



## 1. Voraussetzungen

Um die automatische Kennwortänderung für Servicekonten nutzen zu können, benötigen Sie den Operations Manager ab der Version OMV2.7R038B1071 und den Application Container [Unicat.StandardAppCont.ServiceAccount.PWDReset](#). Nachdem der Application Container eingespielt wurde, stehen Ihnen, neben einer neuen Klasse und einigen zusätzlichen Klassenerweiterungen, im Scope ‚Unicat.Setup‘ die beiden neuen Anträge ‚Unicat.ServiceAccounts.ChangePassword‘ und ‚Unicat.ServiceAccounts.ShowPassword‘ zur Verfügung.

## 2. Ablauf

Um die Sicherheit der Passwörter für Dienstkonten zu erhöhen, wurde der neue Antrag ‚Unicat.ServiceAccounts.ChangePassword‘ entwickelt, der in einem regelmäßigen Intervall die Passwörter der Dienstkonten ändert, deren letzte Passwortänderung am längsten zurückliegt.

An der Klasse ‚OMConfiguration‘ befinden sich die neuen Attribute ‚SAC\_Interval‘, ‚SAC\_Time‘, ‚SAC\_UserCount‘ und ‚SAC\_Waittime‘, in denen definiert werden muss, in welchem Intervall die Passwortänderung vorgenommen werden soll, um wieviel Uhr der Antrag ausgeführt werden soll, für wieviele Benutzer das Passwort geändert wird und wie lange der Antrag auf die Beendigung der OMExecutes warten soll, bis er die Dispatcherdienste wieder startet. Solange diese Attribute nicht gepflegt sind, kann der Antrag zur automatischen Kennwortänderung nicht initiiert werden.

An der Klasse Host wurde das Attribut ‚Dispatcherstatus‘ hinzugefügt, in das der Antrag den Status des Dispatcherdienstes einträgt, bevor er diesen stoppt. Auf diese Weise ist sichergestellt, dass der Dispatcherdienst auch nur auf den Servern wieder gestartet wird, auf denen er vor der Antragsausführung lief.

In der neuen Klasse ‚OMServiceAccount‘ wird zu Beginn jeder Antragsausführung für jedes Dienstkonto, das in der tblCredentials gefunden wird, ein neues Objekt angelegt - sofern es noch nicht existiert - und das Datum der letzten Kennworrücksetzung im Attribut ‚pwdLastSet‘ eingetragen.

Anschließend stoppt der Antrag sämtliche Dispatcherservices und wartet, bis die letzte OMEecute beendet ist, bevor er beginnt, die Kennwörter der Dienstkonten im Active Directory zu ändern und in der tblCredentials entsprechend zu korrigieren. Das neue Kennwort des Dienstkontos wird im OMServiceAccount-Attribut ‚pwdEncrypted‘ verschlüsselt hinterlegt.

Bitte beachten sie, dass sich der Antrag während der Ausführung selbständig wieder in die Warteschlange einstellt. D.h. nach dem erstmaligen manuellen Start des Antrags, läuft der Antrag automatisch in dem im Attribut ‚SAC\_Interval‘ eingetragenen Intervall.

Sollte es notwendig sein, das neue Passwort eines Dienstkontos in Erfahrung zu bringen, kann der Antrag ‚Unicat.ServiceAccounts.ShowPassword‘ gestartet werden. Dieser bietet eine Auswahl aller Dienstkonten und zeigt auf der rechten Seite das Passwort des ausgewählten Dienstkontos im Klartext an. Sobald ein Dienstkonto in diesem Antrag ausgewählt wurde, wird das Attribut ‚pwdLastSet‘ auf den 01.01.1900 zurückgesetzt. Damit ist sichergestellt, dass das Kennwort dieses Dienstkontos bei der nächsten Antragsausführung in jedem Fall geändert wird.