Script Expression Sandboxing

Planned feature

This page describes a feature planned for future midPoint versions.

This feature is roughly designed and it was evaluated as feasible. However, there is currently no specific plan when it will be implemented because there is no funding for this development yet. In case that you are interested in supporting development of this feature, please consider activating midPoint Platform subscription.

Introduction

Script expressions are a code that runs inside midPoint servers. As such, script expressions are incredibly powerful. But with great powers comes great responsibility. Script expressions can do a lot of useful things, but they can also do a lot of harm. There are just a few simple internal safeguards when it comes to expression evaluation. E.g. midPoint script libraries will properly enforce authorization when executing the functions. However, script languages are powerful and a clever expression can find a way around this safeguards. MidPoint is **not** placing expressions in a sandbox, therefore expressions are free to do almost anything.

Sandboxing

The sandbox is not enforced yet from complexity and performance reasons. However we want to apply sandboxing or an equivalent strategy to limit the capabilities of script expressions. Yet, this is not easy. Sandbox privileges need to be chosen carefully and maintained. And then, some expressions may need to do stronger things than others. E.g. reporting expression should be tightly restricted, while scripting hooks should remain very powerful. This is introducing additional complexity.

Expression Profiles

This feature is a part of a much bigger feature set. See Expression Profiles: Full Implementation for more details.

See Also

- **MID-5193** - Getting issue details... STATUS
- Expression
- Script Expression
- Expression Profiles
- Expression Profiles: Full Implementation