Robotic Process Automation/Bot Governance through SailPoint IdentityIQ 7.3

Most of the organizations are implementing Robotic Process Automation (RPA) to eliminate the involvement of their employees in "repetitive manual tasks". Bots can improve an organization's efficiency by reducing costs and speeding up the repetitive tasks. The Machine learning capabilities of these bots improves the overall process over time. Jobs are run using the bot user accounts and we need to make sure that these accounts have the least privilege access to run the jobs. If the necessary action is not taken, it is going to increase access to governance problems in the future.

Bots need effective governance model similar to the one used for human identities.

Some of the governance challenges during the implementation of bots are as follows:

- The necessity to manage all the organisation bots at one place, along with their access.
- Conducting access reviews on bots.
- The need to define policies such that bots have the least access to run the jobs.
- The necessity to show auditors, who owns the bot or who is accountable for the bot account and access reviews.

IdentityIQ 7.3's governance capabilities for bots includes the abilities to:

- Manage bots and their attributes
- Request access for bots
- Certify bots
- Extend access-based policy definitions to bots

Managing bots and their attributes

IdentityIQ 7.3 added three new standard attributes to the identity object in order to support the governance of bots and to help us categorize and govern bot identities. The new attributes are as follows:

Type: It will define type to identity like bot/employee/contractor

Software Version: It will define bot version

Administrator: It will define the owner/person responsible for bot identity

Requesting access for bots

Access will be requested and granted to the bots in a similar way as for any other identity. During that request process we can use the filter to display only bot identities. Then we can select the access items and proceed with the request as usual.

Certifying bots

We can certify bots in the same way we do for any identity. Using the **Targeted Certification** type, we can select the bots from identity type and assign the certifier to perform the Access Reviews. By using the filter, we can choose what needs to be certified during the certification process.

Extend access-based policy definitions to bots

We can apply the "Separation of Duties" policy based upon the identity type to bots and this will meet the business/audit requirements.

Thus, by implementing the SailPoint IdentityIQ 7.3, we can effectively govern the bot user accounts.

Contact for further details

Srikanth Pinninti

Technology Specialist

srikanthp.in@mouritech.com

MOURI Tech