cms-ars-3.1-moderate-red-hat-jboss-eap-6.3-stig-overlay

InSpec profile overlay to validate the secure configuration of Red Hat JBoss EAP 6.3 against DISA's Red Hat JBoss Enterprise Application Platform (EAP) 6.3 STIG Version 1 Release 3 tailored for CMS ARS 3.1 for CMS systems categorized as Moderate.

Getting Started

It is intended and recommended that InSpec run this profile 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 **SSH**.

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

The 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.

```
# description: Command used to connect to the wildfly instance.
connection: ''

# description: List of authorized users with the auditor role (e.g., ['user-auditor']).
auditor_role_users: []

# description: List of authorized users with the administrator role (e.g., ['user-admin']).
administrator_role_users: []

# description: List of authorized users with the SuperUser role (e.g., ['user-superuser', 'u
superuser_role_users: []

# description: List of authorized auditor users (e.g., ['user-auditor']).
auditor_group_users: []

# description: Group owner of files/directories (e.g., 'wildfly').
wildfly_group: ''

# description: User owner of files/directories (e.g., 'wildfly').
wildly_owner: ''
```

```
# description: List of authorized applications (e.g., ['sample.war']).
approved_applications: []

# description: List of authorized users (e.g., ['jboss.management.http.port=9990', 'jboss.ma
auditor_group_users: []

# description: List of authorized users with the auditor role (e.g., ['user-auditor']).
auditor_role_users: []

# description: List of authorized users with the administrator role (e.g., ['user-admin']).
administrator_role_users: []

# description: List of authorized users with the SuperUser role (e.g., ['user-$local', 'user
superuser_role_users: []

# description: List of authorized users with the deployer role (e.g., ['user-deployer']).
deployer_role_users: []

# description: List of authorized users with the maintainer role (e.g., ['user-maintainer'])
maintainer_role_users: []

# description: List of authorized users with the monitor role (e.g., ['user-monitor']).
monitor_role_users: []

# description: 'List of authorized users with the operator role (e.g., [user-operator]).'
operator_role_users: []

# description: 'Set to true if ldap is being used.'
ldap: false

# description: 'Set to true if widlfy is being used as a high-availability cluster.'
high_availability: 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-moderate-red-hat-jboss-eap-6.3-stig-overla
git clone https://github.com/mitre/red-hat-jboss-eap-6.3-stig-baseline.git
cd cms-ars-3.1-moderate-red-hat-jboss-eap-6.3-stig-overlay
bundle install
cd ..
inspec exec cms-ars-3.1-moderate-red-hat-jboss-eap-6.3-stig-overlay --attrs=<path_to_your_at
```

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

```
cd profiles/red-hat-jboss-eap-6.3-stig-baseline
git pull
cd ../cms-ars-3.1-moderate-red-hat-jboss-eap-6.3-stig-overlay
git pull
bundle install
cd ..
inspec exec cms-ars-3.1-moderate-red-hat-jboss-eap-6.3-stig-overlay --attrs=<path_to_your_at
```

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.

Getting Help

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

Authors

- Eugene Aronne
- Danny Haynes

Special Thanks

- Alicia Sturtevant

License

- This project is licensed under the terms of the Apache 2.0 license.

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