cms-ars-3.1-high-microsoft-sql-server-2014-instance-stig-overlay

InSpec profile overlay to validate the secure configuration of Microsoft SQL Server 2014 Instance against DISA's Microsoft SQL Server 2014 Instance STIG Version 1 Release 9 tailored for CMS ARS 3.1 for CMS systems categorized as High.

Getting Started

It is intended and recommended that InSpec and this profile overlay be run from a **"runner"** host (such as a DevOps orchestration server, an administrative management system, or a developer's workstation/laptop) against the target remotely over **winrm**.

For the best security of the runner, always install on the runner the *latest version* of InSpec and supporting Ruby language components.

Latest versions and installation options are available at the InSpec site.

Git is required to download the latest InSpec profiles using the instructions below. Git can be downloaded from the Git site.

The following attributes must be configured in an attributes file for the profile to run correctly. More information about InSpec attributes can be found in the InSpec Profile Documentation.

```
# Username for MSSQL DB Server
user: null

# Password for MSSQL DB Server
password: null

# Hostname for MSSQL DB Server
host: 'hostname'

# Instance name of the MSSQL DB Server
instance: 'MSSQL2014'

# Port of MSSQL DB Server
port: 1433

# Name of the specific database being evaluated within the MSSQL server
db_name: 'master'

# description: 'Set to true If SQL Server Trace is in use for audit purposes'
server_trace_implemented: false
```

```
#   description: 'Set to true If SQL Server Audit is in use for audit purposes'
server_audit_implemented: false

# description: 'Set to true if SQL Server Reporting Services is in use'
  sql_server_reporting_services_used: false

# description: 'Set to true if SQL Server data tools is required'
sql_server_data_tools_required: false

# description: 'Set to true if SQL Server Integration Services is in use'
sql_server_integration_services_used: false

# description: 'Set to true if SQL Server analysis Services is in use'
sql_server_analysis_services_used: false

# description: 'Set to true if SQL Server Distributed Replay Client is in use'
sql_server_distributed_replay_client_used: false

# description: 'Set to true if SQL Server Distributed Replay Controller is in use'
sql_server_distributed_replay_controller_used: false

# description: 'Set to true if SQL Server full-text search is in use'
sql_server_full_text_search_used: false

# description: 'Set to true if master data services is in use'
master_data_services_used: false

# description: 'Set to true if data quality client is in use'
data_quality_client_used: false

# description: 'Set to true if data quality services is in use'
data_quality_services_used: false

# description: 'Set to true if data quality services is in use'
data_quality_services_used: false

# description: 'Set to true if client tools sdk is in use'
client_tools_sdk_used: false

# description: 'Set to true if sql server management tools is in use'
sql_mgmt_tools_used: false

# description: 'Set to true if xp_cmdhsell is required'
sql_mgmt_tools_used: false

# description: 'instance name MSSQL DB Server (e.g., ''WIN-FC4ANINFUFP'')'
```

```
server_instance: ''

#description: 'List of users with permissions - ALTER TRACE, CREATE TRACE EVENT NOTIFICATION
approved_audit_maintainers: []

# description: 'List of users with audit permissions - ALTER ANY SERVER AUDIT, CONTROL SERVE
allowed_audit_permissions: []

# description: 'List of user with permissions -  ALTER ANY SERVER AUDIT, ALTER ANYDATABASE A
allowed_sql_alter_permissions: []

# description: 'List of approved users with access to SQL Server Audits'
approved_users_sql_audits: []

# description: 'List of sql server users with permissions - alter, create, control'
approved_users_server: []

# description: 'List of sql database users with permissions - alter, create, control'
approved_users_database: []

# description: 'List of sql components installed'
sql_components: []

#  description: 'List of authorized network protocols for the SQL server (e.g., [''Shared Me
authorized_protocols: []

# description: 'List of authorized network ports for the SQL server (e.g., [''1433'']').
authorized_ports: []

# description: 'List of authorized network port names for the SQL server (e.g., [''TcpPort''
authorized_ports_name: []

# description: 'List of authorized users for the SQL server'
authorized_sql_users: []

# description: 'List of users allowed to execute privileged functions - create, alter, delet
allowed_users_priv_functions: []

# description: 'List of allowed server permissions'
allowed_server_permissions: []

# description: 'List of allowed database permissions'
allowed_database_permissions: []

# description: 'List of Databases that require encryption'
encrypted_databases: []
```

```
# description: 'Set to true if data at rest encryption is required'
data_at_rest_encryption_required: false

# description: 'Set to true if full disk encryption is in place'
full_disk_encryption_inplace: false

# description: 'List of user allowed to execute privileged functions'
allowed_users: []

# description: 'Set to true xp cmdshell is required'
is_xp_cmdshell_required: false

# description: 'List of accounts managed by the sql server'
sql_managed_accounts: []

# description: 'Set to true if filestream is required'
filestream_required: false

# description: 'Set to true if filestream transact access is required'
filestream_transact_access_only_required: false
```

Running This Overlay

When the **"runner"** host uses this profile overlay for the first time, follow these steps:

```
mkdir profiles
cd profiles
git clone https://github.cms.gov/ispg/cms-ars-3.1-high-microsoft-sql-server-2014-instance-st
git clone https://github.com/mitre/microsoft-sql-server-2014-instance-stig-baseline.git
cd cms-ars-3.1-high-microsoft-sql-server-2014-instance-stig-overlay
bundle install
cd ..
inspec exec cms-ars-3.1-high-microsoft-sql-server-2014-instance-stig-overlay --attrs=<path_t
```

For every successive run, follow these steps to always have the latest version of this overlay and dependent profiles:

```
cd profiles/microsoft-sql-server-2014-instance-stig-baseline
git pull
cd ../cms-ars-3.1-high-microsoft-sql-server-2014-instance-stig-overlay
git pull
bundle install
cd ..
inspec exec cms-ars-3.1-high-microsoft-sql-server-2014-instance-stig-overlay --attrs=<path_t
```

Viewing the JSON Results

The JSON results output file can be loaded into **heimdall-lite** for a user-interactive, graphical view of the InSpec results.

The JSON InSpec results file may also be loaded into a **full heimdall server**, allowing for additional functionality such as to store and compare multiple profile runs.

Authors

- Eugene Aronne
- Danny Haynes

Special Thanks

- Aaron Lippold
- Alicia Sturtevant

Getting Help

To report a bug or feature request, please open an issue.

License

This is licensed under the Apache 2.0 license.

NOTICE

This software was produced for the U. S. Government under Contract Number HHSM-500-2012-00008I, and is subject to Federal Acquisition Regulation Clause 52.227-14, Rights in Data-General.

No other use other than that granted to the U. S. Government, or to those acting on behalf of the U. S. Government under that Clause is authorized without the express written permission of The MITRE Corporation.

For further information, please contact The MITRE Corporation, Contracts Management Office, 7515 Colshire Drive, McLean, VA 22102-7539, (703) 983-6000.

NOTICE

DISA STIGs are published by DISA IASE, see: https://iase.disa.mil/Pages/privacy_policy.aspx