Richtlinien für lokale Konten in Umbrella Active Directory anwenden

Inhalt

Einleitung

In diesem Dokument wird das erwartete Richtlinienverhalten bei der Synchronisierung von Umbrella-Produkten vor Ort mit Active Directory und lokalen Benutzerkonten beschrieben.

Umbrella Virtual Appliance und lokale Kontoerkennung

Die Umbrella Virtual Appliance empfängt Active Directory-Anmeldeinformationen von den Windows-Domänencontrollern. Er speichert Active Directory-Benutzer anhand ihrer Quell-IP-Adresse und identifiziert sie.

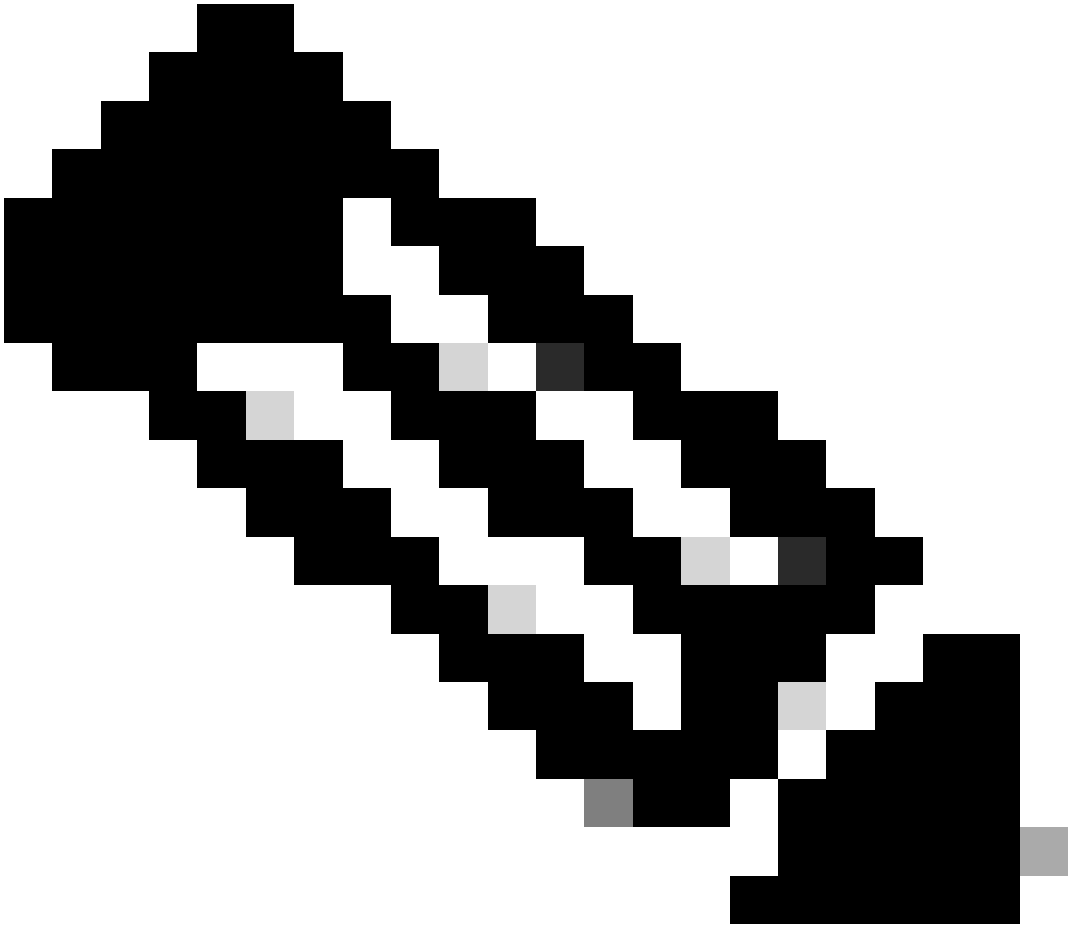
- Der Domänencontroller verfolgt lokale Benutzeranmeldungen nicht, sodass diese Benutzer nicht direkt von der virtuellen Appliance identifiziert werden können.
- Wenn sich ein Active Directory-Benutzer kürzlich von einer IP-Adresse angemeldet hat, kann die zwischengespeicherte Identität weiterhin auf der Grundlage unseres Caches verwendet werden. Die virtuelle Appliance kann nicht wissen, dass der AD-Benutzer durch ein lokales Konto ersetzt wurde.
- Wenn kein zwischengespeicherter Benutzer vorhanden ist, verwendet die virtuelle Appliance eine Standard-Identität (keine AD-Identität). Die Identität kann wie folgt ausgelöst werden:
  - Umbrella-Standortname (z. B. Standardstandort)
  - Internes Netzwerk (interne IP-Adresse)
  - Netzwerk (externe IP-Adresse)

Empfehlungen für Umbrella Virtual Appliance

- Beschränken Sie den Zugriff auf lokale Konten und Kennwörter.
- Erstellen Sie eine separate Richtlinie für den Umbrella-Standortnamen (z. B. Standardstandort). Weisen Sie dieser Richtlinie eine niedrigere Priorität zu als Ihrer Active Directory-Standardbenutzerrichtlinie. Diese restriktivere Richtlinie gilt, wenn kein AD-Benutzer erkannt wird.

- Wenn Sie unterschiedliche Richtlinien für lokale Benutzerkonten benötigen, sollten Sie den Umbrella Roaming Client bereitstellen.

Umbrella-Roaming-Client und lokale Kontorichtlinie



> Anmerkung: Um die Active Directory-Integration mit dem Roaming-Client zu verwenden, navigieren Sie zu Identitäten > Roaming-Computer, und aktivieren Sie die Einstellung Active Directory-Benutzer- und Gruppenrichtliniendurchsetzung aktivieren.

Der Roaming-Client erkennt angemeldete Benutzer aus der Windows-Registrierung und ermöglicht so die Identifizierung von Active Directory-Benutzern anhand ihrer eindeutigen AD-GUID.

- Der Roaming-Client kann lokale Benutzernamen nicht zu Richtlinienzwecken identifizieren.
- Wenn ein AD-Benutzer erkannt wird, gilt die AD-Benutzeridentität für die

Richtliniendurchsetzung, einschließlich der AD-Benutzer, die sich außerhalb des Netzwerks mit zwischengespeicherten Anmeldeinformationen anmelden.
- Wenn kein AD-Benutzer erkannt wird (z. B. wenn ein lokaler Benutzer angemeldet ist), wird die Identität des Roaming-Computers für die Richtliniendurchsetzung verwendet.

Empfehlungen für Umbrella Roaming Client

- Beschränken Sie den Zugriff auf lokale Konten und Kennwörter.
- Erstellen Sie eine separate Richtlinie für Roaming-Computer mit einer niedrigeren Priorität als die AD-Standardbenutzerrichtlinie. Diese Richtlinie gilt für Roaming-Computer, die nicht der Domäne angehören oder von lokalen Benutzern verwendet werden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.