opentext™

OpenText™ Active Directory Administrator

Get started

Version : 1.0

PDF Generated on : 30/04/2025

Table of Contents

1. Get started

In any organization with an Active Directory managed Windows environment, applications and services need to run with the appropriate Windows user identities to access privileged shared resources. This is achieved with the help of service accounts in the organization. The service accounts establish the applications' and services' access and permission levels to the local and network resources, including the Microsoft Active Directory. Since the Active Directory serves as the identity provider in many organizations, any unauthorized and undetected changes to the Active Directory leave the organization vulnerable to security threats.

Service accounts themselves can be privileged accounts, wherein, they are assigned special permissions to perform critical operations in the organization, including changes to the Active Directory. Service accounts are an integral part of an organization and it is essential to manage and monitor their activities. However, the following are some challenges in managing service accounts:

- Service accounts can exist and run on any number of client machines, server machines, and domain controllers in the organization's domain. Therefore, manually monitoring the details and activities of service accounts is a tedious process.
- When a service account password expires or is changed, the applications and services dependent on the service account stop functioning till they are reconfigured with the new password. If the administrators do not have information on where a service account is used, then, manually checking every machine for the application and services using the service account and updating the applications and services with the new password is time-consuming and susceptible to errors. This often results in an increase in the business downtime and a decrease in the throughput, which is not an optimal scenario for the organization. Setting a service account to never expire, or never changing the password for the account is not a solution as it increases the chances of the account being compromised.

Because of these challenges, the task of managing service accounts in organizations is often not conducted, paving the way for security attacks.

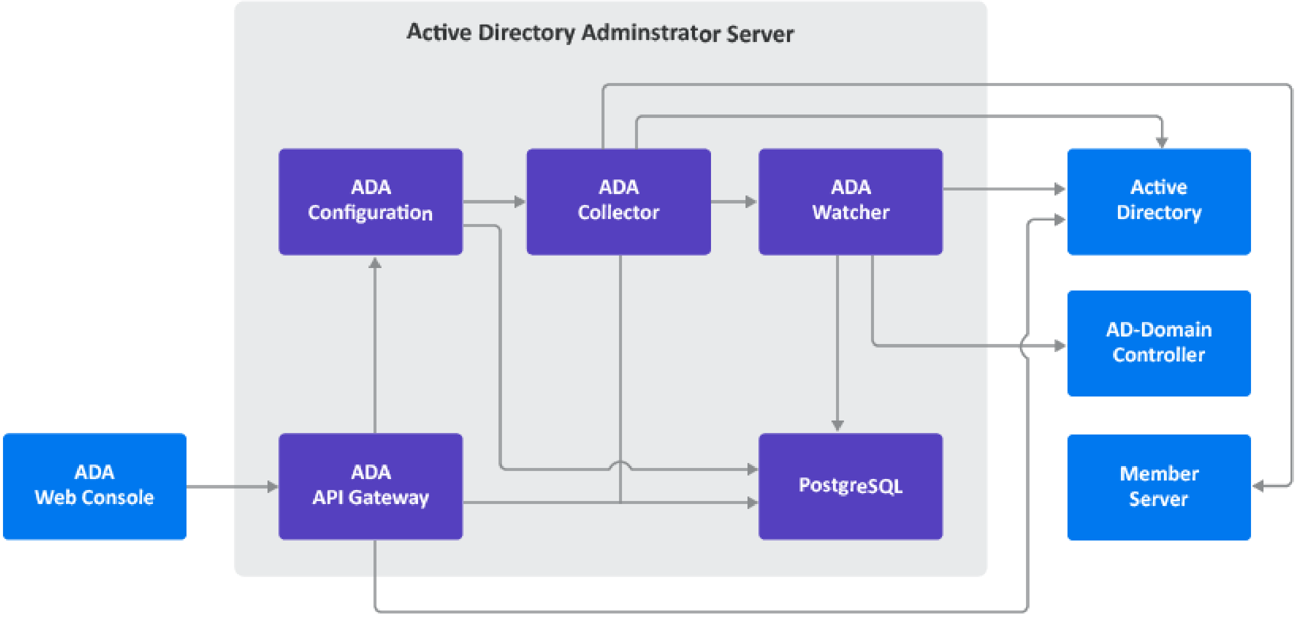
The OpenText Active Directory Administrator helps overcome these challenges.

The OpenText Active Directory Administrator is a powerful solution that provides a visualization of the service accounts and their activity, including changes to the Active Directory, in an organization. This helps administrators gain insights into how robust their organization is against security threats and take necessary actions to avoid potential threats.

- What is Active Directory Administrator
- Functions of the product

1.1. What is Active Directory Administrator

The Active Directory Administrator, as a product, is a one-stop solution to monitor and manage the service accounts in your domain.



The following section describes the terms and entities used in the context of the product:

- **Domain:** A domain refers to a collection of resources such as users, computers, printers, that are mapped to one Active Directory. A domain can have multiple child domains.
- **Service Account:** A service account is a non-user account that is created in the Active Directory. It is associated with one or more Windows services, enabling them to run on the windows operating systems. It establishes their access and permission levels to the local and network resources, including the Active Directory.
- **Services:** Services are the Windows services running and interacting in a Windows domain.
- **Service Account activity**: Activity of a service account refers to the account managing the objects of the Active Directory or modifications being made to the account.
- **Service Account without activity:** A service account without activity indicates that it has not made any modifications to the objects of the Active Directory and that modifications have not been made on the service account.
- **Service Account modifications:** Service account modifications refers to the number of modifications that it does to the user objects of the Active Directory or the number of modifications done to the service account.

1.2. Functions of the product

The following section describes the functions of the product and how the product helps the Active Directory administrators of an organization:

- **Configuring domains and service accounts:** It enables administrators to add domains and child domains, and enable the discovery of their service accounts.
- **Discovering service accounts:** It enables the administrators and the Chief Information Security Officers (CISOs) to get a list all the service accounts in a domain. It also provides a visual representation of the service accounts and their activity in a domain.
- **Configuring domains and discovering their service accounts:** It enables the configuration of domains and the discovery of their service accounts. Discovery of the service accounts of a domain is a two step process. The first step involves specifying a pattern for the kind of service accounts that need to be discovered from the Active Directory of the domain. The second step involves identifying machines of a domain, then discovering the service accounts configured as login accounts for the windows services. The discovery of service accounts enables the product administrators and the Chief Information Security Officers (CISOs) to get a list of all the service accounts in a domain. The product also provides a visual representation of the service accounts and their activity in a domain.
- **Monitoring service account activity:** It helps the product administrators and CISOs track the activity of service accounts and determine if there is any suspicious activity conducted on the service accounts. Services running through a service account or a service account itself making any changes to the user objects of the Active Directory, such as adding a new user account, granting privileges to service accounts, changing user account credentials, and changing user properties are also captured as an activity of the service account. This enables the product administrators and CISOs to quickly identify changes and determine any suspicious activity on the users and groups in the Active Directory. In addition, the product also provides the following functions:
    - **Viewing service account details:** It provides vital information such as the machines where a service account is installed and the services with which the account is associated. This makes it easier for administrators to know where a service account is used so that when the account’s password is changed, all the places where the account is used can be reconfigured with the new password seamlessly.
    - **Managing service account passwords and identifying service accounts not performing any activities:**
        - It provides a snapshot of the password expiration status of the service accounts of a domain. It also lists the password expiration date of each of the service accounts along with an option to notify the service account manager through email when a password has expired or is about to expire. This feature

helps administrators in identifying service accounts that have not been in use for long and taking appropriate actions.

- It helps administrators in determining the last activity related to a service account to understand if the account has become obsolete and poses a risk of being compromised. The administrators can then take appropriate actions on the service account.

opentext™

For more info, visit https://docs.microfocus.com