DESCRIPTION

The following solution is intended to compare actual filesystem permissions with permissions provided in a JSON file and sends an alert if deficiencies are detected.

The JSON file lists objects that consist of file system object Path, security object UserOrGroup that is granted access to the file system object and permission Permission granted to the UserOrGroup to the file system object Path (see https://docs.microsoft.com/en-us/dotnet/api/system.security.accesscontrol.filesystemrights).

An example of the JSON file:

```
[
  {
    "Path":  "C:\\Program Files\\Octeum\\SafetrustConnector",
    "UserOrGroup":  "CREATOR OWNER",
    "Permission":  "FullControl"
  },
  {
    "Path":  "C:\\Program Files\\Octeum\\SafetrustConnector",
    "UserOrGroup":  "NT AUTHORITY\\SYSTEM",
    "Permission":  "FullControl"
  },
  {
    "Path":  "C:\\Program Files\\Octeum\\SafetrustConnector",
    "UserOrGroup":  "BUILTIN\\Users",
    "Permission":  "CreateFiles, Synchronize,AppendData, ReadAndExecute"
  }
]
```

INSTALL INSTRUCTIONS

1. Extract the files from the attached zip file

2. Upload the Power Shell and JSON file to the Shared Files directory of the Managed Files folder: https://helpdesk.kaseya.com/hc/en-gb/articles/360017878358

3. Import the XML into the agent procedure module: https://helpdesk.kaseya.com/hc/en-gb/articles/229012068

4. Execute the procedure on a target machine

5. If a deficiency is found, Navigate to Monitor > Status > Alarm Summary to review existing alerts.