Usage scenario - Azure Active Directory

Last Modified on 05/01/2022 3:49 pm EET

Background

Customer has Azure Active Directory tenant and all workstations are Azure AD joined Windows 10 (or later) devices. Customer does not have any Windows servers.

Target

Customer has specified following targets that need to be met:

1. End users should not have any permanent admin privileges
    1. Existing permanent admin privileges must be removed
    2. Exceptions can be made (when absolutelly needed for performing work tasks) for single workstations by requesting permanent admin privileges from IT support
2. All end users should have possibility to get temporary admin privileges when granted by IT support
3. End users that currently have permanent admin privileges should have possibility to get temporary local admin privileges as self-service (IT support grant not needed)
4. Default permanent admin privileges for Global Admins and Device Administrator Azure AD roles must be removed
    1. Permanent admin privileges must be allowed for specifed Azure AD group to every workstation
5. Default local build-in Administrator account on every workstation must have device specific random password with minimum of 12 characters and include special characters also
6. Utilize cloud based resources as much as possible for the platform. When possible use PaaS resources.
7. Get automatic updates to the platform

Platform

Carillon environment can be deployed to Microsoft Azure PaaS platform. As Customer only has devices connected to Azure AD there is no need to communicate from PaaS platform to Customer on-prem environment. So in this scenario Microsoft Azure PaaS platform can be utilized.

Actions for platform:

1. If needed create new Azure AD group for end users that currently has permanent admin privileges
2. If needed create new dynamic Azure AD group for devices that automatically collects all Windows workstations as group members
3. If needed create new Azure AD group for users that need to have permanent admin privileges to all workstations
4. Deploy two Azure App Service resources (instructions) - **Fulfill target 6**
5. Automate platform deployment (instructions) - **Fulfill target 7**
    - Following the instruction send information that Azure AD group from step 1. needs to have

permissions to use self service with local user account - **Fulfill target 3**

Carillon configuration

Carillon configuration is based on managed rules created at Carillon Portal. Managed group rules are used to control local group memberships and managed user rules are used to control local user accounts. Local users can be defined to Carillon to support randomized passwords or temporary admin elevation using local user account.

Local users

1. Create following local user accounts (instructions)
    1. Temporary Administrator (login name TempAdmin)

> **Tip!**
>
> You can use different name and/or login name for the local account! Temporary Administrator / TempAdmin ar just used as example names.

Managed group rules

Create following managed group rules (instructions) for the Azure AD group from **Platform chapter step 2** (Azure AD group that has all Windows workstations as members) and use group **Administrators** for all rules - **Fulfill target 1.1 and 4**

1. Built-in Administrator
2. Temporary Administrator (from **Local users chapter step 1.1**)
3. Azure AD group from **Platform chapter step 3** (Azure AD group that has users that require permanent admin privileges to all workstations as members) - **Fulfill target 4.1**

> **Info!**
>
> As Carillon will start to manage the local group memberships for the groups where managed group rules exist, the existing members in these groups that does not have active managed group rule will be removed from the local groups. Therefore target 4 is fulfilled as there are no managed group rules for Azure AD roles.

> **Note!**
>
> To **fulfill target 1.2** additional managed group rules for single devices can be created by IT support!

Managed user rules

Create following managed user rules (instructions) for the Azure AD group from **Platform chapter step 2** (Azure AD group that has all Windows workstations as members)

1. For built-in Administrator use **Generate random password and save to database** rule type - **Fulfill target 5**
2. For Temporary Administrator (from **Local users chapter step 1.1**) use **Generate temporary user account that can be activated** rule type - **Fulfill target 2**