cms-ars-3.1-moderate-nginx-overlay

InSpec profile overlay to validate the secure configuration of NGINX based on DISA's Apache 2.2 Server tailored for CMS ARS 3.1 for CMS systems categorized as Moderate.

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 **ssh**.

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.

```
# description: Path for the nginx configuration file (e.g., '/etc/nginx/nginx.conf')
nginx_conf_file: ''

# description: Path to nginx backup repository (e.g., '/usr/share/nginx/html')
nginx_backup_repository: ''

# description: Subnet of the DMZ (e.g., '62.0.0.0/24')
dmz_subnet: ''

# description: Minimum Web vendor-supported version (e.g., '1.12.0').
nginx_min_ver: ''

# description: Nginx owner (e.g., 'nginx')
nginx_owner: ''

# description: The Nginx group (e.g., 'nginx')
nginx_group: ''

# description: The system adminstrator (e.g., ['root','centos'])
sys_admin: []

# description: The system adminstrator group (e.g., 'root')
sys_admin_group: ''
```

```
# description: List of non admin user accounts (e.g., ['user'])
authorized_user_list: []

# description: Monitoring software for CGI or equivalent programs (e.g., ['audit', 'auditd']
monitoring_software: []

# description: List of disallowed packages (e.g., ['postfix'])
disallowed_packages_list: []

# description: List of disallowed compilers (e.g., ['gcc'])
disallowed_compiler_list: []

# description: DoD-approved PKIs such as DoD PKI, DoD ECA, and DoD-approved external partner
dod_approved_pkis: []

# description: File list of documentation, sample code, example applications, and tutorials
nginx_disallowed_file_list: []

# description: File list of allowed documentation, sample code, example applications, and tu
nginx_allowed_file_list: []

# description: List of authorized nginx modules (e.g., ['http_addition', 'http_auth_request'

nginx_authorized_modules: []

# description: List of unauthorized nginx modules.
nginx_unauthorized_modules: []

# description: Path for the nginx binary (e.g., '/usr/sbin/nginx')
nginx_path: ''

# description: domain and port to the OCSP Server (e.g., 'login.live.com:443')
ocsp_server: ''

# description: Frequency at which CRL is updated in days (e.g., 7)
crl_update_frequency:
```

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-nginx-overlay.git
```

```
git clone https://github.com/mitre/nginx-baseline.git
cd cms-ars-3.1-moderate-nginx-stig-overlay
bundle install
cd ..
inspec exec cms-ars-3.1-moderate-nginx-overlay --target=ssh://<your_target_host_name_or_ip_a
```

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

```
cd profiles/nginx-baseline
git pull
cd ../cms-ars-3.1-moderate-nginx-overlay
git pull
bundle install
cd ..
inspec exec cms-ars-3.1-moderate-nginx-overlay --target=ssh://<your_target_host_name_or_ip_a
```

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

- Patrick Muench
- Dominik Richter
- Christoph Hartmann
- Rony Xaiver
- Aaron Lippold

Contributing and Getting Help

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

License

This is licensed under the Apache 2.0 license.