第 10 章 : Microsoft Intune による更新プログラムと Endpoint Protection の管理

演習 : Microsoft Intune による更新プログラムと Endpoint Protection の管理

練習 1 : Intune での更新プログラムの構成

▶ 作業 1 : 製品および更新プログラムの分類を構成する

1. LON-CL1 に切り替え、Internet Explorer を開きます。
2. http://manage.microsoft.com を参照します。
3. Intune 管理コンソールにアクセスするための資格情報を入力します。
4. Intune 管理コンソールで、[管理者] をクリックします。
5. 管理ウィンドウで、[更新プログラム] をクリックします。
6. [製品カテゴリ] で、[すべてのカテゴリ] チェック ボックスをオフにします。
7. [製品カテゴリ] で、次を選択します。
   - Office 2013
   - Windows 10
   - Windows 10 LTSB
8. [更新プログラムの分類] で、次のプログラムのみ選択し (他はすべてオフ)、[保存] をクリックします。
   - セキュリティ問題の修正プログラム
   - 重要な更新
   - 定義更新プログラム
9. [更新プログラム] をクリックします。[すべての更新プログラム] で、選択した分類が表示されていることを確認します。
10. [すべての更新プログラム] をクリックします。
11. [フィルター] ドロップダウン リストで、[承認待ちの新しい更新プログラム] を選択します。[必要] カラムに、各更新プログラムを必要とするコンピューターの数が表示されていることを確認します。更新プログラムが表示されるまで、時間がかかる場合があります。承認待ちの更新プログラムが少なくとも 1 つある必要があります。

注 : 更新プログラムを承認する前に、クライアント コンピューターの更新プログラム ポリシー設定を構成します。

▶ 作業 2 : 更新ポリシー設定を構成する

1. Intune 管理コンソールで、[ポリシー] をクリックします。
2. ポリシー ウィンドウで、[構成ポリシー] をクリックします。
3. ポリシー ウィンドウで、[Microsoft Intune エージェントの設定] ポリシーを選択し、[編集] をクリックします。このポリシーは前の演習で作成されました。
4. [ポリシーの編集] ページで、[更新プログラム] タブをクリックします。
5. [更新プログラム] セクションで、次の設定を構成し、[ポリシーの保存] をクリックします。
   - 更新プログラムおよびアプリケーションの自動検出頻度 (時間) : 12 時間
   - Windows を中断しない更新プログラムの即時インストールを許可する : いいえ
   - スケジュールされた更新プログラムおよびアプリケーションのインストールが実行されなかった場合に、Windows の再起動後インストールを再開するまでの待ち時間 (分) : 30
6. [Microsoft Intune エージェントの設定] ポリシーを選択し、[展開の管理] をクリックします。
7. 選択したグループ ウィンドウで [Research Computers] を選択し、[削除] をクリックします。
8. グループの検索ウィンドウで、[すべてのコンピューター] を選択し、[追加]、[OK] の順にクリックします。

▶ 作業 3 : 更新レポートを表示する

1. Intune 管理コンソールで、[更新プログラム] をクリックします。
2. 更新プログラム ウィンドウで、[概要] をクリックします。
3. [レポート] で、[更新レポートの表示] をクリックします。[更新レポート] ノードが選択された状態で、[レポート] が表示されます。
4. [更新レポート] ページで次の値を選択し、[レポートの表示] をクリックします。
   - 更新プログラムの分類の選択 : 重要な更新プログラム
   - 更新状態の選択 : 必要

   [更新レポート] では、クライアント コンピューターに必要な更新プログラムがすべて表示されます。結果が表示されるまで、時間がかかる場合があります。

注 : このレポートは、他のファイル形式で印刷またはエクスポートできることを確認します。

5. [更新レポート] を閉じます。

▶ 作業 4 : 更新プログラムを承認し展開する

1. Intune 管理コンソールで、[更新プログラム] をクリックします。
2. 更新プログラム ウィンドウで、[重要な更新] をクリックします。
3. 更新プログラム リストで、最初にリストされている更新プログラムを選択し、[承認] をクリックします。
4. [グループの選択] ページで、[すべてのコンピューター]、[追加]、[次へ] の順にクリックします。
5. [展開アクション] ページの [承認] で、[必須のインストール] を選択します。
6. 右にスクロールし、[期限] で [1 週間] を選択して、[完了] をクリックします。

▶ 作業 5 : 自動承認規則を構成する

1. Intune 管理コンソールで、[管理者] をクリックします。
2. 管理ウィンドウで、[更新プログラム] をクリックします。
3. サービスの設定 : 更新ウィンドウで、[自動承認規則] まで下にスクロールします。
4. [自動承認規則] で、[新規作成] をクリックします。
5. 自動承認ルールの作成ウィザードで [全般] ページの [名前] ボックスに「Critical Office Updates」と入力し、[次へ] をクリックします。
6. [製品カテゴリ] ページで、[Office 2013] を選択し、[次へ] をクリックします。
7. [更新の分類] ページで、[重要な更新] チェック ボックスをオンにし、[次へ] をクリックします。
8. [展開] ページで、[すべてのコンピューター] を選択し、[追加] をクリックします。
9. [これらの更新プログラムのインストール期限を適用します。] チェック ボックスをオンにします。
10. [インストールの期限] で、[承認後 7 日] を選択し、[次へ]、[完了] の順にクリックします。

結果 : この練習により、Intune 更新プログラムの機能を構成することができました。

練習 2 : Intune での Endpoint Protection の構成

▶ 作業 1 : Endpoint Protection ポリシー設定を構成する

1. Intune 管理コンソールで、[ポリシー] をクリックします。
2. ポリシー ウィンドウで、[構成ポリシー] をクリックします。
3. ポリシー ウィンドウで、[Microsoft Intune エージェントの設定] ポリシーを選択し、[編集] をクリックします。このポリシーは前の演習で作成されました。
4. [ポリシーの編集] ページで、[Endpoint Protection] タブをクリックします。
5. [Endpoint Protection] セクションで、次の設定を構成し、[ポリシーの保存] をクリックします。
   - Endpoint Protection のインストール : はい
   - 詳しい分析が必要な場合にファイル サンプルを自動的に送信する : 送信しない
   - 毎日のクイック スキャンのスケジュール/スケジュールされた時刻 : 午後 12 時
   - フル スキャンのスケジュール : はい

▶ 作業 2 : マルウェアの検出をテストする

1. LON-CL1 で、エクスプローラーを開き、C:¥Files を参照します。
2. [Sample] ファイルを右クリックし、[編集] をクリックします。
3. ファイルから <remove> という 2 つのセクションを (山かっこを含めて) 削除し、保存して、ファイルを閉じます。

注 : Windows Defender は、直ちにマルウェア ファイルのサンプルを検出し、クリーンアップします。

4. エクスプローラーを閉じます。
5. [スタート]、[すべてのアプリ] の順にクリックします。

6. [Windows Intune Center] をクリックします。

注 : このページから Windows Defender を起動できることを確認します。アプリケーションを取得し、それらの更新プログラムを確認することもできます。

7. [更新プログラムの確認] をクリックします。

▶ 作業 3 : Endpoint Protection 管理タスクを実行する

1. Intune 管理コンソールで、[グループ] をクリックします。
2. グループ ウィンドウで、[すべてのコンピューター] をクリックします。
3. すべてのコンピューター ウィンドウで、[デバイス] をクリックします。
4. [LON-CL1.Adatum.com] を右クリックし、[マルウェア定義の更新] を選択して、ダイアログ ボックスで [閉じる] をクリックします。
5. コンソールの右下隅で、[リモート タスク] をクリックします。
6. リモート タスクの状態ウィンドウで、マルウェア定義の更新タスクの状態を確認し、[閉じる] をクリックします。
7. [保護] をクリックします。
8. [概要] ページで、マルウェアの状態と検出数の最も多いマルウェアを確認します。クライアントから情報を表示するためにしばらく時間がかかる場合があります。
9. [すべてのマルウェア] ノードをクリックし、検出されたマルウェアの名前を確認します。
10. 開いているウィンドウをすべて閉じます。

結果 : この練習により、Intune の Endpoint Protection を構成することができました。

▶ 次の章の準備をする

次の章の演習のために、仮想マシンを起動したままにします。