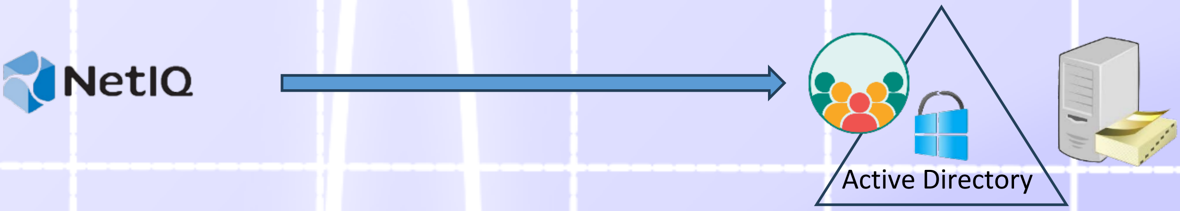
Introduction to ADEMA solution

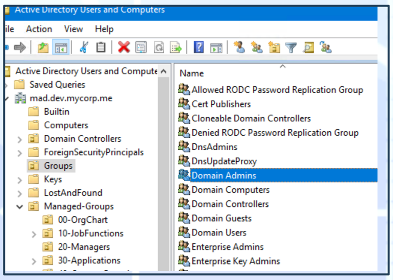
After more than 20 years of experience delivering numerous IAM (IGA) projects & solutions, OPNS observed that the Active Directory platform is increasingly used as **a hub providing authorization services** for multiple applications. These applications, from Microsoft itself and/or third-party providers, do “integrate” with AD to authenticate users and/or **check their AD group memberships for authorization purposes**.

Within a NetIQ IDM environment AD accounts and group memberships are under IDM control; this brings all the benefits associated with automation (provisioning and de-provisioning), an RBAC model (with IDM Roles and Resources), and self-service (IDM request/approval workflows accessible through the Web portal).



In a perfect world all AD groups are part of the model and IAM best practices are applied through various processes, making sure the right people are members of the right AD groups to perform their job, with some auditing and/or Access Review campaigns in place. Also, workflows are configured so that only authorized Users can approve requests that will add AD group memberships to AD accounts. That’s a perfect world…

However, because the world isn’t perfect, and because some **AD groups may grant “highly sensitive” accesses**, strong additional controls should be put in place to make sure no other (“parallel”) process is used to change AD group memberships out of IAM control. This is of primary importance not only for well-known native AD groups like “Domain Admins” or “DnsAdmins”, but also for groups consumed by critical business applications or highly sensitive IT systems like PAM, VPNs and more.



Active Directory Users and Compute
Saved Queries
mad.dev.mycorp.me
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Groups
Keys
LostAndFound
Managed-Groups
00-OrgChart
10-JobFunctions
20-Managers
30-Applications

Name
Allowed RODC Password Replication Group
Cert Publishers
Cloneable Domain Controllers
Denied RODC Password Replication Group
DnsAdmins
DnsUpdateProxy
Domain Admins
Domain Computers
Domain Controllers
Domain Guests
Domain Users
Enterprise Admins
Enterprise Key Admins

We created ADEMA for this purpose: **real-time monitor your critical AD groups**. You configure ADEMA for the AD groups you want to put under supervision and for the events you want to be notified for as, for example, “new member”, “new nested group”, “changed OU” …

For the “new member” event, ADEMA is smart enough to compare with known (legitimate) AD group memberships as registered in NetIQ IDM; when a suspicious change is detected an email alert is sent to designated email addresses, for example to both the IAM and security teams.

ADEMA real-time monitors your critical AD groups and notifies you about suspicious modifications!

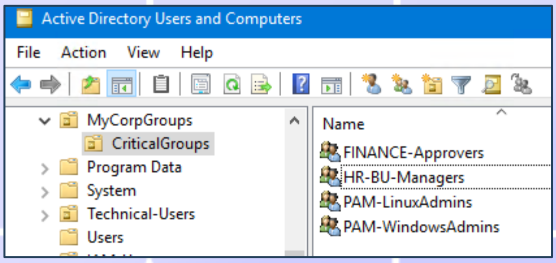
Technically, ADEMA comes as an add-on driver to install on the NetIQ IDM platform.

Either you already have NetIQ IDM in production, or the platform is new to your environment.

In the first scenario, you can self-add ADEMA to your existing environment, without changing anything to your existing AD provisioning driver. Then, through some simple configuration steps, ADEMA will be operational.

In the second scenario ADEMA requires a Windows server, preferably dedicated, where we first install the NetIQ IDM engine and then our ADEMA driver. We then configure connectivity with your AD and the various ADEMA parameters to monitor designated critical groups.

One installed and configured ADEMA is silently monitoring your critical AD groups; it will notify/alert you for the selected events happening on these groups.



MyCorpGroups
CriticalGroups
Program Data
System
Technical-Users
Users

Name
FINANCE-Approvers
HR-BU-Managers
PAM-LinuxAdmins
PAM-WindowsAdmins

By sitting next to AD and running on an independent platform, **ADEMA guarantees you that any abnormal group change operated by any user, any malware or any process is detected & reported**.

Obviously ADEMA is also configurable to send alerts when it is somehow “disabled”, intentionally or not, for example if ADEMA’s technical account is disabled on AD side, preventing ADEMA from operating as it should…

In advanced mode, for customers with a fully deployed NetIQ IDM solution that includes Roles & Resources to manage a complete RBAC model, ADEMA performs smart comparisons to:

- Make sure a legitimate change performed by the AD provisioning driver does not raise an alert.
- Check if a change on AD side is legitimate from an RBAC point of view (the change on AD side, performed by an AD account admin, could be a “fix” for a missing but legitimate group membership).
- Check if the AD account added to a group is mapped to an IDM user and send notifications if not.
- Notify you if some IDM Users (e.g. IAM or security team members) are removed from some AD groups.

ADEMA is part of ***Mir.IAM***, our overarching framework for a maturity level 5 IAM. We base our IAM projects on ***Mir.IAM***, which comes with a solution blueprint, an MVP, a project methodology and all components required to succeed fact and efficiently. Some of our ***Mir.IAM*** sub-components are packaged & available separately as a product, further designed to enrich any existing NetIQ solution. **ADEMA** is only one of these products; contact or visit us to discover other surprisingly smart ***Mir.IAM*** sub-components!