

Intune

Die große Umstellung von OnPrem Umgebungen ist kein technisches Problem, es ist ein konzeptuelles Problem:

OnPrem Umgebungen sind überwiegend Gerätefokussiert, während Intune kaum bis gar nicht Gerätefokussiert sein kann.

Es ist also nicht möglich Richtlinien 1 zu 1 in Intune abzubilden ohne diese von Grund auf neu zu konzipieren.

Ich rede hier fast ausschließlich von Hybridumgebungen.

- Alles was nicht App-Installation ist (weil App-Installationen One-Time sind), ist User-Gebunden
- Auch die auf Computer gebundenen Richtlinien sind von Usern abhängig.
Maschinengebunden bedeutet, dass Intune bei jeder Useranmeldung prüft ob für das Gerät, an dem sich gerade angemeldet wird eine zugewiesene Policy hat und wendet diese bei jeder User-Anmeldung an.
- Der Zustand des angemeldeten Users wird abseits der Useranmeldung laut meines Wissens alle vier Stunden überprüft. (PRT-Token)
- Ist beim regelmäßigen Check kein User angemeldet (auch im gesperrten Zustand) kann der Lizenzcheck nicht vollzogen werden und die Intune Richtlinien werden entfernt.
- Nicht lizenzierte User und lokale User haben keine Intune-Lizenz die bei der Anmeldung geprüft werden könnte, also können für diese auch keine Policies appliziert werden. Auch können lokale User nicht nachvollziehen ob auf dem Gerät Policies aktiv sind, weil auch deren Grundlagen (z.B. Registry-Keys) entfernt werden.
Dies trifft auch alle Richtlinien, die in Ihrer OnPrem-Variante komplett Maschinengebunden waren.

Intune zeigt Policies an, die auf den SYSTEM-User appliziert worden sind. Das Vehikel dafür ist aber weiterhin der lizenzierte Intune-User.

- Da der Zustand ohne angemeldeten User im SYSTEM User-Kontext läuft - welcher nicht intune-lizenziert werden kann - wirken die konfigurierten Intune-Policies nicht im Zustand ohne jegliche User-Anmeldungen.

Die Lösung für das Dilemma ist leider eine Doppelkonfiguration OnPrem GPO und Intune, hier allerdings OnPrem GPOs nur noch dafür genutzt lokale User des Computers zu steuern. Dies bringt uns leider wieder in Richtung Konfliktregulierungen zwischen OnPrem und Intune.