Évaluation des paramètres du certificat Configurer le script LUA pour LDAP

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Configuration

Vérifier

Introduction

Ce document décrit comment configurer un script LUA pour détecter les paramètres de certificat que les utilisateurs doivent avoir quand ils essaient de se connecter au VPN.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Centre de gestion du pare-feu sécurisé (FMC)
- Configuration du VPN d'accès à distance (RAVPN)
- Codage de script LUA de base
- Certificats SSL de base
- Politique d'accès dynamique (DAP)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Secure Firewall version 7.7.0
- Secure Firewall Management Center version 7.7.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

DAP est une fonctionnalité puissante qui permet aux administrateurs réseau de définir des politiques de contrôle d'accès granulaires basées sur divers attributs des utilisateurs et des périphériques qui tentent de se connecter au réseau. L'une des fonctionnalités clés de DAP est la possibilité de créer des politiques qui évaluent les certificats numériques installés sur les périphériques clients. Ces certificats servent de méthode sécurisée pour authentifier les utilisateurs et vérifier la conformité des périphériques.

Dans l'interface Cisco Secure FMC, les administrateurs peuvent configurer des stratégies DAP pour évaluer des paramètres de certificat spécifiques tels que :

- Objet
- Émetteur
- Autre nom du sujet
- Numéro de série
- Magasin de certificats

Cependant, les options d'évaluation de certificat disponibles via l'interface utilisateur graphique FMC sont limitées à ces attributs prédéfinis. Cette limitation signifie que si un administrateur veut appliquer des stratégies basées sur des informations de certificat plus détaillées ou personnalisées, telles que des champs spécifiques dans le certificat ou des extensions personnalisées, cela ne peut pas être réalisé en utilisant la configuration DAP standard seule.

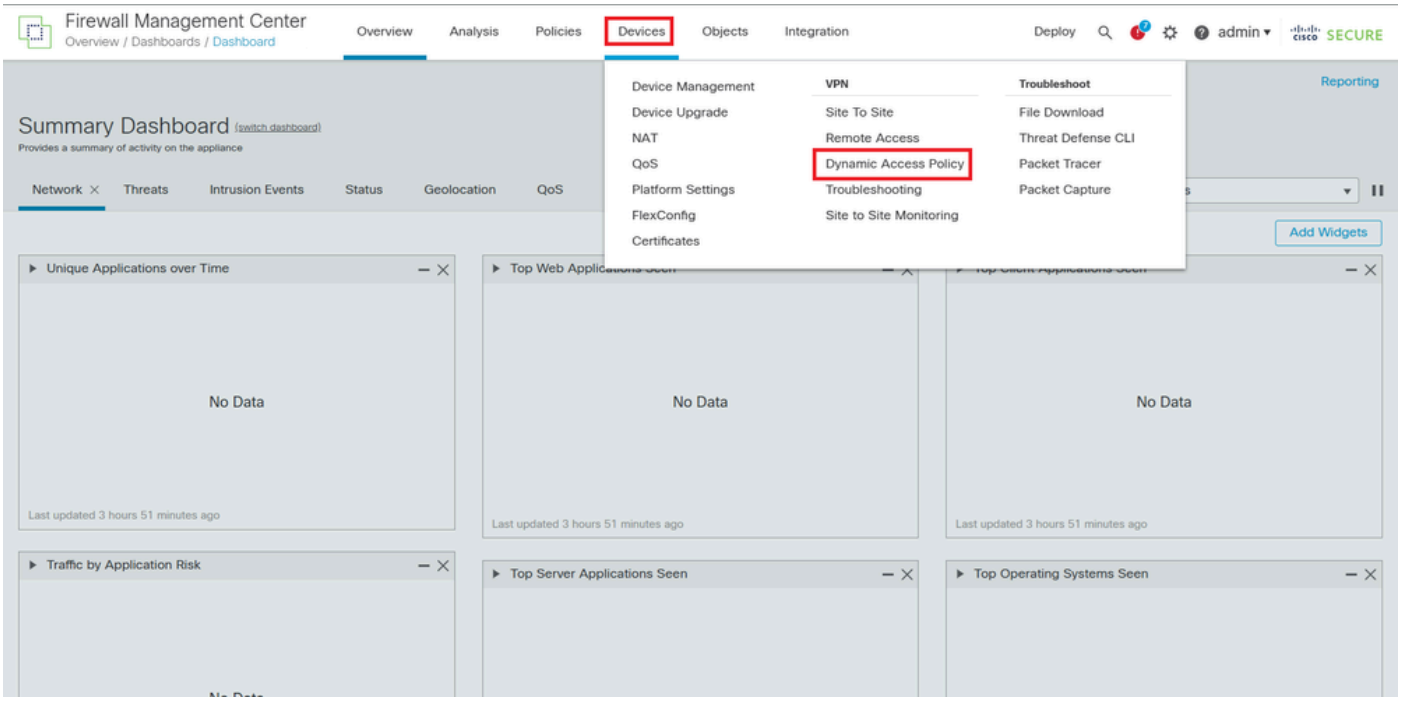
Pour pallier cette limitation, Cisco Secure Firewall prend en charge l'intégration de scripts LUA au sein de DAP. Les scripts LUA offrent la flexibilité d'accéder et d'évaluer des attributs de certificat supplémentaires qui ne sont pas exposés via l'interface FMC. Cette fonctionnalité permet aux administrateurs de mettre en oeuvre des politiques d'accès plus sophistiquées et personnalisées basées sur des données de certificat détaillées.

En exploitant les scripts LUA, il devient possible d'analyser les champs de certificat au-delà des paramètres par défaut, tels que les noms d'organisation, les extensions personnalisées ou d'autres métadonnées de certificat. Cette capacité d'évaluation étendue renforce la sécurité en permettant d'adapter précisément les politiques aux exigences de l'organisation, garantissant que seuls les clients disposant de certificats répondant à des critères précis et détaillés sont autorisés à y accéder.

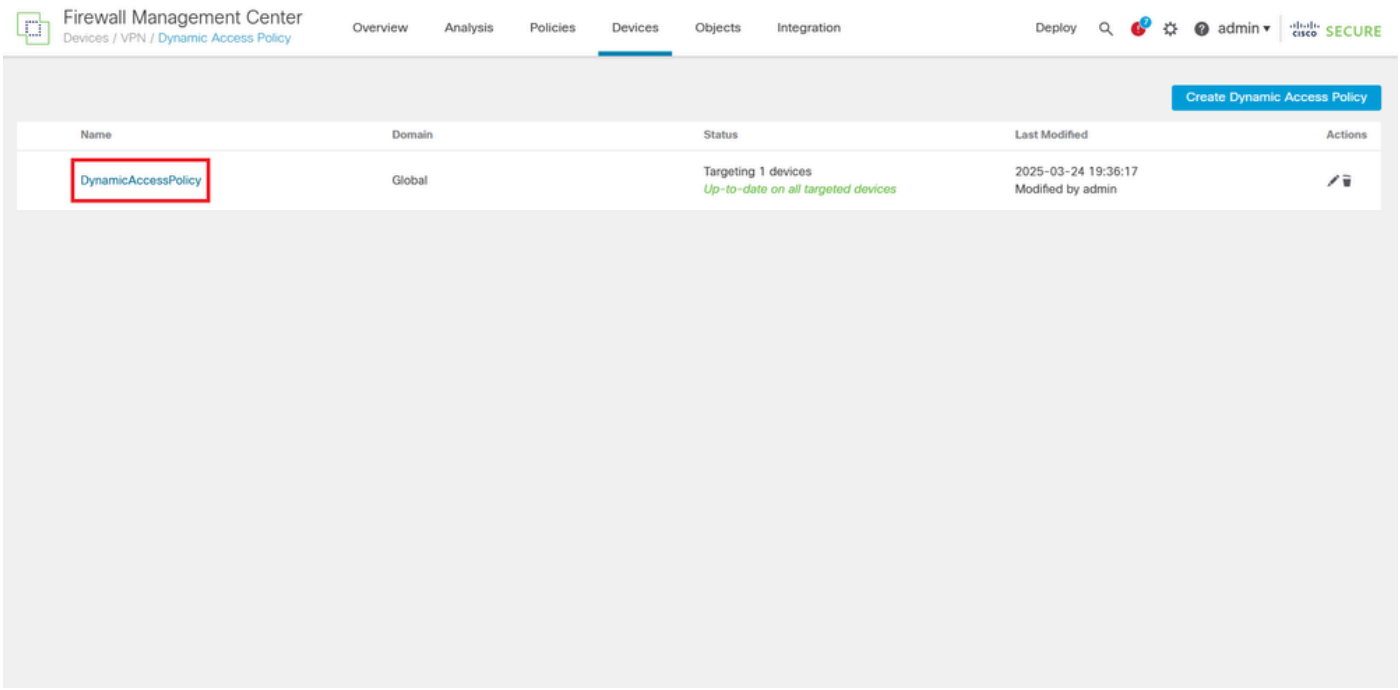
Par conséquent, dans ce document, un script LUA est configuré pour évaluer le paramètre Organization dans un certificat client en exploitant les fonctionnalités de script LUA.

Configuration

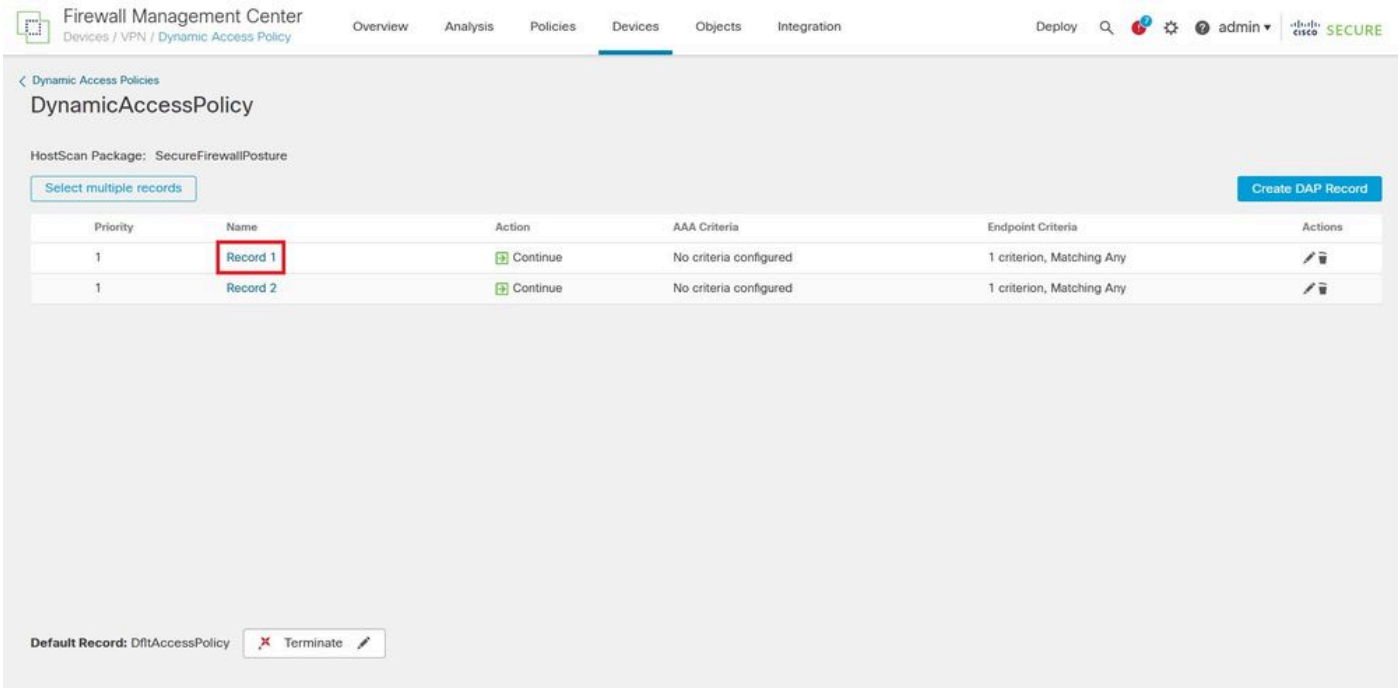
1.Connectez-vous à l'interface utilisateur graphique de FMC, puis, à partir du tableau de bord, accédez à Périphériques > Politique d'accès dynamique dans le menu.



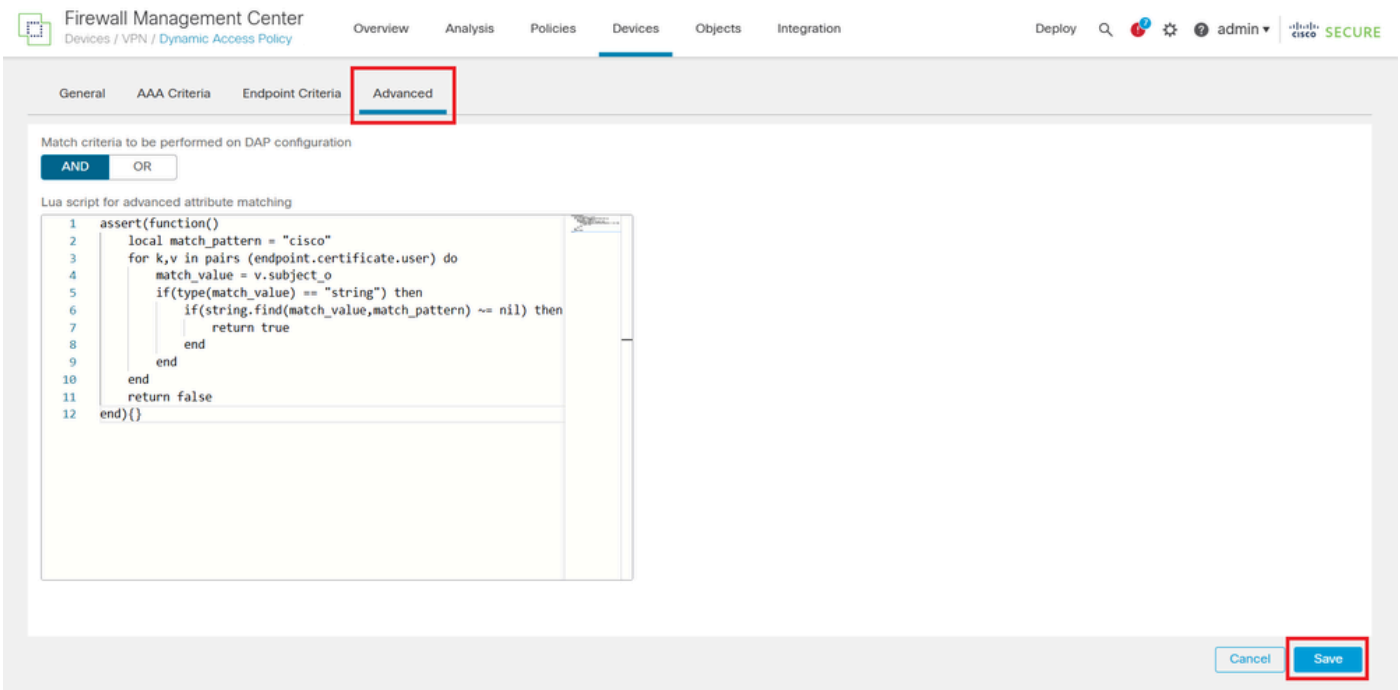
2. Ouvrez la stratégie LDAP appliquée à la configuration RAVPN.



3. Modifiez l'enregistrement souhaité pour configurer le script LUA en cliquant sur le nom de l'enregistrement.



4. Dans l'enregistrement sélectionné, accédez à l'onglet Avancé pour entrer le script LUA qui évalue les paramètres de certificat requis. Après avoir configuré le script, cliquez sur Save pour appliquer les modifications. Une fois les modifications enregistrées dans l'enregistrement DAP, déployez la stratégie pour transmettre la configuration mise à jour au périphérique FTD.



Remarque : Le code présenté dans cet article est conçu pour évaluer les certificats installés sur le périphérique client, en vérifiant spécifiquement qu'il existe un certificat dont le paramètre Organisation dans le champ Objet correspond à la valeur cisco.

<#root>

```
assert(function()
```

```
    local match_pattern = "
cisco
"
    for k,v in pairs (
endpoint.certificate.user
) do
        match_value =
v.subject_o
        if(type(match_value) == "string") then
            if(string.find(match_value,match_pattern) ~= nil) then

return true
            end
        end
    end
    return false
end){}
```

- Le script définit une variable match_pattern définie sur cisco, qui est le nom de l'organisation cible à rechercher.
- Il effectue une itération sur tous les certificats utilisateur disponibles sur le point d'extrémité à l'aide d'une boucle for.
- Pour chaque certificat, il extrait le champ Organisation (subject_o).
- Il vérifie si le champ Organisation est une chaîne, puis recherche le modèle match_pattern dans celui-ci.
- Si une correspondance est trouvée, le script renvoie la valeur true, indiquant que le certificat répond aux critères de stratégie.
- Si aucun certificat correspondant n'est trouvé après la vérification de tous les certificats, le script retourne false, ce qui entraîne le refus de la stratégie d'accès.

Cette approche permet aux administrateurs de mettre en oeuvre une logique de validation de certificat personnalisée au-delà des paramètres standard exposés par l'interface utilisateur graphique du FMC.

Vérifier

Exécutez la commande more dap.xml pour vérifier que le code est présent dans la configuration DAP sur le FTD.

```
<#root>
firepower#
more dap.xml
```

Record 1

and

```
assert(function()
        local match_pattern = "cisco"
        for k,v in pairs (endpoint.certificate.user) do
                match_value = v.subject_o
                if(type(match_value) == "string") then
                        if(string.find(match_value,match_pattern) ~= nil) then
                                return true
                        end
                end
        end
        return false
end) {}
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.