Appliquer les Recommandations de l'ANSSI sur AlmaLinux 9 avec Ansible

Introduction

Ce guide vous aidera à appliquer les recommandations de l'ANSSI à votre machine virtuelle AlmaLinux 9. Nous utiliserons Ansible et OpenSCAP pour améliorer la sécurité de votre système. Suivez attentivement ces étapes, même si vous avez peu d'expérience avec Ansible.

Prérequis

1. **VM AlmaLinux 9**
2. **Ansible installé** sur votre machine locale ou serveur
3. **Accès à la VM** via SSH (accès root)

Étape 1 : Préparer les fichiers de configuration

Pour simplifier le processus d'installation, j'ai créé un dépôt GitHub avec un modèle contenant les fichiers de configuration nécessaires. Vous pouvez cloner ce dépôt et l'ajuster pour qu'il corresponde à votre environnement :

Dépôt GitHub: https://github.com/NeeroCA/Projet_OpenIT_CA

Instructions :

1. Clonez le dépôt sur votre machine locale :

```
git clone https://github.com/NeeroCA/Projet_OpenIT_CA.git
```

2. Accédez au répertoire cloné :

```
cd alma_anssi_template
```

3. Modifiez le fichier `inventory.yml` pour refléter l'adresse IP de votre VM AlmaLinux 9 :

```
all:
  hosts:
    localhost:
        ansible_connection: local
    alma:
      ansible_host: votre_adresse_ip_vm
```

Après avoir mis à jour l'adresse IP, vous pouvez passer à l'Étape 2.

Si vous préférez créer vous-même les fichiers au lieu d'utiliser le code ci-dessus, suivez ces étapes :

Vous devrez créer et configurer certains fichiers pour utiliser Ansible. Créez un dossier de projet sur votre machine locale, par exemple, `openscap_project`, et placez-y les fichiers suivants :

1. Configuration Ansible (ansible.cfg)

```
[defaults]
inventory = ./inventory.yml
remote_user = root
host_key_checking = False
retry_files_enabled = False
timeout = 30

[ssh_connection]
ssh_args = -o ControlMaster=auto -o ControlPersist=60s
pipelining = True

[privilege_escalation]
become = True
become_method = sudo
become_user = root
become_ask_pass = False
```

2. Fichier d'Inventaire (inventory.yml)

Ajoutez l'adresse IP de votre VM AlmaLinux 9 ici :

```
all:
    hosts:
    localhost:
      ansible_connection: local
        alma:
            ansible_host: votre_adresse_ip_vm
```

3. Playbook (playbook.yml)

Ce playbook installe les paquets nécessaires et exécute une analyse de sécurité :

```
---
- name: Appliquer les recommandations de l'ANSSI
  hosts: alma
  roles:
    - anssi_bp28_minimal
#    - anssi_bp28_intermediary
#    - anssi_bp28_high
#    - anssi_bp28_enhanced
    - role_openscap
```

4. Variables Hôtes (group_vars/all/vars.yml)

Ce fichier spécifie le profil de sécurité que vous souhaitez appliquer. Dans ce cas, nous utilisons le profil ANSSI "minimal" :

```
ssg_profile: "xccdf_org.ssgproject.content_profile_anssi_bp28_minimal"
#ssg_profile: "xccdf_org.ssgproject.content_profile_anssi_bp28_intermediary"
#ssg_profile: "xccdf_org.ssgproject.content_profile_anssi_bp28_high"
#ssg_profile: "xccdf_org.ssgproject.content_profile_anssi_bp28_enhanced"
ensure_redhat_gpgkey_installed: false
report_directory: "."
```

Étape 2 : Profils de Sécurité Disponibles (optionnel)

Plusieurs profils de sécurité ANSSI sont disponibles. Vous pouvez choisir l'un des profils suivants en fonction du niveau de sécurité que vous souhaitez appliquer :

- **minimal**
- **intermediary**
- **high**
- **enhanced**

Pour sélectionner un profil, vous devez modifier la variable `ssg_profile` dans le fichier `group_vars/all/vars.yml` pour qu'elle corresponde au profil souhaité. De plus, vous devez vous assurer que le rôle de renforcement correct est appliqué dans votre `playbook.yml` .

Par exemple, si vous souhaitez utiliser le profil **"enhanced"**, vous devrez mettre à jour `vars.yml` ainsi :

```
#ssg_profile: "xccdf_org.ssgproject.content_profile_anssi_bp28_minimal"
#ssg_profile: "xccdf_org.ssgproject.content_profile_anssi_bp28_intermediary"
#ssg_profile: "xccdf_org.ssgproject.content_profile_anssi_bp28_high"
ssg_profile: "xccdf_org.ssgproject.content_profile_anssi_bp28_enhanced"
ensure_redhat_gpgkey_installed: false
report_directory: "."
```

Et votre `playbook.yml` devra appliquer le rôle correspondant :

```
---
- name: Appliquer les recommandations de l'ANSSI
  hosts: alma
  roles:
#    - anssi_bp28_minimal
#    - anssi_bp28_intermediary
#    - anssi_bp28_high
    - anssi_bp28_enhanced
    - role_openscap
```

Étape 3 : Télécharger les Rôles Ansible

Vous devez télécharger les rôles Ansible nécessaires pour appliquer les recommandations de l'ANSSI et utiliser OpenSCAP :

- Ajoutez le rôle ANSSI BP28 et le rôle OpenSCAP à votre fichier `roles/requirements.yml` :

```
---
- name: role_openscap
  src: https://github.com/owen282000/role_openscap.git
  scm: git
  version: main
- name: anssi_bp28_minimal
  src: https://github.com/RedHatOfficial/ansible-role-rhel9-anssi_bp28_minimal.git
  scm: git
  version: main
- name: anssi_bp28_intermediary
  src: https://github.com/RedHatOfficial/ansible-role-rhel9-anssi_bp28_intermediar
y.git
  scm: git
  version: main
- name: anssi_bp28_high
  src: https://github.com/RedHatOfficial/ansible-role-rhel9-anssi_bp28_high.git
  scm: git
  version: main
- name: anssi_bp28_enhanced
  src: https://github.com/RedHatOfficial/ansible-role-rhel9-anssi_bp28_enhanced.git
  scm: git
  version: main
...
```

- Installez les rôles requis en exécutant la commande suivante :

```
ansible-galaxy install -r roles/requirements.yml -p roles
```

Étape 4 : Exécuter le Playbook

Une fois tout correctement configuré, exécutez le playbook pour appliquer les recommandations de l'ANSSI à votre VM AlmaLinux :

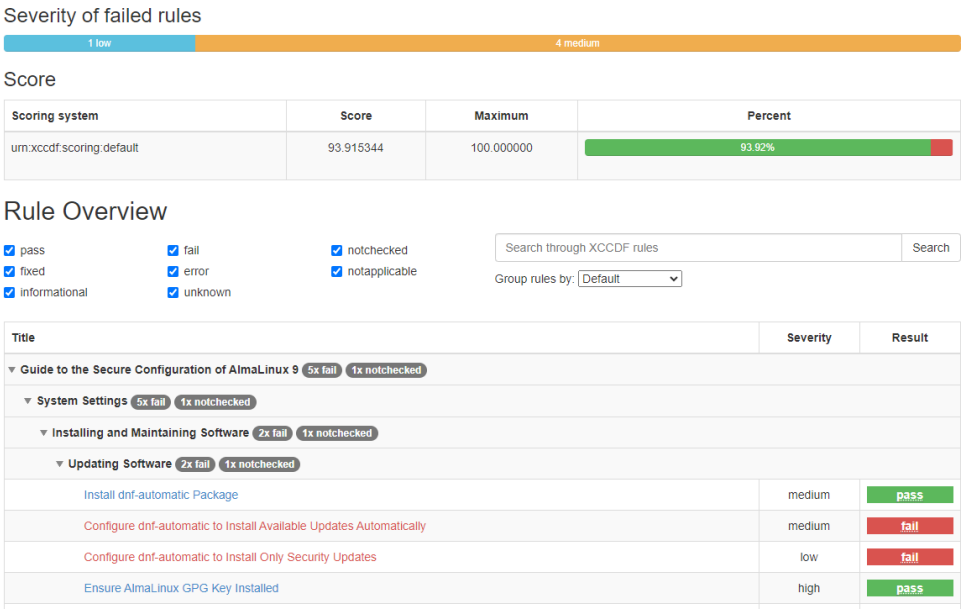
```
ansible-playbook playbook.yml -u your_user -kK
```

Étape 5 : Vérification des Résultats de l'Analyse de Sécurité

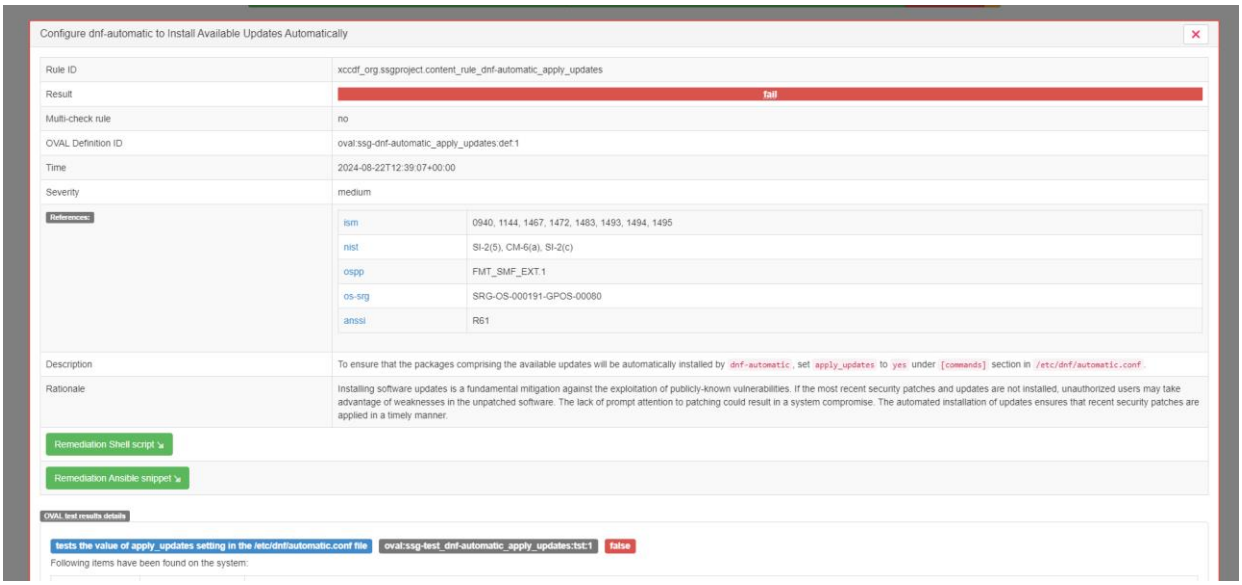
Après la fin de l'analyse de sécurité, un rapport sera généré dans le répertoire de projet où vous avez exécuté le playbook Ansible. Ce rapport détaillera les mesures de sécurité appliquées et celles qui doivent encore être améliorées.

Étape 6 : Vérification du Rapport de Sécurité et Application des Correctifs

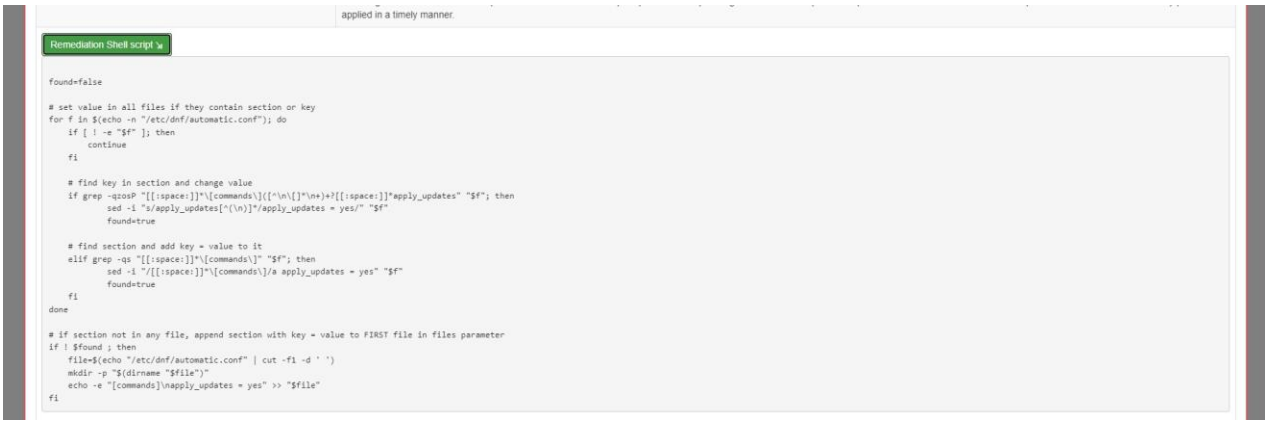
1. **Ouvrir le Rapport :**
   Ouvrez le fichier HTML créé dans un navigateur web pour vérifier l'état de sécurité. Le rapport mettra en évidence les contrôles réussis (en vert) et les échecs (en rouge).
2. **En cas de Problèmes :**
   Si certains contrôles sont marqués en rouge (échec), vous devrez peut-être appliquer des correctifs supplémentaires.
   Par exemple, dans le scénario suivant :



Cliquez sur la tâche échouée :



Cliquez sur "Remediation Shell Script"



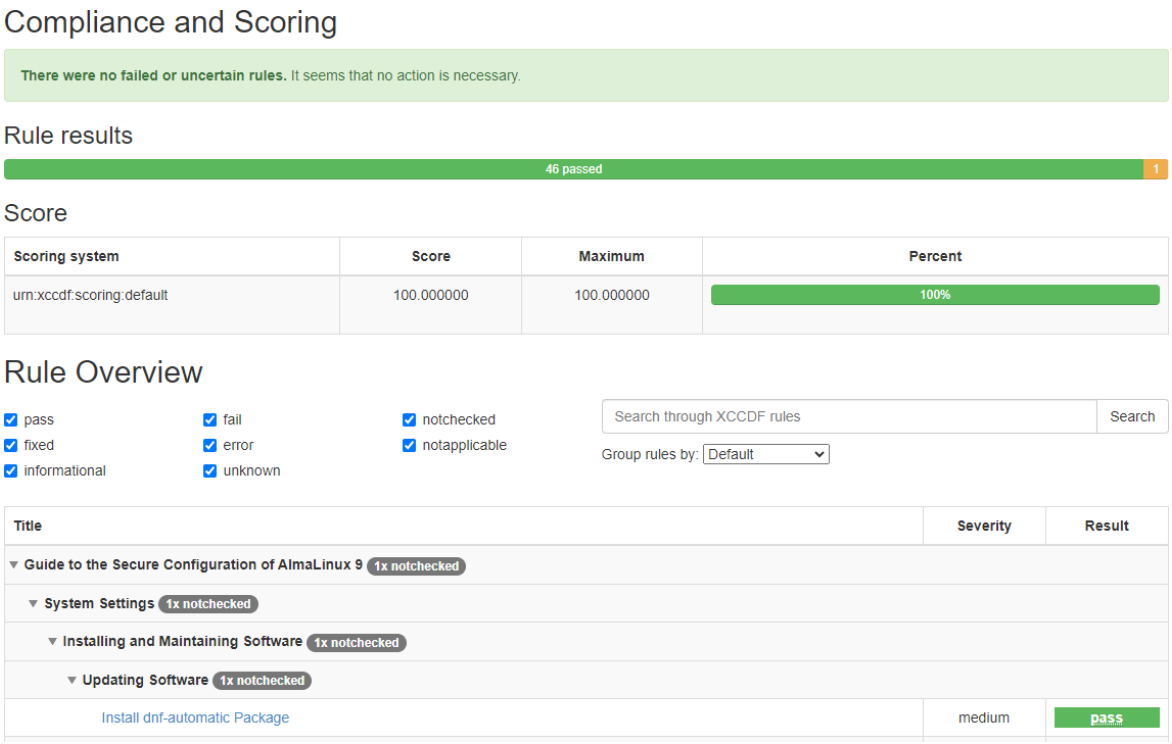
Copiez ce bloc et exécutez-le sur votre VM Alma 9 (donc dans la ligne de commande, collez ceci)

```
[root@alma ~]# found=false

# set value in all files if they contain section or key
for f in $(echo -n "/etc/dnf/automatic.conf"); do
    if [ ! -e "$f" ]; then
        continue
    fi

    # find key in section and change value
    if grep -qzosP "[[:space:]]*\[commands\]([^\n\[]*\n+)+?[[:space:]]*apply_updates" "$f"; then
            sed -i "s/apply_updates[^(\n)]*/apply_updates = yes/" "$f"
            found=true

    # find section and add key = value to it
    elif grep -qs "[[:space:]]*\[commands\]" "$f"; then
            sed -i "/[[:space:]]*\[commands\]/a apply_updates = yes" "$f"
            found=true
    fi
done

# if section not in any file, append section with key = value to FIRST file in files parameter
if ! $found ; then
    file=$(echo "/etc/dnf/automatic.conf" | cut -f1 -d ' ')
    mkdir -p "$(dirname "$file")"
    echo -e "[commands]\napply_updates = yes" >> "$file"
fi
[root@alma ~]#
```

3. Après avoir exécuté tous les scripts de remédiation des tâches échouées, relancez le playbook en utilisant

```
ansible-playbook playbook.yml -u your_user -kK
```

4. Vérifiez le rapport nouvellement créé et voyez si tout est en ordre maintenant, dans mon cas, tout est bon:



Compliance and Scoring

There were no failed or uncertain rules. It seems that no action is necessary.

Rule results

46 passed 1

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	100.000000	100.000000	100%

Rule Overview

pass fail notchecked
fixed error notapplicable
informational unknown

Search through XCCDF rules Search

Group rules by: Default

Title	Severity	Result
Guide to the Secure Configuration of AlmaLinux 9 1x notchecked		
System Settings 1x notchecked		
Installing and Maintaining Software 1x notchecked		
Updating Software 1x notchecked		
Install dnf-automatic Package	medium	pass

Résultat

Le playbook va :

- Installer OpenSCAP pour effectuer des analyses de sécurité.
- Appliquer les recommandations de l'ANSSI en fonction du profil choisi (par exemple, **minimal**, **élevé**, **renforcé**).
- Générer un rapport HTML avec des résultats détaillés concernant l'état de sécurité actuel de votre VM.