eole-radius - Tâche #34588

Scénario # 33051 (Terminé (Sprint)): Faire un point sur les évolutions Radius intégrées en 2.8.1

point etude

12/09/2022 11:37 - Ludwig Seys

Statut:	Fermé	**Début:**	05/09/2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Ludwig Seys	**% réalisé:**	100%
Version cible:	Prestation Cadoles MEN 2022 36-39	**Temps estimé:**	0.00 heure
		Temps passé:	0.00 heure

Description

Demandes liées:

Lié à eole-radius - Scénario #31641: Gérer l'authentification AD en plus de L...	**Partiellement Réalisé**	06/12/2022	**31/12/2023**
Lié à eole-radius - Scénario #31640: Supprimer le support MD5 (étude pour EOL...	**Partiellement Réalisé**	06/12/2022	**01/01/2024**
Lié à eole-radius - Scénario #31639: Revoir l'option "Mode d'utilisation de F...	**Partiellement Réalisé**	06/12/2022	**31/12/2023**
Lié à eole-radius - Scénario #35809: EOLE 2.10 : refonte de eole-freeradius	**Nouveau**		

Historique

#1 - 12/09/2022 11:37 - Ludwig Seys

- Statut changé de Nouveau à En cours

#2 - 12/09/2022 12:34 - Ludwig Seys

- % réalisé changé de 0 à 90

freeradius

version EOLE :
-2.7
-2.8
-2.9
Attention différence entre les version 2.7 et 2.8
Pas de choix pour le type de protocole en 2.7
=> Il faut ajouter la variable type de protocole d'authentification en 2.8 et 2.9
Pas d'option "Authentifier les comptes utilisateurs sur un annuaire LDAP" en 2.7
=> Il faut ajouter l'option Authentifier les comptes utilisateurs sur un annuaire LDAP en 2.8 et 2.9

ajouter des liens vers la documentation officielle ? (type de protocole et autre ?)

Refaire plusieurs copie d'écran (à mettre à jour) à basculer en écran.unit dans scenari, pour simplifier leurs utilisation.

port par défaut non spécifié dans le chapitre onglet freeradius. ajouter un bloc remarque !
1812 & 1813

Explication à fournir dans la documentation :
-Mode d'utilisation de freeradius.
802.1x & accounting => explication faite dans la documentation

Ajouter un bloc remarque sur l'équivalence entre les deux modes ?

-type de protocole d'authentification.
md5 & tls
ATTENTION : ajouter un paragraphe attention stipulant l'usage exclusive de tls 1.2 !
ATTENTION : ajouter un paragraphe attention stipulant que le mode md5 est obsolète. (liens vers post ?)
extrait :
Il existe plusieurs version de EAP (Extensible Authentication Protocol) dans freeradius : https://wiki.freeradius.org/protocol/EAP

La version historique et la plus basic est la version MD5. Mais ce mode n'est plus considéré comme sécurisé et ne permet pas d'identifier le poste.

La version EAP-TLS permet d'avoir un trafic chiffré entre le client et le serveur mais permet aussi, optionnellement (même si ce n'est pas optionnel dans le cadre de ce scénario), d'identifier le certificat présent sur le poste client.

Pour activer EAP-TLS, mettre "tls" dans la nouvelle variable "Type de protocole d'authentification".

PETIT PLUS :
Pouvoir désactiver l'authentification LDAP
L'authentification LDAP permet de s'assurer que l'utilisateur est autoriser à accéder aux réseaux. Mais si on gère une flotte de machine, l'authentification par clé TLS peut être jugée comme suffisant.

Pour désactiver l'authentification LDAP, désactiver "Authentifier les comptes utilisateurs sur un annuaire LDAP".

fichier de conf :
/etc/freeradius/3.0/radiusd.conf
/etc/freeradius/3.0/clients.conf

module
/etc/freeradius/3.0/mods-available/eap => freerad-eap
/etc/freeradius/3.0/mods-available/ldap => freerad-ldap
/etc/freeradius/3.0/mods-available/mschap => freerad-mschap
/etc/freeradius/3.0/mods-config/files/authorize => freerad-authorize
/etc/freeradius/3.0/mods-config/preprocess/huntgroups => freerad-huntgroups

Partie nginx
/etc/freeradius/3.0/sites-available/default => freerad-default
/etc/freeradius/3.0/sites-available/inner-tunnel => freerad-inner-tunnel

certificats
/etc/freeradius/3.0/certs/ca.cnf source=freerad-ca.cnf
/etc/freeradius/3.0/certs/client-tmpl.cnf source=freerad-client.cnf
/etc/freeradius/3.0/certs/server.cnf source=freerad-server.cnf

depuis genconfig :
Dans authentification en mode normal et expert variable présente pour activer le service.

si activé :
un onglet freeradius apparaît. Variable pour les modes basique/normal/expert, attention l'onglet n'est pas disponible en mode basique, donc pas de documentation en mode basique.

#3 - 14/09/2022 14:36 - Ludwig Seys

- Statut changé de En cours à À valider

- % réalisé changé de 90 à 100

La question qui nous paraît la plus importante est de savoir comment pouvons-nous tester les modifications.
À l'époque, les tests avaient été réalisés sur l'infra de la Savoie qui était à disposition, mais ce n'est plus le cas.

Concernant les demandes :

---

https://dev-eole.ac-dijon.fr/issues/31641

Remarque : il est possible qu'Eap-Ttls ne soit pas compatible avec un mode AD. (donc des tests sont nécessaires pour déterminer la compatibilité entre Eap-Ttls et le mode AD et s'il faut désactiver l'une ou l'autre feature)

ACTION #########

Modification de :
smb.conf
/etc/krb5.conf
/etc/nsswitch.conf
Mise en place de test (code)
code : setfacl -m u:radiusd:rx winbindd_privileged
/mods-available/mschap
/mods-available/eap
/raddb/users
/usr/local/openssl/ssl

Dans la documentation [[https://wiki.freeradius.org/guide/FreeRADIUS-Active-Directory-Integration-HOWTO]], il y a les actions suivantes en plus :

```
Before executing the script, check the following line in the CA.all script

echo "newreq.pem" | /usr/local/openssl/ssl/misc/CA.pl -newca

CA.all is located in the scripts subdirectory of FREERADIUS' source directory. In case of doubt try the comman
d.

find / -name CA.all

When executing CA.all, we produce the 9 following certificates

root.pem, root.p12, root.der
cert-clt.pem, cert-clt.p12, cert-clt.der
cert-srv.pem, cert-srv.p12, cert-srv.der

The server needs the files root.pem and cert.srv.pem in order to work with PEAP.
```

Fin ACTION #########

Il faut faire une étude préliminaire plus poussée pour définir les cas qui fonctionnent et ceux qui ne fonctionnent pas à partir de la documentation et en testant.
Cela permettrait de tester, par exemple, si l'on peut réutiliser nos propres certificats ou non.

---

https://dev-eole.ac-dijon.fr/issues/31640

-Il serait, en effet, opportun de supprimer le mode md5

ACTION #########

Fichiers liés :
26_freeradius.xml
freerad-default (commentaire)
freerad-eap (commentaire)
radius.conf :
condition à modifier lignes 99 à 108

Fin ACTION #########

Estimation : 1 point sous réserve que l'on puisse tester facilement.

-Pour implémenter le mode EAP-TTLS

La différence entre le mode EAP-TLS et le mode EAP-TTLS :

EAP-TLS : Les deux parties ont besoin d'un certificat. Il offre une bonne sécurité et est obligatoire sur tout matériel estampillé WPA ou WPA2.
Un mot de passe compromis n'est pas suffisant pour outre-passer la sécurité car l'attaquant à aussi besoin du certificat du client.

La limitation de EAP-TLS est de nécessiter un certificat coté client, ce qui peut être complexe et coûteux sur un très grand parc. Est alors apparu EAP-TTLS. A-t-on vocation à avoir plus de mille postes en wifi ? Dans un tel cas, une autre solution est généralement mise en place. (portail captif séparé etc..)

EAP-TTLS : D'abord, le serveur est authentifié de manière sécurisée auprès du client via son certificat et optionnellement, le client est authentifié auprès du serveur. Ensuite, le serveur utilise la connexion sécurisée établie "tunnel" pour authentifier le client (par annuaire cette fois-ci par exemple).

Attention, EAP-TTLS n'est pas natif sur de nombreux éléments, notamment Microsoft et cisco.

Estimation : 6 points sous réserve que l'on puisse tester facilement.

Il faut faire en un sens quasi la même quantité de travail que pour EAP-TLS, mais avec une partie de configuration non trouvée pour le moment.

---

https://dev-eole.ac-dijon.fr/issues/31639

Remplacement des deux options de "Mode d'utilisation de FreeRADIUS", soit "accounting" et "802.1x" par :
Une option de type "oui/non" appelée "Activer la gestion des VLAN par groupe"

Nécessite une reprise de toute la génération des fichiers de conf, car celle-ci sont différentes suivant les deux modes. Et nécessite d'avoir une maquette pour pouvoir tester l'hypothèse que les deux modes rendent le même service.

Estimation : Le scénario pourrait être séparé en deux. Une partie proposition et une partie réalisation.

2 points de test/étude/proposition sous réserve que l'on puisse tester facilement.
Détail :

- Valider le fait que les deux modes rendent le même service
- Choisir le mode le plus pertinent, ou faire un mix des deux.
- Définir des variables à renommer, modifier, ou supprimer.
- Estimer le temps nécessaire pour la réalisation.

#4 - 26/09/2022 16:30 - Benjamin Bohard

- Statut changé de À valider à Résolu

#5 - 29/09/2022 15:19 - Joël Cuissinat

- Lié à Scénario #31641: Gérer l'authentification AD en plus de LDAP dans eole-radius (étude pour EOLE 2.10) ajouté

#6 - 29/09/2022 15:20 - Joël Cuissinat

- Lié à Scénario #31640: Supprimer le support MD5 (étude pour EOLE 2.10) ajouté

#7 - 29/09/2022 15:20 - Joël Cuissinat

- Lié à Scénario #31639: Revoir l'option "Mode d'utilisation de FreeRADIUS" (étude pour EOLE 2.10) ajouté

#8 - 29/09/2022 15:21 - Joël Cuissinat

- Statut changé de Résolu à Fermé

- Restant à faire (heures) mis à 0.0

#9 - 12/03/2024 11:44 - Joël Cuissinat

- Lié à Scénario #31639: Revoir l'option "Mode d'utilisation de FreeRADIUS" (étude pour EOLE 2.10) supprimé

#10 - 12/03/2024 11:44 - Joël Cuissinat

- Lié à Scénario #31639: Revoir l'option "Mode d'utilisation de FreeRADIUS" (étude pour EOLE 2.10) ajouté

#11 - 12/03/2024 11:46 - Joël Cuissinat

- Lié à Scénario #35809: EOLE 2.10 : refonte de eole-freeradius ajouté