ASSURMER AP n°8

Présentation du fonctionnement de RADIUS

Date version	Auteur	Validateur	Destinataires	Diffusion document	Nbr. de pages	Commentaires
07/01/25	Maxence MARTIN-PARENT + Antoine Rodrigues	Aucun	Service DSI	Interne via Teams	10	Document intégral

TABLE DES MATIERES

Qu’est-ce que RADIUS ?

RADIUS (Remote Authentication Dial-In User Service) est un protocole réseau utilisé pour fournir des services d'authentification, d'autorisation et de comptabilisation (AAA : Authentication, Authorization, Accounting). Développé initialement pour les connexions d'accès à distance, il est aujourd'hui largement utilisé pour sécuriser les réseaux Wi-Fi et Ethernet, notamment dans les environnements professionnels.

RADIUS permet de centraliser la gestion des identités des utilisateurs et des périphériques, ce qui facilite l'administration et renforce la sécurité.

Les rôles principaux de RADIUS

RADIUS assure trois fonctions clés :

1. **Authentification** : Vérification des informations d'identification (nom d'utilisateur et mot de passe, certificat, etc.) pour confirmer l'identité de l'utilisateur.
2. **Autorisation** : Détermination des droits d'accès de l'utilisateur une fois qu'il est authentifié.
3. **Comptabilisation** : Suivi des activités de l'utilisateur, comme la durée de connexion ou les données échangées.

Le fonctionnement de RADIUS

Le protocole RADIUS s'appuie sur une architecture client-serveur et fonctionne comme suit :

Étape 1 : Demande d'accès

- Un utilisateur ou un périphérique (client) tente de se connecter à un réseau sécurisé (Wi-Fi ou filaire).
- L'accès est médié par un serveur (ici symbolisé par un contrôleur de domaine Active Directory), qui est contacté par le périphérique réseau gérant le réseau demandé par le client, comme un switch ou une borne Wi-Fi. Ici, nous prendrons l'exemple d'une borne Wi-Fi.

Étape 2 : Transmission au serveur RADIUS

- La borne Wi-Fi agit comme un client RADIUS et envoie les informations d'identification de l'utilisateur (nom d'utilisateur, mot de passe ou certificat) au serveur RADIUS via le protocole UDP sur les ports 1812 (authentification et autorisation) et 1813 (comptabilisation).

Étape 3 : Authentification

- Le serveur RADIUS vérifie les informations d'identification en les comparant à une base de données ou un annuaire d'entreprise (comme Active Directory).
- Selon la méthode d'authentification configurée, cela peut inclure une vérification de paires nom d'utilisateur/mot de passe, ou l'utilisation d'EAP (Extensible Authentication Protocol) pour les certificats ou d'autres mécanismes avancés.

Étape 4 : Autorisation

- Si l'utilisateur est authentifié, le serveur RADIUS renvoie une réponse positive (Access-Accept) contenant les droits d'accès spécifiques de l'utilisateur (par exemple, VLAN assigné, bande passante maximale, etc.).
- En cas d'échec, une réponse Access-Reject est envoyée.

Étape 5 : Comptabilisation (facultatif)

- Le NAS peut envoyer des informations au serveur RADIUS sur la session de l'utilisateur (début, fin, durée, données échangées, etc.).

Les composants de RADIUS

Serveur RADIUS

- Centralise la gestion des utilisateurs et des périphériques.
- Logiciels populaires : FreeRADIUS (open-source), Microsoft NPS (Network Policy Server), Aruba ClearPass, etc.

Client RADIUS

- Généralement le point d'accès Wi-Fi, switch ou contrôleur réseau qui relaie les demandes des utilisateurs au serveur.

Base de données ou annuaire

- Le serveur RADIUS interagit avec une base de données ou un annuaire comme Active Directory pour valider les informations d'identification.

Les protocoles d’authentification

RADIUS supporte plusieurs méthodes d'authentification, dont :

- **PAP (Password Authentication Protocol)** : Basique et peu sécurisé.
- **CHAP (Challenge-Handshake Authentication Protocol)** : Plus sécurisé que PAP.
- **EAP (Extensible Authentication Protocol)** : Utilisé dans les réseaux Wi-Fi d'entreprise (WPA2-Enterprise) pour offrir un haut niveau de sécurité. Exemples :
    - **EAP-TLS** : Basé sur les certificats.
    - **PEAP** et **EAP-TTLS** : Basés sur une combinaison de certificats et de mots de passe.

Avantages et limites de RADIUS

Avantages

RADIUS est largement adopté dans les environnements professionnels pour la gestion de l'accès réseau. Voici les principaux avantages qui expliquent son succès :

Centralisation de l'authentification

RADIUS permet de centraliser la gestion des identités et des droits d'accès des utilisateurs dans un point unique, comme un serveur RADIUS relié à une base de données ou un annuaire (par exemple, Active Directory). Cela simplifie la gestion des comptes, surtout dans les environnements complexes avec de nombreux utilisateurs et périphériques.

Sécurité renforcée

En combinaison avec des protocoles modernes comme EAP-TLS ou PEAP (utilisés dans WPA2-Enterprise), RADIUS offre un haut niveau de sécurité en exigeant une authentification forte basée sur des certificats ou des identifiants chiffrés.

Les politiques d'accès granulaires permettent de limiter les droits d'accès en fonction des besoins spécifiques des utilisateurs ou des appareils.

Compatibilité avec les standards

RADIUS est compatible avec de nombreux standards de l'industrie, comme 802.1X, ce qui le rend utilisable dans des environnements variés, aussi bien filaires que sans fil. La majorité des équipements réseau, comme les points d'accès Wi-Fi, les commutateurs ou les routeurs, supporte RADIUS nativement.

Extensibilité

RADIUS peut gérer des milliers d’utilisateurs répartis sur plusieurs sites, ce qui en fait une solution adaptée pour les grandes entreprises et les organisations multinationales. Il peut également être configuré en cluster pour améliorer sa tolérance aux pannes et sa capacité.

Traçabilité et comptabilisation

Grâce à la fonction de comptabilisation, RADIUS permet de suivre les connexions des utilisateurs et leurs activités réseau (temps de connexion, volume de données échangées, etc.). Cela offre une visibilité importante pour le contrôle et l’audit.

Limites

Bien que RADIUS soit largement utilisé et efficace, il présente certaines limites qu'il est important de connaître pour évaluer son utilisation dans un réseau :

Protocole ancien

Conçu dans les années 1990, RADIUS n'a pas été initialement pensé pour les environnements modernes où les besoins en cybersécurité sont plus complexes. Bien que des mises à jour aient été apportées, certaines limitations structurelles demeurent.

Sécurité des communications

Les échanges entre le client RADIUS (NAS) et le serveur RADIUS utilisent le protocole UDP, qui est moins sécurisé que TCP en raison de l'absence de mécanismes de contrôle d'intégrité natifs.

Bien que les informations d'identification soient souvent encapsulées dans des protocoles sécurisés (comme EAP-TLS), certains champs de communication, comme les attributs d'autorisation, peuvent être vulnérables.

Manque de chiffrement complet

RADIUS chiffre uniquement le mot de passe de l'utilisateur dans les communications, laissant les autres champs (comme le nom d'utilisateur ou les informations d'autorisation) en texte clair. Cela peut exposer ces données à des attaques si le trafic n'est pas protégé par un tunnel sécurisé (comme IPsec ou TLS).

Problèmes de scalabilité

Dans les très grandes infrastructures, avec un trafic RADIUS intense, le protocole peut montrer des signes de faiblesse. La gestion d'un grand nombre de requêtes simultanées peut nécessiter une architecture renforcée avec plusieurs serveurs RADIUS en cluster.

Complexité de configuration et de maintenance

La mise en place et l'administration de RADIUS peuvent être complexes, notamment dans des environnements où des mécanismes d'authentification avancés (comme EAP-TLS) sont utilisés. Cela nécessite des connaissances approfondies sur les certificats, les politiques d'accès et l'intégration avec des bases de données ou annuaires.

Limites de compatibilité

Certaines implémentations spécifiques de RADIUS ou de ses extensions peuvent ne pas être totalement interopérables avec des solutions tierces. Cela peut poser problème dans des environnements hétérogènes.

Conclusion

RADIUS est un protocole incontournable dans la sécurisation des accès réseau grâce à sa capacité à centraliser l'authentification, l'autorisation et la comptabilisation des utilisateurs. Il s'intègre parfaitement dans des infrastructures modernes en offrant des mécanismes de contrôle précis et une compatibilité avec des standards largement utilisés, comme 802.1X. Ses avantages, notamment la centralisation, la sécurité renforcée et la traçabilité, en font une solution adaptée aux entreprises de toutes tailles. Cependant, ses limites, telles que l'absence de chiffrement complet ou sa complexité de mise en œuvre, soulignent l'importance de l'associer à des technologies complémentaires, comme le WPA2-Enterprise ou les tunnels sécurisés, pour pallier ses faiblesses. Ainsi, RADIUS reste une solution fiable et éprouvée, indispensable pour gérer les accès dans un réseau d'entreprise en quête de performance et de sécurité.