AP 8 : PRÉSENTATION DU PROTOCOLE RADIUS	HUYNH Michael SAKO Bah FRANÇAIS Benjamin 2B-SISR

ASSURMER

Version	Auteur	Date	Nombre de pages	À l'attention de	Mode de diffusion	Validateur
1.0	HUYNH Michael	08/01/2025	7	Assurmer-IT	Document PDF	Aucun

PRÉSENTATION DU PROTOCOLE RADIUS

Table des matières

1. **Introduction au protocole RADIUS…….. 3**
2. **Fonctionnement du protocole RADIUS…….. 4**
3. **Rôle des certificats RADIUS…….. 5**
4. **Avantages du protocole RADIUS…….. 6**
5. **Webographie…….. 7**

Introduction au protocole RADIUS

Le protocole RADIUS (*Remote Authentication Dial-In User Service*), développé initialement par Livingston Enterprises en 1991, est aujourd'hui une solution standardisée pour la gestion de la sécurité dans les réseaux informatiques.
Conçu pour gérer de manière centralisée trois fonctions essentielles : authentification, autorisation et comptabilité. Il est particulièrement adapté aux environnements nécessitant une gestion stricte des accès réseau.

Dans un contexte où les réseaux Wi-Fi sont devenus omniprésents, RADIUS joue un rôle fondamental en assurant une gestion sécurisée des connexions. Chaque tentative d'accès au réseau passe par une vérification systématique des identifiants de l'utilisateur ou certificats numériques, garantissant ainsi que seuls les utilisateurs autorisés peuvent accéder aux ressources sensibles. Cette vérification est souvent à l'Active Directory ou le LDAP, pour une gestion cohérente des droits d'accès.

Enfin, RADIUS ne se limite pas à la gestion des accès Wi-Fi. Il est également utilisé dans d'autres contextes, tels que l'accès VPN, les solutions d'accès distant ou encore les environnements multi-sites. Sa flexibilité et son interopérabilité avec une grande variété de systèmes et de périphériques en font un choix privilégié pour les entreprises souhaitant renforcer leur posture de sécurité.

Fonctionnement du protocole RADIUS

Comme indiqué dans l'introduction, le protocole RADIUS est une solution centralisée qui assure trois fonctions principales au sein des réseaux informatiques :

Authentification centralisée

Le processus d'authentification est le suivant : lorsqu'un utilisateur tente de se connecter à un réseau, ses informations d'identification ou son certificat numérique sont transmises par le client RADIUS (par exemple, un point d'accès Wi-Fi) au serveur RADIUS. Ce dernier vérifie ces informations en les comparant à une base de données centralisée comme l'Active Directory ou le LDAP. Si les informations sont correctes, le serveur envoie une réponse positive, autorisant ainsi l'accès de l'utilisateur au réseau.

Autorisation

Puis l'attribution des permissions se fait après l'authentification. Le serveur RADIUS détermine les droits d'accès de l'utilisateur en fonction de son profil. Par exemple, un employé peut obtenir un accès complet aux ressources internes de l'entreprise, tandis qu'un invité peut être restreint à une simple connexion internet. Ces autorisations sont définies par des attributs spécifiques renvoyés au client RADIUS, qui applique ensuite les restrictions appropriées.

Comptabilisation

Enfin il y a le suivi des connexions grâce au serveur RADIUS qui peut enregistrer des informations détaillées sur chaque session utilisateur, telles que l'heure de début et de fin de la connexion, la durée, le volume de données transférées, et les ressources réseau utilisées. Ces données sont précieuses pour l'administration réseau, permettant une surveillance efficace, une facturation précise, et une analyse des usages pour optimiser les performances du réseau.

Rôle des certificats RADIUS

Ensuite les certificats numériques jouent un rôle crucial dans la sécurisation des communications entre les clients, les points d'accès et le serveur RADIUS.

Sécurisation des communications

Les certificats permettent d'établir des connexions chiffrées, protégeant ainsi les données échangées contre les interceptions et les écoutes non autorisées. L'utilisation de protocoles tels que EAP-TLS (*Extensible Authentication Protocol - Transport Layer Security*) assure une authentification forte basée sur des certificats, renforçant la sécurité globale du réseau.

Authentification mutuelle

Grâce aux certificats, le client peut vérifier l'authenticité du serveur RADIUS, et vice versa. Cette authentification bidirectionnelle garantit que les deux parties impliquées dans la communication sont légitimes, empêchant ainsi les attaques de type usurpation d'identité ou *man-in-the-middle*.

Gestion des certificats

La mise en place et la gestion des certificats reposent sur une Autorité de Certification (AC), responsable de l'émission, de la distribution et de la révocation des certificats pour les serveurs et les clients. Une gestion efficace des certificats est essentielle pour maintenir un haut niveau de sécurité et assurer la confiance dans les communications réseau.

Avantages du protocole RADIUS

Avantage	Description
Sécurité renforcée	- Authentification robuste grâce aux certificats numériques. - Chiffrement des communications pour protéger les données sensibles.
Gestion centralisée des accès	- Administration simplifiée via une authentification et une autorisation centralisées. - Contrôle unifié des politiques de sécurité.
Flexibilité et compatibilité	- Support de multiples appareils et systèmes d'exploitation. - Prise en charge de diverses méthodes d'authentification.
Traçabilité et audit	- Suivi détaillé des connexions et des activités des utilisateurs. - Facilitation des audits de sécurité et de la conformité.

Webographie

RCDevs - Protocole RADIUS

Cisco - Fonctionnement RADIUS

Fortinet - Protocole RADIUS

IGM université - RADIUS

IFSA - Fonctionnement RADIUS

MonoDefense