Datasheet

Management of password of local Administrator account

Prepared by

Jiri Formacek

Local Administrator Password Management Datasheet

Published: June 2015

Last Updated: June 2018

Author:

Jiri Formacek, Microsoft

Abstract: This document gives a brief overview of Local Administrator Password Solution (LAPS)

1 Overview

Solution automatically manages local administrator password on domain joined computers, so as the password is:

- Unique on each managed computer
- Randomly generated
- Securely stored in AD infrastructure

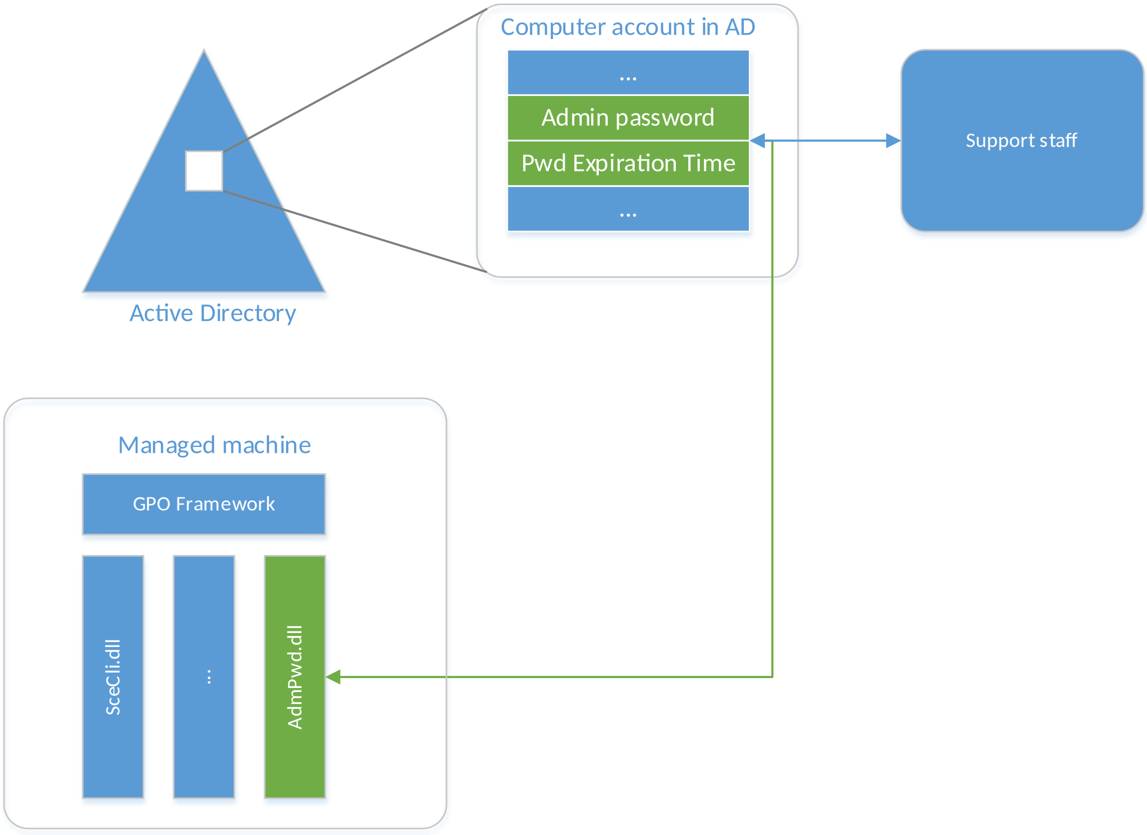
Solution is built upon just AD infrastructure, so there is no need to install and support other technologies.

Solution itself is a Group Policy Client Side Extension that is installed on managed machines and performs all management tasks

Management tools delivered with the solution allow for easy configuration and administration.

2 Architecture

Architecture of the solution is shown below:



Core of the solution is GPO Client side Extension (CSE) that performs the following tasks during GPO update:

- Checks whether the password of local Administrator account has expired or not
- Generates the new password when old password expired or is required to be changed prior to expiration
- Changes the password of Administrator account

- Reports the password to password Active Directory, storing it in confidential attribute with computer account in AD
- Reports the next expiration time to Active Directory, storing it in confidential attribute with computer account in AD
- Password then can be read from AD by users who are allowed to do so
- Password can be forced to be changed by eligible users

3 Features

Solution features include:

- Security:
    - Random password that automatically regularly changes on managed machines
    - Effective mitigation of Pass-the-hash attack
    - Password is protected during the transport via Kerberos encryption
    - Password is protected in AD by AD ACL, so granular security model can be easily implemented
- Manageability
    - Configurable password parameters: age, complexity and length
    - Ability to force password reset on per-machine basis
    - Security model integrated with AD ACLs
    - End use UI can be any AD management tools of choice, plus custom tools (PowerShell and Fat client) are provided
    - Protection against computer account deletion
    - Easy implementation and minimal footprint

4 Requirements

Solution has the following requirements:

- Active Directory:
    - Windows 2003 SP1 and above
- Managed machines:
    - Windows Vista with current SP or above; x86 or x64
    - Windows 2003 with current SP and above; x86 or x64 (Itanium not supported)
- Management tools:
    - .NET Framework 4.0
    - PowerShell 2.0 or above