

PRESENTATION DU FONCTIONNEMENT D'UNE SOLUTION RADIUS ET DES CERTIFICATS

ASSURMER

Montpellier, Occitanie, France

Ezequiel-junior VARELA-
MONTEIRO

Kévin BOULIER

SISR 2B



PARTENAIRE
OFFICIEL

Version	Date version	Auteur	Validateur et date	Destinataires	Diffusion document	Nbr. de pages	Commentaires
1	14/01/24	Ezequiel-junior VARELA MONTEIRO	Aucun	Service DSI	Interne via Teams	5	

Table des matières

Introduction.	3
Fonctionnement d'une solution RADIUS.	3
Les éléments fondamentaux d'une solution RADIUS.	4
Le rôle et l'importance des certificats.	
Avantages d'une solution RADIUS avec certificats.	4
Conclusion.	4

Introduction

Le protocole RADIUS (Remote Authentication Dial-In User Service) constitue une solution centralisée idéale pour gérer efficacement l'authentification, l'autorisation et le suivi des utilisateurs au sein d'un réseau. Il joue un rôle crucial dans la sécurisation des accès WIFI en offrant une gestion granulaire et centralisée des connexions réseau.

Dans ce contexte, les certificats sont essentiels pour garantir l'authenticité des échanges entre les utilisateurs, les points d'accès et le serveur d'authentification. Ils assurent un niveau de confiance élevé et une communication sécurisée.

Fonctionnement d'une solution RADIUS

Le fonctionnement d'un serveur RADIUS repose sur trois volets principaux :

L'**authentification centralisée** est le premier point de contact. Lorsqu'un utilisateur tente de se connecter au réseau WIFI, ses informations d'identification sont transmises au serveur RADIUS via le point d'accès. Celui-ci vérifie ces informations (souvent un nom d'utilisateur et un mot de passe ou un certificat) en les comparant à une base de données centralisée, comme Active Directory ou LDAP. Si les informations sont correctes, l'accès est autorisé.

Le second volet est l'**autorisation**. Une fois authentifié, l'utilisateur se voit attribuer des permissions spécifiques en fonction de son profil. Par exemple, un employé peut obtenir un accès complet à l'intranet de l'entreprise, tandis qu'un invité pourrait se limiter à une navigation internet basique.

Enfin, la **comptabilisation** permet de tracer les connexions des utilisateurs. Le serveur RADIUS peut consigner des informations telles que la durée de connexion ou l'utilisation des ressources réseau. Ce suivi offre une vue d'ensemble précieuse pour l'administration réseau.

Les éléments fondamentaux d'une solution RADIUS

Une solution RADIUS repose sur plusieurs composants essentiels. Le serveur RADIUS lui-même, qui peut être déployé sur des plateformes variées comme Windows Server (via NPS) ou Linux (avec FreeRADIUS), constitue le cœur de la solution. Il interagit directement avec les bases de données d'utilisateurs pour valider les connexions.

Les points d'accès WIFI jouent également un rôle crucial en acheminant les demandes d'authentification vers le serveur. Ces points d'accès doivent être configurés pour fonctionner harmonieusement avec le serveur RADIUS, en respectant des protocoles comme EAP (Extensible Authentication Protocol) pour garantir des échanges sécurisés.

La base de données des utilisateurs, souvent intégrée à un annuaire tel qu'Active Directory, contient les informations nécessaires à l'authentification. Elle constitue une référence fiable pour le serveur RADIUS.

Le rôle et l'importance des certificats

Dans un environnement RADIUS, les certificats jouent un rôle clé en matière de sécurité et de fiabilité. Ils permettent avant tout de sécuriser les communications. Grâce au chiffrement, ils empêchent toute tentative d'interception des données échangées entre les utilisateurs et le serveur.

Les certificats garantissent également une authentification mutuelle. Le client, lors de la connexion, vérifie que le certificat du serveur est valide, confirmant ainsi qu'il interagit avec un serveur légitime. Dans des scénarios avancés, le serveur peut exiger un certificat client, renforçant davantage la sécurité.

La gestion des certificats repose sur une autorité de certification (AC). Celle-ci est responsable de la génération et de la validation des certificats, qu'il s'agisse de certificats serveur ou client. Le certificat serveur est essentiel pour identifier le serveur RADIUS, tandis que le certificat client (optionnel) offre une couche supplémentaire de sécurité pour les utilisateurs.

Avantages d'une solution RADIUS avec certificats

Une solution RADIUS couplée à l'utilisation de certificats offre des avantages significatifs. Elle garantit une sécurité renforcée en minimisant les risques d'usurpation d'identité ou d'interception des données. De plus, elle centralise la gestion des utilisateurs, simplifiant ainsi l'administration réseau.

Cette solution se distingue par sa flexibilité, car elle est compatible avec une grande variété d'appareils et de systèmes. Enfin, elle favorise une traçabilité précise des connexions grâce aux journaux générés par le serveur RADIUS, offrant un suivi détaillé des activités réseau.

Conclusion

L'intégration d'une solution RADIUS associée à l'utilisation de certificats constitue une réponse robuste aux besoins croissants de sécurisation des réseaux WIFI en entreprise. En centralisant l'authentification et en renforçant la sécurité des échanges grâce aux certificats, cette approche garantit une protection optimale des données et une gestion efficace des accès utilisateurs.