:*
   ```

2. 出力を Tenable Identity Exposure の詳細な監査ポリシー要件と比較します。Tenable Identity Exposure が必要とする設定ごとに、有効なポリシーもその設定をカバーしていることを確認してください。

   - Tenable Identity Exposure が「成功」または「失敗」を必要とし、設定が「成功および失敗」である場合など、有効なポリシーの範囲がより広い場合は問題ありません。
   - 有効なポリシーが不十分な場合、より高い優先度を持つ GPO が競合する設定を定義することになります。

GPO の優先順位を修正するには

1. 「強制」モードでより高いレベル(ドメインまたはサイト)にリンクされており、監査ポリシーの詳細設定を定義している GPO を探します。
2. コマンドラインインターフェースで、ドメインコントローラーに対して次のコマンドを実行し、優先する GPO をピンポイントで特定します。

   ```
   gpresult /scope:computer /h gpo.html
   ```

3. Tenable Identity Exposure の最小要件を満たすように、GPO の対応する監査ポリシーの詳細設定の設定を変更します。例
   - Tenable Identity Exposure が「成功」を必要とし、より高い優先度の GPO が「失敗」を定義する場合、設定を「成功および失敗」に変更します。
   - Tenable Identity Exposure が「成功および失敗」を必要とし、より高い優先度の GPO が「成功」を定義する場合、設定を「成功および失敗」に変更します。
4. 設定を変更した後、更新済みの GPO が適用されるのを待つか、gpupdate コマンドで強制的に適用することができます。
5. GPO の優先度をチェックするには の手順を繰り返して、新しい有効なポリシーをチェックします。

イベントログリスナーの検証

攻撃インジケーターのインストールスクリプトは、マシンのメモリのイベントウォッチャーと Windows Management Instrumentation (WMI) プロデューサー/コンシューマーを設定します。WMI は Windows コンポーネントの一種で、ローカルやリモートのコンピューターシステムのステータス情報を知らせます。

正しい WMI 登録があるかをチェックするには

- PowerShell で次のコマンドを実行します。

```
Get-WmiObject -Class '__FilterToConsumerBinding' -Namespace 'root\subscription' -Filter "Filter
= ""__EventFilter.name='AlsidForAD-Launcher'"""
```

- 少なくとも 1 つのコンシューマーが存在する場合、次のようなタイプの出力が得られます。

```
> Get-WmiObject -Class '__FilterToConsumerBinding' -Namespace 'root\subscription' -Filter
"Filter = ""__EventFilter.name='AlsidForAD-Launcher'"""


__GENUS                 : 2
__CLASS                 : __FilterToConsumerBinding
__SUPERCLASS            : __IndicationRelated
__DYNASTY               : __SystemClass
__RELPATH               : __
FilterToConsumerBinding.Consumer="ActiveScriptEventConsumer.Name=\"AlsidForAD-Launcher\"",F
                          ilter="__EventFilter.Name=\"AlsidForAD-Launcher\""
__PROPERTY_COUNT        : 7
__DERIVATION            : {__IndicationRelated, __SystemClass}
__SERVER                : DC-999
__NAMESPACE             : ROOT\subscription
__PATH                  : \\DC-999\ROOT\subscription:__
FilterToConsumerBinding.Consumer="ActiveScriptEventConsumer.Name
                          =\"AlsidForAD-Launcher\"",Filter="__EventFilter.Name=\"AlsidForAD-
Launcher\""
Consumer                : ActiveScriptEventConsumer.Name="AlsidForAD-Launcher"
CreatorSID              : {1, 1, 0, 0...}
DeliverSynchronously    : False
DeliveryQoS             :
Filter                  : __EventFilter.Name="AlsidForAD-Launcher"
MaintainSecurityContext : False
SlowDownProviders       : False
PSComputerName          : DC-999
```

  - 登録されている WMI コンシューマーがない場合、コマンドは何も返しません。
  - これは、WMI の DC でプロセスを実行するための前提条件です。

WMI プロセスを取得するには (バージョン 3.19 以前の場合)

- PowerShell で次のコマンドを実行します。

```
gcim win32_process | Where-Object { $_.CommandLine -match "TenableADWMIListener"}
```

- 有効な結果の例

```
> gcim win32_process | Where-Object { $_.CommandLine -match "TenableADWMIListener"}

ProcessId Name           HandleCount WorkingSetSize VirtualSize
--------- ----           ----------- -------------- -----------
952       powershell.exe 502         26513408       2199678185472
```

イベントログリスナーを取得するには (バージョン 3.29 以上の場合)

- PowerShell で次のコマンドを実行します。

```
gcim win32_process | Where-Object { $_.CommandLine -match "Register-
TenableADEventsListener.exe"}
```

- 有効な結果の例

```
PS C:\IOAInstall> gcim win32_process | Where-Object { $_.CommandLine -match "Register-
TenableADEventsListener.exe"}

ProcessId Name                                HandleCount WorkingSetSize VirtualSize

5748      Register-TenableADEventsListener.exe 152         4096000        4384534528
```

Tenable Identity Exposure ログファイル

GPO および WMI コンシューマーを検証した後も、まだ攻撃インジケーターアラートが表示されない場合は、Tenable Identity Exposure の内部ログを確認できます。

Ceti ログ

- CETI ログで次のエラーメッセージがないかチェックします。

```
[2022-02-22 22:23:27:570 UTC WARNING] Some domain controllers are not generating IOA
events: 'CORP-DC'. {SourceContext="DirectoryEventToCetiAdObjectMessageMapper",
DirectoryId=2, Dns="corp.bank.com", Host="10.10.20.10", Source=SYSVOL, Version="3.11.5"}
```

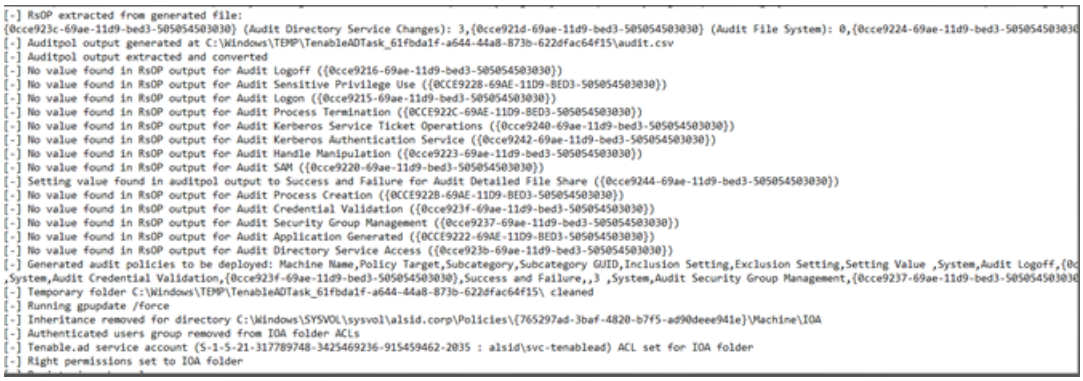
- このメッセージがある場合は、GPO 設定と WMI コンシューマーが、上記のエラーメッセージにリストされているドメインコントローラー (DC) で実行されていることを確認してください。

監査設定

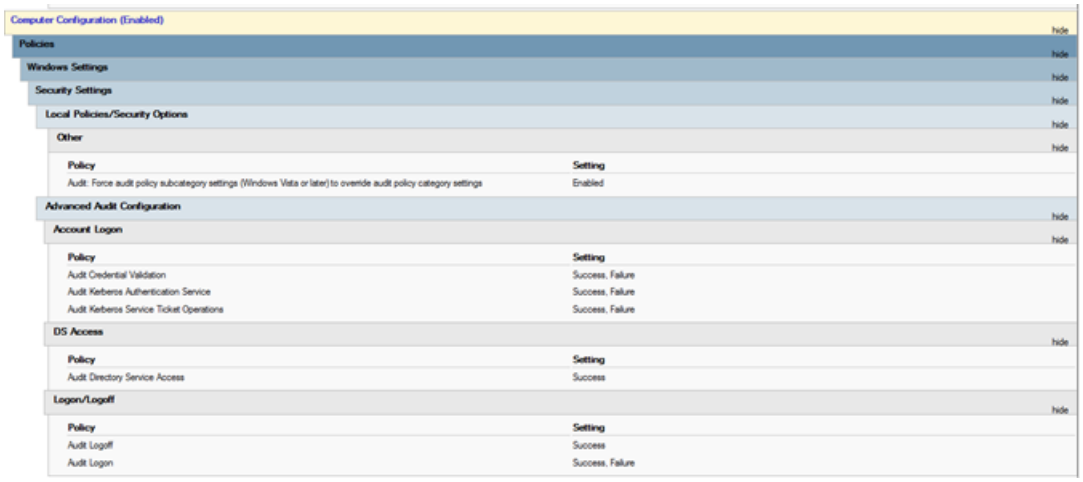
- 「Tenable Identity Exposure には監査ポリシーが必要です...」に類似したエラーが表示された場合、既存の GPO をチェックして、必要な監査ポリシーを「監査しない」に設定していないことを確認してください。

```
> 2022-02-10 16:54:21 [2022-02-10 21:54:21:845 UTC ERROR] Detected transcript '\\alsid.corp\sysvol\alsid.corp\
                      _ce599bf8-57cc-4dd9-9fb9-f06a263c3b6a.log' with errors: 'Tenable.ad requires the audit p
> 2022-02-10 16:54:07 this could prevent IOA engine from working. {SourceContext="FileProcessor", DirectoryId=
> 2022-02-10 16:54:07 Tenable.ad requires the audit policy Audit Detailed'
> 2022-02-10 16:54:07 [2022-02-10 21:54:07:849 UTC ERROR] Detected transcript '\\alsid.corp\sysvol\alsid.corp\
                      _ce599bf8-57cc-4dd9-9fb9-f06a263c3b6a.log' with errors: 'Tenable.ad requires the audit p
> 2022-02-10 16:54:07 this could prevent IOA engine from working. {SourceContext="FileProcessor", DirectoryId=
> 2022-02-10 16:54:07 Tenable.ad requires the audit policy Audit Detailed'
> 2022-02-10 16:54:07 [2022-02-10 21:54:07:773 UTC ERROR] Detected transcript '\\alsid.corp\sysvol\alsid.corp\
                      _ce599bf8-57cc-4dd9-9fb9-f06a263c3b6a.log' with errors: 'Tenable.ad requires the audit p
> 2022-02-10 16:54:07 this could prevent IOA engine from working. {SourceContext="FileProcessor", DirectoryId=
> 2022-02-10 16:54:07 Tenable.ad requires the audit policy Audit Detailed'
> 2022-02-10 16:54:07 [2022-02-10 21:54:07:662 UTC ERROR] Detected transcript '\\alsid.corp\sysvol\alsid.corp\
                      _ce599bf8-57cc-4dd9-9fb9-f06a263c3b6a.log' with errors: 'Tenable.ad requires the audit p
```

- 「RSOP ...」というエラーが表示される場合



- 監査ポリシーをチェックし、Sysvol フォルダーのトランスクリプトファイルを参照して、インストール中に問題が発生したかどうかを確認します。



Cygni ログ

Cygni は攻撃をログに記録し、Tenable Identity Exposure がアラートを生成するために呼び出した特定の .gz ファイルを一覧表示します。

I-DCSync

```
2022-03-15 11:39:31
[2022-03-15 15:39:30:759 UTC INFORMATION] Anomaly 'ControlAccess' has been raised for Indicator 'I-
DCSync' and Event '110052' {SourceContext="AttackEngine", CodeName="I-DCSync", ProfileId=4,
AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-GoldenTicket

```
2022-03-15 11:40:31
[2022-03-15 15:40:31:490 UTC INFORMATION] Anomaly 'Logon' has been raised for Indicator 'I-
GoldenTicket' and Event '110061' {SourceContext="AttackEngine", CodeName="I-GoldenTicket",
ProfileId=3, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-ProcessInjectionLsass

```
022-03-15 12:47:09
[2022-03-15 16:47:09:811 UTC INFORMATION] Anomaly 'ProcessAccess' has been raised for Indicator 'I-
ProcessInjectionLsass' and Event '115948' {SourceContext="AttackEngine", CodeName="I-
ProcessInjectionLsass", ProfileId=1, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\
{08D6D98F-7455-464B-BBEC-23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0,
Version="3.16.0"}
```

I-DCShadow

```
2022-03-15 11:30:30
[2022-03-15 15:30:30:657 UTC INFORMATION] Anomaly 'ControlAccess' has been raised for Indicator 'I-
DCShadow' and Event '109948' {SourceContext="AttackEngine", CodeName="I-DCShadow", ProfileId=4,
AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-BruteForce

```
2022-03-15 08:02:11
[2022-03-15 12:02:11:231 UTC INFORMATION] Anomaly 'An account failed to log on' has been raised for
Indicator 'I-BruteForce' and Event '109082' {SourceContext="AttackEngine", CodeName="I-BruteForce",
ProfileId=6, AdObjectId="3:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{765297AD-3BAF-4820-B7F5-
AD90DEEE941E}\\Machine\\IOA\\dc-vm-10.0.17763-8_.gz", Event.Id=0, Version="3.16.0"}
```

I-PasswordSpraying

```
2022-03-15 12:39:43
[2022-03-15 16:39:43:793 UTC INFORMATION] Anomaly 'An account failed to log on.' has been raised for
Indicator 'I-PasswordSpraying' and Event '115067' {SourceContext="AttackEngine", CodeName="I-
PasswordSpraying", ProfileId=4, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\
{08D6D98F-7455-464B-BBEC-23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0,
Version="3.16.0"}
```

I-PetitPotam

```
2022-03-15 12:43:02
[2022-03-15 16:43:02:737 UTC INFORMATION] Anomaly 'PetitPotamEFSError' has been raised for Indicator
'I-PetitPotam' and Event '115844' {SourceContext="AttackEngine", CodeName="I-PetitPotam",
ProfileId=4, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-ReconAdminsEnum

```
022-03-15 12:55:31
[2022-03-15 16:55:31:638 UTC INFORMATION] Anomaly 'LocalAdmin enumeration (BloodHound/SharpHound).
Version 2016+' has been raised for Indicator 'I-ReconAdminsEnum' and Event '116085'
{SourceContext="AttackEngine", CodeName="I-ReconAdminsEnum", ProfileId=4,
AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-Kerberoasting

```
022-03-15 12:51:30
[2022-03-15 16:51:30:236 UTC INFORMATION] Anomaly 'Kerberos TGS requested on honey account' has been
raised for Indicator 'I-Kerberoasting' and Event '116013' {SourceContext="AttackEngine", CodeName="I-
Kerberoasting", ProfileId=3, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-
7455-464B-BBEC-23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-NtdsExtraction

```
2022-03-15 12:03:51
[2022-03-15 16:03:50:949 UTC INFORMATION] Anomaly 'Shadow copy created on 2012 and above' has been
raised for Indicator 'I-NtdsExtraction' and Event '111168' {SourceContext="AttackEngine",
CodeName="I-NtdsExtraction", ProfileId=4,
AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

Cephei ログ

次のログエントリは、Cephei が攻撃を書き込んでいることを検証しています。重要な値は、攻撃のタイプを指定する **attackTypeID** です。これを使用して、Cygni エントリとの関連付けを行うことができます。

I-DCSync attackTypeID:1

```
2022-03-15 11:39:52
2022-03-15T15:39:52.037023041Z stdout F [2022-03-15 15:39:52:035 UTC INFORMATION] [Equuleus] POST
```

```
http://equuleus:3004/attacks/write responded 204 in 32.16 ms : Request Body=
{"timestamp":"1647358722449","directoryId":5,"profileId":4,"attackTypeId":1,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-GoldenTicket attackTypeID:2

```
2022-03-15 11:40:52
2022-03-15T15:40:52.084931986Z stdout F [2022-03-15 15:40:52:084 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 24.6607 ms : Request Body=
{"timestamp":"1647358773608","directoryId":5,"profileId":4,"attackTypeId":2,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-ProcessInjectionLsass attackTypeID:3

```
2022-03-15 12:47:52
2022-03-15T16:47:52.29927328Z stdout F [2022-03-15 16:47:52:298 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 35.7532 ms : Request Body=
{"timestamp":"1647362812784","directoryId":5,"profileId":1,"attackTypeId":3,"count":2}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-DCShadow attackTypeID:4

```
2022-03-15 11:30:52
2022-03-15T15:30:51.949399295Z stdout F [2022-03-15 15:30:51:944 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 24.2605 ms : Request Body=
{"timestamp":"1647358182800","directoryId":5,"profileId":3,"attackTypeId":4,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-BruteForce attackTypeID:5

```
2022-03-15 08:02:54
2022-03-15T12:02:54.698814039Z stdout F [2022-03-15 12:02:54:698 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 30.7623 ms : Request Body=
{"timestamp":"1647345728023","directoryId":3,"profileId":6,"attackTypeId":5,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-PasswordSpraying attackTypeID:6

```
2022-03-15 12:39:52
2022-03-15T16:39:52.187309945Z stdout F [2022-03-15 16:39:52:186 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 21.9422 ms : Request Body=
{"timestamp":"1647362356837","directoryId":5,"profileId":4,"attackTypeId":6,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-PetitPotam attackTypeID:7

```
022-03-15 12:43:52
2022-03-15T16:43:52.226125918Z stdout F [2022-03-15 16:43:52:223 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 15.8402 ms : Request Body=
{"timestamp":"1647362570534","directoryId":5,"profileId":1,"attackTypeId":7,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-ReconAdminsEnum attackTypeID:8

```
2022-03-15 12:55:52
2022-03-15T16:55:52.399889635Z stdout F [2022-03-15 16:55:52:399 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 40.6632 ms : Request Body=
{"timestamp":"1647363305295","directoryId":5,"profileId":4,"attackTypeId":8,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-Kerberoasting attackTypeID:10

```
2022-03-15 12:51:52
2022-03-15T16:51:52.352432644Z stdout F [2022-03-15 16:51:52:351 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 21.0547 ms : Request Body=
{"timestamp":"1647363026345","directoryId":5,"profileId":4,"attackTypeId":10,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-NtdsExtraction attackTypeID:11

```
022-03-15 12:03:52
2022-03-15T16:03:52.137547488Z stdout F [2022-03-15 16:03:52:137 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 13.0304 ms : Request Body=
{"timestamp":"1647360224606","directoryId":5,"profileId":4,"attackTypeId":11,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

Electra ログ

次 のエントリが表 示されます。

[2022-03-15T14:04:39.151Z] INFO: server/4016 on WIN-UQRSCEN0CI3: Message received from MQ: attack-alert (namespace=electra)

```
[2022-03-15T14:04:39.151Z]  INFO: server/4016 on WIN-UQRSCEN0CI3: Message received from MQ: attack-
alert (namespace=electra)
[2022-03-15T14:04:39.168Z]  INFO: server/4016 on WIN-UQRSCEN0CI3: Sending ws message to listeners.
alertIoA (namespace=electra)
```

Eridanis ログ

次 のエントリが表 示されます。

```
022-03-15T14:04:39.150Z]  INFO: server/4988 on WIN-UQRSCEN0CI3: KAPTEYN get /attack-alerts/2010 200
122 - 7ms (namespace=hapi)
[2022-03-15T14:04:39.165Z]  INFO: server/4988 on WIN-UQRSCEN0CI3: notifyAttackAndAttackAlertCreation
success { attackId: 2011 } (namespace=eridanis)
[2022-03-15T14:04:39.170Z]  INFO: server/4988 on WIN-UQRSCEN0CI3: KAPTEYN get /attack-alerts/2011 200
122 - 6ms (namespace=hapi)
```

DFS レプリケーションの問題の緩和

攻撃インジケーターのデプロイメントスクリプトの追加パラメーター `-EventLogsFileWriteFrequency X` を使用すると、分散ファイルシステム(DFS)レプリケーションの遅延または破損に関する潜在的な問題に対処できます。

このパラメーターはオプションであり、Tenable では、DFS レプリケーションの問題が発生している場合や IoA スクリプトのデプロイ以降に問題に気づいた場合にのみ使用することを推奨しています。通常の状況では、パラメーターはデフォルト値のままであるため、スクリプトを実行する際にコマンドラインにパラメーターを含める必要はありません。

パラメーターを変更するタイミング

パラメーター `-EventLogsFileWriteFrequency X` の `[X]` 値は、Tenable Identity Exposureリスナーが非 PDCe ドメインコントローラー(DC)のイベントログファイルを生成する頻度です。Tenable Identity Exposure リスナーが使用するデフォルトの推奨値は 15 秒です。ただし、カスタマイズされた値は PDCe DC に適用されません。攻撃検出機能が完全に動作するように、デフォルトの 15 秒間隔のままになります。Tenable では、インフラが DFS レプリケーションの問題に直面している場合やその問題の影響を受けやすい場合にのみ、このパラメーターを使用して値をデフォルトの 15 秒から最大 300 秒 (5 分) に増やすことを推奨しています。

推奨事項

イベントログファイルの書き込み頻度を引き上げると、ファイルが生成される頻度が減り、攻撃検出の遅延が増大することに注意してください(例: ファイルが非 PDCe DC でデフォルトの 15 秒ではなく 30 秒ごとに生成される場合)。また、遅延が大きくなると、生成されたイベントログファイルのサイズが 技術的な変更と潜在的な影響 で定義されている設定された制限内で大きくなります。そのため、このパラメーターは緩和戦略としてのみ使用し、DFS レプリケーションの問題を適切に調査することの代替方法としては使用しないでください。

パラメーターを適用するには

1. 手順で説明されているように、IoA 用のドメインを設定します。詳細は、攻撃インジケーターのインストール を参照してください。

2. 管理者権限で PowerShell ターミナルを開きます。
3. スクリプトを実行して、IoA のドメインコントローラーを設定し、`-EventLogsFileWriteFrequency X` パラメーターを追加します。この `[X]` は、イベントログファイルに対して設定される頻度です。

認証

Tenable Identity Exposure ユーザーを認証する方法は、次のようにいくつかあります。

- Tenable Identity Exposure アカウントを使用した認証
- LDAP を使用した認証
- SAML を使用した認証

Tenable One を使用した認証

必要なライセンス: Tenable One

注意: Tenable One ライセンスがある場合、すべての認証設定は Tenable Vulnerability Management で管理します。詳細については、*Tenable Vulnerability Management ユーザーガイド*のアクセス制御を参照してください。

Tenable One を使用した認証を設定するには

1. Tenable Identity Exposure で、**[システム]** > **[設定]** をクリックします。

   設定ペインが表示されます。

2. **[認証]** セクションにある **[Tenable One]** をクリックします。

3. **[デフォルトのプロファイル]** ドロップダウンボックスで、ユーザーのプロファイルを選択します。

4. **[デフォルトのロール]** ボックスで、ユーザーのロールを選択します。

   ヒント: これまで Tenable Identity Exposure に接続したことがないものの Tenable One で認証を受けているユーザーは、Tenable Identity Exposure にログインすると自動的にアカウントを入手します。デフォルトでは、デフォルトのプロファイルとロールがユーザーに適用されます。**例外**: Tenable Vulnerability Management で「管理者」のロールを持つユーザーは、Tenable Identity Exposure の「グローバル管理者」のロールも付与されます。

5. **[保存]** をクリックします。

Tenable Identity Exposure アカウントを使用した認証

最もシンプルな認証方法は、ユーザー名とパスワードを必要とする Tenable Identity Exposure アカウントを使用するものです。

この認証方法にはロックアウトポリシー、つまり認証機構に対する総当たり攻撃を緩和するよう設計されたセキュリティ制御が提供されます。ユーザーアカウントへのログイン失敗が何度も繰り返されると、アカウントはロックされます。アカウントがロックされると、ユーザーは Tenable Identity Exposure API にアクセスすることができません。

Tenable Identity Exposure アカウントを使用した認証を設定するには

1. Tenable Identity Exposure で、**[システム]** > **[設定]** をクリックします。

   設定ペインが表示されます。

2. **[認証]** セクションにある **[Tenable Identity Exposure]** をクリックします。

3. **[デフォルトのプロファイル]** ドロップダウンボックスで、ユーザーのプロファイルを選択します。

4. **[デフォルトのロール]** ボックスで、ユーザーのロールを選択します。

5. ロックアウトポリシー設定を行います。

設定	説明	デフォルト値
有効	• **[有効]** – ログインの試行に一定の回数失敗すると、Tenable Identity Exposure はアカウントをブロックします。 • **[無効]** – ログインの試行に何回失敗しても、Tenable Identity Exposure はアカウントをロックしません。	有効
ロックアウト期間	アカウントでのログインの試行が Tenable Identity Exposure によってロックされる期間です。この期間が経過した後、Tenable Identity Exposure はアカウントのロックを自動的に解除し、ユーザーは再びログインの試行が可能になります。 ロックアウト期間を設定するには、次を実行します。 1. スライダーをクリックして、ロックアウト期間を設定します。 2. 設定した期間後にアカウントのロックを自動的に解除したくない場合は、**[無期限]** を選択します。 **注意**:「グローバル管理者」グループ内のすべてのアカウントがロックされた場合、Tenable Identity Exposure は 10 秒後にデフォルトの管理アカウントをロック解除します。	300 秒
ロックアウトまでの試行回数	Tenable Identity Exposure がアカウントをロックするまでに許容するログイン試行失敗の回数です。	3
猶予期間	Tenable Identity Exposure が失敗したログイン試行をカウントする期間です。この期間内にログイン試行に一定の回数失敗すると、Tenable Identity Exposure はアカウントをロックします。 猶予期間を設定するには、次を実行します。	900 秒

	1. スライダーをクリックして、期間を設定します。 2. Tenable Identity Exposure がアカウントをロックするまでに失敗したログインの試行回数をカウントする期間を設定したくない場合は、[無期限]を選択します。	

6. **[保存]**をクリックします。

ロックアウトポリシーを無効にするには

1. Tenable Identity Exposure で、**[システム]** > **[設定]**をクリックします。

   設定ペインが表示されます。

2. **[有効]**トグルをクリックして、ロックアウトポリシーをオフにします。

注意: ロックアウトポリシーを無効にした場合、ロックされていたユーザーアカウントが再接続できるようになります。

ロックされているアカウントの一覧を表示するには

- Tenable Identity Exposure で、**[アカウント]** > **[ユーザーアカウント管理]**に移動します。

  ユーザーの一覧で、Tenable Identity Exposure はロックされたアカウントに赤い南京錠のアイコン付けて表示します。アカウントがロックされたユーザーには Tenable Identity Exposure から「認証の試行に失敗した回数が多すぎるため、アカウントがブロックされています。管理者に連絡してください。」のメッセージが表示されます。

アカウントのロックを解除するには

アカウントのロックを解除するには、ユーザーを編集するアクセス許可が必要です。

1. Tenable Identity Exposure で、**[アカウント]** > **[ユーザーアカウント管理]**をクリックします。

   [ユーザーアカウント管理]ペインが表示されます。

2. ユーザーの一覧で、ロックされたアカウントを見つけます。
3. 鉛筆アイコンをクリックして、ロックされたユーザーアカウントを編集します。

ユーザーの情報ペインが表示されます。

4. **[ロックアウトの削除]** ボタンをクリックします。

ロックアウトポリシーを設定するアクセス許可をユーザーロールに付与するには

1. Tenable Identity Exposure で、**[アカウント]** > **[ロール管理]** をクリックします。

   [ロール管理] ペインが表示されます。

2. ロール名の横にある鉛筆アイコンをクリックして、ロールを編集します。

   [ロールの編集] ペインが表示されます。

3. **[システム設定エンティティ]** タブをクリックします。

4. **[アクセス許可管理]** セクションで、**[アカウントロックアウトポリシー]** チェックボックスをオンにします。

5. トグルをクリックして、**[不許可]** または **[許可]** にします。

   Tenable Identity Exposure がユーザーのアクセス許可を更新したことを確認するメッセージが表示されます。

   > **注意**: 読み取りのアクセス許可しかないユーザーの場合、Tenable Identity Exposure はこのペインのロックアウトポリシー設定を無効にします。

LDAP を使用した認証

Tenable Identity Exposure のユーザーは、Lightweight Directory Access Protocol (LDAP) を使用して認証できます。

LDAP 認証を有効にするには、以下が必要です。

- Active Directory にアクセスするためのユーザーとパスワードが事前設定されたサービスアカウント
- 事前設定された Active Directory グループ

LDAP 認証を設定した後、LDAP オプションがログインページのタブに表示されます。

LDAP 認証を設定するには

1. Tenable Identity Exposure で、**[システム]** > **[設定]** をクリックします。

   設定ペインが表示されます。

2. **[認証]** セクションで **[LDAP]** をクリックします。
3. **[LDAP 認証の有効化]** トグルをクリックして有効にします。

   LDAP 情報フォームが表示されます。

4. 以下の情報を入力します。

   - **[LDAP サーバーのアドレス]** ボックスに、`ldap://` で始まりドメイン名とポート番号で終わる、LDAP サーバーの IP アドレスを入力します。

     > **注意**: LDAPS サーバーを使用する場合は、`ldaps://` で始まりドメイン名とポート番号で終わるアドレスを入力してください。LDAPS のカスタムの信頼できる認証局 (CA) の証明書を追加するには の手順を参照して、LDAPS の設定を完了してください。

   - **[LDAP サーバーをクエリするために使用されるサービスアカウント]** ボックスに、LDAP サーバーへのアクセスに使用する識別名 (DN)、SamAccountName、UserPrincipalName のいずれかを入力します。
   - **[サービスアカウントのパスワード]** ボックスに、このサービスアカウントのパスワードを入力します。
   - **[LDAP 検索ベース]**ボックスに、DC= または OU= で始まる LDAP ディレクトリを入力します。Tenable Identity Exposure はこのディレクトリを使用して、接続を試みるユーザーを

検索します。これは、ルートディレクトリまたは特定の組織単位にすることができます。

- **[LDAP 検索フィルター]** ボックスに、Tenable Identity Exposure がユーザーにフィルターを掛けるのに使用する属性を入力します。Active Directory の認証の標準属性は `sAMAccountname={{login}}` です。`login` の値は、ユーザーが認証時に入力する値です。

5. **[SASL バインディングの有効化]** で、次のいずれかを実行します。
   - サービスアカウントに SamAccountName を使用している場合は、**[SASL バインディングの有効化]** トグルをクリックして有効にします。
   - サービスアカウントに識別名か UserPrincipalName を使用している場合は、**[SASL バインディングの有効化]** を無効のままにしておきます。
6. **[デフォルトのプロファイルとロール]** セクションで、**[LDAP グループの追加]** をクリックして、認証を許可するグループを指定します。

   LDAP グループ情報フォームが表示されます。
   - **[LDAP グループ名]** ボックスに、グループの識別名を入力します (例: `CN=TAD_User`、`OU=Groups`、`DC=Tenable`、`DC=ad`)。
   - **[デフォルトのプロファイル]** ドロップダウンボックスで、許可するグループのプロファイルを選択します。
   - **[デフォルトのロール]** ボックスで、許可するグループのロールを選択します。
7. 必要に応じて、⊕ アイコンをクリックし、新しい許可グループを追加します。
8. **[保存]** をクリックします。

LDAPS のカスタムの信頼できる認証局 (CA) の証明書を追加するには

1. Tenable Identity Exposure で、**[システム]** をクリックします。
2. **[設定]** タブをクリックして、設定ペインを表示します。
3. **[アプリケーションサービス]** セクションで、**[信頼できる認証局]** をクリックします。
4. **[追加の CA 証明書]** ボックスに、会社の信頼できるCA証明書を PEM エンコードして貼り付けて、Tenable Identity Exposure が使用できるようにします。
5. **[保存]** をクリックします。

セキュリティプロファイルとロールの詳細については、以下を参照してください。

- セキュリティプロファイル
- ユーザーロール

SAML を使用した認証

Tenable Identity Exposure ユーザーが Tenable Identity Exposure にログインするときに ID プロバイダーによるシングルサインオン (SSO) を使用できるように、SAML 認証を設定できます。

始める前に

- Tenable Identity Exposure で使用するために SAML を設定する方法については、Tenable SAML 設定クイックリファレンスガイドにある手順を確認してください。
- アイデンティティプロバイダー (IDP) の次のものがあることを確認します。
  - SAML v2 のみ
  - 「アサーション暗号化」が有効になりました。
  - Tenable Identity Exposure ウェブポータルで Tenable Identity Exposure がアクセス権を付与するために使用する IDP グループ
  - SAML サーバーの URL
  - `-----BEGIN CERTIFICATE-----` で始まり `-----END CERTIFICATE----` で終わる PEM エンコード形式で、SAML サーバー証明書に署名した信頼できる認証局 (CA)

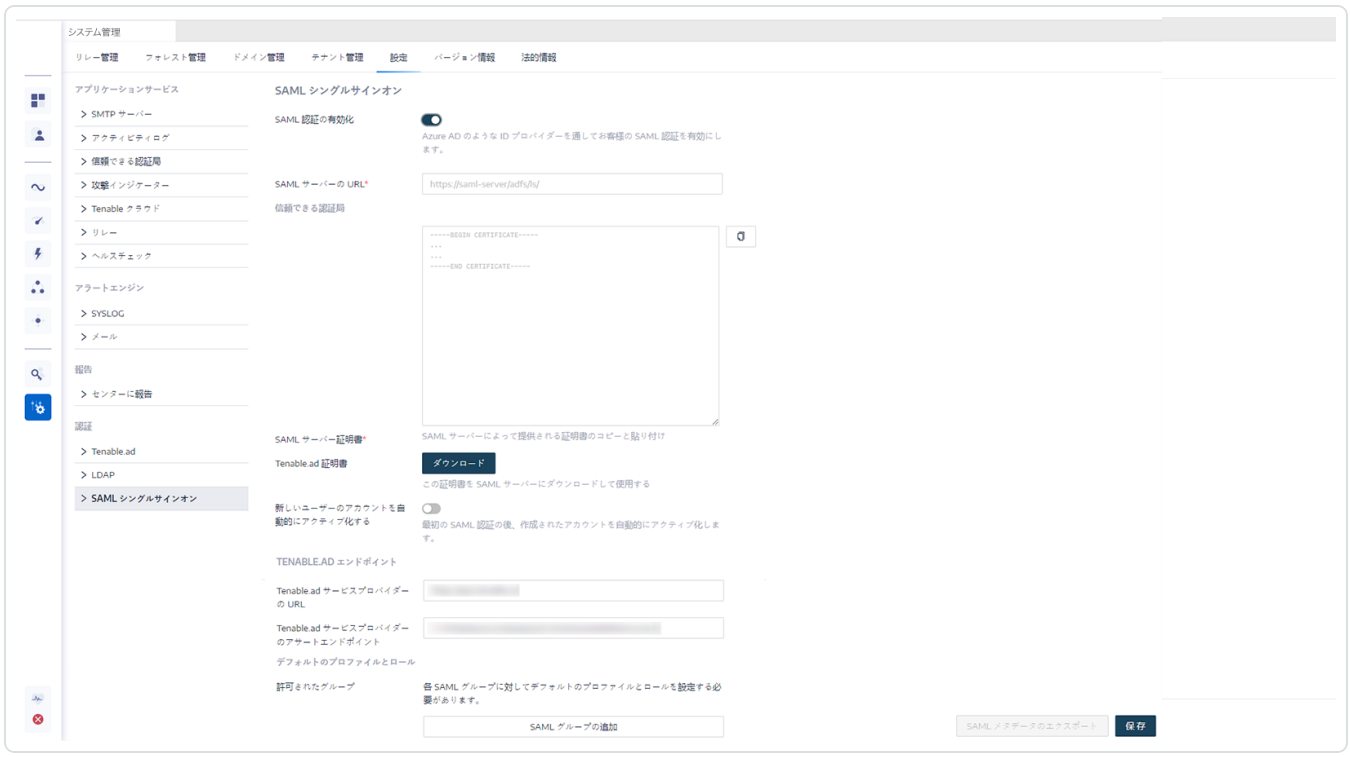
SAML 認証を設定するには:

1. Tenable Identity Exposure で、**[システム]** > **[設定]** をクリックします。

   設定ペインが表示されます。

2. **[認証]** セクションで **[SAML シングルサインオン]** をクリックします。
3. **[SAML 認証の有効化]** トグルをクリックします。

   SAML 情報フォームが表示されます。



4. 以下の情報を入力します。

   - **[SAML サーバーの URL]** ボックスに、Tenable Identity Exposure が接続する必要がある IDP の SAML サーバーの完全な URL を入力します。
   - **[信頼された認証局]** ボックスに、SAML サーバーの証明書に署名した CA を貼り付けます。

5. **[Tenable Identity Exposure 証明書]**ボックスで、**[生成してダウンロード]** をクリックします。これにより、新しい自己署名証明書が生成され、データベースの SAML 設定が更新され、ダウンロードする新しい証明書が返されます。

   警告: このボタンをクリックすると、SAML 設定が中断されます。これは、IDP が依然として以前の証明書(存在する場合)を使用しているのに、Tenable Identity Exposure は IDP が直近に生成された証明書ですぐに認証することを想定しているためです。新しい Tenable Identity Exposure 証明書を生成する場合は、新しい証明書を使用するように IDP を再設定する必要があります。

6. 最初の SAML ログイン後に新しいユーザーのアカウントをアクティブ化するには、**[新しいユーザーのアカウントを自動的にアクティブ化する]** トグルをクリックします。

7. **[Tenable Identity Exposure エンドポイント]** で、以下の情報を入力します。

- Tenable Identity Exposure サービスプロバイダーの URL
- Tenable Identity Exposure サービスプロバイダーのアサートエンドポイント

8. **[デフォルトのプロファイルとロール]** セクションで、**[SAML グループの追加]**をクリックして、認証を許可するグループを指定します。

   SAML グループ情報フォームが表示されます。

9. 以下の情報を入力します。
   - **[SAML グループ名]** ボックスに、許可されているグループの名前を入力します。この名前が SAML サーバーに表示されます。
   - **[デフォルトのプロファイル]** ドロップダウンボックスで、許可するグループのプロファイルを選択します。
   - **[デフォルトのロール]** ボックスで、許可するグループのロールを選択します。
10. 必要に応じて、⊕ アイコンをクリックし、新しい許可グループを追加します。
11. **[保存]** をクリックします。

    SAML 認証をセットアップした後、SAML オプションがログインページのタブに表示されます。

セキュリティプロファイルとロールの詳細については、以下を参照してください。

- セキュリティプロファイル
- ユーザーロール

ユーザーアカウント

[ユーザーアカウント管理] ページで、Tenable Identity Exposure ユーザーアカウントを追加、編集、削除したり、またはその詳細情報を表示したりすることができます。

ユーザーは次の 2 つのカテゴリのいずれかに属します。

- グローバル管理者 – すべてのアクセス許可を持つ管理者ロール
- ユーザー – ビジネスデータのみに対する読み取り専用アクセス許可を持つ単純なユーザーロール

詳細については、次を参照してください。

- ユーザーの作成
- ユーザーの編集
- ユーザーの無効化
- ユーザーの削除

ユーザーの作成

必須のユーザーロール: 適切なアクセス許可を持つ管理者または組織のユーザー

注意: 次の手順は、Tenable Identity Exposure のスタンドアロンインスタンスに当てはまるものです。Tenable Vulnerability Management にリンクされたインスタンスの場合、Tenable Vulnerability Management でユーザーを作成してください。これが後に Tenable Identity Exposure に伝播されます。

ユーザーを作成するには:

1. Tenable Identity Exposure で、**[アカウント]** > **[ユーザーアカウント管理]** をクリックします。

   [ユーザーアカウント管理] ペインが表示されます。

2. 右側にある **[ユーザーの作成]** ボタンをクリックします。

   [ユーザーの作成] ペインが表示されます。

3. **[主要な情報]** セクションで、ユーザーに関する以下の情報を入力します。

   - 名
   - 姓 (名字)
   - E メール
   - パスワード (12 文字以上、少なくとも 1 つの小文字、1 つの大文字、1 つの数字、1 つの特殊文字を含む)
   - パスワードの確認
   - 部署
   - 経歴

4. **[認証を許可]** トグルをクリックして、ユーザーをアクティブ化します。

5. **[ロール管理]** セクションで、ユーザーに適用するロールを選択します。

6. **[作成]** をクリックします。

   Tenable Identity Exposure が選択されたロールでユーザーを作成したことを確認するメッセージが表示されます。

関連項目

- ユーザーの編集
- ユーザーの無効化
- ユーザーの削除

ユーザーの編集

必要なユーザーロール: 適切なアクセス許可を持つ管理者または組織のユーザー

ユーザーを編集するには

1. Tenable Identity Exposure で、**[アカウント]** > **[ユーザーアカウント管理]** をクリックします。

   [ユーザーアカウント管理] ペインが表示されます。

2. ユーザーのリストで、ユーザーの名前が表示されている行にカーソルを合わせ、行末の アイコンをクリックします。

   [ユーザーの編集] ペインが表示されます。

3. **[主要な情報]** セクションで、必要に応じてユーザーに関する情報を変更します。
   - 名
   - 姓 (名字)
   - E メール
   - パスワード: 8 文字以上
   - パスワードの確認
   - 部署
   - 経歴
4. **[ロール管理]** セクションで、必要に応じてユーザーのロールを変更します。
5. **[編集]** をクリックします。

   Tenable Identity Exposure が選択したロールのユーザーを更新したことを確認するメッセージが表示されます。

関連項目

- ユーザーの作成
- ユーザーの無効化
- ユーザーの削除

ユーザーの無効化

必要なユーザーロール: 適切なアクセス許可を持つ管理者または組織のユーザー

ユーザーを無効化するには

1. Tenable Identity Exposure で、**[アカウント]** > **[ユーザーアカウント管理]** をクリックします。

   [ユーザーアカウント管理] ペインが表示されます。

2. ユーザーのリストで、ユーザーの名前が表示されている行にカーソルを合わせ、行末の アイコンをクリックします。

   [ユーザーの編集] ペインが表示されます。

3. **[認証を許可]** トグルをクリックして、ユーザーを無効化します。

4. **[編集]** をクリックします。

   Tenable Identity Exposure がユーザーを更新したことを確認するメッセージが表示されます。

関連項目

- ユーザーの作成
- ユーザーの編集
- ユーザーの削除

ユーザーの削除

必要なユーザーロール: 適切なアクセス許可を持つ管理者または組織のユーザー

ユーザーを削除するには

1. Tenable Identity Exposure で、**[アカウント]** > **[ユーザーアカウント管理]** をクリックします。

   [ユーザーアカウント管理] ペインが表示されます。

2. ユーザーのリストで、削除するユーザーの名前が表示されている行にカーソルを合わせ、行末の アイコンをクリックします。

   削除の確認を求めるメッセージが表示されます。

3. **[削除]** をクリックします。

   Tenable Identity Exposure がユーザーを削除したことを確認するメッセージが表示されます。

関連項目

- ユーザーの作成
- ユーザーの編集
- ユーザーの無効化

セキュリティプロファイル

必要なユーザーロール: 適切なアクセス許可を持つ管理者または組織のユーザー

プロファイルを使用すると、Active Directory に影響を与えるリスクを表示する独自のビューを作成してカスタマイズできます。

各プロファイルには、そのプロファイルを持つユーザーのために設定された露出と攻撃のシナリオが表示されます。たとえば、データ分析に対する IT 管理者の一般的な見方は、AD インフラが直面するすべてのリスクの包括的な見解を示すセキュリティチームの見方とは異なる可能性があります。

セキュリティプロファイルを適用すると、異なる種類のユーザーが、そのセキュリティプロファイルのインジケーターで定義されたとおり、データ分析を異なる見方で検証できるようになります。

[セキュリティプロファイル管理] ペインでは、さまざまなレポート角度からセキュリティ分析をレビューできるように、さまざまなユーザータイプを維持管理できるようになっています。セキュリティプロファイルでも、露出インジケーターと攻撃インジケーターの動作をカスタマイズできます。

注意: Tenable Identity Exposure には「Tenable」と呼ばれるデフォルトのセキュリティプロファイルが用意されています。**この Tenable プロファイルを変更または削除することはできません**。ただし、これをテンプレートとして使用し、必要に応じて設定を調整して他のセキュリティプロファイルを作成することはできます。

セキュリティプロファイルを新規作成するには

1. Tenable Identity Exposureで、**[アカウント]** > **[セキュリティプロファイル管理]** をクリックします。

   [セキュリティプロファイル管理] ペインが表示されます。

2. 右側にある **[プロファイルの作成]** ボタンをクリックします。

   [プロファイルの作成] ペインが表示されます。

3. アクションドロップダウンボックスから、次のいずれかを実行できます。

   - **新しいプロファイルを作成する**
   - 新しいプロファイルの作成元になる既存のセキュリティプロファイルを**コピー**する (例:「Tenable」プロファイル)

4. **[新しいプロファイルの名前]** ボックスに、新しいプロファイルの名前を入力します。

> **注意：** Tenable Identity Exposureは英数字とアンダースコアのみ使用できます。

5. 右下隅の**[作成]**ボタンをクリックします。

   Tenable Identity Exposure がプロファイルを作成したことを示すメッセージが表示されます。**[プロファイルの設定]**ペインが表示されます。

セキュリティプロファイルを削除するには

1. Tenable Identity Exposureで、**[アカウント]** > **[セキュリティプロファイル管理]**をクリックします。

   [セキュリティプロファイル管理]ペインが表示されます。

2. セキュリティプロファイルのリストで、削除するセキュリティプロファイルにカーソルを合わせ、行末の🗑アイコンをクリックします。

   削除の確認を求めるメッセージが表示されます。

3. **[削除]**をクリックします。

   Tenable Identity Exposure がプロファイルを削除したことを確認するメッセージが表示されます。

次の手順

プロファイル作成を完了するための詳細は、インジケーターのカスタマイズを参照してください。

詳細については、次を参照してください。

- インジケーターのカスタマイズ
- インジケーターのカスタマイズの調整

インジケーターのカスタマイズ

必要なユーザーロール: 適切なアクセス許可を持つ管理者または組織のユーザー

セキュリティプロファイルの露出インジケーターと攻撃インジケーターをカスタマイズできます。

各セキュリティプロファイルは独立して動作し、あるプロファイルが別のプロファイルの結果に影響を与えないようにしてください。「Tenable」プロファイルは、カスタマイズしたり逸脱をホワイトリストに登録したりすることはできないため、あくまで参考として使用してください。特定の要件を満たすには、独自のカスタムプロファイルを作成する必要があります。

インジケーターのカスタマイズペインの「グローバルカスタマイズ」という用語は、すべてのプロファイルではなく**すべてのドメインに関連しています**。その結果、あるセキュリティプロファイルの「グローバルカスタマイズ」に適用した設定が、「Tenable」プロファイルや別のプロファイルに影響を与えることはありません。

ヒント:「Tenable」セキュリティプロファイルの設定を表示するには、行末の 👁 アイコンをクリックします。

インジケーターをカスタマイズするには

1. Tenable Identity Exposureで、**[アカウント]** > **[セキュリティプロファイル管理]** をクリックします。

   [セキュリティプロファイル管理] ペインが表示されます。

2. セキュリティプロファイルのリストで、カスタマイズするインジケーターが含まれているセキュリティプロファイルにカーソルを合わせます。セキュリティプロファイル名が表示されている行の末尾にある ✎ アイコンをクリックします。

   [プロファイルの設定] ペインが表示されます。

3. **[露出インジケーター]** または **[攻撃インジケーター]** タブを選択します。

4. (オプション) **[インジケーターの検索]** ボックスに、インジケーター名を入力します。

5. カスタマイズするインジケーターの名前をクリックします。

   [インジケーターのカスタマイズ] ペインが表示されます。

6. インジケーターに必要なカスタマイズを行います。

   注意: 特定のインジケーターオプションでは、正規表現 (regex) を使用する必要があります。正規表現は、「部分」一致であり「完全」一致ではありません。例: 入力オプションとして「admin」を指定すると、

「samAccountName=admin」のユーザーと「samAccountName=admintoto」のユーザーをホワイトリストに登録できます。
- 完全一致にするには、正規表現の特殊文字(「^...$」)構文を使用する必要があります。
- また、正規表現を使用する場合は、バックスラッシュで特殊文字をエスケープする必要があります。例:「domain\user」および「CN=Vincent C. (Test),DC=tenable,DC=corp」を宣言するには、「domain\\user」および「CN=Vincent C. \(Test\),DC=tenable,DC=corp」と入力します。

7. **[ドラフトとして保存]** をクリックします。

   Tenable Identity Exposure がカスタマイズオプションを保存したことを確認するメッセージが表示されます。

カスタマイズを適用するには

1. 次のいずれかを行うことができます。

   - **[プロファイルの設定]** ペインで、右下隅の **[保留中のカスタマイズを適用する]** をクリックします。
   - **[セキュリティプロファイル管理]** ペインで、セキュリティプロファイル名が表示されている行の末尾にある ✓ アイコンをクリックします。

   カスタマイズを適用するとすべてのデータが消去され、監視対象の Active Directory の完全な分析が必要になり、これには時間がかかることがあることを警告するメッセージが表示されます。

2. **[OK]** をクリックします。

   Tenable Identity Exposure がカスタマイズオプションを適用したことを確認するメッセージが表示されます。**[セキュリティプロファイル管理]** テーブルの *[セキュリティ分析]* 列に表示されている **[待機中]** は、セキュリティプロファイルに基づいた分析が実行待ちであることを示します。

カスタマイズを破棄するには

- 次のいずれかを行うことができます。
  - **[プロファイルの設定]** ペインで、右下隅の **[保留中のカスタマイズを元に戻す]** をクリックします。
  - **[セキュリティプロファイル管理]** ペインで、セキュリティプロファイル名が表示されている行の末尾にある ↶ アイコンをクリックします。

Tenable Identity Exposure がカスタマイズオプションを取り消したことを確認するメッセージが表示されます。

関連項目

- インジケーターのカスタマイズの調整

インジケーターのカスタマイズの調整

必要なユーザーロール: 適切なアクセス許可を持つ管理者または組織のユーザー

セキュリティプロファイルのインジケーターをさらにカスタマイズすることで、特定のドメインのインジケーターオプションを選択できます。デフォルトでは、グローバルカスタマイズがすべてのドメインに適用されます。

インジケーターのカスタマイズを調整するには

1. Tenable Identity Exposureで、**[アカウント]** > **[セキュリティプロファイル管理]** をクリックします。

   [セキュリティプロファイル管理] ペインが表示されます。

2. セキュリティプロファイルのリストで、カスタマイズするインジケーターが含まれているセキュリティプロファイルにカーソルを合わせます。セキュリティプロファイル名が表示されている行の末尾にある アイコンをクリックします。

   [プロファイルの設定] ペインが表示されます。

3. **[露出インジケーター]** または **[攻撃インジケーター]** タブを選択します。

4. (オプション) **[インジケーターの検索]** ボックスに、インジケーター名を入力します。

5. カスタマイズするインジケーターの名前をクリックします。

   [インジケーターのカスタマイズ] ペインが表示されます。

6. **[グローバルなカスタマイズ]** タブの横にある + アイコンをクリックします。

   [カスタマイズ番号1] タブが表示されます。

7. **[適用先]** ボックスをクリックします。

   [フォレストとドメイン] ペインが表示されます。

8. (オプション) 検索ボックスに、フォレストまたはドメインの名前を入力します。

9. そのドメインを選択します。

10. **[選択内容でフィルター]** をクリックします。

11. 必要に応じて、選択したドメインのインジケーターをさらにカスタマイズします。

12. **[ドラフトとして保存]** をクリックします。

調整したカスタマイズを破棄するには

1. カスタマイズのタブをクリックします。
2. ペインの下部にある **[この設定を削除]** をクリックします。

関連項目

- インジケーターのカスタマイズ

ユーザーロール

Tenable Identity Exposure では、企業内のデータや機能に安全にアクセスするために、ロールベースのアクセス制御 (RBAC) を使用しています。ユーザーのロールに応じて、ユーザーが自分のアカウントからアクセスできる情報のタイプが決まります。

適切なアクセス許可を持つユーザーは自分のロールに基づいて、他のユーザーに以下のアクションを実行できるアクセス許可を割り当てることができます。

- コンテンツとメニュー、システム、露出インジケーターの設定の読み取り
- コンテンツとメニュー、システム、攻撃インジケーターの設定の編集
- アカウント、セキュリティプロファイル、ロールの作成

関連項目

- ロールの管理
- ロールのアクセス許可の設定
- ユーザーインターフェースエンティティに対するアクセス許可の設定 (例)

ロールの管理

新しいロールを作成するには

1. Tenable Identity Exposureで、**[アカウント]** > **]ロール管理]** に移動します。
2. 右上隅の **[ロールの作成]** ボタンをクリックします。

   [ロールの作成] ペインが表示されます。
3. 名前ボックスにロールの名前を入力します。
4. 説明ボックスに、ロールに関する情報を入力します。
5. 右下隅の **[追加]** をクリックします。

   Tenable Identity Exposure がロールを作成したことを確認するメッセージが表示されます。ロールのアクセス許可を設定する **[ロールの編集]** ペインが表示されます。

注意: Tenable Identity Exposure 管理者ロール(グローバル管理者と呼ばれる)は変更できません。👁 アイコンをクリックすると、Tenable Identity Exposure のロール設定が表示されます。

ロールを削除するには

1. Tenable Identity Exposureで、**[アカウント]** > **]ロール管理]** に移動します。
2. ロールのリストで、削除するロールにカーソルを合わせ、右側の 🗑 アイコンをクリックします。

   削除の確認を求めるメッセージが表示されます。
3. [削除]をクリックします。

   ロールが削除されたことを確認するメッセージが表示されます。

関連項目

- ロールのアクセス許可の設定

ロールのアクセス許可の設定

必要なユーザーロール: 適切なアクセス許可を持つ管理者または組織のユーザー

Tenable Identity Exposure はロールベースのアクセス制御 (RBAC) を使用して、データへのアクセスを保護しています。ロールは、組織における職能的役割に応じて、ユーザーがアクセスできる情報の種類を決定します。Tenable Identity Exposure で新しいユーザーを作成するとき、関連するアクセス許可を持つ特定のロールをそのユーザーに割り当てます。

ロールのアクセス許可を設定するには

1. Tenable Identity Exposure で、**[アカウント]** > **[ロール管理]** をクリックします。
2. アクセス許可を設定するロールにカーソルを合わせ、右側の アイコンをクリックします。

   [ロールの編集] ペインが表示されます。
3. **[アクセス許可管理]** で、エンティティタイプを選択します。
   - データエンティティ
   - ユーザーエンティティ
   - システム設定エンティティ
   - インターフェースエンティティ
4. エンティティ名のリストで、アクセス許可を設定するエンティティを選択します。
5. **[読み取り]**、**[編集]**、**[作成]** の列のトグルをクリックして、[許可] または [不許可] にします。
6. 次のいずれかを行うことができます。
   - [適用] をクリックしてアクセス許可を適用し、**[ロールの編集]** ペインを開いたままにして、さらに変更を行います。
   - [適用して閉じる] をクリックしてアクセス許可を適用し、**[ロールの編集]** ペインを閉じます。

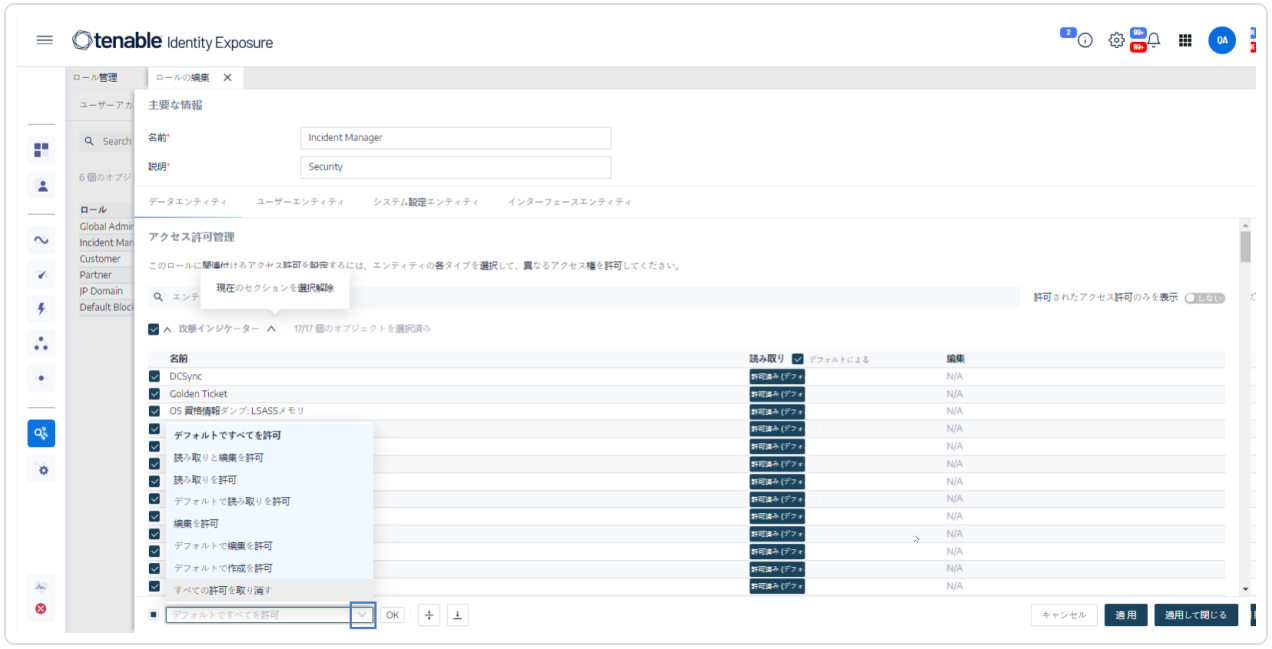
   Tenable Identity Exposure がロールを更新したことを確認するメッセージが表示されます。

ロールのアクセス許可を一括設定するには

1. Tenable Identity Exposure で、**[アカウント]** > **[ロール管理]** をクリックします。
2. アクセス許可を設定するロールにカーソルを合わせ、右側の アイコンをクリックします。

   [ロールの編集] ペインが表示されます。
3. **[アクセス許可管理]** で、エンティティタイプを選択します。
4. アクセス許可を設定するエンティティまたはエンティティのセクション(露出インジケーターなど)を選択します。
5. ページの下部で、ドロップダウンボックスの矢印をクリックして、アクセス許可のリストを表示します。
6. ロールのアクセス許可を選択します。
7. **[OK]** をクリックします。

   Tenable Identity Exposure がエンティティのアクセス許可を設定したことを確認するメッセージが表示されます。



アクセス許可の種類

アクセス許可	説明
読み	オブジェクトまたは設定を表示するアクセス許可です。

取り	
編集	オブジェクトまたは設定を変更するアクセス許可です。変更を適用するには、読み取りアクセス許可が必要です。
作成	オブジェクトまたは設定を作成するアクセス許可です。**[作成]**アクセス許可には、許可されたリソースに対して許可されたアクションを行うための**[読み取り]**と**[編集]**のアクセス許可が必要です。

エンティティの種類

Tenable Identity Exposure には、アクセス許可が必要な 4 つのタイプのエンティティがあり、企業の各ユーザーロールに合わせて調整できます。

エンティティの種類	含まれるもの	アクセス許可
データエンティティ		
このエンティティは、監視対象の Active Directory をセットアップしたり、Tenable Identity Exposure でデータ分析を設定したりするためのアクセス許可を制御します。	• 攻撃インジケーター • 露出インジケーター • フォレスト • ドメイン • プロファイル • ユーザー • メールによるアラート • Syslog によるアラート • ロール • エンティティリレー • レポート	読み取り、編集、作成
ユーザーエンティティ		

このエンティティは、ユーザーがデータ分析のために Tenable Identity Exposure で表示される情報を設定したり、個人情報や環境設定を変更したりする権限を制御します。	• 環境設定 • ダッシュボード • ウィジェット • API キー • 個人情報	編集、作成
システム設定エンティティ		
このエンティティは、Tenable Identity Exposure プラットフォームとサービスへのアクセスを制御します。	• アプリケーションサービス (SMTP、ログ、認証 Tenable Identity Exposure、攻撃インジケーター、信頼できる認証局) • 公開 API によるスコア • ライセンス • LDAP 認証 • SAML 認証 **注意**: Tenable Vulnerability Management ライセンスがある場合、LDAP および SAML 認証のアクセス許可は利用できません。 • トポロジー • アカウントロックアウトポリシー • ドメインの再クロール • アクティビティログ • Tenable クラウドサービス (Tenable クラウドのデータ収集) • Microsoft Entra ID のサポート • ヘルスチェック	読み取り、編集

	• ユーザー自身のトレースのみを表示	
インターフェースエンティティ		
このエンティティは、Tenable Identity Exposure のユーザーインターフェースと機能の特定の部分にアクセスするためのアクセス許可を定義します。	Tenable Identity Exposure の特定の機能へのアクセスパス。詳細は、ユーザーインターフェースエンティティに対するアクセス許可の設定 (例)を参照してください。	許可、不許可

関連項目

- ユーザーアカウント
- ユーザーロール

ユーザーインターフェースエンティティに対するアクセス許可の設定（例）

Tenable Identity Exposure は特定のユーザーインターフェース機能へのアクセスに使用されるパスに沿ってアクセス許可を適用します。次の例は、Syslog の設定を許可するアクセス許可を設定する方法を示しています。

Syslog パラメーターに到達するには、Tenable Identity Exposure の **[システム]** > **[設定]** > **[SYSLOG]** のパスで設定されているアクセス許可がユーザーに必要です。

- システム設定: **[管理]** > **[システム]**
- 設定パラメーター: **[管理]** > **[システム]** > **[設定]**
- Syslog アラート: **[管理]** > **[システム]** > **[設定]** > **[アラートエンジン]** > **[SYSLOG]**

Syslog 設定のアクセス許可を設定するには

1. Tenable Identity Exposure で、**[アカウント]** > **[ロール管理]** をクリックします。
2. アクセス許可を設定するロールにカーソルを合わせ、右側の アイコンをクリックします。

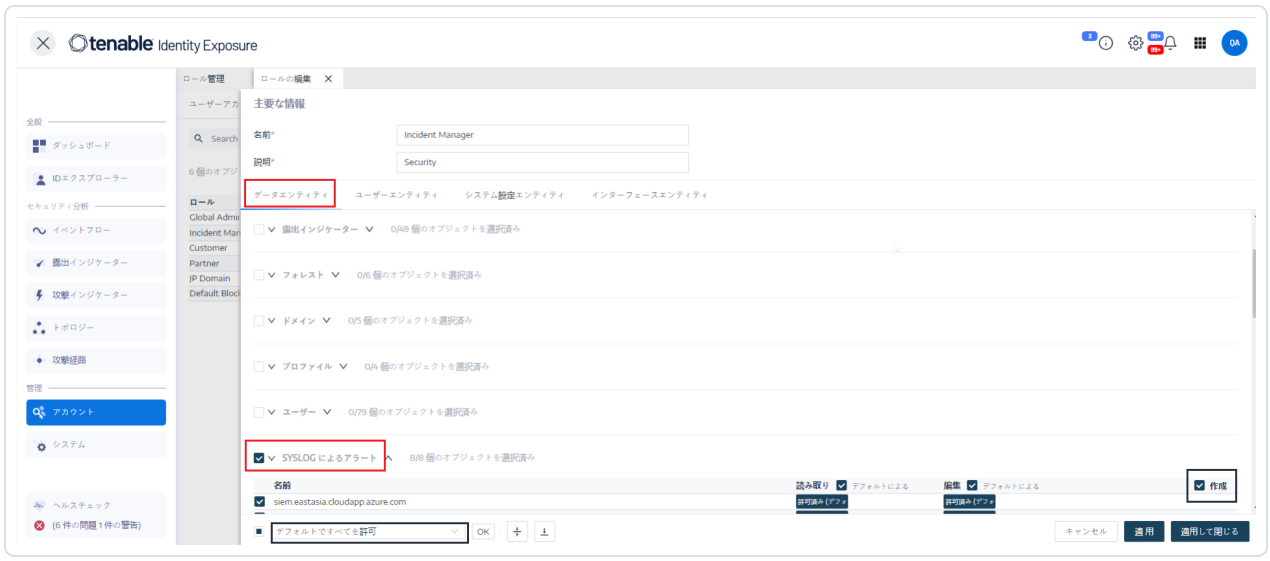
   [ロールの編集] ペインが表示されます。
3. **[アクセス許可管理]** で、**[インターフェースエンティティ]** を選択します。
4. エンティティのリストで、次の操作を実行します。
   - **[管理]** > **[システム]** を選択し、アクセストグルをクリックして **[許可]** に切り替えます。
   - **[管理]** > **[システム]** > **[設定]** を選択し、アクセストグルをクリックして **[許可]** に切り替えます。
   - **[管理]** > **[システム]** > **[設定]** > **[アラートエンジン]** > **[SYSLOG]** を選択し、アクセストグルをクリックして **[許可]** に切り替えます。
5. **[適用]** をクリックします。

   Tenable Identity Exposure がエンティティのアクセス許可を更新したことを確認するメッセージが表示されます。

6. **[アクセス許可管理]** で、**[データエンティティ]** を選択します。
7. エンティティリストのセクションで、**[Syslog によるアラート]** を選択します。
8. **[作成]** アクセス許可を選択します。

   Tenable Identity Exposure は暗黙的に読み取りおよび編集のアクセス許可を付与します。
9. **[適用して閉じる]** をクリックします。

   Tenable Identity Exposure がエンティティのアクセス許可を更新したことを確認するメッセージが表示されます。


tenable Identity Exposure
ロール管理
ロールの編集
主要な情報
名前*
Incident Manager
説明*
Security
データエンティティ
ユーザーエンティティ
システム設定エンティティ
インターフェースエンティティ
露出インジケーター
0/49 個のオブジェクトを選択済み
フォレスト
0/6 個のオブジェクトを選択済み
ドメイン
0/5 個のオブジェクトを選択済み
プロファイル
0/4 個のオブジェクトを選択済み
ユーザー
0/79 個のオブジェクトを選択済み
SYSLOG によるアラート
8/8 個のオブジェクトを選択済み
名前
読み取り
編集
作成
siem.eastasia.cloudapp.azure.com
デフォルトですべてを許可
OK
キャンセル
適用
適用して閉じる
ダッシュボード
IDエクスプローラー
イベントフロー
露出インジケーター
攻撃インジケーター
トポロジー
攻撃経路
アカウント
システム
ヘルスチェック
(6 件の問題 1 件の警告)

フォレスト

Active Directory (AD) フォレストは、共通のスキーマ、設定、信頼関係を共有するドメインの集合体です。リソースを管理して整理できる階層構造が提供されるため、企業内の多数のドメインを集中管理したりセキュアな認証を行ったりすることが可能になります。

フォレストの管理

フォレストを追加するには

1. Tenable Identity Exposure で、**[システム]** > **[フォレスト管理]** をクリックします。
2. 右側の **[フォレストの追加]** をクリックします。

   フォレストの追加ペインが表示されます。
3. **[名前]** ボックスにフォレスト名を入力します。
4. **[アカウント]** セクションで、Tenable Identity Exposure が使用するサービスアカウントの以下の情報を入力します。

   - **ログイン**: サービスアカウントの名前を入力します
     形式: ユーザープリンシパル名 (例: `tenablead@domain.example.com`)(Kerberos 認証との互換性を得るために推奨)、または NetBIOS (例: `DomainNetBIOSName\SamAccountName`
   - **パスワード**: このサービスアカウントのパスワードを入力します

   注意: 保護されたユーザーは NTLM 認証を使用できないため、Tenable Identity Exposure の AD サービスアカウントを保護されたユーザーグループのメンバーとして設定する必要がある場合は、Tenable Identity Exposure 設定で Kerberos 認証 がサポートされていることを確認してください。
5. **[追加]** をクリックします。

   新しいフォレストの追加を確認するメッセージが表示されます。

フォレストを編集するには

1. Tenable Identity Exposure で、**[システム]** > **[フォレスト管理]** をクリックします。
2. フォレストのリストで、変更するフォレストにカーソルを合わせ、右側の ✎ アイコンをクリックします。

   [フォレストの編集] ペインが表示されます。
3. 必要に応じて変更します。
4. **[編集]** をクリックします。

   Tenable Identity Exposure がフォレストを更新したことを確認するメッセージが表示されます。

サービスアカウントの保護

Tenable は、ユーザーアカウント制御 (UAC) 属性を正しく設定することでサービスアカウントを保護し、セキュリティを維持することを推奨しています。これにより、委任の防止、事前認証の要求、より強力な暗号化の使用、パスワードの期限切れと要件の強制実行、承認されたパスワードの変更の許可が可能になります。このような手段を講じることにより、認証されていないアクセスや潜在的なセキュリティ侵害のリスクを軽減しつつ、企業のシステムとデータの整合性を確保できます。

Windows ポリシーエディターを使用して設定を変更するには

適切な管理者権限を使用して Windows のローカルセキュリティポリシーエディターまたはグループポリシーエディターを使用して、ユーザーアカウント制御設定を変更できます。

- エディターで、**[ローカル ポリシー]** > **[セキュリティ オプション]** に進み、次の設定を見つけて設定します (この手順はご使用の Windows のバージョンによって異なる場合があります)。
    - *「ネットワーク アクセス: ネットワーク認証のためにパスワードと認証情報の保存を許可しない」* を **[有効]** に設定します。
    - *「アカウント: Kerberos 事前認証を必須にしない」* を **[無効]** に設定します。
    - *「ネットワーク セキュリティ: Kerberos に許可される暗号化タイプの設定」* が *「このアカウントに Kerberos DES 暗号化タイプを使用する」* オプションに選択されて**いない**ことを確認します。
    - *「アカウント: パスワードの最大有効期限」* でパスワードの有効期限を設定します (たとえば、30 日、60 日、または 90 日にすると `PasswordNeverExpires = FALSE` となります)。
    - *「アカウント: ローカル アカウントでの空白のパスワードの使用をコンソールログオンのみに制限」* を **[無効]** に設定します。
    - *「インタラクティブ ログオン: キャッシュする過去のログオン回数 (ドメインコントローラーが使用できない場合)」* でユーザーが自分のパスワードを変更できるようにするには、「10」など希望する値を設定します。

Powershell 使用して設定を変更するには

- AD をホストしているマシンで、適切な管理者権限を使用して PowerShell を開き、次のコマンドを実行します。

```
Set-ADAccountControl -Identity <AD_ACCOUNT> -AccountNotDelegated $true -UseDESKeyOnly
$false -DoesNotRequirePreAuth $false -PasswordNeverExpires $false -PasswordNotRequired
$false -CannotChangePassword $false
```

<AD_ACCOUNT> に、変更する Active Directory アカウントの名前を入れます。

ドメイン

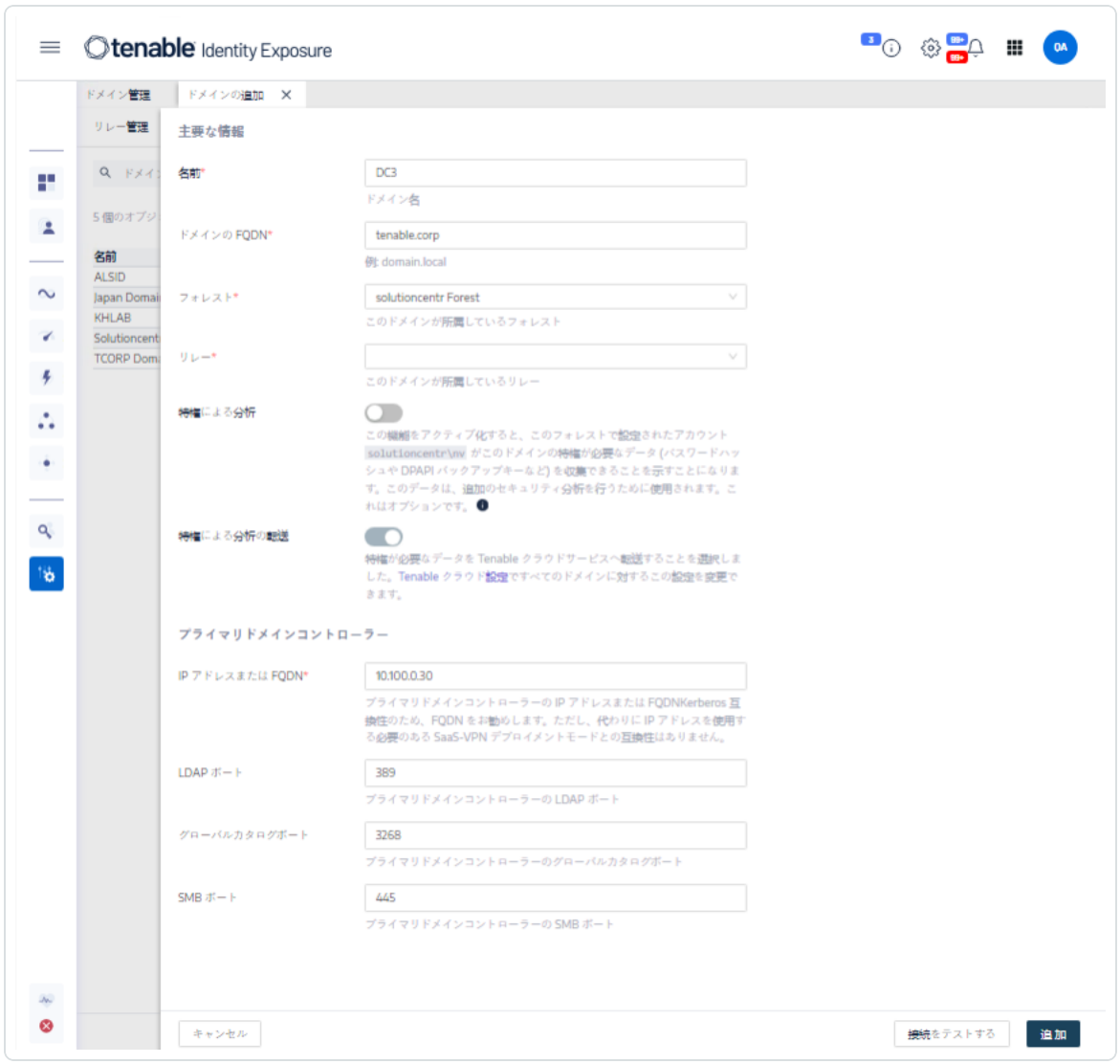
Tenable Identity Exposure は、共通の設定を共有するオブジェクトをグループ化するドメインを、論理的に一元管理して監視します。

ドメインを追加するには

1. Tenable Identity Exposure で、**[システム]** をクリックします。
2. **[ドメイン管理]** タブをクリックします。

   [ドメイン管理] ペインが表示されます。
3. 右上隅の **[ドメインの追加]** をクリックします。

   [ドメインの追加] ペインが表示されます。



4. **[主要な情報]**セクションで、以下の情報を入力します。

    - **[名前]**ボックスにドメイン名を入力します。
    - **[ドメインの FQDN]**ボックスに、ドメインの完全修飾ドメイン名 (FQDN) を入力します。
    - **[フォレスト]**ドロップダウンボックスで、ドメインが所属するフォレストを選択します。

5. **権限分析** (オプション): このトグルを有効にすると、このフォレストの「dcadmin」アカウントがこのドメインの権限付きデータを収集して、高度なセキュリティ分析を実行できるようになります。

6. **権限分析の転送**: このオプションの詳細については、Tenable クラウドのデータ収集を参照してください。

7. **[プライマリドメインコントローラー]** セクションで、以下の情報を入力します。

   - **[IP アドレスまたはホスト名]** ボックスに、プライマリドメインコントローラーのホスト名 (Kerberos 認証 との互換性を確保するには必須だが、SaaS-VPN デプロイメントモードとの互換性はない) または IP アドレスを入力します。

     > Tenable Identity Exposure はロードバランサーをサポートしていません。

   - **[LDAP ポート]** ボックスに、プライマリドメインコントローラーの LDAP ポートを入力します。

     > **注意**: ポート TCP/636 (LDAPS) を使用してドメインに接続する場合、Tenable Identity Exposure はその接続を確立するために、Active Directory の認証局 (CA) の証明書にアクセスして、AD 証明書を有効化する必要があります。セキュアリレー環境では、リレーマシンに CA 証明書をインストールできます。この設定は、IPSEC VPN 環境ではできません。

   - **[グローバルカタログポート]** ボックスに、プライマリドメインコントローラーのグローバルカタログポートを入力します。

   - **[SMB ポート]** ボックスに、プライマリドメインコントローラーの SMB ポートを入力します。

8. **[追加]** をクリックします。

   Tenable Identity Exposure がドメインを追加したことを確認するメッセージが表示されます。

ドメインを編集するには

1. Tenable Identity Exposure で、**[システム]** をクリックします。
2. **[ドメイン管理]** タブをクリックします。

   [ドメイン管理] ペインが表示されます。
3. 編集するドメイン名にカーソルを合わせると、右側に ✎ アイコンが表示されます。
4. ✎ アイコンをクリックします。

   [ドメインの編集] ペインが表示されます。
5. ドメインの情報を編集します。
6. **[編集]** をクリックします。

   Tenable Identity Exposure がドメインを更新したことを確認するメッセージが表示されます。

ドメインを削除するには

1. Tenable Identity Exposure で、**[システム]** をクリックします。
2. **[ドメイン管理]** タブをクリックします。

   [ドメイン管理] ペインが表示されます。
3. 削除するドメイン名にカーソルを合わせると、🗑 アイコンが表示されます。
4. 🗑 アイコンをクリックします。

   削除の確認を求めるメッセージが表示されます。
5. **[削除]** をクリックします。

   Tenable Identity Exposure がドメインを削除したことを確認するメッセージが表示されます。

関連項目

- ドメインのデータの強制更新
- ハニーアカウント
- Kerberos 認証

ドメインのデータの強制更新

ドメインのデータを強制的に更新するには

1. Tenable Identity Exposure で、**[システム]** をクリックします。
2. **[ドメイン管理]** タブをクリックします。

   [ドメイン管理] ペインが表示されます。
3. 強制的にデータを更新するドメイン名にカーソルを合わせると、右側に アイコンが表示されます。
4. アイコンをクリックします。

   データの更新アクションに関する情報が記載されたメッセージが表示されます。
5. **[確認]** をクリックします。

関連項目

- ハニーアカウント

ハニーアカウント

必要なユーザーロール: ローカルマシンの管理者

ハニーアカウントは、Active Directory を介してネットワークを侵害しようとする攻撃者を検出することを目的とする、おとりアカウントです。

これは Tenable Identity Exposure の攻撃インジケーターが Kerberoasting の悪用の試みを検出するための前提条件です。攻撃者は、サービスチケットをリクエストして抽出し、サービスアカウントの認証情報をオフラインで割り出して、サービスアカウントへのアクセスを取得しようとします。ハニーアカウントがログイン試行またはチケットリクエストを受けると、Kerberoasting 攻撃インジケーターはアラートを送信します。

ドメインごとに 1 つのハニーアカウントを関連付けます。ハニーアカウントはセキュリティプロファイルに関連していません。

ハニーアカウントを追加するには

1. Tenable Identity Exposure で、**[システム]** > **[ドメイン管理]** をクリックします。

   [ドメイン管理] ペインが表示されます。

2. ハニーアカウントを追加するドメインにカーソルを合わせます。

3. **[ハニーアカウントの設定ステータス]** で、**[+]** をクリックします。

   [ハニーアカウントの追加] ペインが表示されます。

4. **[名前]** ボックスに、ハニーアカウントとして使用するユーザーアカウントの識別名 (DN) を入力します。

   ヒント: 任意の文字列を入力すると、Tenable Identity Exposure はその文字列を検索し、そのユーザーアカウントがすでに Active Directory に存在する場合は、一致するユーザーアカウント名をドロップダウンボックスに表示します。

5. **[デプロイメント]** セクションで、Tenable Identity Exposure はハニーアカウントのデプロイを実行するスクリプトを適切な設定で生成します。 をクリックして、このスクリプトをコピーします。

6. **[追加]** をクリックします。

   Tenable Identity Exposure がハニーアカウントを追加したことを確認するメッセージが表示されます。[ドメイン管理] ペインに、選択したドメインの **[ハニーアカウントの設定ステータス]** がオレンジ色

(●) で表示されます。これは、ハニーアカウントデプロイメントスクリプトを実行してアカウントをアクティブにする必要があることを示しています。

> **注意**: **[ハニーアカウントの設定ステータス]** が赤 (●) の場合、Tenable Identity Exposure がActive Directory 内でこのユーザーアカウントを検出できなかったことを示しています。このユーザーアカウントを作成してから、次の手順に進む必要があります。

7. Active Directory モジュールがあるマシンの Windows PowerShell で、コピーしたハニーアカウントデプロイメントスクリプトを実行します。

   [ドメイン管理] ペインで、選択したドメインの **[ハニーアカウントの設定ステータス]** がアクティブであることを示す緑色のステータス (●) で表示されます。

   > **注意**: Tenable Identity Exposure は、ハニーアカウントの処理と有効化に時間がかかる場合があります。

ハニーアカウントを編集するには

1. Tenable Identity Exposure で、**[システム]** > **[ドメイン管理]** をクリックします。

   [ドメイン管理] ペインが表示されます。

2. ハニーアカウントを追加するドメインにカーソルを合わせます。

3. **[ハニーアカウントの設定ステータス]** で、右側にある アイコンをクリックします。

   [ハニーアカウントの編集] ペインが表示されます。

4. **[名前]** ボックスで、必要に応じてユーザーアカウントを変更します。

5. **[デプロイメント]** セクションで をクリックして、ハニーアカウントデプロイメントスクリプトをコピーします。

6. **[編集]** をクリックします。

   Tenable Identity Exposure がハニーアカウントを更新したことを確認するメッセージが表示されます。[ドメイン管理] ペインに、選択したドメインの **[ハニーアカウントの設定ステータス]** がオレンジ色 (●) で表示されます。これは、ハニーアカウントデプロイメントスクリプトを実行してアカウントをアクティブにする必要があることを示しています。

   > **注意**: **[ハニーアカウントの設定ステータス]** が赤 (●) の場合、Tenable Identity Exposure がActive Directory 内でこのユーザーアカウントを検出できなかったことを示しています。このユーザーアカウントを作成してから、次の手順に進む必要があります。

7. Active Directory モジュールがあるマシンの Windows PowerShell で、コピーしたハニーアカウント デプロイメント スクリプトを実行します。

   [ドメイン管理] ペインで、選択したドメインの **[ハニーアカウントの設定ステータス]** が設定済みであることを示す緑色のステータス (●) で表示されます。

   > **注意**: Tenable Identity Exposure は、ハニーアカウントの処理と有効化に時間がかかる場合があります。

ハニーアカウントを削除するには

1. Tenable Identity Exposure で、**[システム]** > **[ドメイン管理]** をクリックします。

   [ドメイン管理] ペインが表示されます。

2. ハニーアカウントを追加するドメインにカーソルを合わせます。

3. **[ハニーアカウントの設定ステータス]** で、右側にある アイコンをクリックします。

   [ハニーアカウントの編集] ペインが表示されます。

4. **[削除]** をクリックします。

   Tenable Identity Exposure がハニーアカウントを削除したことを確認するメッセージが表示されます。

関連項目

- ドメインのデータの強制更新

Kerberos 認証

Tenable Identity Exposure は、入力した認証情報を使用して、設定済みのドメインコントローラーの認証を行います。これらの DC は、NTLM または Kerberos 認証のいずれかを受け入れます。NTLM はセキュリティ上の問題が文書化されているレガシープロトコルであり、Microsoft およびすべてのサイバーセキュリティ基準は現在使用を推奨していません。一方、Kerberos はより堅牢なプロトコルであり、考慮する必要があります。Windows は常に Kerberos を最初に試行し、Kerberos が利用できない場合にのみ NTLM を使用します。

Tenable Identity Exposure は、いくつかの例外を除いて、NTLM と Kerberos の両方と互換性があります。Tenable Identity Exposure は、Kerberos がすべての必要条件を満たす場合に、推奨プロトコルとして優先させます。このセクションでは、要件について説明し、Kerberos を確実に使用するよう Tenable Identity Exposure を設定する方法を紹介します。

Kerberos の代わりに NTLM を使用することは、SYSVOL 堅牢化が Tenable Identity Exposure と干渉する原因にもなります。詳細は、SYSVOL 堅牢化の Tenable Identity Exposure に対する干渉 を参照してください。

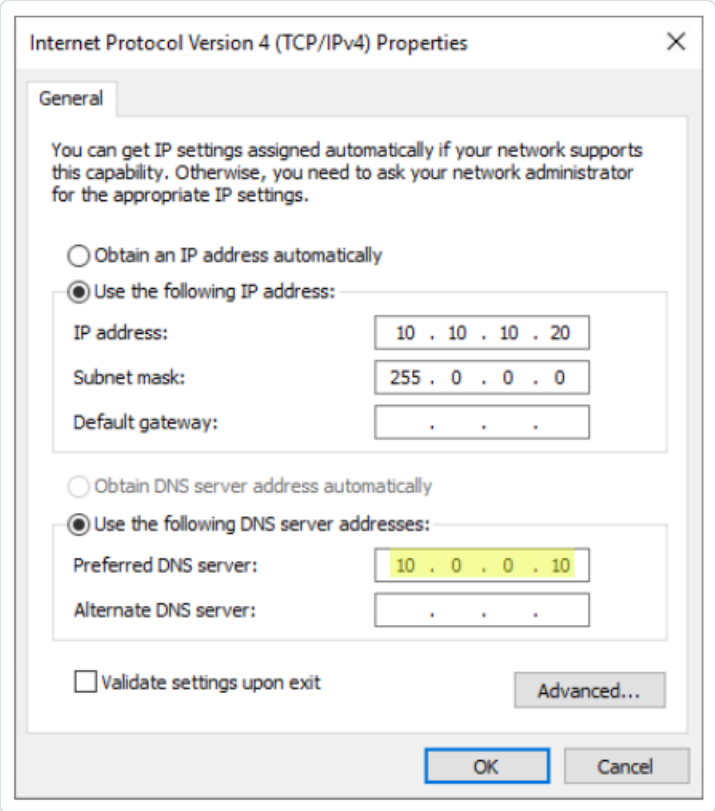
Tenable Identity Exposure デプロイメントモードとの互換性

デプロイメントモード	Kerberos サポート
オンプレミス	○
SaaS-TLS (レガシー)	○
セキュアリレー を備えた SaaS	○
VPN を備えた SaaS	× - インストールを セキュアリレー デプロイメントモードに切り替える必要があります

技術要件

- **Tenable Identity Exposure で設定された AD サービスアカウントには、UserPrincipalName (UPN) が必要です**。手順については、サービスアカウントとドメイン設定を参照してください。

- **DNS 設定および DNS サーバーは、すべての必要な DNS エントリの解決を許可する必要があります**。ドメインコントローラーを認識する DNS サーバーを使用するようディレクトリリスナーまたはリレーマシンを設定する必要があります。Tenable Identity Exposure では推奨されませんが、ディレクトリリスナーまたはリレーマシンがドメインに参加している場合は、すでにこの要件を満たしている必要があります。通常はドメインコントローラーが DNS も実行しているため、ドメインコントローラー自体を優先 DNS サーバーとして使用するのが最も簡単な方法です。例:



> **注意**: ディレクトリリスナーまたはリレーマシンが複数のドメインに接続されており、複数のフォレストにある可能性がある場合は、設定された DNS サーバーがすべてのドメインに必要なすべての DNS エントリを解決できることを確認してください。そうでない場合は、複数のディレクトリリスナーまたはリレーマシンを設定する必要があります。

- **Kerberos「サーバー」(KDC) の到達可能性** – これには、ディレクトリリスナーまたはリレーから、ポート TCP/88 経由でドメインコントローラーにつながるネットワーク接続が必要です。Tenable では推奨していませんが、ディレクトリリスナーまたはリレーがドメインに参加している場合は、すでにこの要件を満たしているはずです。設定された各 Tenable Identity Exposure フォレストには、サービスアカウントを含むそれぞれのドメイン内の少なくとも 1 つのドメインコントローラー、および接続された各ドメイン内の少なくとも 1 つのドメインコントローラーとの Kerberos ネットワーク接続が必要です。

要件の詳細については、ネットワークフローマトリクス および TLS ネットワークマトリクス を参照してください。

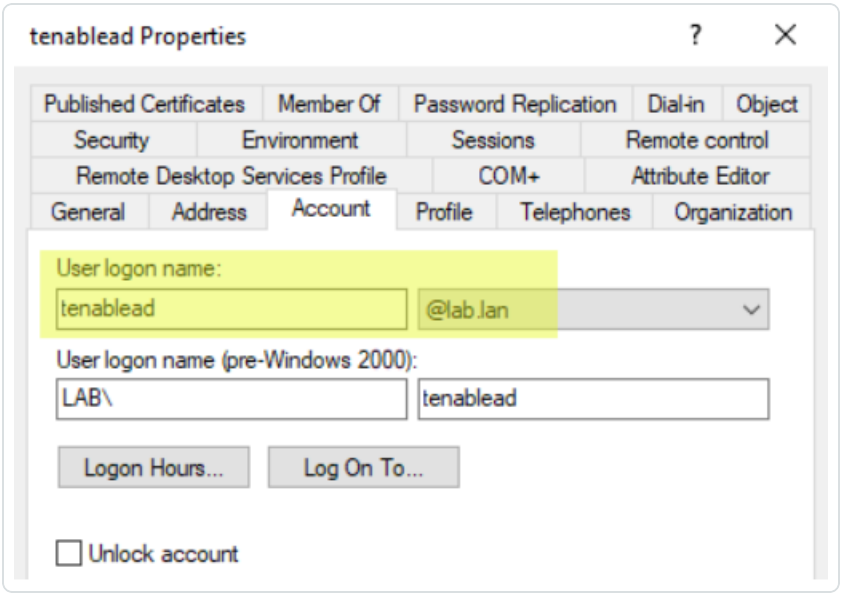
> **注意**: Kerberos を使用するために、ディレクトリリスナーまたはリレーマシンをドメインに参加させる必要はありません。

サービスアカウントとドメイン設定

Tenable Identity Exposure の AD サービスアカウントと AD ドメインが Kerberos を使用するように設定するには

1. ログインには User PrincipalName (UPN) 形式を使用します。この例では、UPN 属性は「`tenablead@lab.lan`」です。

a. 次のように、サービスアカウントを含むフォレストのドメインで UPN 属性を見つけます。



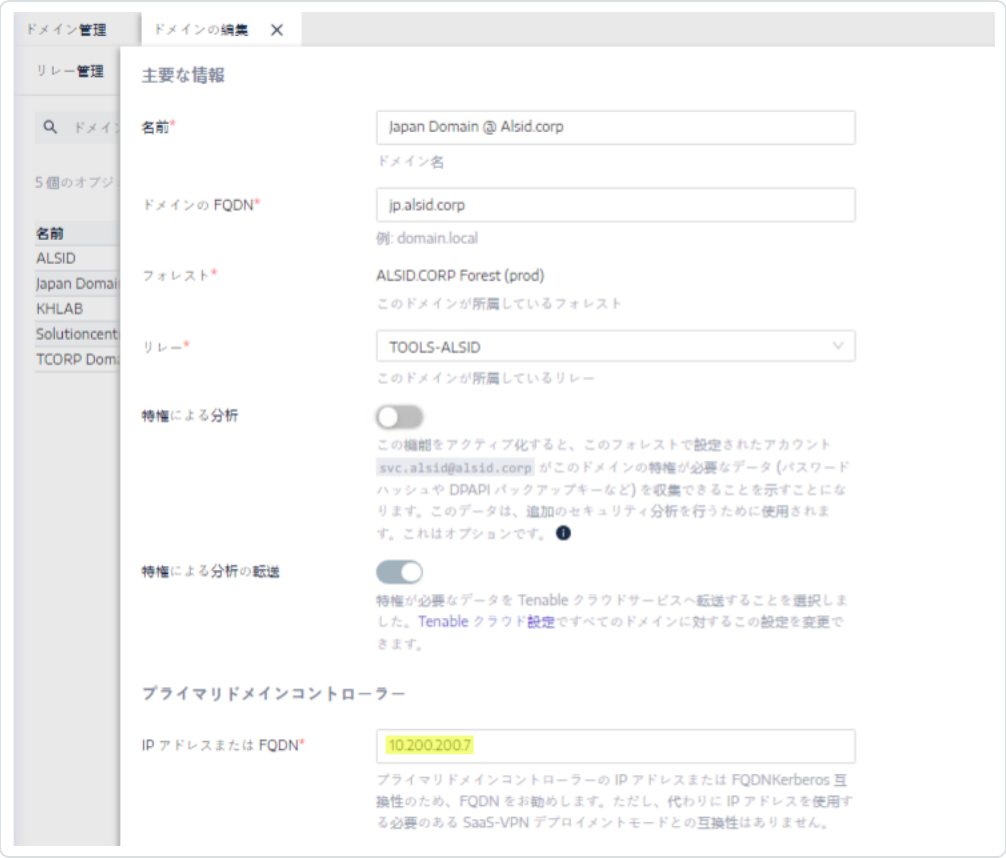

```
PS C:\Users\admin> Get-ADUser tenablead


DistinguishedName : CN=tenablead,CN=Users,DC=lab,DC=lan
Enabled           : True
GivenName         : tenablead
Name              : tenablead
ObjectClass       : user
ObjectGUID        : 70020328-b176-40d0-8a79-7948c1d4cb74
SamAccountName    : tenablead
SID               : S-1-5-21-1891480667-311803191-3341389180-22602
Surname           :
UserPrincipalName : tenablead@lab.lan
```

注意: UPN はメールアドレスと似ており、ユーザーのメールと同じである場合がほとんどです。

b. Tenable Identity Exposure のフォレスト設定セクションで、次のように、短い「ユーザー名」形式または NetBIOS「ドメイン\ユーザー名」形式の代わりにこの UPN を設定します。

2. Tenable Identity Exposure のドメイン設定にある完全修飾ドメイン名 (FQDN) を使用して、プライマリドメインコントローラー (PDC) に対して、IP ではなく FQDN を設定します。

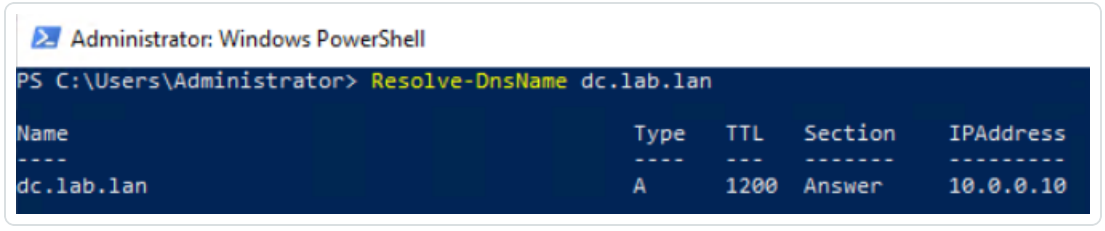


トラブルシューティング

Kerberos が適切に動作するには、いくつかの設定手順が必要です。必要な設定手順を行っていない場合、Windows は、拡張 Tenable Identity Exposure により、NTLM 認証に自動的にフォールバックします。

DNS

ディレクトリリスナーまたはリレーマシンで使用されている DNS サーバーが、次のように入力された PDC FQDN を解決できることを確認します。



Kerberos

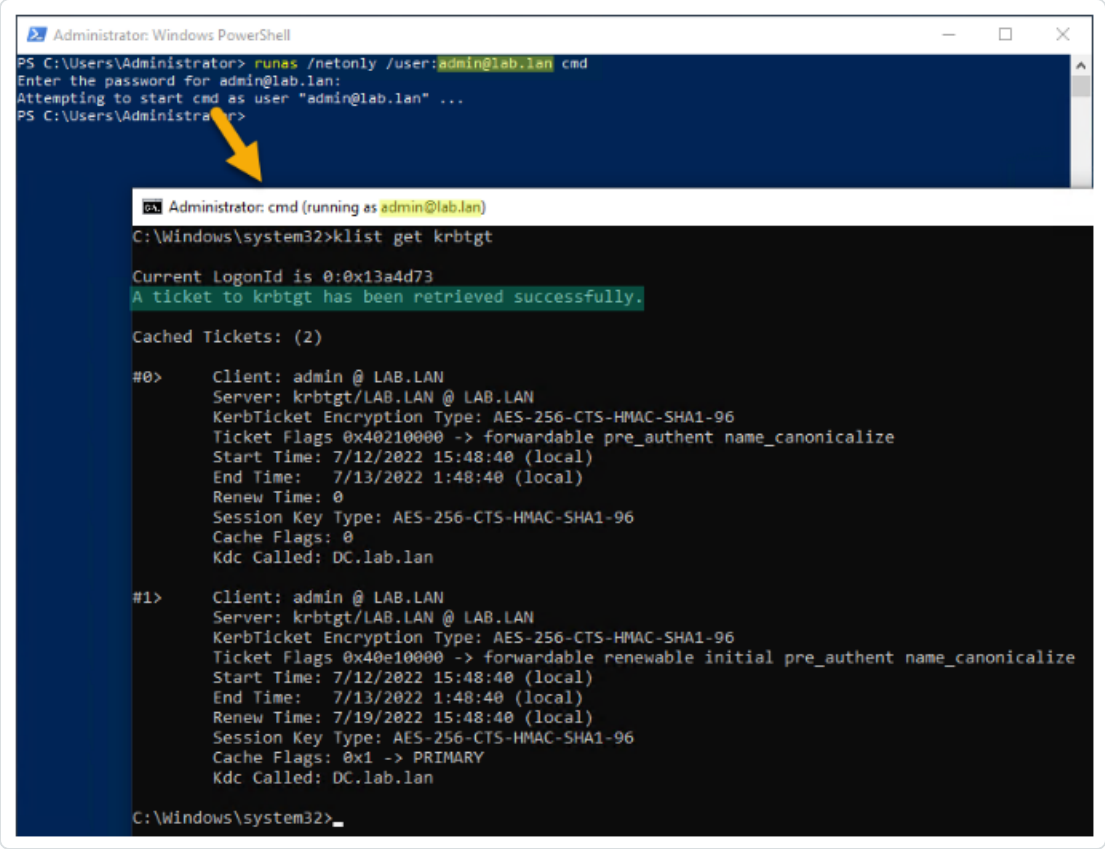
ディレクトリリスナーまたはリレーマシンでコマンドを実行して Kerberos が動作することを検証するには

1. Tenable Identity Exposure で設定された AD サービスアカウントが TGT を取得できることを確認します。

   a. コマンドラインまたは PowerShell で、「`runas/netonly/user:<UPN> cmd `」を実行し、パスワードを入力します。「`/netonly`」フラグにより検証が行われないため、パスワードの入力または貼り付けを行う際は特に注意が必要です。

   b. 2 番目のコマンドプロンプトで「`klist get krbtgt`」を実行して、TGT チケットをリクエストします。

   次の例は、成功した結果を示しています。

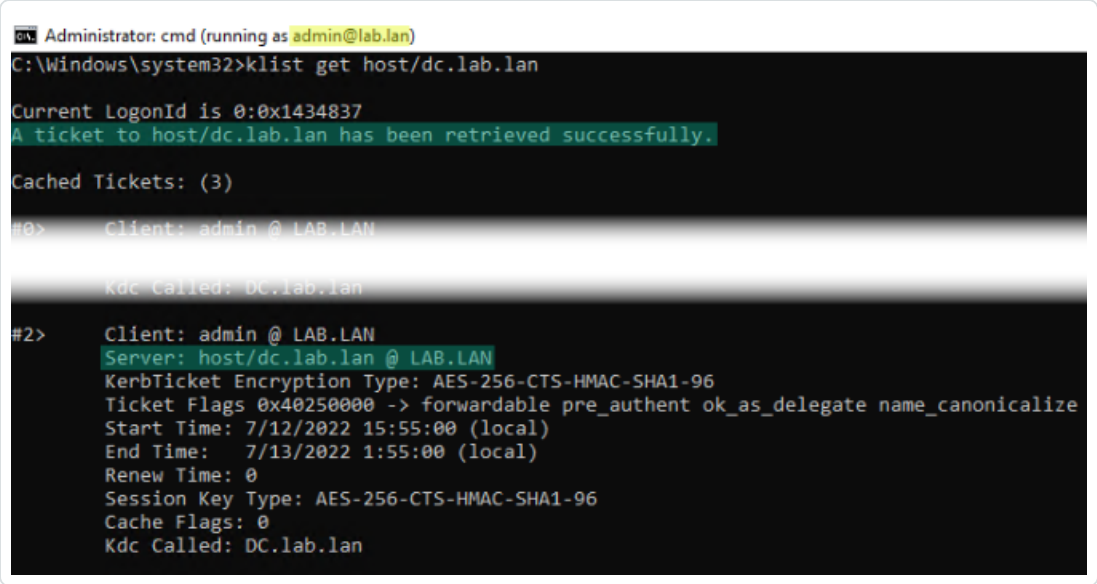


   次のようなエラーコードが表示される場合があります。

- `0xc0000064`:「スペルが間違っているまたは不正なユーザーアカウントを使用したユーザーログオン」-> ログインをチェックします (UPN の「@」より前の部分)
- `0xc000006a`:「スペルが間違っているまたは不正なパスワードを使用したユーザーログオン」-> パスワードをチェックします
- `0xc000005e`:「現在、ログオンリクエストを処理するために利用できるログオンサーバーがありません。」-> DNS 解決が動作し、サーバーが返された KDC などに接続できることを確認します
- その他のエラーコード: 4625 イベントに関連する Microsoft ドキュメントを参照します

2. Tenable Identity Exposure で設定されたドメインコントローラーがサービスチケットを取得できることを確認します。同じ 2 番目のコマンドプロンプトで、「`klist get host/<DC_FQDN>`」を実行します (「`<DC_FQDN>`」を置き換える)。

   次の例は、成功した結果を示しています。



アラート

必要なライセンス: 送信するアラートのタイプによっては、攻撃インジケーターまたは露出インジケーターのライセンスが必要な場合があります。

Tenable Identity Exposure のアラートシステムは、監視対象の Active Directory におけるセキュリティの劣化や攻撃を特定するのに役立ちます。メールまたは Syslog 通知を使って、脆弱性や攻撃に関する分析データをリアルタイムでプッシュします。

- SMTP サーバー設定
- メールアラート
- Syslog アラート
- Syslog とメールアラートの詳細

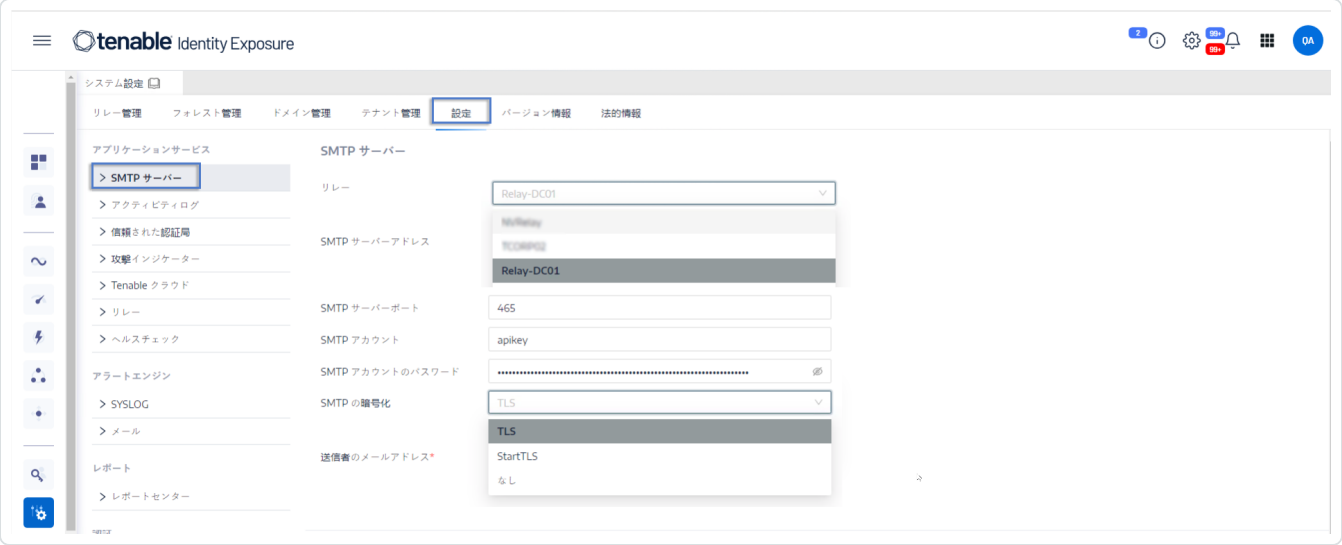
SMTP サーバー設定

アラート通知を送信するには、Tenable Identity Exposure で Simple Mail Transfer Protocol (SMTP) を設定する必要があります。

SMTP サーバーを設定するには

1. Tenable Identity Exposure で、**[システム]** > **[設定]** をクリックします。
2. **[アプリケーションサービス]** で、**[SMTP サーバー]** を選択します。

   [SMTP サーバー] ペインが開きます。



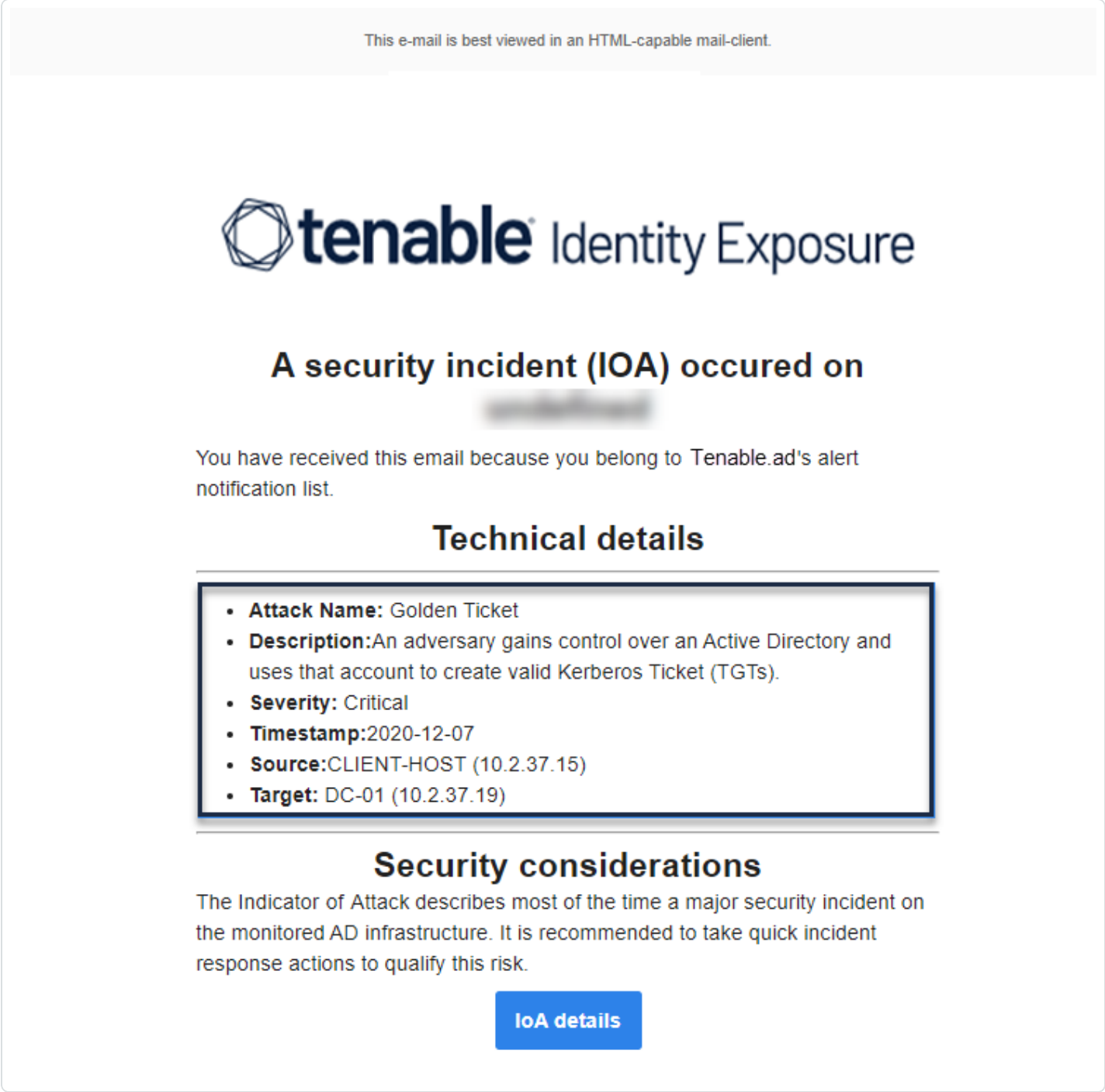
3. **ネットワークでセキュアリレーを使用している場合：[リレー]** ボックスの矢印をクリックして、SMTP サーバーと通信するリレーをドロップダウンリストから選択します。
4. 以下の情報を入力します。
   - SMTP サーバーアドレス
   - SMTP サーバーポート
   - SMTP アカウント
   - SMTP アカウントのパスワード

5. [SMTP 暗号化]ボックスで、矢印をクリックして、ドロップダウンリストから暗号化方式を選択します。
6. **[送信者のメールアドレス]** ボックスに、Tenable Identity Exposure がメールの送信時に使用するメールアドレスを入力します。
7. **[保存]** をクリックします。

   Tenable Identity Exposure が SMTP パラメーターを更新したことを確認するメッセージが表示されます。

メールアラート

Tenable Identity Exposure は、イベントが特定の深刻度しきい値に達し、修正アクションが必要な場合に、メールアラートを送信して自動的に通知します。以下はメールアラートの例です。



メールアラートを追加するには

1. Tenable Identity Exposure で、**[システム]** > **[設定]** > **[メール]** をクリックします。
2. 右側にある **[メールアラートの追加]** ボタンをクリックします。

   [メールアラートの追加] ペインが表示されます。
3. **[主要な情報]** セクションに、以下を入力します。
   - **[メールアドレス]** ボックスに、通知を受け取る受信者のメールアドレスを入力します。
   - **[説明]** ボックスに、受信者アドレスの説明を入力します。
4. **[アラートのトリガー]** ドロップダウンリストで、次のいずれかを選択します。
   - **各逸脱時**: Tenable Identity Exposure は逸脱 IoE を検出するたびに通知を送信します。
   - **各攻撃時**: Tenable Identity Exposure は逸脱 IoA を検出するたびに通知を送信します。
   - **各ヘルスチェックステータスの変更時**: Tenable Identity Exposure は、ヘルスチェックステータスが変わるたびに通知を送信します。
5. **[プロファイル]** ボックスで、このメールアラートに使用するプロファイルをクリックして選択します (該当する場合)。
6. **初期分析フェーズ中に逸脱が検出された場合にアラートを送信する**: 次のいずれかを実行します (該当する場合)。
   - チェックボックスを選択する: システムの再起動でアラートが発生すると、Tenable Identity Exposure は大量のメール通知を送信します。
   - チェックボックスの選択を解除する: システム再起動でアラートが発生しても、Tenable Identity Exposure はメール通知を送信しません。
7. **深刻度のしきい値**: ドロップダウンボックスの矢印をクリックして、Tenable Identity Exposure がアラートを送信するしきい値を選択します (該当する場合)。
8. これまでに選択したアラートトリガーに応じて、以下のようになります。
   - **露出インジケーター**: **[各逸脱時]** にアラートがトリガーされるように設定した場合は、各深刻度レベルの横の矢印をクリックして露出インジケーターのリストを展開し、アラートを送信するインジケーターを選択します。

- **攻撃インジケーター**: **[各攻撃時]** にアラートがトリガーされるように設定した場合は、各深刻度レベルの横の矢印をクリックして攻撃インジケーターのリストを展開し、アラートを送信するインジケーターを選択します。
- **ヘルスチェックステータスの変更**: **[ヘルスチェック]** をクリックし、アラートをトリガーするヘルスチェックタイプを選択し、**[選択内容でフィルター]** をクリックします。

9. **[ドメイン]** ボックスをクリックして、Tenable Identity Exposure がアラートを送信するドメインを選択します。

   フォレストとドメインペインが表示されます。

   a. フォレストまたはドメインを選択します。

   b. **[選択内容でフィルター]** をクリックします。

10. **[設定のテスト]** をクリックします。

    Tenable Identity Exposure がメールアラートをサーバーに送信したことを確認するメッセージが表示されます。

11. **[追加]** をクリックします。

    Tenable Identity Exposure がメールアラートを作成したことを確認するメッセージが表示されます。

メールアラートを編集するには

1. Tenable Identity Exposure で、**[システム]** > **[設定]** > **[メール]** をクリックします。
2. メールアラートのリストで、変更するメールアラートにカーソルを合わせ、行末の ✎ アイコンをクリックします。

   [メールアラートの編集] ペインが表示されます。
3. 手順メールアラートを追加するにはに記載されている必要な変更を行います。
4. **[編集]** をクリックします。

   Tenable Identity Exposure がアラートを更新したことを確認するメッセージが表示されます。

メールアラートを削除するには

1. Tenable Identity Exposure で、**[システム]** > **[設定]** > **[メール]** をクリックします。
2. メールアラートのリストで、削除するメールアラートにカーソルを合わせ、行末の 🗑 アイコンをクリックします。

   削除の確認を求めるメッセージが表示されます。
3. **[削除]** をクリックします。

   Tenable Identity Exposure がアラートを削除したことを確認するメッセージが表示されます。

関連項目

- SMTP サーバー設定
- Syslog とメールアラートの詳細

Syslog アラート

企業によっては SIEM (Security Information and Event Management) を使用して、潜在的な脅威やセキュリティ上のインシデントに関するログを収集しています。Tenable Identity Exposure は、Active Directory 関連のセキュリティ情報を SIEM Syslog サーバーにプッシュすることによって、既存のアラートメカニズムを強化することができます。

新しい Syslog アラートを追加するには

1. Tenable Identity Exposure で、**[システム]** > **[設定]** > **[Syslog]** をクリックします。
2. 右側にある **[Syslog アラートの追加]** ボタンをクリックします。

   [Syslog アラートの追加] ペインが表示されます。

3. **[主要な情報]** セクションに、以下を入力します。

- **ネットワークでセキュアリレーを使用している場合：[リレー]** ボックスの矢印をクリックして、SIEM と通信するリレーをドロップダウンリストから選択します。
- **[コレクターの IP アドレスまたはホスト名]** ボックスに、通知を受信するサーバー IP かホスト名を入力します。
- **[ポート]** ボックスに、コレクターのポート番号を入力します。
- **[プロトコル]** ボックスで、矢印をクリックして UDP か TCP をクリックします。
  - TCP を選択した場合、TLS セキュリティプロトコルを有効にしてログを暗号化するには、**[TLS]** オプションのチェックボックスを選択します。
- **[説明]** ボックスに、コレクターの簡単な説明を入力します。

4. **[アラートのトリガー]** ドロップダウンリストで、次のいずれかを選択します。
   - **変更時**: Tenable Identity Exposure は指定したイベントが発生するたびに通知を送信します
   - **各逸脱時**: Tenable Identity Exposure は逸脱 IoE を検出するたびに通知を送信します。
   - **各攻撃時**: Tenable Identity Exposure は逸脱 IoA を検出するたびに通知を送信します。
   - **各ヘルスチェックステータスの変更時**: Tenable Identity Exposure は、ヘルスチェックステータスが変わるたびに通知を送信します。
5. **[プロファイル]** ボックスで、この Syslog アラートに使用するプロファイルをクリックして選択します。
6. **初期分析フェーズ中に逸脱が検出された場合にアラートを送信する**: 次のいずれかを実行します (該当する場合)。
   - チェックボックスを選択する: システムの再起動でアラートが発生すると、Tenable Identity Exposure は大量のメール通知を送信します。
   - チェックボックスの選択を解除する: システム再起動でアラートが発生しても、Tenable Identity Exposure はメール通知を送信しません。
7. **深刻度のしきい値**: ドロップダウンボックスの矢印をクリックして、Tenable Identity Exposure がアラートを送信するしきい値を選択します (該当する場合)。
8. これまでに選択したアラートトリガーに応じて、以下のようになります。

- **イベント変更**: **変更時**にトリガーするアラートを設定する場合は、イベント通知をトリガーする式を入力します。

  アイコンをクリックして検索ウィザードを使用するか、検索ボックスにクエリ式を入力して**[検証]**をクリックします。詳細は、イベント情報のクエリをカスタマイズするを参照してください。

- **露出インジケーター**: **[各逸脱時]**にアラートがトリガーされるように設定した場合は、各深刻度レベルの横の矢印をクリックして露出インジケーターのリストを展開し、アラートを送信するインジケーターを選択します。

- **攻撃インジケーター**: **[各攻撃時]**にアラートがトリガーされるように設定した場合は、各深刻度レベルの横の矢印をクリックして攻撃インジケーターのリストを展開し、アラートを送信するインジケーターを選択します。

- **ヘルスチェックステータスの変更**: **[ヘルスチェック]**をクリックし、アラートをトリガーするヘルスチェックタイプを選択し、**[選択内容でフィルター]**をクリックします。

9. **[ドメイン]**ボックスをクリックして、Tenable Identity Exposure がアラートを送信するドメインを選択します。

   [フォレストとドメイン]ペインが表示されます。

   a. フォレストまたはドメインを選択します。

   b. **[選択内容でフィルター]**をクリックします。

10. **[設定のテスト]**をクリックします。

    Tenable Identity Exposure が Syslog アラートをサーバーに送信したことを確認するメッセージが表示されます。

11. **[追加]**をクリックします。

    Tenable Identity Exposure が Syslog アラートを作成したことを確認するメッセージが表示されます。

Syslog アラートを編集するには

1. Tenable Identity Exposure で、**[システム]** > **[設定]** > **[Syslog]**をクリックします。
2. Syslog アラートのリストで、変更するアラートにカーソルを合わせ、行末の アイコンをクリックします。

[Syslogアラートの編集] ペインが表示されます。

3. 手順新しい Syslog アラートを追加するには に記載されている必要な変更を行います。
4. **[編集]** をクリックします。

   Tenable Identity Exposure がアラートを更新したことを確認するメッセージが表示されます。

Syslog アラートを削除するには

1. Tenable Identity Exposure で、**[システム]** > **[設定]** > **[Syslog]** をクリックします。
2. Syslog アラートのリストで、削除するアラートにカーソルを合わせ、行末の 🗑 アイコンをクリックします。

   削除の確認を求めるメッセージが表示されます。
3. **[削除]** をクリックします。

   Tenable Identity Exposure がアラートを削除したことを確認するメッセージが表示されます。

関連項目

- Syslog とメールアラートの詳細

Syslog とメールアラートの詳細

Syslog またはメールアラートを有効にすると、Tenable Identity Exposure は、逸脱、攻撃、または変更を検出したときに通知を送信します。

アラートヘッダー

Syslog アラートヘッダー (RFC-3164) は共通イベント形式 (CEF) を使用しています。これは、Security Information and Event Management (SIEM) を統合するソリューションで共通で使用されている形式です。

露出インジケーター (IoE) のアラートの例

IoE アラートヘッダー

```
<116>Jan  9 09:24:42 qradar.alsid.app AlsidForAD[4]: "0" "1" "Alsid Forest" "emea.corp" "C-PASSWORD-
DONT-EXPIRE" "medium" "CN=Gustavo Fring,OU=Los_Pollos_Hermanos,OU=Emea,DC=emea,DC=corp" "28" "1" "R-
DONT-EXPIRE-SET" "2434" "TrusteeCn"="Gustavo Fring"
```

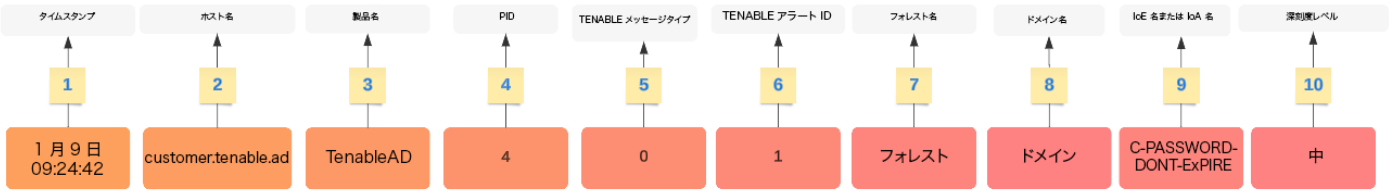
攻撃インジケーター (IoA) のアラートの例

IoA アラートヘッダー

```
<116>Jan  9 09:24:42 qradar.alsid.app AlsidForAD[4]: "2" "1337" "Alsid Forest" "emea.corp" "DC Sync"
"medium" "yoda.alsid.corp" "10.0.0.1" "antoinex1x.alsid.corp" "10.1.0.1" "user"="Gustavo Fring" "dc_
name"="MyDC"
```

アラート情報

一般的な要素

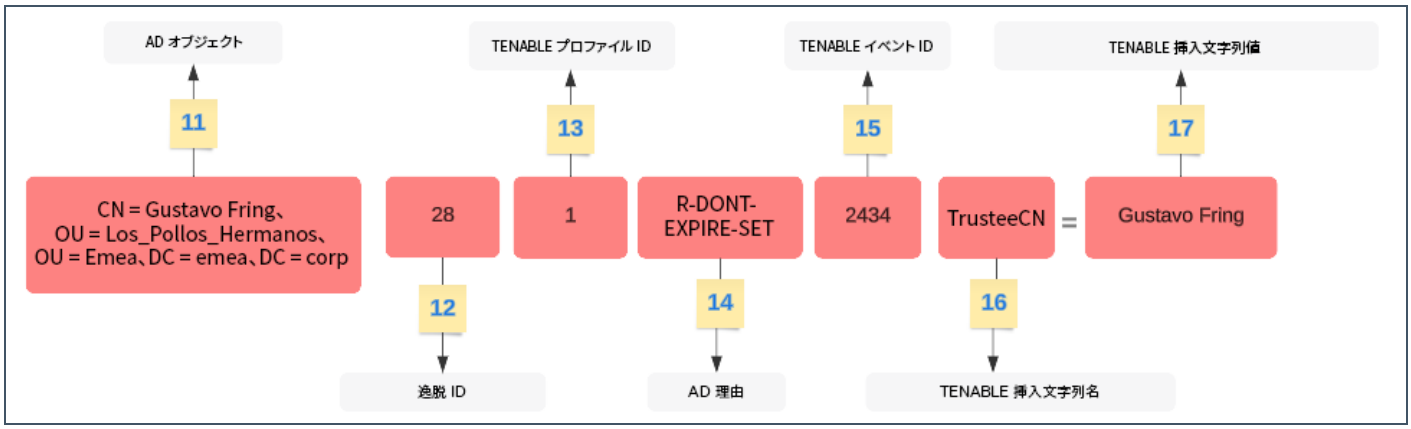


ヘッダー構造には、表で説明されている次の部分が含まれています。

パート	説明

1	**Time Stamp** – 検出日。例: "Jun 7 05:37:03"
2	**Hostname** – アプリケーションのホスト名。例: "customer.tenable.ad"
3	**Product Name** – 逸脱が発生した製品名。例: "TenableAD"、"AnotherTenableADProduct"
4	**PID** – 製品 (Tenable Identity Exposure) ID。例: [4]
5	**Tenable Msg Type** – イベントソースの識別子。例: "0" (= 各逸脱時)、"1" (= 変更時)、"2" (= 各攻撃時)
6	**Tenable Alert ID** – アラートの一意の ID。例: "0"、"132"
7	**Forest Name** – 関連するイベントのフォレスト名。例: "Corp Forest"
8	**Domain Name** – イベントに関連するドメイン名。例: "tenable.corp"、"zwx.com"
9	**Tenable Codename** - 露出インジケーター (IoE) または攻撃インジケーター (IoA) のコード名。例: "C-PASSWORD-DONT-EXPIRE"、"DC Sync"。
10	**Tenable Severity Level** – 関連する逸脱の深刻度レベル。例: "critical"、"high"、"medium"

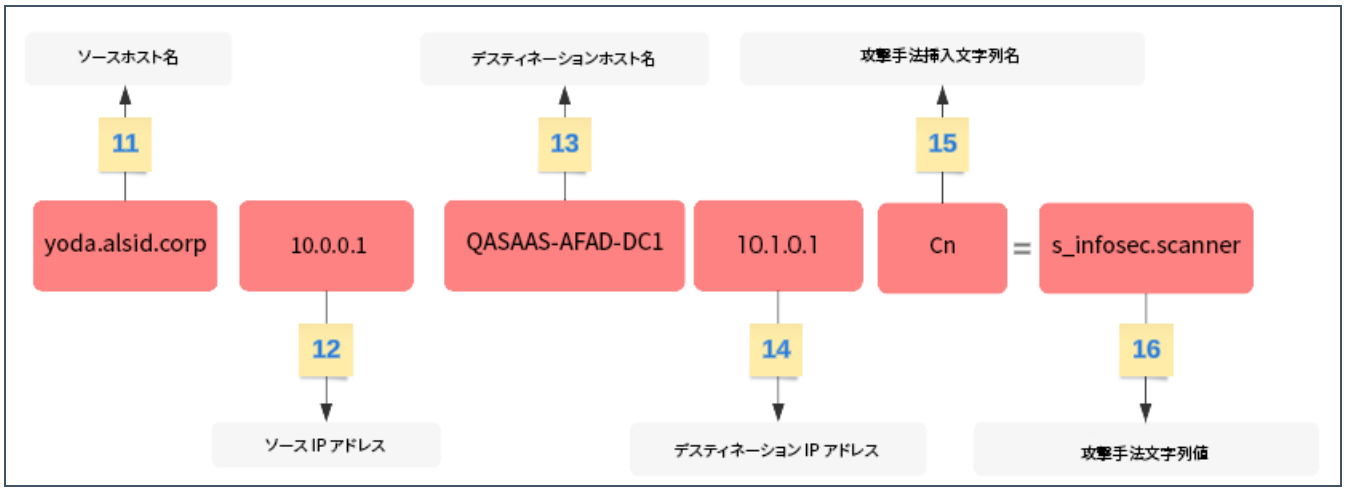
IoE 固有の要素



パート	説明
11	**AD Object** – 逸脱オブジェクトの識別名。例: "CN=s_infosec.scanner,OU=ADManagers,DC=domain,DC=local"

12	**Tenable Deviance ID** – 逸脱の ID。例: "24980"、"132"、"28"
13	**Tenable Profile ID** – Tenable Identity Exposure が逸脱をトリガーしたプロファイルの ID。例: "1" (Tenable)、"2" (soc_team)
14	**AD Reason Codename** – 逸脱理由のコード名。例: "R-DONT-EXPIRE-SET"、"R-UNCONST-DELEG"
15	**Tenable Event ID** – 逸脱によって発生したイベントの ID。例: "40667"、"28"
16	**Tenable Insertion Strings Name** – 逸脱オブジェクトで発生した属性名。例: "Cn"、"useraccountcontrol"、"member"、"pwdlastset"
17	**Tenable Insertion Strings Value** – 逸脱オブジェクトで発生した属性の値。例: "s_infosec.scanner"、"CN=Backup Operators,CN=Builtin,DC=domain,DC=local"

IoA 固有の要素



パート	説明
11	**Source hostname** – 攻撃ホストのホスト名。値は「不明」の場合もあります。
12	**Source IP Address** – 攻撃ホストの IP アドレス。値は IPv4 または IPv6 です。
13	**Destination Hostname** – 攻撃されたホストのホスト名。
14	**Destination IP Address** – 攻撃されたホストの IP アドレス。値は IPv4 または IPv6 です。
15	**Attack Vector Insertion Strings Name** – 逸脱オブジェクトがトリガーした属性名。
16	**Attack Vector Insertion Strings Value** – 逸脱オブジェクトがトリガーした属性値。

例

イベント情報のイベント詳細

次の例は、以下を含むイベント情報に表示されるイベントの詳細を示しています。

- タイムスタンプ (1)
- 逸脱オブジェクトの名前 (11)
- フォレスト (7) とドメイン (8) の名前
- 逸脱オブジェクトがトリガーした属性の値 (17)

イベントソース

この例は、イベントのソースを示しています (5)。このパラメーターは Syslog 設定ページで設定したものです。詳細は、Syslog アラート を参照してください。

アラート ID

この例は、アラートの一意の ID を示しています (6)。これは、Tenable Identity Exposure の **[システム]** > **[設定]** > **[メール]** で設定したメールアドレスのリストで確認できます。

ヘルスチェック

Tenable Identity Exposure の**ヘルスチェック**機能は、ドメインとサービスアカウントの設定を 1 つの統合ビューでリアルタイムで可視化します。そこからドリルダウンして、インフラにおける接続問題やその他の問題につながる設定異常がないか調査することができます。この機能により、すべてが適切に設定され、Tenable Identity Exposure がスムーズに動作することを確認でき、迅速で正確な対応措置を取ることで問題を修正できるようになります。また、Tenable Identity Exposure が効率的に機能するように最適な設定になっているという確信に繋がります。

ヘルスチェックは、管理ロールの場合はデフォルトで、特定のユーザーロールの場合はアクセス許可に応じて表示されます。ヘルスチェックのステータスが変わるたびに、Syslog またはメールアラートを作成することもできます。

ヘルスチェックと DC 同期攻撃の検出

ヘルスチェックは、Tenable Identity Exposure サービスのステータスとユーザビリティに関する貴重な情報を提供してくれます。ヘルスチェックは、サービスアカウントの機能を検証し、特権分析に使用されるパスワードハッシュや DPAPI バックアップキーなどの機密情報を収集します。ヘルスチェックレポートで、Tenable はサービスアカウントに特権分析機能が適切に設定されているかどうかを判断するために、機密データの収集を試みます。特権分析機能が使用されていない場合は何も収集しません。このプロセス中に DCSync 攻撃が検出されるのを防ぐために、Tenable は提供されたサービスアカウントを DCSync の攻撃インジケーターのホワイトリストに自動的に追加します。

ドメインステータス

Tenable Identity Exposure は各ドメインの以下の項目をチェックします。

- AD ドメインへの認証 – LDAP 設定とステータス、認証情報、SMB アクセス。
- ドメインの到達可能性 – 動的 RPC ポートへの動作中の接続、到達可能な SMB サーバー、到達可能なドメインコントローラーの IP アドレスまたは FQDN、RPC ポートへの動作中の接続、到達可能な LDAP サーバー、到達可能なグローバルカタログ LDAP サーバー。
- アクセス許可 – AD ドメインデータにアクセスし、特権データを収集できること。
- リレーにリンクされたドメイン – ドメインがリレーサービスに正しく関連付けられていること。

プラットフォームステータス

Tenable Identity Exposure は、プラットフォーム設定に関して次の項目をチェックします。

- リレーサービスの実行 – トラブルシューティングのヒントを使ってリレー設定が正しいかどうか。
- リレーバージョンの整合性 – リレーバージョンが Tenable Identity Exposure のバージョンと整合しているかどうか。
- AD データコレクターサービスの実行 – データコレクターサービス、ブローカー、コレクターブリッジが動作可能で、データを他のサービスにリレーできるかどうか。

ヘルスチェックにアクセスするには

1. Tenable Identity Exposure ページの左下隅の  アイコンにカーソルを合わせると、インフラのグローバルステータスが表示されます。
2. このアイコンをクリックすると、**[ヘルスチェック]** ページが開きます。**[ドメインステータス]** または **[プラットフォームステータス]** タブに、次のいずれかが表示されます。
    - すべてのヘルスチェックに合格したというメッセージ
    - 特定のステータスを示す警告または問題のリスト

	チェックに合格し、正常な結果を示している。
	チェックに不合格となり、問題が特定されている。
	チェックに不合格となったが、この問題は Tenable Identity Exposure の正常な動作を妨げるものではない。 たとえば、クライアント側の Active Directory の設定ミスが原因でサービスアカウントが特権データを収集できない場合、データ収集のチェックは不合格になります。ただし、Tenable Identity Exposure のこのドメインで特権分析機能がアクティブ化されていないため、深刻な問題とはなりません。そのため、この警告となっています。しかし、特権分析をアクティブ化すると、チェックは即座に不合格となります。
	依存性チェックで不合格となったため、チェックは不明な結果を示している。たとえば、認証のチェックで不合格になると、ネットワーク到達性のチェックに進めなくなります。

すべてのヘルスチェックを表示するには

- 右側のヘルスチェックのリストの上の**[成功したチェックの表示]**のトグルをクリックして有効にし、Tenable Identity Exposure が実行したすべてのチェックを一覧表示します。以下の情報が含まれます。
    - ヘルスチェック名
    - ステータス(合格、不合格、不合格だがブロックなし、不明)
    - 影響を受けるドメインとそれに関連付けられているフォレスト (ドメインステータスチェックのみ)
    - 最後にチェックが実行された時刻
    - チェックがこのステータスを保持している長さ

ヘルスチェックページを更新するには

- Tenable Identity Exposure は、ヘルスチェックを定期的に実行しますが、ページをリアルタイムの結果で更新することはありません。 をクリックして、結果のリストを更新してください。

ヘルスチェックのタイプまたはドメインで結果をフィルタリングするには

1. 右側のヘルスチェックのリストの上にある**[n/n 個のヘルスチェック]**または**[n/n 個のドメイン]**(ドメインステータスのみ)をクリックします。

   [ヘルスチェック]または**[フォレストとドメイン]**ペインが開きます。
2. ヘルスチェックのタイプまたはフォレスト / ドメイン(該当する場合)を選択し、**[選択内容でフィルター]**をクリックします。

各ヘルスチェックの詳細情報をドリルダウンするには

1. ヘルスチェックのリストで、ヘルスチェック名または行末の青い矢印 (→) をクリックします。

   [詳細]ペインが開き、チェックの説明と関連する詳細のリストが表示されます。

ヘルスチェック名	タイプ	チェックの説明	理由
ドメイン到達可能性	ドメイン	AD ドメインとの接続を確立する能力	• IP-UNREACHABLE R-LDAP-GLOBAL-CATALOG-

			UNREACHABLE • LDAP-SERVER-UNREACHABLE • SMB-SERVER-UNREACHABLE • DYNAMIC-RPC-CONNECTION-NOT-WORKING • RPC-CONNECTION-NOT-WORKING
AD ドメインへの認証	ドメイン	AD ドメインへの認証能力	• INCORRECT-CREDENTIALS • LDAP-SERVER-BUSY • LDAP-SERVER-UNAVAILABLE • LDAP-SERVER-ACCESS-DENIED • SMB-SERVER-ACCESS-DENIED
AD ドメインデータを収集するためのアクセス許可	ドメイン	AD ドメインデータを収集する能力	• MISSING-PERMISSIONS-PRIVILEGED-DATA
AD コンテナへのアクセス許可	ドメイン	AD コンテナにアクセスできる能力	• MISSING-PERMISSIONS-DELETED-OBJECTS-ACCESS • MISSING-

			PERMISSIONS-PASSWORD-SETTINGS-ACCESS
リレーにリンクされたドメイン	ドメイン	ドメインはリレーにリンクされています	• LINKED-TO-RELAY-DOWN
リレーサービス稼働中	プラットフォーム	リレーが期待通りに動作しています	• RELAY-DOWN
リレーサービスバージョン	プラットフォーム	リレーバージョンが製品と一致しています	• VERSION-MISMATCH
AD データコレクター稼働中	プラットフォーム	AD データコレクターが期待通りに動作しています	• DATA-COLLECTOR-SERVICE-DOWN • DATA-COLLECTOR-BRIDGE-DOWN • BROKER-DOWN

2. 詳細行の末尾にある矢印をクリックして展開すると、結果に関する情報がさらに表示されます。

ヘルスチェックステータスアイコンを非表示にするには

Tenable Identity Exposure はデフォルトで画面左下隅にヘルスチェックステータスアイコンを表示します。

1. Tenable Identity Exposure で、左側のナビゲーションバーの **[システム]** に移動し、**[設定]** タブを選択します。

   または、ヘルスチェックページの右上隅の ··· をクリックし、**[設定]** を選択することもできます。

2. **[アプリケーションサービス]** で、**[ヘルスチェック]** を選択します。
3. **[グローバルヘルスチェックステータスを表示する]** のトグルをクリックして、無効にします。

   Tenable Identity Exposure は画面左下隅のヘルスチェックステータスアイコンを非表示にします。

ユーザーロールにヘルスチェックのアクセス許可を割り当てるには

1. Tenable Identity Exposure で、左側のナビゲーションバーの **[アカウント]** に移動し、**[ロール管理]** タブを選択します。
2. ロールのリストで、ユーザーロールを選択し、行末にある をクリックします。

   [ロールの編集] ペインが開きます。
3. **[システム設定エンティティ]** タブを選択します。
4. **[ヘルスチェック]** エンティティを選択し、アクセス許可のトグルをクリックして、**[不許可]** から **[許可]** に切り替えます。
5. **[適用して閉じる]** をクリックします。

アクセス許可についての詳細は、ロールのアクセス許可の設定を参照してください。

ヘルスチェックステータス変更のアラートを設定するには

1. Tenable Identity Exposure で、左側のナビゲーションバーの **[システム]** に移動し、**[設定]** タブを選択します。

   または、ヘルスチェックページの右上隅の をクリックし、**[アラート]** を選択することもできます。
2. **[アラートエンジン]** の下にある、**[Syslog]** または **[メール]** を選択します。
3. **[Syslog アラートの追加]** または **[メールアラートの追加]** をクリックします。

   新しいペインが開きます。完全な手順については、アラートを参照してください。
4. **[アラートパラメーター]** の下にある **[アラートのトリガー]** ボックスで、ドロップダウンメニューから **[ヘルスチェックのステータス変更時]** を選択します。
5. **[ヘルスチェック]** ボックスの矢印をクリックして、アラートをトリガーするヘルスチェックのタイプを選択し、**[選択内容でフィルター]** をクリックします。
6. **[追加]** をクリックします。

レポートセンター

Tenable Identity Exposure の**レポートセンター**には、重要なデータを企業内の主要ステークホルダー向けのレポートとしてエクスポートできる便利な機能があります。レポートセンターでは、事前定義されたリストからレポートを作成することができ、プロセスが効率的で簡潔になります。

管理者は、最大 1 四半期の柔軟なレポート期間で、異なるユーザー向けにさまざまなタイプのレポートを作成できます。Tenable Identity Exposure から重要なアイデンティティデータを共有できるため、企業は積極的にリスクを軽減し、アイデンティティベースの攻撃の可能性を特定できるようになります。

ユーザーがレポートをダウンロードするには、管理者から受け取ったメールに記載された URL のリンク先ページにレポートのアクセスキーを入力します。レポートは 30 日間ダウンロードでき、その後期限切れとなり、Tenable Identity Exposure により削除されます。Tenable Identity Exposure が指定された期間分の新しいレポートを生成し、過去のレポートを上書きする前に、ユーザーはレポートをダウンロードする必要があります。

レポートセンターにアクセスするには

1. Tenable Identity Exposure で、**[システム]** > **[設定]** を選択します。
2. **[レポート]** の **[レポートセンター]** をクリックします。

   ペインが開き、設定済みレポートのリストとそれに関連する情報 (レポート名、タイプ、ドメイン、プロファイル、期間、頻度、受信者のメールアドレスなど) が表示されます。

レポートを作成するには

1. **[レポートセンター]** ペインで、**[レポートの作成]** をクリックします。

   [レポートの設定] ペインが開きます。
2. **[レポートタイプ]** で、次の情報を入力します。
   a. **[レポートタイプ]** で、**[逸脱]** または **[攻撃]** を選択します。
   b. **[インジケーター]** で、**[n/n 個のインジケーター]** をクリックして **[露出インジケーター]** (逸脱の場合) または **[攻撃インジケーター]** (攻撃の場合) を選択し、**[選択内容でフィルター]** をクリックします。

c. **[ドメイン]** で、**[n/n 個のドメイン]** をクリックしてレポートに含めるフォレストまたはドメインを選択し、**[選択内容でフィルター]** をクリックします。

d. **[プロファイル]** の矢印をクリックして、ドロップダウンメニューからプロファイルを選択します。

3. **[レポート名]** にレポートの名前を入力します。
4. **[生成パラメーター]** で次の設定を選択します。

a. **データのタイムフレーム** – レポートは、現在の期間に先行する期間 (前日、前週、前月、前四半期など) を網羅します。

b. **頻度** - Tenable Identity Exposure は、ここで定義された各タイムフレームの間隔でレポートを新しく生成します。矢印をクリックして、ドロップダウンメニューから対応する値を選択します。

c. **タイムゾーン** - レポートに関連付けられたタイムゾーンです。

5. **[受信者]** で、**[メールの追加]** をクリックし、受信者のメールアドレスを入力します。受信者は必要な数だけ追加できます。]

   レポート受信者のメールを設定する方法については、SMTP サーバー設定を参照してください。

6. **[レポートを作成]** をクリックします。

ユーザーがレポートをダウンロードするのを許可するには

- **[レポートセンター]** ペインの上にある **[レポートのアクセスキー]** で、 をクリックしてコピーします。このアクセスキーは、受信者に送信されたメールにあるリンクからレポートをダウンロードする際に必要です。このキーは、すべてのユーザーとレポートに一意のものです。
- 必要に応じて、 をクリックして新しいアクセスキーを生成します。

> **注意**: 新しいアクセスキーを生成すると、以前のアクセスキーは使用できなくなります。新しいアクセスキーでのみ、既存のレポートにアクセスできます。

レポート設定を編集するには

1. レポートのリストでレポートを選択し、行末にある をクリックして **[レポート設定]** ペインを開きます。
2. 必要に応じて変更します。

3. **[保存]** をクリックします。

レポートを削除するには

1. レポートのリストでレポートを選択し、行末にある をクリックして削除します。

   削除の確認を求めるメッセージが表示されます。

2. **[削除]** をクリックします。

   このレポート設定に関連付けられた最後に生成されたレポートはダウンロードできなくなります。

ロールにアクセス許可を付与するには

- **[データエンティティ]** > **[レポート]** の下にある **[アクセス許可の管理]** で、管理者はユーザーロールに、すべてまたは特定のレポート設定を作成、読み取り、編集するアクセス許可を付与できます。

  詳細は、ロールのアクセス許可の設定 を参照してください。

関連項目

- ウィジェット

Microsoft Entra ID のサポート

Tenable Identity Exposure は Active Directory のほかに Microsoft Entra ID (旧 Azure AD または AAD) もサポートし、企業内で使用できる ID の範囲を広げています。この機能では、Microsoft Entra ID に固有のリスクにフォーカスした、新しい露出インジケーター (IoE) が使用されます。

Microsoft Entra ID を Tenable Identity Exposure と統合するには、次のオンボーディングプロセスに厳密に従ってください。

1. 前提条件を満たす
2. アクセス許可をチェックする
3. Microsoft Entra ID 設定を行う
4. Microsoft Entra ID のサポートを有効化する
5. テナントスキャンを有効にする

前提条件

Microsoft Entra ID をサポートしている機能を使用するには、**Tenable Vulnerability Management アカウント**が必要です。このアカウントがあれば、Microsoft Entra ID にかける Tenable スキャンを設定したり、スキャン結果を収集したりできます。

アクセス許可

Microsoft Entra ID をサポートするには、ユーザー、グループ、アプリケーション、サービスプリンシパル、ロール、アクセス許可、ポリシー、ログなどのデータを Microsoft Entra ID から収集する必要があります。このデータは、Microsoft の推奨に従い、Microsoft Graph API とサービスプリンシパル認証情報を使用して収集されます。

- Microsoft Graph で**テナント全体の管理者の同意を付与するアクセス許可を持つユーザー**として Microsoft Entra ID にサインインする必要があります。つまり、Microsoft が定めた条件によると、グローバル管理者または特権ロール管理者のロール (または適切なアクセス許可を持つカスタムロール) がなければなりません。
- Microsoft Entra ID の設定とデータ視覚化にアクセスするには、**Tenable Identity Exposure ユーザーロール**に適切なアクセス許可がなければなりません。詳細は、ロールのアクセス許可の設定 を参照してください。

Microsoft Entra ID 設定を行う

次の手順 (Microsoft のクイックスタート : Microsoft ID プラットフォームにアプリケーションを登録するのドキュメントから引用) を使用して、Microsoft Entra ID で必要なすべての設定を行います。

1. **アプリケーションを作成する**

   a. Azure 管理者ポータルで、**[アプリの登録]** ページを開きます。

   b. **[+ 新規登録]** をクリックします。

   c. アプリケーションに名前を付けます (例 : Tenable Identity Collector)。その他のオプションについては、デフォルト値のままにしておくことができます。

   d. **[登録]** をクリックします。

   e. この新たに作成されたアプリの [概要] ページにある、「アプリケーション (クライアント) ID」と「ディレクトリ (テナント) ID」を書き留めます。

2. **認証情報をアプリケーションに追加する**

   a. Azure 管理者ポータルで、**[アプリの登録]** ページを開きます。

   b. 作成したアプリケーションをクリックします。

   c. 左側のメニューにある **[証明書とシークレット]** をクリックします。

   d. **[+ 新しいクライアント シークレット]** をクリックします。

   e. **[説明]** ボックスに、このシークレットに実際に使用する名前と、ポリシーに準拠した**有効期限**の値を入力します。有効期限が近づいたら忘れずにこのシークレットを更新します。

   f. シークレットは Azure に 1 度しか表示されないため、シークレットの値を安全な場所に保存してください。紛失した場合は再作成する必要があります。

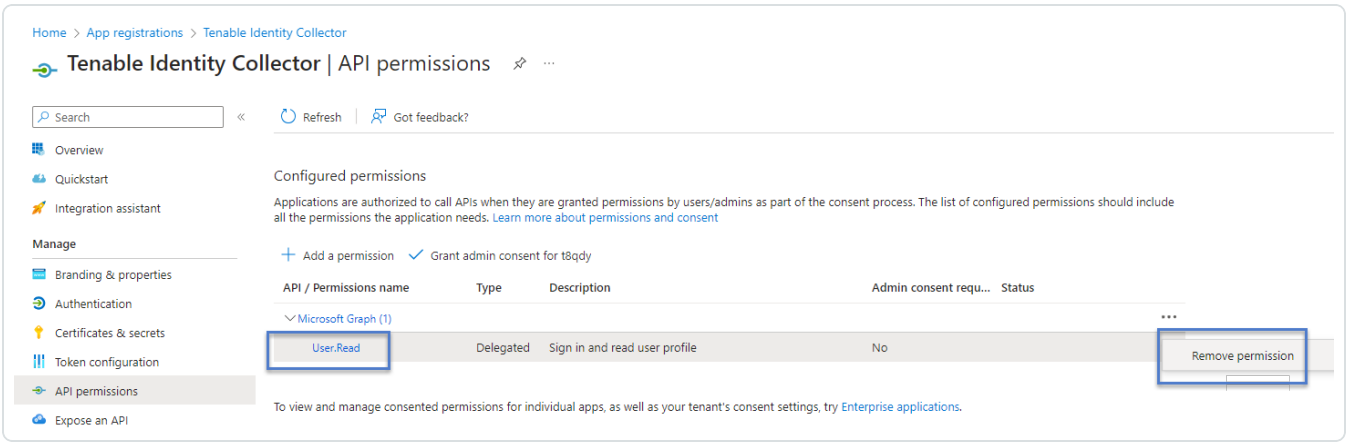
3. **アプリケーションにアクセス許可を割り当てる**

   a. Azure 管理者ポータルで、**[アプリの登録]** ページを開きます。

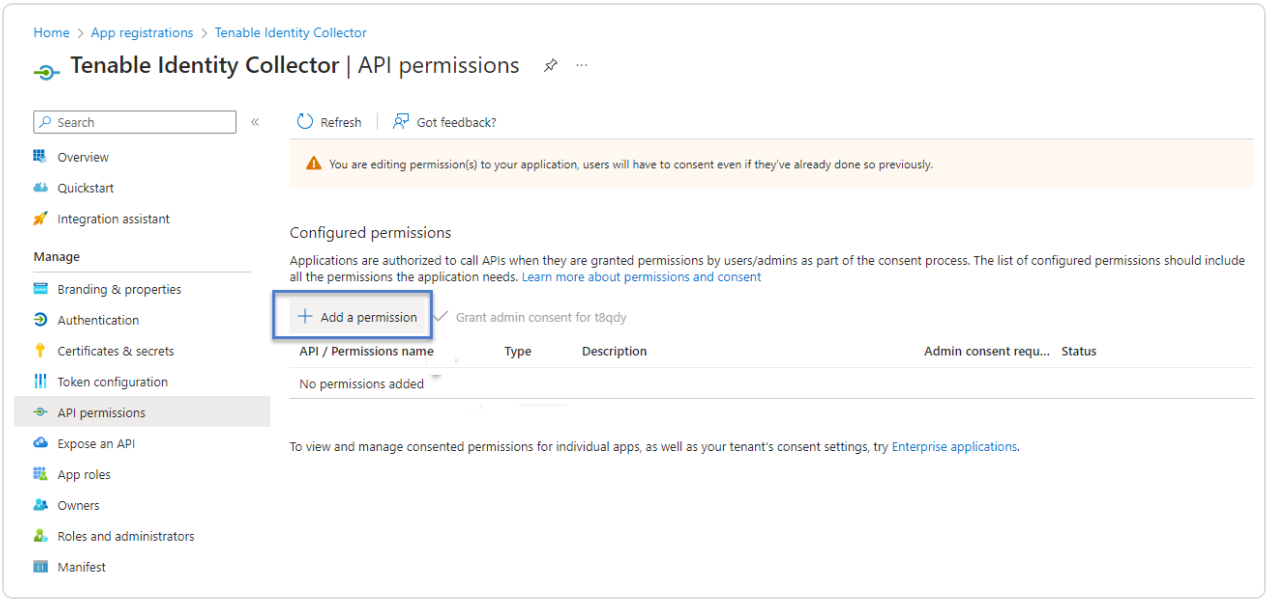
   b. 作成したアプリケーションをクリックします。

   c. 左側のメニューにある **[API のアクセス許可]** をクリックします。

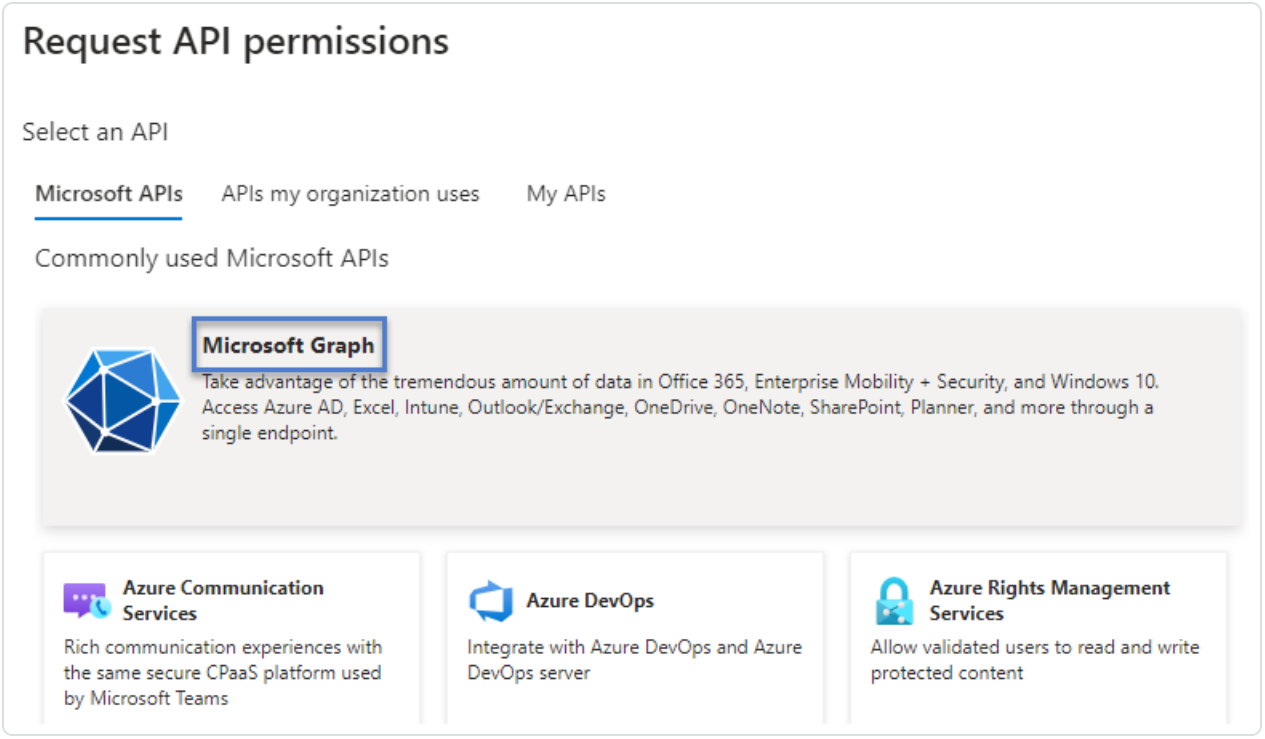
d. 既存の User.Read アクセス許可を削除します。



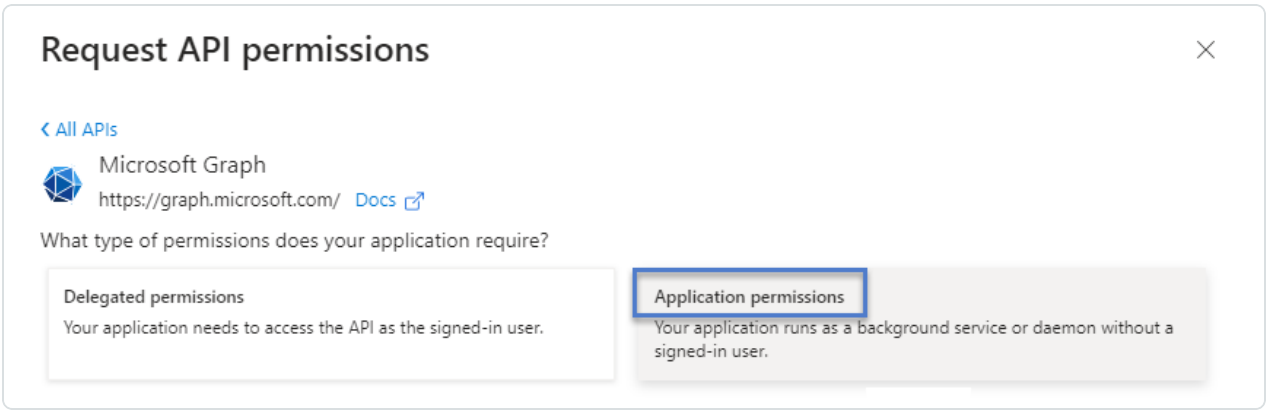
e. **[+ アクセス許可の追加]** をクリックします。



f. **[Microsoft Graph]** を選択します。



g. **[アプリケーションのアクセス許可]** を選択します ([委任されたアクセス許可] ではありません)。



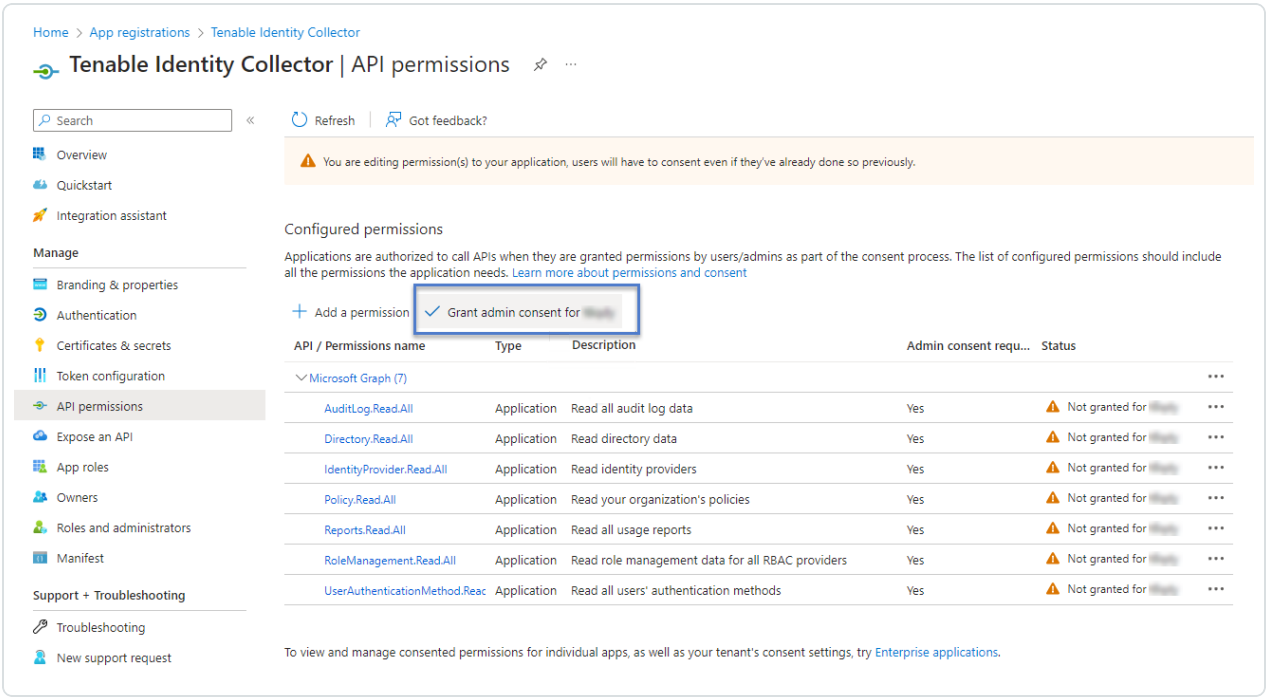
h. リストか検索バーを使用して、次のすべてのアクセス許可を見つけて選択します。

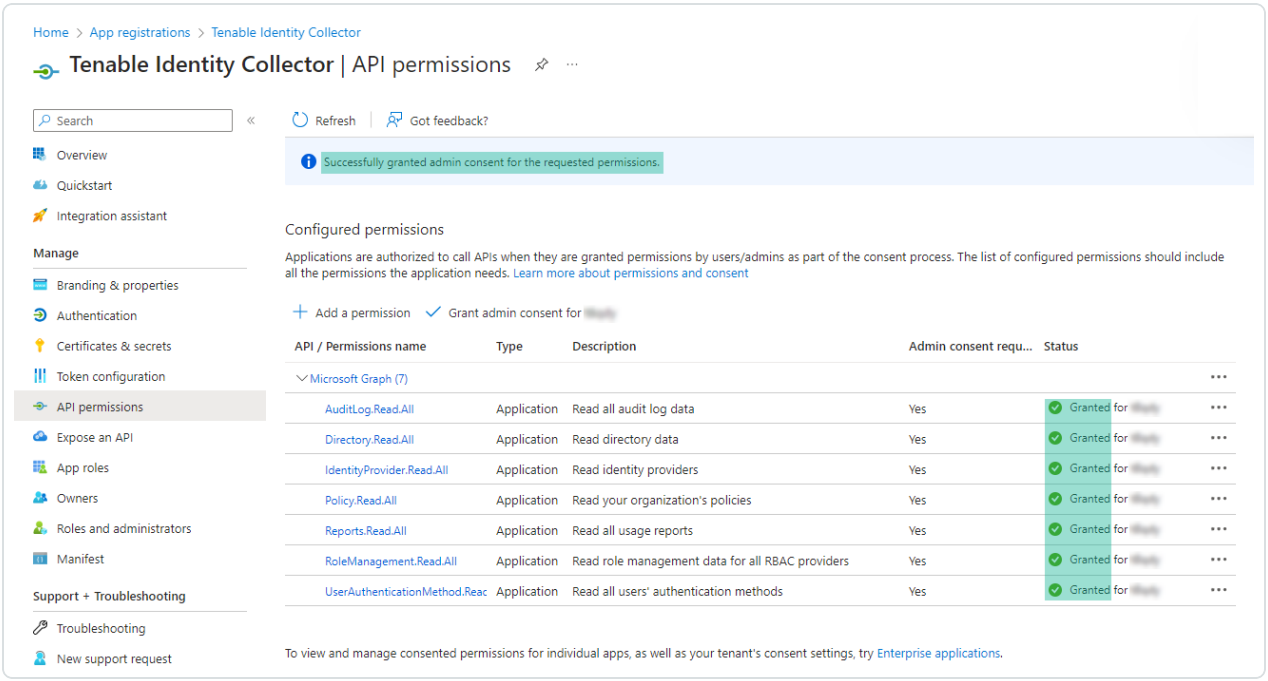
- `AuditLog.Read.All`
- `Directory.Read.All`
- `IdentityProvider.Read.All`
- `Policy.Read.All`
- `Reports.Read.All`

- RoleManagement.Read.All
- UserAuthenticationMethod.Read.All

i. **[アクセス許可の追加]** をクリックします。

j. **[<テナント名> に管理者の同意を付与する]** をクリックし、**[はい]** をクリックして確定します。





4. Microsoft Entra ID で必要なすべての設定をしたら、以下を実行します。

    a. Tenable Vulnerability Management で「Microsoft Azure」タイプの新しい認証情報を作成します。

    b. 「キー」認証方法を選択し、前の手順で取得した値（テナント ID、アプリケーション ID、クライアントシークレット）を入力します。

Microsoft Entra ID のサポートを有効化する

のサポートを有効化するには

注意：この機能を有効化するには、このアクセスキーとシークレットキーを作成した Tenable クラウドユーザーが、Tenable Identity Exposure ライセンスで参照されている Tenable クラウドコンテナで、管理者権限を持っていなければなりません。詳細は、Tenable Identity Exposure のライセンシング を参照してください。

1. Tenable Identity Exposure で、左側のナビゲーションメニューのシステムアイコン  をクリックします。
2. **[設定]** タブをクリックします。

    [設定] ページが開きます。
3. アプリケーションサービスで、**[Tenable クラウド]** をクリックします。
4. **[Microsoft Entra ID サポートの有効化]** のトグルをクリックして有効にします。
5. Tenable クラウドにログインしたことがない場合は、リンクをクリックしてログインページに移動します。

    a. **[パスワードをお忘れですか?]** をクリックし、パスワードリセットをリクエストします。

    b. Tenable Identity Exposure ライセンスに関連付けられているメールアドレスを入力し、**[パスワードのリセットをリクエスト]** をクリックします。

    Tenable はそのアドレスに、パスワードをリセットするためのリンクが記載されたメールを送信します。

    注意：メールアドレスが Tenable Identity Exposure ライセンスに関連付けられているものと異なる場合は、カスタマーサポートに連絡してサポートを受けてください。
6. Tenable Vulnerability Management にログインします。

7. Tenable Vulnerability Management で API キーを生成するには、Tenable Vulnerability Management の **[設定]** > **[マイアカウント]** > **[API キー]** に移動します。

8. Tenable Vulnerability Management「管理者」ユーザーの AccessKey と SecretKey を入力して、Tenable Identity Exposure と Tenableクラウド サービスの間の接続を設定します。

9. **[キーを編集する]** をクリックして、API キーを送信します。

Tenable Identity Exposure に、API キーを更新したことを確認するメッセージが表示されます。

テナントスキャンを有効にする

新しい テナントを追加するには

テナントを追加すると、Tenable Identity Exposure と Microsoft Entra ID テナントがリンクして、そのテナントでスキャンを実行できるようになります。

1. [設定] ページで、**[テナント管理]** タブをクリックします。

   [テナント管理] ページが開きます。

2. **[テナントの追加]** をクリックします。

   [テナントの追加] ページが開きます。

3. **[テナントの名前]** ボックスに名前を入力します。
4. **[認証情報]** ボックスのドロップダウンリストをクリックして、認証情報を選択します。
5. 使用する認証情報がリストに表示されない場合は、次のいずれかを行うことができます。
    - Tenable Vulnerability Management (Tenable Vulnerability Management > **[設定]** > **[認証情報]**) で作成します。詳細については、Tenable Vulnerability Management の Azure タイプの認証情報を作成する手順を参照してください。
    - Tenable Vulnerability Management で、認証情報に「使用可能」または「編集可能」アクセス許可があることを確認してください。これらのアクセス許可がない限り、Tenable Identity Exposure のドロップダウンリストに認証情報が表示されません。
6. **[更新]** をクリックして、認証情報のドロップダウンリストを更新します。
7. 作成した認証情報を選択します。
8. **[追加]** をクリックします。

Tenable Identity Exposure がテナントを追加したことを確認するメッセージが表示され、テナント管理ページのリストに表示されるようになります。

テナントのスキャンを有効にするには

注意: テナントスキャンはリアルタイムでは行われず、アイデンティティエクスプローラーに Microsoft Entra ID のデータが表示されるまで少なくとも 45 分必要です。

- リストでテナントを選択し、トグルをクリックして **[スキャン可能]** に切り替えます。

Tenable Identity Exposure はテナントでのスキャンをリクエストし、その結果が露出インジケーターページに表示されます。

注意: 2 つのスキャン間の必須の最小遅延時間は **30 分**です。

Tenable クラウドのデータ収集

Tenable クラウド – Tenable Identity Exposure のデータ収集機能は、情報をプライベートクラウドに転送して、セキュリティ分析とサービスを提供します。データ収集の詳細については、Tenable の 信頼と保証 のステートメントを参照してください。

Tenable クラウドを使用するには

1. Tenable Identity Exposure で、サイドナビゲーションバーの **[システム]** をクリックし、**[システム]** をクリックします。

   [システム設定] ペインが開きます。

2. **[設定]** タブを選択します。

3. **[アプリケーションサービス]** セクションで、**[Tenable クラウド]** をクリックします。

   [Tenable クラウド] ペインが開きます。

4. [Tenable クラウドサービスの使用] トグルをクリックして **[有効]** に切り替えます。

   Tenable Identity Exposure が情報転送の設定を更新したことを確認するメッセージが表示されます。

特権分析

特権分析は Tenable Identity Exposure のオプション機能で、保護データを取得し、より多くのセキュリティ分析を提供するために、他の機能とは対照的により多くの権限を必要とします。

データ取得

> 注意: 特権分析機能には、昇格された権限が必要です。特権分析のアクセスを参照してください。

特権分析を有効にすると、次の追加データが取得されます。

- **パスワードハッシュ** - Tenable Identity Exposure はパスワード分析のために LM および NT ハッシュを取得します。Tenable Identity Exposure は、古くて弱いアルゴリズムを使用する LM ハッシュの存在について警告するためだけに LM ハッシュを取得しますが、保存はしません。ハッシュコレクションの範囲には以下が含まれます。
    - すべての有効なユーザーアカウント
    - すべての有効なドメインコントローラーコンピューターアカウント

データ保護

Active Directory (AD) 自体はユーザーパスワードを直接保存しません。元のパスワードの回復できないように、LM または NT ハッシュアルゴリズムを使ってハッシュ化のみを行います。Tenable Identity Exposure は、LM ハッシュを保存しません。

SAAS-VPN プラットフォームでリレーをホストしているクライアントを除き、リレーのみがパスワードを処理するため、パスワードがクライアントのインフラから離れることはありません。リレーはパスワードを保存しませんが、分析に必要になるたびにユーザーのパスワードを取得し、一時的に(通常は数ミリ秒のみ) キャッシュに保存します。ただし、Tenable Identity Exposure は、K-匿名性分析を実行して同一のパスワードを使用するユーザーをチェックするためだけに、最小限のビット数のパスワードハッシュデータをリレーの RAM に安全に保存します。

> **注意**: SaaS-VPN プラットフォームクライアントの場合も動作は同じですが、Tenable がリレーをホストします。

アクティビティログ

Tenable Identity Exposure のアクティビティログにより、特定の IP アドレス、ユーザー、アクションに関連する、Tenable Identity Exposure プラットフォームで発生したすべてのアクティビティの痕跡を確認することができます。

アクティビティログを設定するには

1. Tenable Identity Exposure サイドナビゲーションペインの **[管理]** で、**[システム]** をクリックします。

   [システム設定] ペインが開きます。

2. **[アプリケーションサービス]** セクションで、**[アクティビティログ]** をクリックします。

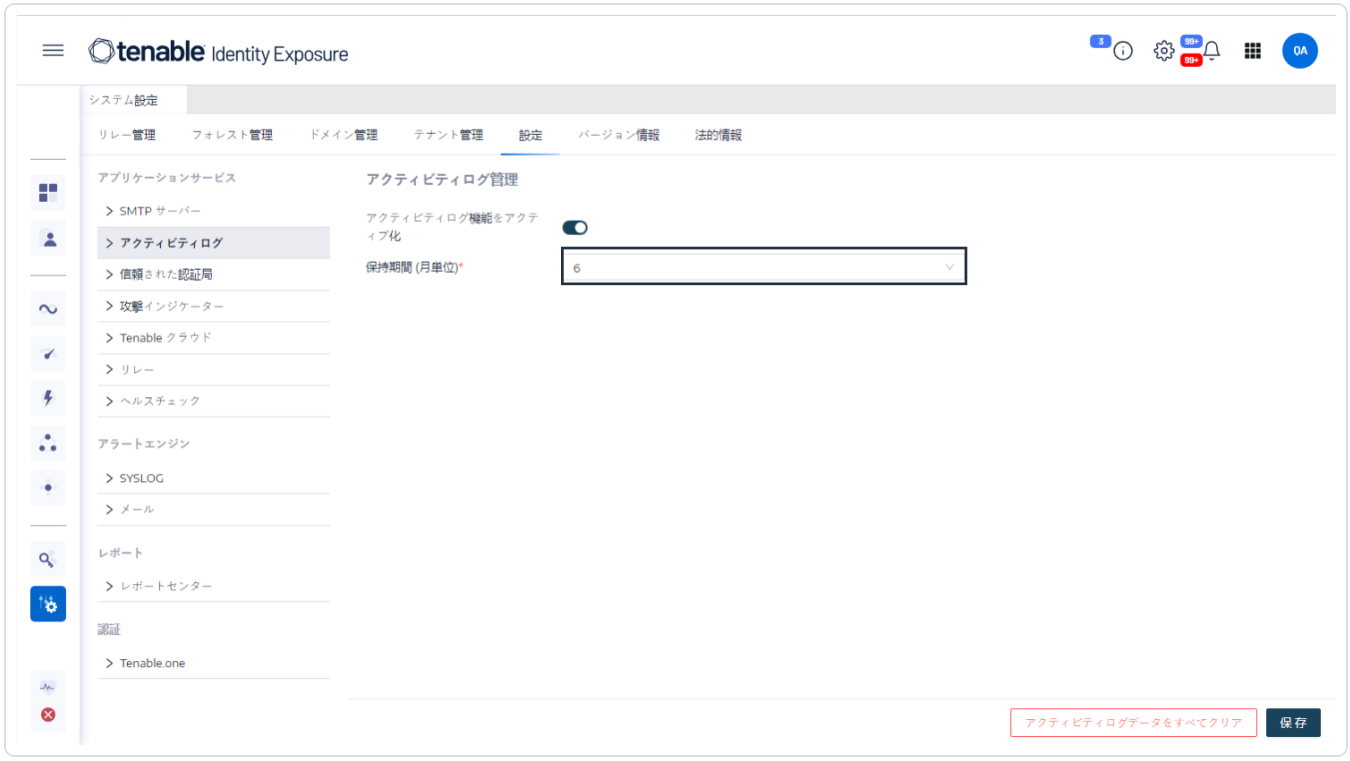
   [アクティビティログ管理] ペインが開きます。

3. アクティビティログ機能を有効にするには、トグルをクリックして **[有効]** にします。

4. [保持期間 (月単位)] ボックスで、**>** をクリックして、アクティビティを記録する月数を選択します。

5. **[保存]** をクリックします。

   Tenable Identity Exposure が設定を更新したことを確認するメッセージが表示されます。



アクティビティログデータを消去するには

1. Tenable Identity Exposure サイドナビゲーションペインの **[管理]** で、**[システム]** をクリックします。

   [システム設定] ペインが開きます。

2. **[アプリケーションサービス]** セクションで、**[アクティビティログ]** をクリックします。

   [アクティビティログ管理] ペインが開きます。

3. **[アクティビティログデータをすべてクリア]** で、**[クリア]** をクリックします。

   確認を求めるメッセージが表示されます。

4. **[確認]** をクリックします。

   Tenable Identity Exposure が設定を更新したことを確認するメッセージが表示されます。

ユーザーが自身のアクティビティログにアクセスするためのアクセス許可を設定するには

1. Tenable Identity Exposure サイドナビゲーションペインの **[管理]** で、**[アカウント]** をクリックします。

   [ユーザーアカウント管理] ペインが開きます。

2. **[ロール管理]** タブを選択します。

3. ロールのリストで、このアクセス許可を必要とするユーザーロールにカーソルを合わせ、行の末尾にある アイコンをクリックします。

   [ロールの編集] ペインが開きます。

4. **[主要な情報]** セクションで、**[システム設定エンティティ]** タブを選択します。

5. **[アクセス許可管理]** セクションで、以下を実行します。

   - **[アクティビティログ]** のアクセス許可の *[不許可]* を選択解除します。
   - **[ユーザー自身のトレースのみを表示]** のアクセス許可を選択して、*[許可]* にします。

6. **[適用して閉じる]** をクリックします。

Tenable Identity Exposure がユーザーロールを更新したことを確認するメッセージが表示されます。

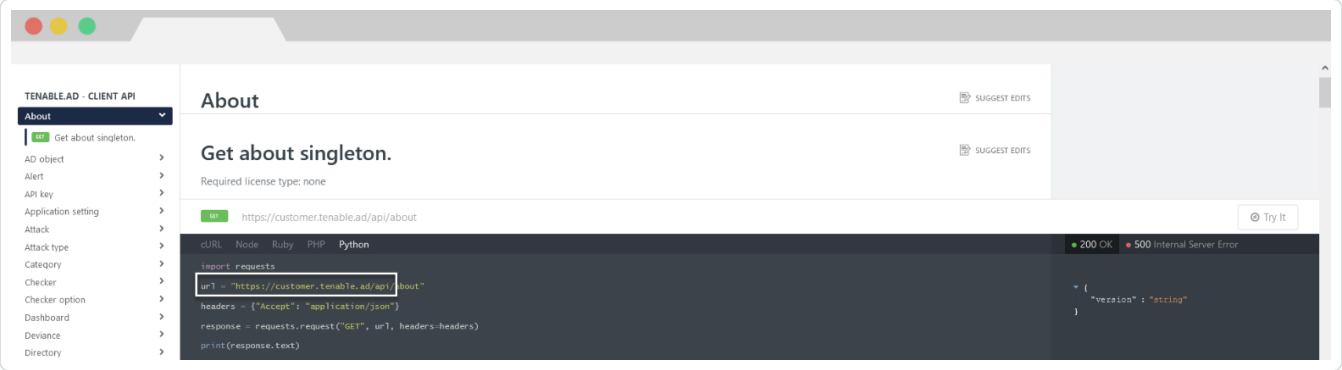
Tenable Identity Exposure 公開 API

Tenable Identity Exposure の API を使用すると、そのデータベースサービスと通信できます。

Tenable Identity Exposure の API の構造とリソースが含まれている OpenAPI ファイルは、こちら から入手できます。

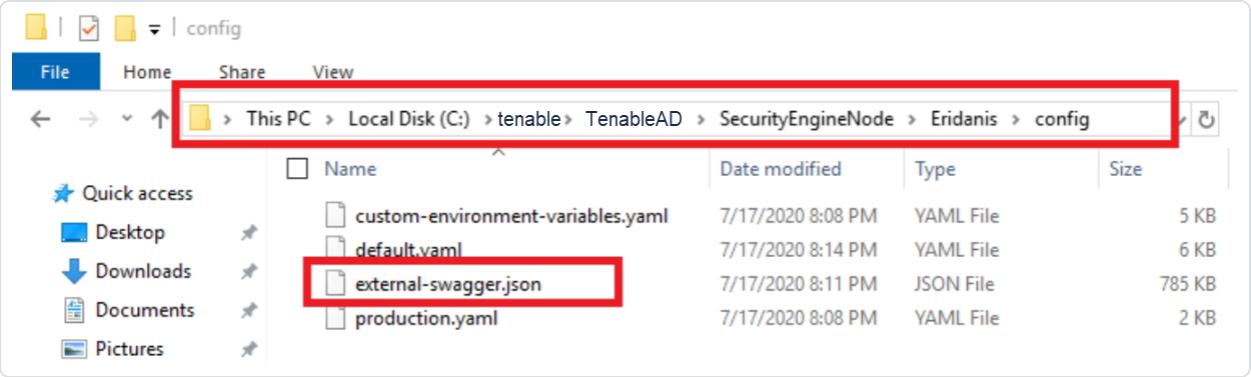
Tenable Identity Exposure インスタンスの API にアクセスするには

- ブラウザで、次の URL を開きます。



OpenAPI ファイルをダウンロードするには

- オンプレミスインストールの場合は、セキュリティエンジンノードの次のパスをたどります。



- SaaS インストールの場合は、Tenable Identity Exposure API Explorer に移動します。

API キーを取得するには

1. Tenable Identity Exposure で、ユーザープロファイルアイコンをクリックし、**[環境設定]** を選択します。

   環境設定ペインが開きます。

2. メニューから、**[API キー]** を選択します。

   Tenable Identity Exposure が現在の API キーを表示します。

3. API キーをクリップボードにコピーするには、 アイコンをクリックします。

API キーを更新するには

[API キーの更新] をクリックするか、API キーまたはアクセストークンを生成する権利を失うと、アクセストークンが期限切れになります。有効期限は、時間や API リクエストの数とは関係ありません。API キーの生成または更新は現在のユーザーに固有のものであり、他のアカウントの API キーには影響しません。API キーを取得すると、リフレッシュトークンも受け取ります。このリフレッシュトークンを使用して、新しい API トークンを取得できます。

注意: API キーを更新すると、Tenable Identity Exposure は現在の API キーを無効にします。リフレッシュトークンも受け取ります。

1. **[API キーの更新]** をクリックします。

   確認を求めるメッセージが表示されます。

2. **[確認]** をクリックします。

データ管理

Tenable Identity Exposure はデータを 6 か月間保持します。このデータ管理期間は設定できません。

デプロイメントリージョン

Tenable Identity Exposure SaaS は現在、次の Azure リージョンにデプロイされています。

国	Azure リージョン
南北アメリカ	
ブラジル – サンパウロ	ブラジル南部
カナダ – ケベックシティ	カナダ東部
カナダ – トロント	カナダ中部
米国 – カリフォルニア	米国西部
米国 – アイオワ	米国中部
米国 – バージニア	米国東部 2
ヨーロッパ、中近東、アフリカ	
フランス – パリ	フランス中部
アイルランド	北ヨーロッパ
オランダ	西ヨーロッパ
南アフリカ – ヨハネスブルグ	南アフリカ北部
スイス – チューリッヒ	スイス北部
アラブ首長国連邦 – ドバイ	アラブ首長国連邦北部
英国 – ロンドン	英国南部
アジア太平洋地域	
オーストラリア – ニューサウスウェールズ	オーストラリア東部
オーストラリア – ビクトリア	オーストラリア南東部
香港	東アジア
インド – プネー	中央インド

日本 – 大阪	西日本
シンガポール	東南アジア

Tenable Identity Exposure のライセンシング

このトピックでは、スタンドアロン製品としての Tenable Identity Exposure のライセンス付与プロセスを説明します。また、資産のカウント方法と、ライセンスの超過または有効期限が切れた場合の対応についても説明します。Tenable Identity Exposure の使用方法については、Tenable Identity Exposure ユーザーガイドを参照してください。

Tenable Identity Exposure のライセンス付与

Tenable Identity Exposure には、クラウドバージョンとオンプレミスバージョンの 2 つのバージョンがあります。Tenable は、場合によってはサブスクリプション価格も提供しています。

Tenable Identity Exposure を使用するには、所属する組織のニーズと環境に基づいてライセンスを購入してください。Tenable Identity Exposure は、組織の*資産*(ディレクトリサービスで有効になっているユーザー)にそれらのライセンスを割り当てます。

環境が拡張すると資産数も増えるため、その変化に合わせてライセンスを追加購入する必要があります。Tenable ライセンスは累進的な価格設定を使用するため、多く購入するほど単価は低くなります。価格については、Tenable の担当者までお問い合わせください。

ヒント: 現在のライセンス数と利用可能な資産を表示するには、Tenable の上部のナビゲーションバーで をクリックし、**[ライセンス情報]** をクリックします。詳細については、ライセンス情報ページを参照してください。

注意: Tenable は、マネージドセキュリティサービスプロバイダー(MSSP)にシンプルな価格設定を提供しています。詳細については、Tenable の担当者にお問い合わせください。

資産のカウント方法

購入する各 Tenable Identity Exposure ライセンスにつき、ユーザーの一意の ID またはデジタル表現を 1 件スキャンすることができます。Tenable は ID を二重にカウントしません。たとえば、Microsoft Active Directory と Microsoft Entra ID の両方で同じ ID に対して有効になっているユーザーアカウントは、1 つの Tenable ライセンスとしてカウントされます。

Tenable Identity Exposure コンポーネント

Tenable Identity Exposure のどちらのバージョンでも、以下のコンポーネントが含まれています。

- イベントフロービュー
- トポロジービュー
- 露出インジケーター
- 攻撃インジケーター
- 攻撃経路
- ID エクスプローラー
- Microsoft Entra ID サポート

ライセンスの流用

ライセンスを購入した場合、追加のライセンスを購入しない限り、契約期間中はライセンスの合計数は変わりません。ただし、環境のディレクトリサービスから有効なユーザーを削除すると、Tenable Identity Exposure はリアルタイムでライセンスを流用します。

ライセンス制限の超過

ハードウェアの更新、急激な環境の拡張、予期しない脅威などによる、使用率の急増に対応できるよう、Tenable ライセンスは柔軟に提供されます。ただし、ライセンス保有数より多くの資産をスキャンした場合、Tenable は超過分を明確に通知し、その後 3 段階にわたって機能が制限されます。

シナリオ	結果
3 日間連続で、ライセンスが付与されている ID より多くの ID を有効にしている	Tenable Identity Exposure に、メッセージが表示されます。
15 日以上連続で、ライセンスが付与されている ID より多くの ID を有効にしている	Tenable Identity Exposure に、制限された機能に関するメッセージと警告が表示されます。
45 日以上連続で、ライセンスが付与されている ID より多くの ID を有効にしている	Tenable Identity Exposure にメッセージが表示され、エクスポート機能が無効になります。

期限切れのライセンス

購入した Tenable Identity Exposure ライセンスは、契約期間中ずっと有効です。ライセンスの有効期限が切れる 30 日前になると、ユーザーインターフェースに警告が表示されます。この更新期間中に、Tenable の担当者と連携して、製品の追加や削除、ライセンス数の変更を行ってください。

ライセンスの有効期限が切れると、Tenable プラットフォームにサインインできなくなります。

ライセンスの管理

Tenable Identity Exposure には、Tenable または認定エンタープライズパートナーから入手したライセンスファイルが必要です。ライセンスユーザー数には、有効なユーザーとサービスアカウントがすべて含まれます。

Tenable Identity Exposure を設定して使用するには、このライセンスファイルをアップロードする必要があります。

Tenable Identity Exposure のライセンスには以下の機能が含まれます。

- 攻撃インジケーター
- 露出インジケーター
- 上記の両方

ライセンスを表示するには

- Tenable Identity Exposure で、**[システム]** > **[情報]** タブをクリックします。

  ライセンスが表示されます。

ライセンス消費

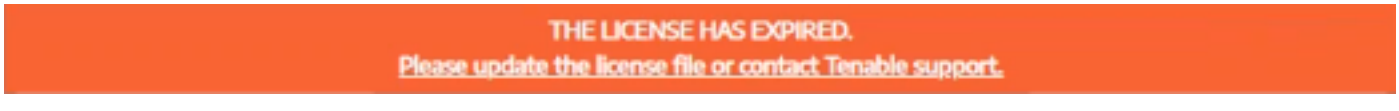
オンプレミスインストールの Tenable Identity Exposure では、インターネットに接続されている間はライセンス消費が追跡されます。

ライセンスの有効性

Tenable Identity Exposure のライセンスは、以下の条件を満たしている場合に限り有効です。

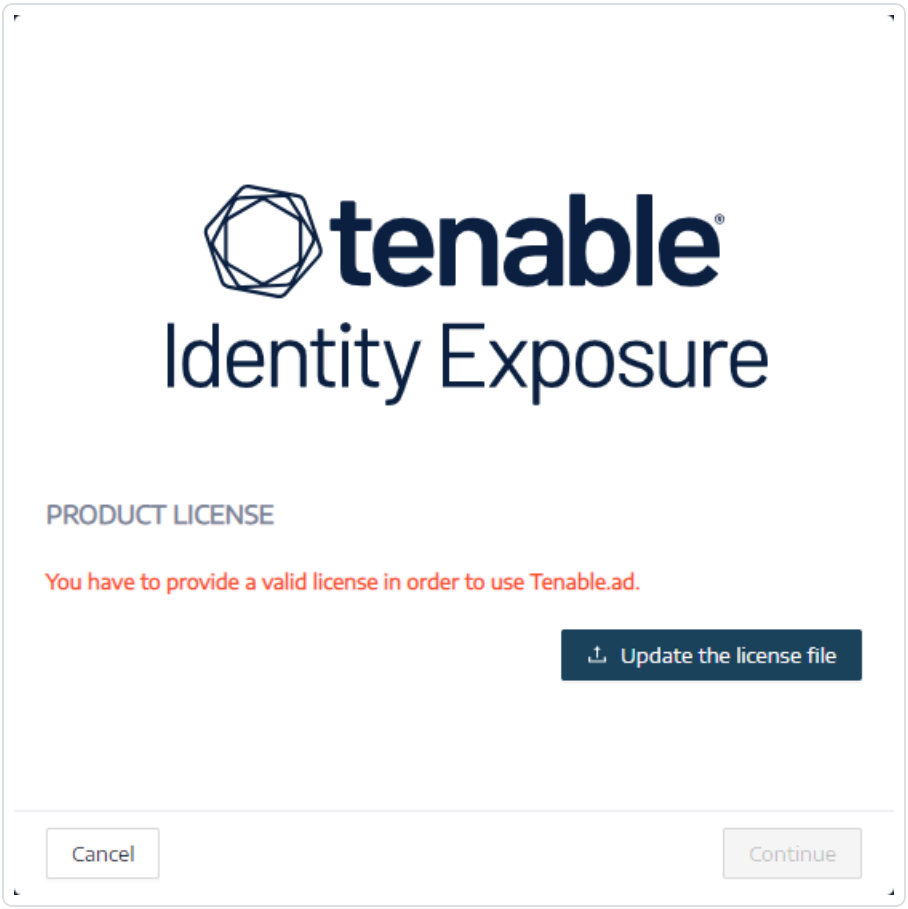
- ユーザーの数が、ライセンス付与された人数を超えていない
- 有効期限が切れていない

上記の条件のいずれかを満たしていない場合、Tenable Identity Exposure はライセンスのアップデートを求める次の警告を表示します。



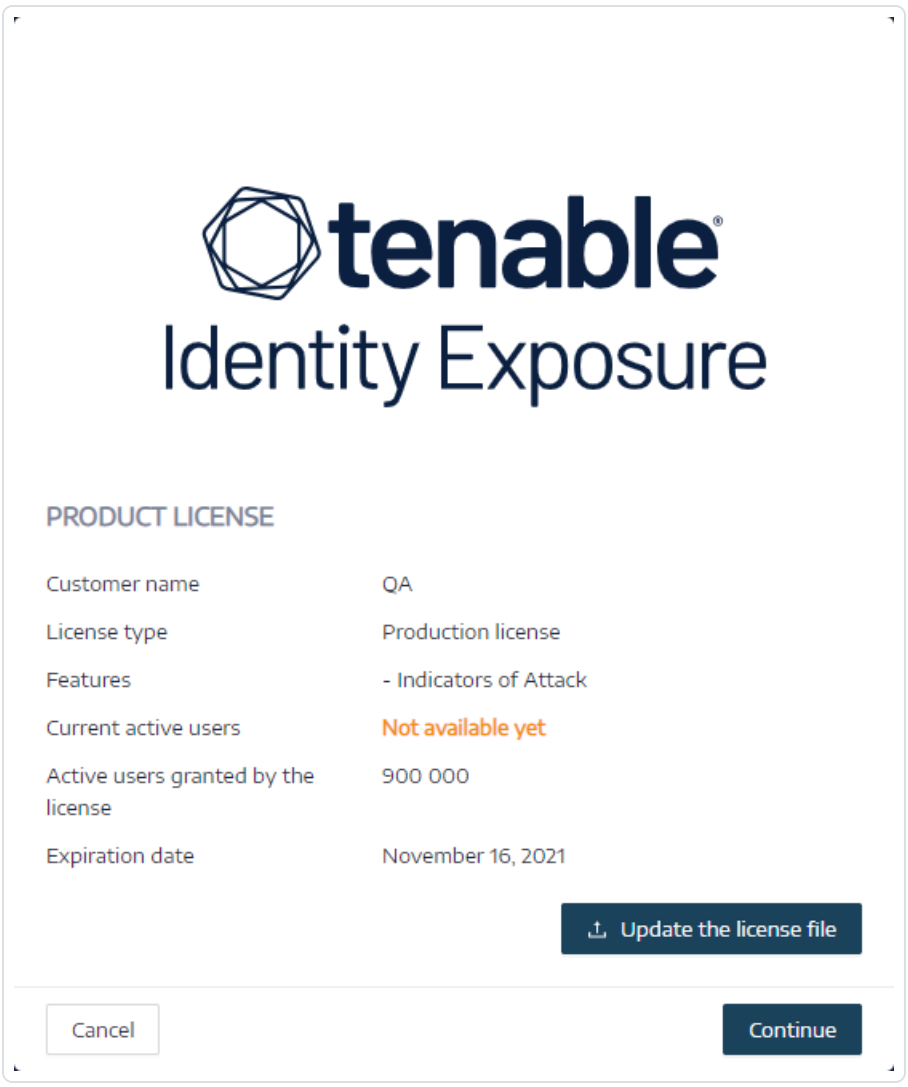
ライセンスファイルをアップロードするには

1. ログインウィンドウで **[ライセンスファイルの更新]** をクリックします。



2. ライセンスファイルの場所を参照し、**[開く]** をクリックします。

   以下の例は、ライセンスファイルが正しく適用された状態を示しています。



3. **[続行]** をクリックして Tenable Identity Exposure を開きます。

ライセンスファイルをアップデートするには

1. Tenable Identity Exposure で、**[システム]** > **[バージョン情報]** の順にクリックします。
2. **[ライセンスファイルの更新]** をクリックします。
3. ライセンスファイルの場所を参照し、**[開く]** をクリックします。

   Tenable Identity Exposure がライセンスファイルを更新します。ライセンスファイルが無効な場合は、カスタマーサポートに連絡してください。

Tenable Identity Exposure のトラブルシューティング

以下のトピックは、Tenable Identity Exposure (旧 Tenable.ad) の使用時に発生する可能性がある問題の解決に役立ちます。

- Tenable Identity Exposure 診断ツール
- SYSVOL 堅牢化の Tenable Identity Exposure に対する干渉

Tenable Identity Exposure 診断ツール

Tenable Identity Exposure は、Tenable Identity Exposure のインストールに関連するログ情報を取得できる診断ツールを提供しています。これにより、カスタマーサポートは問題の分析とサポートを行うことができます。

この診断ツールは、Tenable ダウンロードポータルからダウンロードします。

注意: この診断ツールは、Tenable Identity Exposure の**オンプレミスのインストール**に対してのみ機能します。

診断ツールでは、次の内容を実行できます。

- 現在のマシン(実行可能ファイルを起動した場所)が、ストレージマネージャー(SM)、セキュリティエンジンノード(SEN)、またはディレクトリリスナー(DL)をホストしているかどうかを特定します。
- 環境をスキャンして、ネットワークで利用可能な他の Tenable Identity Exposure のインストールを見つけます。
- Tenable Identity Exposure のインストールに関するログソースのリストを検出し、関連する情報を調べて取得します。
- Tenable Identity Exposure のインストール試行の失敗に関する MSI ログを取得します。

最良の結果を得るためのヒント

- SEN で診断ツールを実行します。
- 権限昇格したユーザーで診断ツールを実行して、ほとんどまたはすべてのログソースをアクティブにします。
- SM またはその他のインストールを検出するには、次の条件が揃っていることを確認してください。
    - リモートコマンドをリモートコンピューターで実行できる設定になっている(Invoke-Command コマンドレット)
    - ディスクへのリモートアクセスが可能な設定になっている
    - WMI が有効化されていて、現在のユーザーアカウントに許可されている

診断ツールを実行するには

1. Tenable ダウンロードポータルから `TenableAdDiagnosticTool.OnPrem.Console.exe` ファイルをダウンロードします。
2. 実行可能ファイルを管理者として Tenable Identity Exposure マシン、できれば SEN をホストしているマシンで実行します。
3. プロンプトで、次のいずれかのオプションを入力します。
   - `E` – すべてのログ(デフォルトオプション)
   - `Msi` – Tenable Identity Exposure のインストールに関連するログ
   - `Tenable` – Tenable Identity Exposure に関連するログ
4. Enter を押します。

   診断ツールがインストールをスキャンします。スキャンが完了すると、現在のディレクトリに圧縮されたファイルが出力されます。
5. この圧縮ファイルを Tenable Identity Exposure カスタマーサポートに送信します。ファイルの内容を変更しないように注意してください。

コマンドラインを使用して診断ツールを実行するには

1. コマンドラインで、実行可能ファイル `TenableAdDiagnosticTool.OnPrem.Console.exe` を管理者として Tenable Identity Exposure マシンで、できれば SEN をホストしているマシンで実行します。

   診断ツールがインストールをスキャンします。スキャンが完了すると、現在のディレクトリに zip ファイルが出力されます。
2. この圧縮ファイルを Tenable Identity Exposure カスタマーサポートに送信します。ファイルの内容を変更しないように注意してください。

その他のオプション

診断ツールは、コマンドラインで起動すると次のオプションも利用できます。

- `--help` – 診断ツールの使用法の簡単な説明
- `--commands` – マシンの能力をテストし他のインストールをスキャンする Powershell/WMI クエリのリスト

SYSVOL 堅牢化の Tenable Identity Exposure に対する干渉

SYSVOL は、Active Directory ドメインの各ドメインコントローラー(DC)にある共有フォルダーです。SYSVOL には、グループポリシー(GPO)用のフォルダーとファイルが保存されます。SYSVOL のコンテンツはすべての DC で複製され、`\\<example.com>\SYSVOL` や `\\<DC_IP_or_FQDN>\SYSVOL` などの汎用命名規則 (UNC) パスを使ってアクセスできます。

SYSVOL 堅牢化とは、強化された UNC パスパラメーターの使用のことで、「UNC の強化されたアクセス」、「強化された UNC パス」、「UNC パスの堅牢化」、または「強化されたパス」とも呼ばれています。この機能は、グループポリシーの MS15-011 (KB 3000483) の脆弱性に対処するために導入されました。CIS ベンチマークなどの多くのサイバーセキュリティ標準では、この機能の強制実行が義務付けられています。

この堅牢化パラメーターをサーバーメッセージブロック(SMB)クライアントに適用すると、ドメインに参加しているマシンのセキュリティが実際に向上し、SYSVOL から取得する GPO コンテンツがネットワーク上の攻撃者に改ざんされないようになります。ただし、特定の状況では、このパラメーターが Tenable Identity Exposure の操作に干渉することもあります。

強化された UNC パスが Tenable Identity Exposure と SYSVOL 共有間の接続を乱していることに気付いた場合は、このトラブルシューティングセクションにあるガイダンスに従ってください。

影響を受ける環境

次の Tenable Identity Exposure デプロイメントオプションでは、この問題が発生する可能性があります。

- オンプレミス
- セキュアリレーを備えた SaaS

次のデプロイメントオプションは影響を受けません。

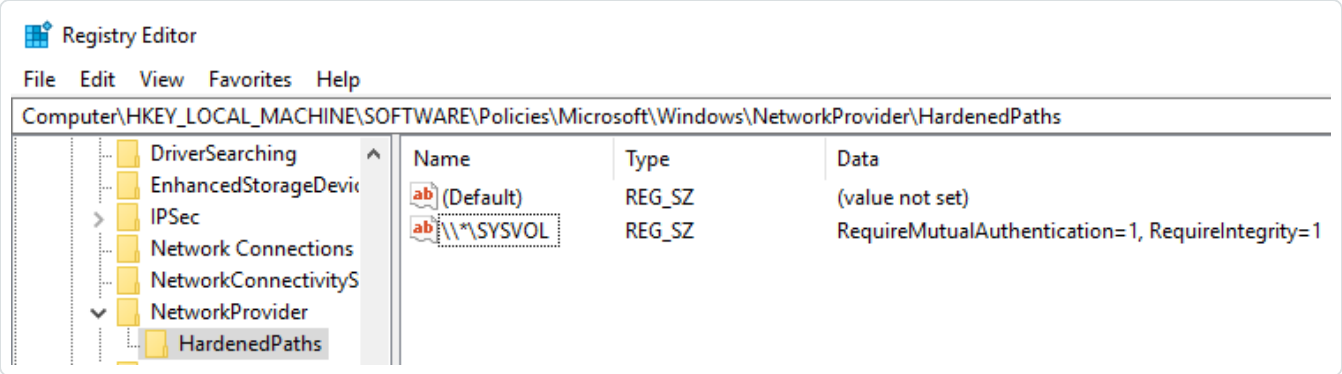
- VPN を備えた SaaS

SYSVOL 堅牢化はクライアント側のパラメーターであり、ドメインコントローラーではなく、SYSVOL 共有に接続するマシンで動作します。

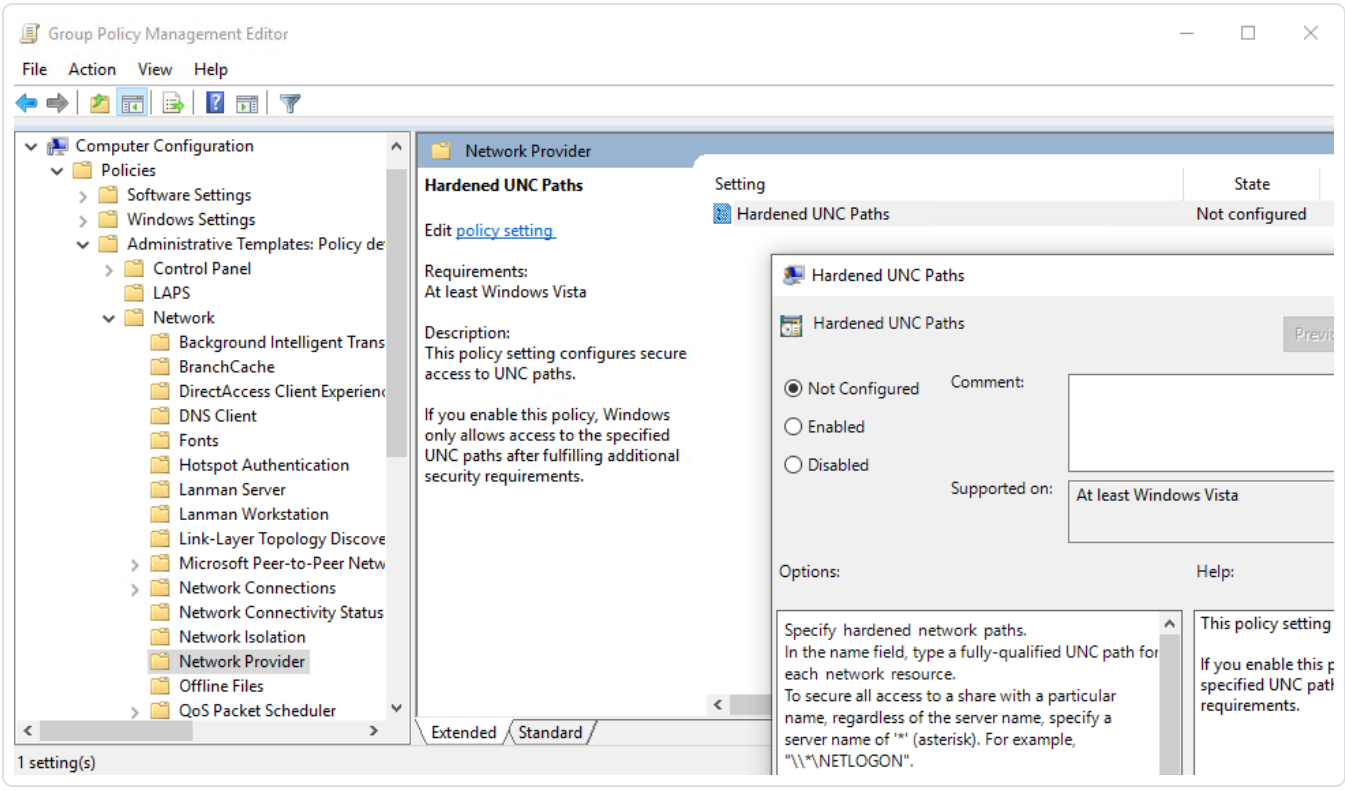
Windows はこのパラメーターをデフォルトで有効にし、Tenable Identity Exposure に干渉する場合があります。

企業によっては、関連する GPO 設定を使用するか、対応するレジストリキーを直接設定することで、このパラメーターを確実にアクティブ化し強制実行したいと思うかもしれません。

- UNC 堅牢化パスに関連するレジストリキーは、「HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths」にあります。



- 対応する GPO 設定は、「Computer Configuration/Administrative Templates/Network/Network Provider/Hardened UNC paths」にあります。



SYSVOL 堅牢化の強制実行は、SYSVOL を参照する UNC パス(「*\SYSVOL」など)にパラメーター「RequireMutualAuthentication」があり、「RequireIntegrity」の値が「1」に設定されている場合に発生します。

SYSVOL 堅牢化の問題の兆候

SYSVOL 堅牢化が Tenable Identity Exposure に干渉していることが疑われる場合は、次の点をチェックします。

1. Tenable Identity Exposure で、**[システム]** > **[ドメイン管理]** に進み、各ドメインの LDAP と SYSVOL 初期化ステータスを表示します。

   接続性に問題のないドメインでは緑のインジケーターが表示されますが、接続性に問題のあるドメインでは無限に続くクロールインジケーターが表示されます。

2. ディレクトリリスナーまたはリレーマシンで、ログフォルダー `<Installation Folder>\DirectoryListener\logs` を開きます。

3. Ceti ログファイルを開き、「SMB mapping creation failed」(SMB マッピング作成が失敗しました) または「Access is denied」(アクセスが拒否されました) という文字列を検索します。このフレーズを含むエラーログがある場合、UNC 堅牢化がディレクトリリスナーまたはリレーマシンに存在する可能性が高いことを示しています。

修正オプション

Kerberos 認証に切り替えるまたはSYSVOL 堅牢化の無効化の 2 つの修正オプションがあります。

Kerberos 認証に切り替える

このオプションは、堅牢化機能を無効にする必要がないため、推奨されています。

SYSVOL 堅牢化が Tenable Identity Exposure と干渉するのは、NTLM 認証を使用して監視対象のドメインコントローラーに接続する場合のみです。これは、NTLM が「RequireMutualAuthentication=1」パラメーターと互換性がないためです。Tenable Identity Exposure は Kerberos もサポートしています。Kerberos を適切に設定および使用する場合は、SYSVOL 堅牢化を無効にする必要はありません。詳細は、Kerberos 認証を参照してください。

SYSVOL 堅牢化の無効化

Kerberos 認証に切り替えることができない場合は、SYSVOL 堅牢化を無効にすることもできます。

Windows はデフォルトで SYSVOL 堅牢化を有効にするため、レジストリキーまたは GPO 設定を削除するだけでは不十分です。SYSVOL 堅牢化を明示的に無効にし、この変更をディレクトリリスナー(オンプレミス)またはリレー(セキュアリレーを備えた SaaS)をホストしているマシンにのみ適用する必要があります。これはその他のマシンには影響しないため、ドメインコントローラー自体で SYSVOL 堅牢化を無効にする必要はありません。

ディレクトリリスナー(オンプレミス)またはリレー(セキュアリレーを備えた SaaS)をホストしているマシンで使用される Tenable Identity Exposure インストーラーでは、すでにローカルで SYSVOL 堅牢化を無効にしています。ただし、環境内の GPO またはスクリプトが、このレジストリキーを削除したり上書きしたりする可能性があります。

これには、2 つのケースが考えられます。

- ディレクトリリスナーまたはリレーマシンが**ドメインに参加していない**場合 – GPO を使用してマシンを設定できません。レジストリで SYSVOL 堅牢化を無効にする必要があります(レジストリ - GUI またはレジストリ - PowerShell を参照)。
- ディレクトリリスナーまたはリレーマシンが**ドメインに参加している**場合 (Tenable Identity Exposure では非推奨) – レジストリで設定を直接適用するか(レジストリ - GUI またはレジストリ - PowerShell を参照)、GPO を使用することができます。これらのうちいずれかの方法を使用する場合は、GPO またはスクリプトがレジストリキーを上書きしないようにする必要があります。これは、次のいずれかの方法で実行できます。
    - このマシンに適用されるすべての GPO を慎重に確認する
    - 変更を適用して少し待機するか、「gpupdate /force」で GPO の適用を強制し、レジストリキーが値を保持していることを確認する

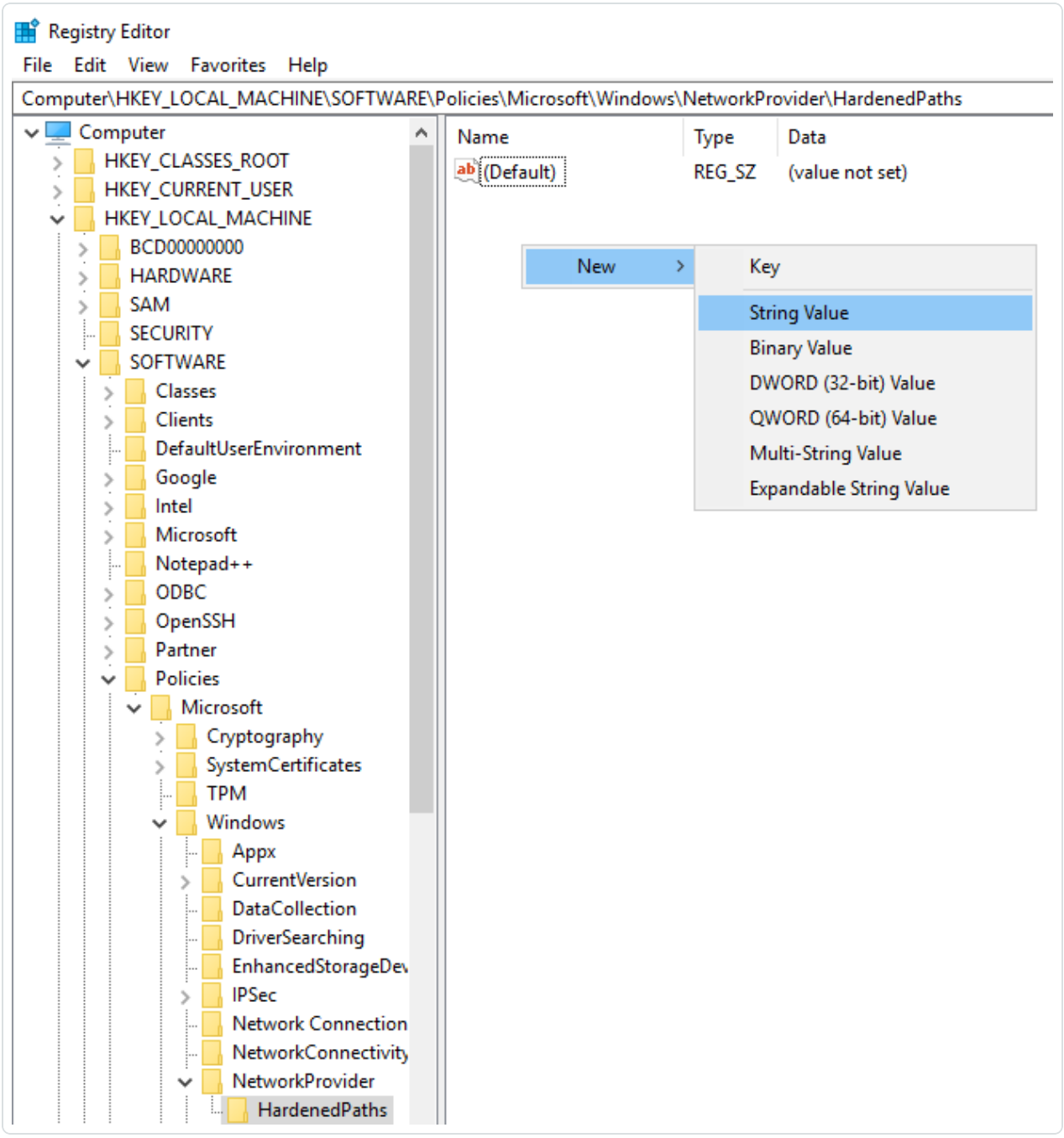
ディレクトリリスナーまたはリレーマシンが再起動したら、変更されたドメインのクロールインジケーターが緑色に変わるはずです。

レジストリ - GUI

GUI を使用してレジストリで SYSVOL 堅牢化を無効にするには

1. 管理者権限でディレクトリリスナーまたはリレーマシンに接続します。
2. レジストリエディターを開き、HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths に移動します。
3. 「*\SYSVOL」という名前のキーが存在しない場合は、次の方法で作成します。

a. 右ペインを右クリックし、**[新規]** > **[文字列の値]** を選択します。

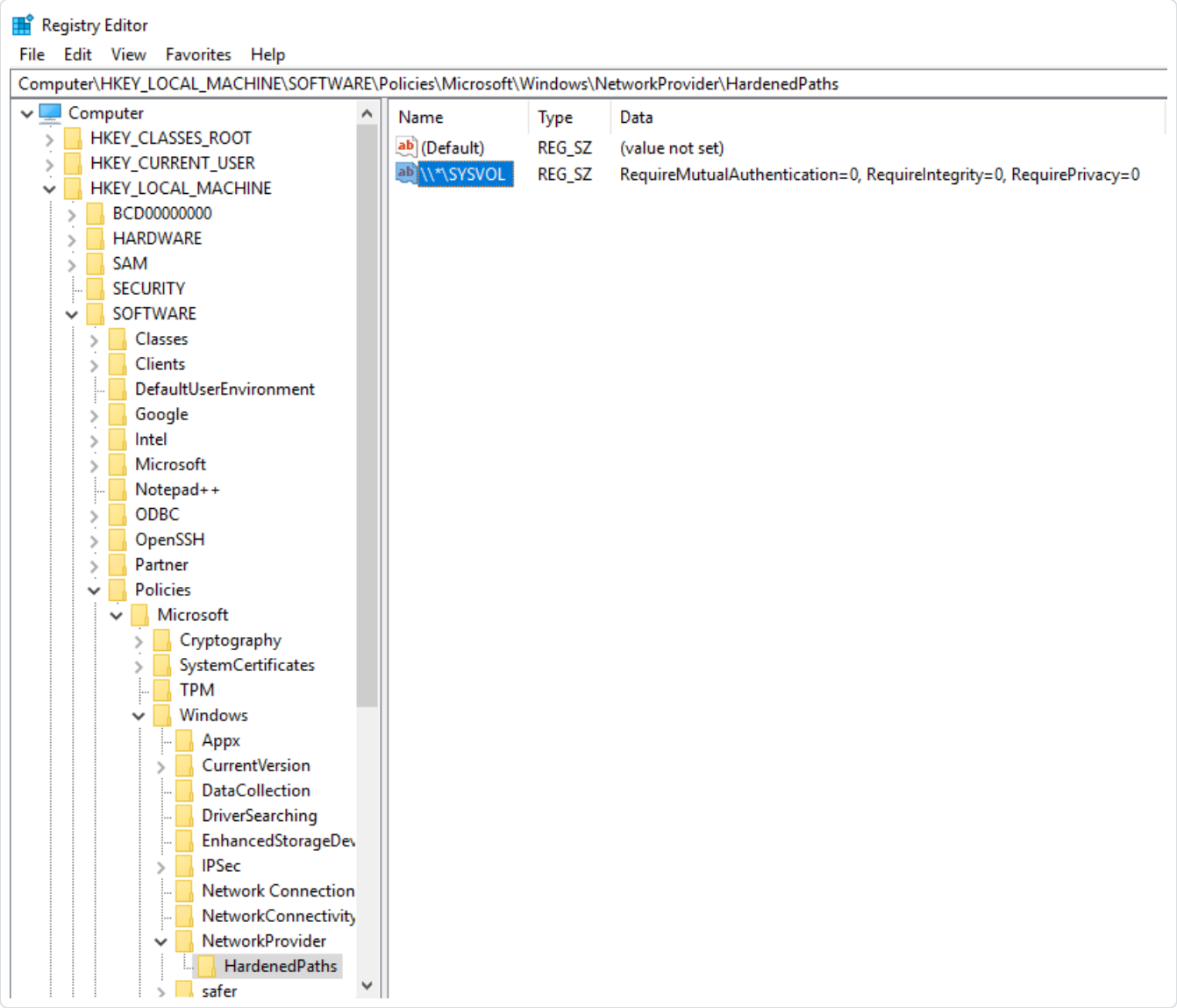


b. [名前] フィールドに *\SYSVOL と入力します。

4. 新規作成された、または以前から存在する「*\SYSVOL」キーをダブルクリックして、**[文字列の編集]** ウィンドウを開きます。

5. **[値]** データフィールドに、`RequireMutualAuthentication=0`、`RequireIntegrity=0`、`RequirePrivacy=0` を入力します。
6. **[保存]** をクリックします。

   結果は次のようになります。



7. マシンを再起動します。

レジストリ - PowerShell

PowerShell を使用してレジストリで SYSVOL 堅牢化を無効にするには

1. 次の PowerShell コマンドを使用して、参照用の UNC 堅牢化パスレジストリキーの現在の値を収集します。

```
Get-Item -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths"
```

2. 推奨値を設定します。

```
New-ItemProperty -Path
"HKLM:\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths" -Name "\\*\SYSVOL" -
Value "RequireMutualAuthentication=0, RequireIntegrity=0, RequirePrivacy=0"
```

3. マシンを再起動します。

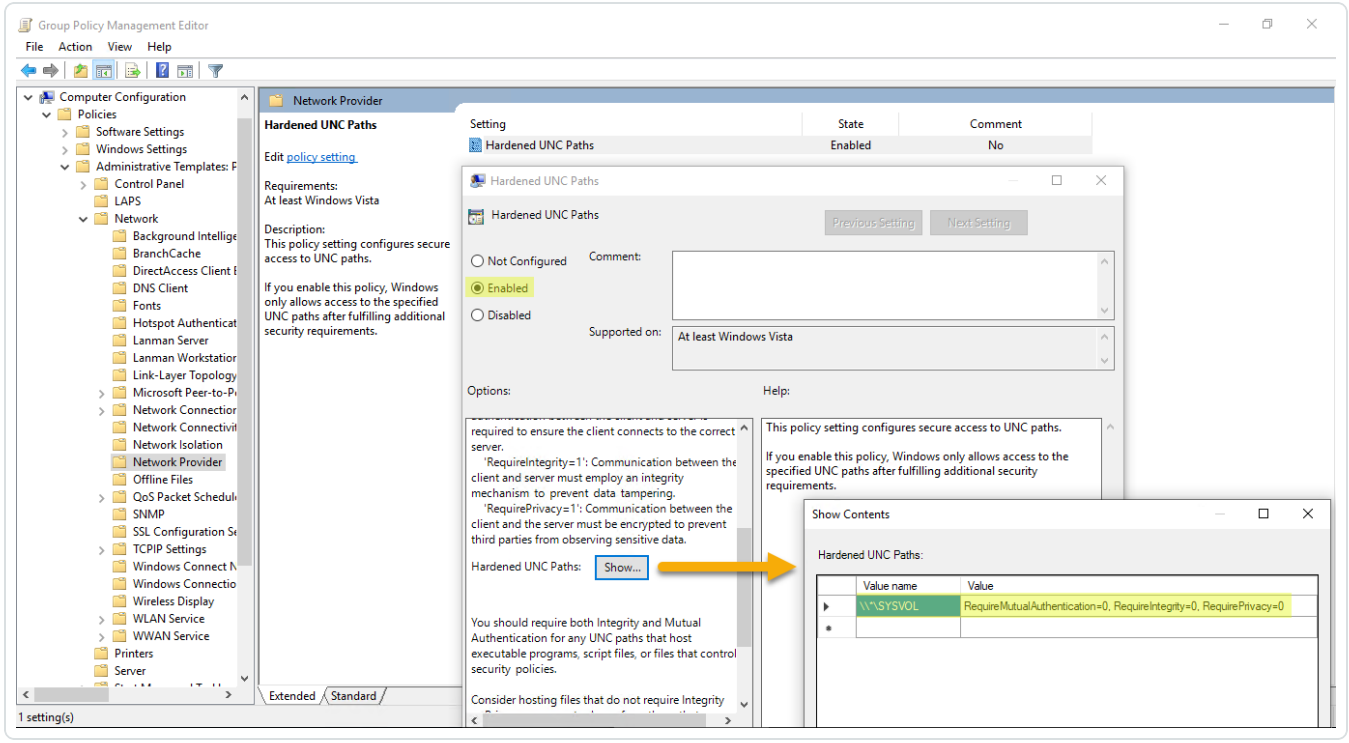
GPO

前提条件: ドメインで GPO を作成でき、Tenable Identity Exposure ディレクトリリスナーまたはリレーマシンを含む組織単位にリンクできる権限を持つ Active Directory ユーザーとして接続する必要があります。

GPO を使用して SYSVOL 堅牢化を無効にするには

1. グループポリシー管理コンソールを開きます。
2. 新しい GPO を作成します。
3. GPO を編集し、次の場所に移動します: コンピューターの設定 / 管理テンプレート / ネットワーク / ネットワークプロバイダー / 強化された UNC パス。
4. この設定を有効にし、次を使用して新しい強化された UNC パスを作成します。
    - 値の名前 = *\SYSVOL
    - 値 = RequireMutualAuthentication=0, RequireIntegrity=0, RequirePrivacy=0

    結果は次のようになります。



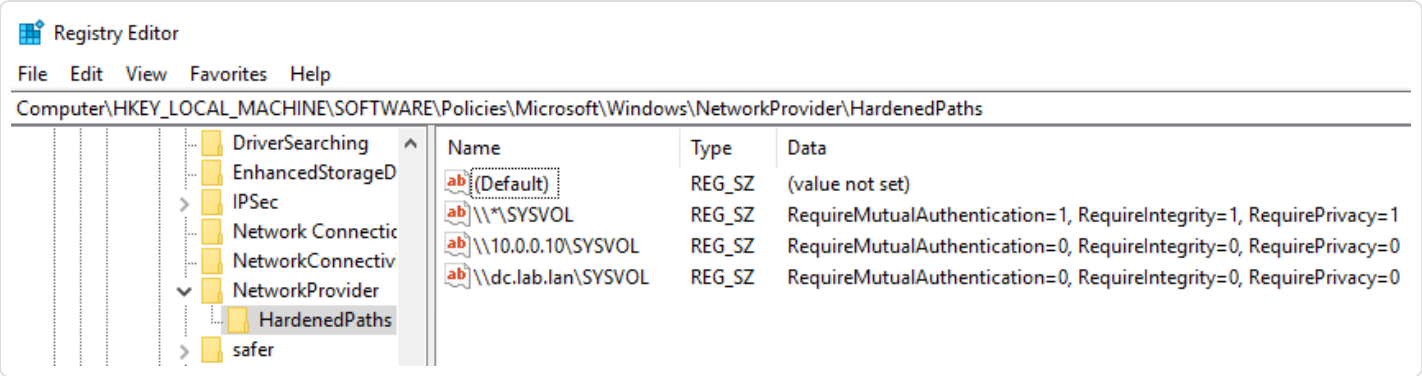
5. **[OK]** をクリックして確認します。

6. この GPO を、Tenable Identity Exposure ディレクトリリスナーまたはリレーマシンを含む組織単位にリンクします。セキュリティグループフィルターの GPO 機能を使用して、この GPO がこのマシンにのみ適用されるようにすることもできます。

特定の UNC パスの例外

前述の手順では、ワイルドカード UNC パス「*\SYSVOL」を使用して SYSVOL 堅牢化を無効にします。特定の IP アドレスまたは FQDN に対してのみ無効にすることもできます。つまり、「*\SYSVOL」に対して UNC の強化されたパス設定を有効な状態 (値「1」) に保ったまま、Tenable Identity Exposure で設定されているドメインコントローラーの IP アドレスまたは FQDN ごとに対応する例外を作成することができます。

次の画像は、「`10.0.0.10`」および「`dc.lab.lan`」(Tenable Identity Exposure で設定されているドメインコントローラー) を除くすべてのサーバー (「*」) に対して有効にされた SYSVOL 堅牢化の例を示しています。



これらの追加設定は、上述したように、レジストリを使うか GPO 方式を使用して追加できます。

注意: Tenable Identity Exposure で設定されている正確な値を指定する必要があります (たとえば、Tenable Identity Exposure 設定が FQDN を使用している場合、IP アドレスは指定できません)。また、Tenable Identity Exposure ドメイン管理ページで IP アドレスや FQDN を変更するたびに、これらのキーを忘れずに更新してください。

SYSVOL 堅牢化を無効にした場合のリスク

SYSVOL 堅牢化はセキュリティ機能であり、無効にすると重大な懸念が生じる可能性があります。

- ドメインに参加していないマシン - SYSVOL 堅牢化を無効にしてもリスクはありません。これらのマシンは GPO を適用していないため、SYSVOL 共有から GPO を実行するコンテンツを取得しません。
- Tenable Identity Exposure が推奨しないドメイン参加マシン (ディレクトリリスナーまたはリレーマシン) – 攻撃者がディレクトリリスナーまたはリレーマシンとドメインコントローラーとの間の「中間者」になるという状態が発生する潜在的なリスクがある場合、SYSVOL 堅牢化を無効にするのは安全ではありません。この場合、Tenable Identity Exposure は代わりに Kerberos 認証に切り替えることを推奨しています。

この非アクティブ化の範囲は、ディレクトリリスナーまたはリレーマシンにのみであり、その他のドメインコンピューターは対象になりません。また、ドメインコントローラーは決して対象になりません。