INFRAMON
THE CLOUD TRANSFORMATION SPECIALISTS

MANUAL FOR SQL MONITORING CONFIGURATION SCRIPTS

Documentation

PUBLIC

Thursday, 04 August 2016

Contents

1. REVISION HISTORY

RELEASE DATE	CHANGES	VER	AUTHOR
8th July 2016	Initial draft	0.1	Sandor Makai

2. INTRODUCTION

2.1 Scope

This document is for giving the reader the necessary information to work with the PowerShell scripts detailed below. This is a script package with consist of

- 2 PS1 script files
- 1 XML configuration files

The whole package contains scripts for executing the following tasks:

- Configure required permissions on agent managed SQL machine
- Configure required permissions on specified SQL Instances (not implemented yet)
- Configure settings in SCOM environment for the specified SQL agent managed computer (not implemented yet)

3. DESCRIPTION

3.1 Configure permissions on agent managed SQL machine

This is the first part of the package and it is responsible for setting up the necessary basic permissions for the specified AD Objects. This part uses

2 PS1 script files

- Logging.ps1 – Contains functions for logging operations
- SCOM_SQL_BasicPermissions.ps1 – Contains the main script

and 1 XML configuration files

- BasicConfiguration.xml – Holds the necessary configuration information

By executing the script, the following tasks will be done:

- Adding the required AD objects into local groups
- Setting up permissions on the required registry keys
- Setting up permissions on the required folders in the file-system
- Setting up permissions on the required WMI Namespaces

Note: The process requires “Allow logon locally” rights for specific Active Directory objects (all 3 user accounts), but because in most cases it is done by GPO the script won’t touch this configuration. Make sure the required object has this rights assigned in the security policy.

3.1.1 Preparation

For successfully running the script and have the desired result you need to have the following prerequisites:

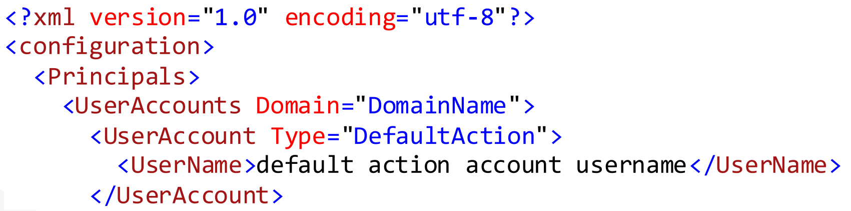
- Account with administrative privileges on the agent machine
- Information of account used for SQL Default Action Account in SCOM (DOMAIN, Username)
- Information of account used for SQL Monitoring in SCOM (DOMAIN, Username)
- Information of account used for SQL Discovery in SCOM (DOMAIN, Username)

- Information of group used for Low Privilege environments described in the SCOM SQL Management Pack guide (DOMAIN, Groupname)
- Version of SQL Server Engine installed on the agent machine (2012/2014)
- List of SQL instances where the permissions needs to be set

Before the execution of the script the configuration file must be modified with the correct information. This file is an XML formatted file with the following sections:

- **Principals** – Holds information about the Active Directory Objects
  - ***UserAccounts*** – Holds information about the 3 Active Directory user accounts used for SQL Monitoring in SCOM as Default Action Account, Monitoring Account and Discovery Account. As it can be seen in the example file all 3 accounts need to be in the same domain. This is why the domain information is defined in the base section of the accounts. One level deeper all the 3 account information (Username) needs to be added to the proper section
  - ***Group*** – Holds information about the Active Directory security group created according to the recommendation of Microsoft described in the “Low Privilege Environment” part of the Management Pack guide for SQL Server monitoring management pack. If the group is used in the settings the “Used” field must be “True”, otherwise the script will ignore the settings and will work with only the 3 user account described in the previous point.
- **Instances** – Holds information about the installed SQL Engine and instances. This section has 4 different fields. The “Type” define that the script needs to work with “Database” engines of the SQL. The “Version field defines the version of installed SQL engine. The “ServerName” field is to describe if the script do the settings on the local or a remote server. Currently it can only use the “local” settings. The “InstanceName” fields are for listing all the instances running on the specified servers where we want to have the permissions to be set. If the first instancename is set to “All”, the script will apply the permissions for all the installed SQL instances.

Here is an example script



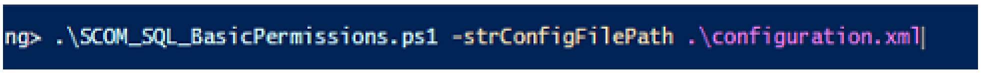
```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <Principals>
    <UserAccounts Domain="DomainName">
      <UserAccount Type="DefaultAction">
        <UserName>default action account username</UserName>
      </UserAccount>
```

```
        <UserAccount Type="Discovery">
        <UserName>discovery account username</UserName>
      </UserAccount>
      <UserAccount Type="Monitoring">
        <UserName>monitoring account username</UserName>
      </UserAccount>
    </UserAccounts>
    <Group Domain="DomainName" Used="True">
      <GroupName>lowprivilege groupname</GroupName>
    </Group>
  </Principals>
  <Instances Type="Database" Version="2012" ServerName="local">
    <InstanceName>All</InstanceName>
    <InstanceName>Second</InstanceName>
    <InstanceName>Third</InstanceName>
  </Instances>
</configuration>
```

When the configuration file is correctly modified the package is almost ready to roll. All the 3 files (2 PS1 and 1 XML) must be copied to the server where the settings need to be applied. Make sure all 3 files are in the same folder.

3.1.2 Execution

To execute the script, make sure the account used has administrative rights (WMI permission can only be set by Administrators) on the agent machine. Start a PowerShell console session with “Run As Administrator” mode. Change the folder to the one where the files are copied and execute the script using a command like this:



```
ng> .\SCOM_SQL_BasicPermissions.ps1 -strConfigFilePath .\configuration.xml
```

The script is designed to be verbose, so every step is written to the console. When the script runs it creates a .log file with the same name as the .ps1 which contains all the information about every run of the script. If you run into issues, check this file for information about the error.

3.2 Configure permissions on SQL Instances

Not ready yet

3.2.1 Preparation

3.2.2 Execution

3.3 Configure settings in SCOM environment

Not ready yet

3.3.1 Preparation

3.3.2 Execution