THEME : AUDIT

TRACABILITE DES ACCÈS ET DES ACTIONS

SOMMAIRE

1. INTRODUCTION
2. ETUDE COMPARATIVE DES AUDITES SOUS WINDOWS ET SOUS LINUX
3. Sous Windows

-Web

-Dns

-Ssh

1. Sous Linux.

-Web

-Dns

-Ssh

1. ETUDE COMPARATIVE ADDS (windows) ET LDAP (linux)

1. AD (windows)

2. LDAP (linux)

1. ETUDE COMPARATIVE
2. DIFFÉRENCE
3. AVANTAGES ET INCONVÉNIENTS DE L’AUDIT

1.AVANTAGES

2.INCONVÉNIENTS

1. CONCLUSION
2. INTRODUCTION
3. ETUDE COMPARATIVE DES AUDITES SOUS WINDOWS ET SOUS LINUX
4. Sous Windows

-Web

-Dns

-Ssh

1. Sous Linux.

-Web

-Dns

-Ssh

1. ETUDE COMPARATIVE AD (windows) ET LDAP (linux)
2. AD (windows)

Active Directory, AD en abrégé, est un serveur d'annuaire développé par Microsoft qui permet de stocker des informations de service d'annuaire telles que les utilisateurs et les appareils dans une base de données centralisée et hiérarchique. AD est livré avec de nombreux services tels que l'authentification, les politiques d'accès et la gestion des groupes.

1. LDAP (linux)

Le protocole LDAP (Lightweight Directory Access Protocol) est un protocole que les applications peuvent utiliser pour communiquer avec des services d'annuaire tels qu'Active Directory. Le protocole LDAP interroge les informations de l'utilisateur pour les lire, les modifier ou les mettre à jour.

1. ETUDE COMPARATIVE

LDAP et Active Directory sont deux termes courants dans la gestion des identités et des accès (IAM). Certaines personnes les utilisent de manière interchangeable. Néanmoins, ce n'est pas la même chose. Alors qu'Active Directory est un serveur d'annuaire qui stocke des informations sur les utilisateurs telles que les noms d'utilisateur, les numéros de téléphone et les adresses e-mail, LDAP est un protocole qui permet de lire et de modifier ces informations. Vous pouvez également utiliser LDAP pour authentifier les utilisateurs à l'aide de l'opération Bind. Bien que LDAP soit le protocole principal derrière Active Directory, vous pouvez utiliser LDAP pour interroger n'importe quelle autre base de données d'annuaire qui le prend en charge, par exemple, OpenLDAP et FreeIPA

1. DIFFERENCE

La principale différence entre Active Directory et LDAP est qu'Active Directory est une base de données de services d'annuaire, tandis que LDAP est un protocole qui lui parle.

|  |  |  |
| --- | --- | --- |
|  | **LDAP** | **AD** |
| **Nom et prénom** | Protocole d'accès à l'annuaire léger | Active Directory |
| **Fonction** | Protocole | Fournisseur de services d'annuaire (serveur d'annuaire) |
| **Standard** | Open source | Propriétaire |
| **Systèmes pris en charge** | Multiplateforme : Windows, Linux, macOS | Pour les utilisateurs et les applications Windows |
| **Utilisation principale** | Interrogation et modification d'éléments dans les fournisseurs de services d'annuaire | Fournir l'authentification, les politiques, la gestion des groupes et des utilisateurs, et de nombreux autres services sous la forme d'une base de données d'annuaire |

Des abréviations telles que LDAP et AD peuvent ne pas vous en dire beaucoup sur ces technologies. Cependant, les noms complets contiennent déjà un indice. LDAP est l'abréviation de Lightweight Directory Access Protocol. Le nom complet indique clairement que LDAP est un protocole léger que vous pouvez utiliser pour accéder à un répertoire. Un répertoire comme Active Directory. AD et LDAP ont des fonctions différentes. LDAP est un protocole. Active Directory est un serveur d'annuaire. LDAP est une norme ouverte multiplateforme, mais Active Directory est le logiciel propriétaire de Microsoft destiné aux utilisateurs et aux applications Windows.

L'utilisation principale de LDAP est d'interroger et de modifier les serveurs d'annuaire. D'autre part, l'utilisation principale d'Active Directory est de stocker les informations utilisateur, de fournir une authentification et de permettre aux administrateurs de gérer les groupes, les utilisateurs et les stratégies.

1. AVANTAGES ET INCONVÉNIENTS DE L’AUDIT

1.AVANTAGES

* **Réduction des risques**

La réduction des risques est l’avantage le plus important et le plus significatif d’un audit informatique. Un audit réussi de l’informatique de votre entreprise permettra d’identifier et d’évaluer les risques auxquels votre informatique est confrontée, et de formuler des recommandations sur les mesures à prendre pour atténuer ou traiter ces risques.

* **Renforcer les contrôles**

Un audit informatique vous donne la possibilité de renforcer vos contrôles internes et d’améliorer votre sécurité externe, rendant ainsi votre organisation

Plus sûre et plus résiliente face aux menaces et aux vulnérabilités internes et externes.

* **Se conformer à la réglementation**

La conformité aux réglementations peut être l’un des éléments les plus complexes et les plus difficiles à gérer pour un département informatique, notamment en raison de la diversité des réglementations et des organismes de réglementation à prendre en compte. Un audit informatique est une partie essentielle dSu processus de conformité, garantissant que les exigences de ces réglementations sont pleinement comprises et respectées.

* **Faciliter la communication**

Les canaux de communication entre le département informatique et le reste de l’organisation ne sont souvent pas aussi efficaces qu’ils le devraient. L’un des principaux avantages d’un audit informatique est d’ouvrir ces canaux et de faciliter une meilleure communication entre le département informatique et l’ensemble de l’entreprise.

* **Améliorer l’efficacité**

La gouvernance informatique relève de la compétence des dirigeants et du conseil d’administration et vise essentiellement à s’assurer que l’informatique contribue à l’orientation stratégique permanente et aux objectifs déclarés d’une organisation. En identifiant et en réduisant les risques et en renforçant les contrôles internes, l’audit informatique contribue à améliorer la gouvernance du département informatique.

* **Aide à atténuer les risques**

Les audits réduisent les chances ou les risques de se produire dans une entreprise. Grâce à l’examen minutieux du système informatique de l’entreprise, à la mise en place d’un pare-feu efficace et à de nombreux autres dispositifs de sécurité informatique, la réalisation d’un audit informatique réduit les risques encourus par une organisation, car l’audit met en évidence les forces et les faiblesses du système informatique d’une entreprise donnée

3. INCONVÉNIENTS

Perte en productivité

Faible implémentation en sécurité

Donner de la valeur à votre infrastructure informatique

Ne pas etre en vigueur avec les lois

V. CONCLUSION

L’évolution des systèmes informatiques étant de plus en plus nécessaire et fréquente, l’audit informatique apparaît essentiel dans l’entreprise d’aujourd’hui

D’une part, choisir de le faire réaliser pour ses propres besoins devrait être une évidence dans l’objectif de rester performant et compétitif. Bien qu’il puisse s’avérer coûteux, il permet de prendre du recul sur son environnement tout en gardant une vision exhaustive, innovante et pragmatique du ou des métiers exercés.

D’autres part, il demeure la solution la plus sûre pour engager une relation commerciale avec partenaires, des fournisseurs et des clients.