Credentials Protection

Protected Users Group

Was ist die Protected Users Group?
Die Protected-Users-Group ist eine globale Sicherheistruppe für das AD, um sich vor Credential-Diebstahl schützen zu können. Die Gruppe triggered Schutzmaßnahmen welche nicht explizit konfiguriert wurden, damit Credential Caching verhindert werden kann.

Vorraussetzungen
- Windows Client läuft auf Windows 8.1 oder später
- Windows Server 2012 R2 oder später
- Domain Functional Level muss Windows Server 2012 R2 oder später sein
- Protected Global Security Group Memberships bregenzen Admins nur AES für Kerberos zu verwenden. Demnach müssen Mitglieder in der Lage sein, sich mit AES authentifizieren zu können.

User kann man entweder mittels UI-Tools wie dem Admin-Center, Active Directory Users und Computers oder durch Powershell-Commandos hinzufügen.

Enterprise-Admins und Domain-Admins sollten nicht zur Protected-Users-Group gehören. Service- und Computer-Accounts ebenfalls nicht in die Protected-Users-Group hinzufügen. Es würde sich nicht auszahlen, da Passwörter am lokalen Host immer verfügbar sind.

Checkliste Protected Users Group

- [ ] Vorraussetzungen wie oben beschrieben erfüllt.
- [ ] Powershell öffnen

Folgenden Command ausführen:

```
Get-ADGroup -Identity "Protected Users" | Add-ADGroupMember –Members
"CN=Adam,CN=Users,DC=corp,DC=example,DC=com"
```

Credetial Guard

Was ist der Credential Guard?
Der Credential Guard ist eine Sicherheitsfunktion in Windows 10 und Windows Server 2016, die dazu dient, Anmeldeinformationen zu schützen. Der Credential Guard verwendet virtualisierungsbasierte Sicherheit, um Anmeldeinformationen zu schützen, indem sie in einem geschützten Bereich des Systems gespeichert werden.

Vorraussetzungen für Win 11, 22H2 oder später
- [ ] Lizenzanforderungen wurden erfüllt
- [ ] Hard- und Softwareanforderungen wurden erfüllt
- [ ] Credential Guard wurde nicht explizit deaktiviert

Vorraussetzungen für Windows Server
- [ ] Die Lizensierunganforderungen wurden erfüllt
- [ ] Die Hard- und Software Anforderungen wurden erfüllt
- [ ] Credential Guard wurde explizit nicht deaktiviert
- [ ] Teil einer Domäne
- [ ] Kein Domain Controller

Featureanforderungen damit der Credential Guard funktioniert:

- [ ] Virtualized-based Security (VBS)
- [ ] Secure Boot

Optionale features wären:
- [ ] Trusted Platform Module (TPM)
- [ ] UEFI lock

Checkliste Credential Guard
- [ ] Vorraussetzungen wie oben beschrieben erfüllt
- [ ] Secure Boot aktiviert
- [ ] Group Policy Management öffnen
- [ ] Neue Gruppenrichtlinie erstellen
- [ ] Zu folgendem Pfad navigieren: Computer Configuration -> Administrative Templates -> System -> Device Guard -> Turn on Virtualization Based Security
- [ ] Gruppenrichtlinie aktivieren
- [ ] gpupdate /force in der Powershell ausführen
- [ ] Überprüfung durch Systeminformationen