Operační systémy Windows kap. 8

Správa aplikací část 1

Úvod

AppLocker je nástroj ve Windows, který umožňuje administrátorům řídit, které aplikace mohou být spuštěny na počítačích v síti. Pomocí AppLockeru můžete povolit nebo zakázat aplikace na základě různých kritérií, včetně vydavatele (publisher), cesty ke spustitelnému souboru nebo hash souboru. Tento postup vám ukáže, jak vytvořit pravidla AppLocker pro povolení a zakázání aplikace Mozilla Thunderbird na základě jejího vydavatele pomocí grafického uživatelského rozhraní (GUI).

Applocker

Předpoklady

Verze Windows:

- AppLocker je dostupný pouze ve verzích Windows Pro, Enterprise, Education. Ujistěte se, že používáte jednu z těchto verzí na serveru nebo desktopu.

Oprávnění:

- Potřebujete **administrátorská práva** na počítači, kde budete AppLocker konfigurovat.

Digitální Certifikát Vydavatele:

- Aplikace, kterou chcete povolit nebo zakázat, musí být podepsána digitálním certifikátem vydavatele. Mozilla Thunderbird je digitálně podepsána, což umožňuje vytváření pravidel na základě vydavatele.

AppLocker Funkce:

- Ujistěte se, že AppLocker je povolen a správně nakonfigurován ve vaší doméně nebo na místním počítači.

Příklad: kroky k povolení a zakázání aplikace Mozilla Thunderbird pomocí AppLocker GUI

1. Otevření Editoru skupinových politik

- AppLocker je spravován prostřednictvím **Group Policy Management Editor** (GPME) pro síťové doménové prostředí Windows nebo pomocí **Local Security Policy** (secpol.msc) pro lokální počítače.
- **Pro doménové prostředí:**
  - Otevřete Group Policy Management Console (GPMC):

    Stiskněte `Win + R`, napište `gpmc.msc` a stiskněte **Enter**.

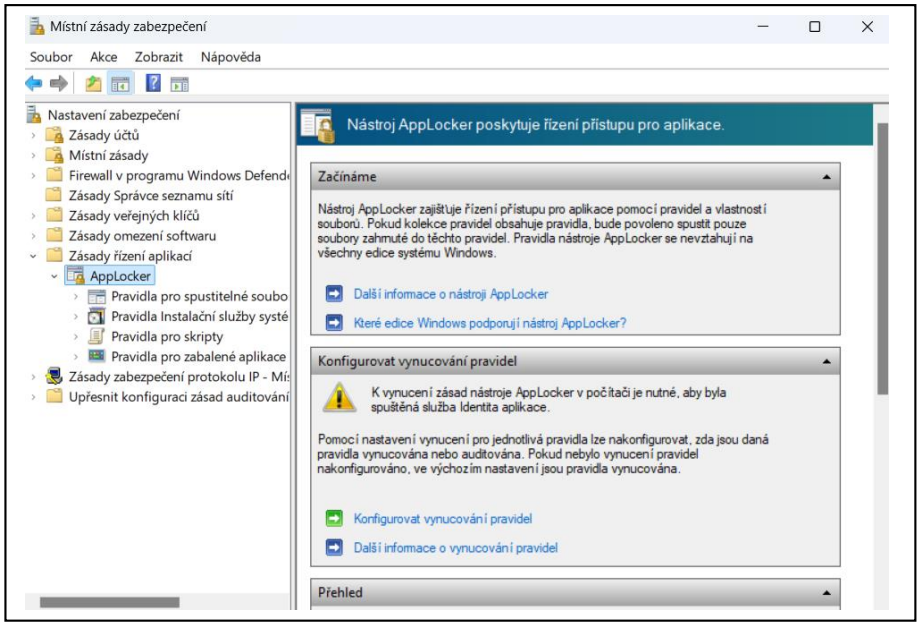
  - Vytvořte nebo upravte GPO:

Pravým tlačítkem klikněte na příslušnou organizační jednotku (OU) nebo doménu, vyberte **Create a GPO in this domain, and Link it here...**, pojmenujte nové GPO (např. `AppLocker Policies`).

Pravým tlačítkem klikněte na nové GPO a vyberte **Edit**.

- Pro lokální počítač:
  - Otevřete Local Security Policy:

    Stiskněte Win + R, napište `secpol.msc` a stiskněte Enter.



2. Navigace k Nastavení AppLockeru

- V Group Policy Management Editoru nebo Local Security Policy:

  Navigujte do:

  `Computer Configuration > Windows Settings > Security Settings > Application Control Policies > AppLocker`

- Inicializace AppLockeru (pokud ještě není inicializován):
  - Klikněte pravým tlačítkem na **AppLocker** a vyberte **Configure rule enforcement**.
  - Ujistěte se, že jsou zaškrtnuté pravidla pro **Executable Rules**, **Windows Installer Rules**, **Script Rules**, a **Packaged App Rules**, pokud jsou potřeba.
  - Klikněte na **OK**.

3. Vytvoření Publisher Rule pro **povolování** Mozilla Thunderbird

- Navigace do Executable Rules:

  Klikněte pravým tlačítkem na **Executable Rules** a vyberte **Create New Rule...**.

- Průvodce Vytvářením pravidla:
  - První krok – Úroveň pravidla:
    - **Action:** Vyberte **Allow** (povolit).
    - Klikněte na **Next**.

- Druhý krok – Uživatelé nebo Skupiny:
  - Vyberte uživatele nebo skupinu, kterým chcete pravidlo aplikovat (např. **Everyone**, nebo specifické skupiny jako **IT Administrators**).
  - Klikněte na **Next**.
- Třetí krok – Podmínky pravidla:
  - Vyberte **Publisher** a klikněte na **Next**.
- Čtvrtý krok – Vybrání Aplikace:
  - Klikněte na **Browse...**.
  - Najděte spustitelný soubor **Mozilla Thunderbird** (`thunderbird.exe`). Obvykle se nachází v:

    ```
    C:\Program Files\Mozilla Thunderbird\thunderbird.exe
    ```

  - Vyberte `thunderbird.exe` a klikněte na **Open**.
- Pátý krok – výběr Publisheru:
  - Po výběru aplikace bude vyplněna informace o vydavateli. Zkontrolujte, zda jsou údaje správné (např. název vydavatele, verze atd.).
  - Můžete specifikovat další parametry, jako je **Product name** a **File name**, pokud je to potřeba.
  - Klikněte na **Next**.
- Šestý krok – Výjimky pravidla (volitelné):
  - Pokud chcete vytvořit výjimky pro specifické soubory nebo cesty, můžete je přidat zde. Pro tento příklad není potřeba.
  - Klikněte na **Next**.
- Sedmý krok – Název a Popis pravidla:
  - **Name:** Zadejte název pravidla, např. `Allow Mozilla Thunderbird`.
  - **Description:** (Volitelné) Přidejte popis, např. `Povoluje spuštění Mozilla Thunderbird na základě vydavatele.`
  - Klikněte na **Create**.

Dokončení:

Pravidlo bude nyní zobrazeno v seznamu **Executable Rules** a bude aplikováno na vybrané uživatele nebo skupiny.

4. Vytvoření Publisher Rule pro **zakázání** aplikace na základě vydavatele

Pro tento příklad budeme předpokládat, že chcete **zakázat** všechny aplikace vydavatele, který není **Mozilla Foundation**.

- Navigace do Executable Rules:

  Klikněte pravým tlačítkem na **Executable Rules** a vyberte **Create New Rule...**.

- Průvodce Vytvářením pravidla:
  - První krok – Úroveň pravidla:
    - **Action:** Vyberte **Deny** (zakázat).
    - Klikněte na **Next**.
  - Druhý krok – Uživatelé nebo Skupiny:
    - Vyberte uživatele nebo skupinu, kterým chcete pravidlo aplikovat (např. Everyone).
    - Klikněte na Next.
  - Třetí krok – Podmínky pravidla:

Vyberte **Publisher** a klikněte na **Next**.

- Čtvrtý krok – Vybrání Aplikace:
  - Klikněte na **Browse...**.
  - Najděte a vyberte libovolný soubor, který je podepsán vydavatelem, kterého chcete zakázat. Pro jednoduchost můžete použít obecnou cestu nebo existující aplikaci.
  - Vyberte soubor a klikněte na **Open**.
- Pátý krok – výběr Publisheru:
  - Zadejte parametry pro zakázání. V tomto případě budete zakazovat aplikace od všech vydavatelů kromě **Mozilla Foundation**.
  - Bohužel, AppLocker neumožňuje přímo negovat pravidla na základě vydavatele. Místo toho můžete vytvořit pravidla, která explicitně povolují aplikace od **Mozilla Foundation** a zakazují vše ostatní.
- Šestý krok – Výjimky pravidla (Volitelné):
  - Pokud chcete vytvořit výjimky, můžete je přidat zde. Pro tento příklad není potřeba.
  - Klikněte na **Next**.
- Sedmý krok – Název a Popis pravidla:
  - **Name:** Zadejte název pravidla, např. `Deny All Other Publishers`.
  - **Description:** (Volitelné) Přidejte popis, např. `Zakazuje spuštění aplikací od všech vydavatelů kromě Mozilla Foundation.`
  - Klikněte na **Create**.
- Uspořádání Pravidel:

  Ujistěte se, že pravidlo **Allow Mozilla Thunderbird** je na vyšší úrovni než pravidlo **Deny All Other Publishers**. AppLocker zpracovává pravidla v pořadí, ve kterém jsou definována, a první pravidlo, které odpovídá aplikaci, bude použito.

  Pokud je potřeba, můžete pravidla přetáhnout, aby byla v požadovaném pořadí.

- Dokončení:

  Pravidlo bude nyní zobrazeno v seznamu **Executable Rules** a bude aplikováno na vybrané uživatele nebo skupiny.

5. Aplikace a testování pravidel

- **Aktualizace Group Policy:**
  - Pro doménové prostředí:
    - na klientském počítači spusťte příkaz:
      `gpupdate /force`
    - toto zajistí, že se nové pravidla AppLockeru aplikují okamžitě.
  - Pro lokální počítač:
    - pravidla by se měla aplikovat automaticky, ale můžete restartovat počítač nebo znovu načíst Group Policy pomocí příkazu:
      `gpupdate /force`
- **Testování Pravidel:**
  - Povolení aplikace:

    Na klientském počítači se pokuste spustit **Mozilla Thunderbird**. Aplikace by se měla úspěšně spustit.

  - Zakázání aplikace:

Pokuste se spustit aplikaci od jiného vydavatele (např. nějakou jinou aplikaci), kterou jste nezahrnuli do povolených pravidel. Aplikace by měla být zablokována s chybovou zprávou, že její spuštění bylo zablokováno politikou.

6. Řešení Potenciálních Problémů

- **pravidla nefungují:**
  - **Kontrola Služeb:**
    - Ujistěte se, že služby **AppIDSvc** a **Application Identity** běží. Tyto služby jsou nezbytné pro fungování AppLockeru.
    - Otevřete **Services.msc**, najděte **Application Identity**, a ujistěte se, že je nastaveno na **Automatic** a spuštěno.
- **AppLocker výjimky:**

  Pokud potřebujete umožnit určité aplikace mimo hlavní pravidla, můžete vytvořit specifická povolení nebo zakázání pravidla s vyšší prioritou.

- **Logování a Auditing:**

  Pro sledování a diagnostiku pravidel AppLockeru můžete povolit **auditování**:

  - Navigujte do:

  ```
  Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Object Access > Audit Application Control
  ```

  - Aktivujte **Success** a **Failure** pro **Audit Application Control**.

    V **Event Viewer** pod **Windows Logs > Security** budete moci vidět události související se spouštěním aplikací a aplikací pravidel AppLockeru.

Tipy:

Zálohujte pravidla: Před provedením změn si zazálohujte stávající pravidla AppLockeru.

Testujte pravidla v Audit Mode: Než začnete pravidla vynucovat, spusťte je v režimu auditování, abyste zjistili, jaká aplikace budou ovlivněny, aniž byste je zablokovali.

Udržujte pravidla aktuální: Pravidelně revidujte a aktualizujte pravidla AppLockeru podle změn ve vaší síti a aplikacích.

Řešené otevřené otázky k tématu

Otázka 1:

Popište krok za krokem, jak pomocí AppLocker GUI (nebo ekvivalentně pomocí Group Policy Management Editoru) vytvořit pravidlo, které povolí spouštění aplikace na základě jejího digitálního podpisu (vydavatele). Uveďte příklad pro aplikaci Mozilla Thunderbird, a vysvětlete, jak administrátor ověřuje informace o vydavateli.

Odpověď:
Administrátor otevře Group Policy Management Console (`gpedit.msc`) a přejde do cesty:

`Computer Configuration > Windows Settings > Security Settings > Application Control Policies > AppLocker`

Poté klikne pravým tlačítkem na **Executable Rules** a vybere **Create New Rule...**. V průvodci pravidly zvolí akci **Allow** a dále vybere podmínku **Publisher**. Následně administrátor klikne na možnost **Browse Files...** a vyhledá soubor `thunderbird.exe` (např. v `C:\Program Files\Mozilla Thunderbird\thunderbird.exe`). Po výběru se automaticky načtou informace o digitálním podpisu, jako je název vydavatele, produkt, verze a datum vydání. Administrátor ověří tyto detaily (například zkontroluje, že vydavatel odpovídá "Mozilla Corporation" nebo jinému očekávanému názvu) a pokračuje dál, kde přiřadí pravidlo vybrané skupině uživatelů (např. `Group_A`), pojmenuje pravidlo a uloží ho. Tímto pravidlem se pak povolí spuštění aplikace Mozilla Thunderbird pro uživatele patřící do dané skupiny.

Otázka 2:

Jakým způsobem administrátor odděluje pravidla pro dvě různé skupiny uživatelů (například Group_A a Group_B) pomocí AppLockeru založeného na digitálním podpisu aplikací? Uveďte příklad, kdy Group_A má povoleno spouštění obou aplikací (Mozilla Thunderbird a Total Commander) a Group_B pouze Mozilla Thunderbird.

Odpověď:
Administrátor vytvoří dvě sady pravidel v AppLockeru, které se liší podmínkou pro přiřazení ke skupinám:

Pro **Group_A** vytvoří dvě pravidla: jedno s akcí **Allow** pro Mozilla Thunderbird a druhé s akcí **Allow** pro Total Commander.

Pro **Group_B** vytvoří pravidlo **Allow** pro Mozilla Thunderbird a zároveň pravidlo **Deny** pro Total Commander.
Klíčovým krokem je při vytváření každého pravidla v části **Select User, Computer, Service Account, or Group** správně zadat název skupiny (`Group_A` nebo `Group_B`). Aby se zabránilo konfliktům, pravidla s akcí Allow by měla být umístěna výše (má vyšší prioritu) než pravidlo Deny. Takto administrátor zajistí, že Group_B může spustit Thunderbird (protože má explicitně povolené pravidlo) a zároveň nemůže spouštět Total Commander (protože existuje explicitní Deny pravidlo na Total Commander pro Group_B).

Otázka 3:

Jaké informace o vydavateli se zobrazují při vytváření pravidla na základě Publisher podmínky v AppLockeru a proč je tato informace důležitá?

Odpověď:
Při výběru podmínky **Publisher** v AppLockeru se zobrazují informace, které jsou získány z digitálního podpisu souboru. Mezi tyto informace typicky patří:

- **Název vydavatele** (Publisher)
- **Produkt** (Product Name)
- **Verze souboru** (File Version)
- **Datum vydání** (Date)

Tyto informace jsou důležité, protože pomáhají administrátorovi přesně identifikovat, od kterého vydavatele aplikace skutečně pochází. Na základě toho lze vytvořit pravidla, která povolí pouze důvěryhodné aplikace od specifických vydavatelů a zamezit spuštění aplikací z neznámých nebo nedůvěryhodných zdrojů. Správné nastavení tohoto parametru zvyšuje bezpečnost a snižuje riziko spuštění malwaru.

Otázka 4:

Jaké kroky je třeba podniknout pro aktualizaci a aplikaci nově vytvořených pravidel AppLockeru pomocí GUI a jak ověřit, že pravidla fungují dle očekávání?

Odpověď:
Po vytvoření a konfiguraci pravidel AppLockeru pomocí GUI administrátor provede následující kroky:

Aktualizace Group Policy**:**
Spustí příkaz `gpupdate /force` na klientských strojích, aby se nová pravidla okamžitě aplikovala.

Testování pravidel:
Přihlásí se jako uživatel, který je členem dané skupiny, a otestuje spuštění aplikací. Pro Group_A by Mozilla Thunderbird a Total Commander měly fungovat, zatímco pro Group_B by měl fungovat pouze Mozilla Thunderbird a Total Commander by měl být zablokován.

Záznamy v Event Vieweru:
Otevře Event Viewer (`eventvwr.msc`) a podívá se do logů v `Applications and Services Logs > Microsoft > Windows > AppLocker > EXE and DLL` pro záznamy o tom, které aplikace byly povoleny či zamítnuty. Tyto kroky potvrzují, že pravidla jsou správně nakonfigurována a aplikována podle očekávání.

Otázka 5:

Proč je důležité správně řadit (prioritizovat) pravidla v AppLockeru při použití více pravidel pro stejný objekt (například v případě skupiny Group_B, kde je povoleno Thunderbird a zakázán Total Commander)? Jaký princip se zde uplatňuje?

Odpověď:
AppLocker zpracovává pravidla v pořadí, v jakém jsou aplikována, a první pravidlo, které odpovídá danému spouštění aplikace, určuje, zda je aplikace povolena nebo zakázána. Pokud pro jednu skupinu existují dvě pravidla (Allow pro Thunderbird a Deny pro Total Commander), je nezbytné, aby pravidla umožňující (Allow) měly vyšší prioritu nebo byly aplikována dříve, než pravidla, která zakazují (Deny). Tento princip se nazývá **princip nejmenšího oprávnění** a **pravidla zpracovávaná v pořadí**, kde konkrétní pravidla, které povolují důvěryhodné aplikace, musí být upřednostněna před globálním pravidlem, které by mohlo zakázat všechny ostatní aplikace. Správné řazení pravidel zabraňuje nechtěnému blokování aplikací, jež mají být povoleny, a zajišťuje, že pouze ty aplikace, které explicitně nemají povoleno spuštění, jsou zablokovány.

Odkazy:

Microsoft.com

Chatgpt