Mise en place d'un contrôleur de domaine (AD DS) pour la gestion d'accès aux données dans l'entreprise de domaine Virgin.ca

Elhadji Abdoulaye Diankha, étudiant en maitrise technologie de l'information à l'uqo.

1. INTRODUCTION

La gestion des accès aux ressources réseau est un enjeu crucial pour les entreprises, notamment dans un contexte où la sécurité et l'efficacité des systèmes d'information sont primordiales. Ce rapport traite de la mise en place d'un contrôleur de domaine (Active Directory Domain Services - AD DS) pour l'entreprise Virgin.ca, permettant une administration centralisée des utilisateurs, des machines et des droits d'accès.
L'objectif est de configurer un environnement réseau composé de deux machines :

- Une **machine serveur** promue en contrôleur de domaine (administrateur).
- Une **machine utilisateur** jointe au domaine pour bénéficier des services AD DS.

Nous aborderons les étapes techniques (adressage IP, promotion du serveur, création d'utilisateurs, gestion des groupes et partages), ainsi qu'une analyse comparative avec des approches existantes en contrôle d'accès basé sur les rôles (RBAC).

2. PRÉSENTATION DU SUJET ET SON IMPORTANCE

A. Contexte :

Les services **AD DS** de Microsoft permettent de centraliser la gestion des identités et des ressources réseau via :

- **Authentification unique** (Single Sign-On).
- **Gestion des stratégies de groupe** (Single Sign-On).
- **Authentification unique** (Single Sign-On).

Sujet :
La configuration d'un contrôleur de domaine AD DS pour Virgin.ca vise à :

- Centraliser la gestion des utilisateurs (administrateurs et clients).
- Implémenter une authentification unique (SSO).
- Attribuer des droits d'accès via des groupes (IT, RH).

Importance :

- **Sécurité :** Contrôle granulaire des accès (ex : restriction des installations logicielles pour les utilisateurs standards).
- **Efficacité :** Simplification de l'administration via des outils comme Utilisateurs et ordinateurs Active Directory.
- **Audit :** Traçabilité des accès aux ressources partagées (dossiers IT, RH, Notes).

3. REVUE DE LA LITTÉRATURE

A. Références clés

- **[1] Sandhu et al. (1996) :** Modèle RBAC fondateur, appliqué ici via les groupes AD.
- **[2] Microsoft (2012) :** Bonnes pratiques pour les niveaux fonctionnels AD (Windows Server 2012 R2).
- **[3] Bertino et al. (2001) :** Sécurité des flux de données en environnement domaine.

B. Comparaison avec les travaux existants

- **Similarités :** Utilisation des groupes pour attribuer des rôles (ex : IT = droits complets sur le dossier IT).
- **Différences :** Implémentation spécifique avec AD DS et intégration de stratégies horaires.

C. Synthèse

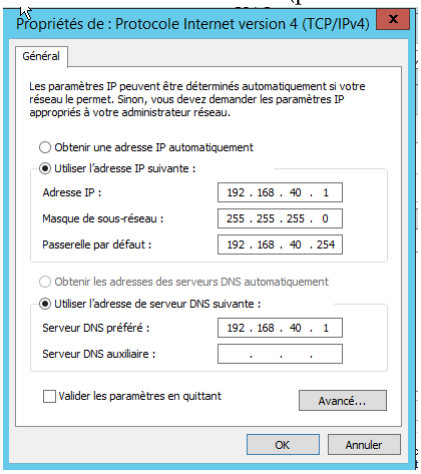
- Ces travaux soulignent l'importance de l'AD DS pour implémenter l'RBAC, aligné avec notre configuration de groupes IT/RH et de partage de dossiers.

4. MÉTHODOLOGIE DÉTAILLÉE

A. Adressage IP et configuration réseau

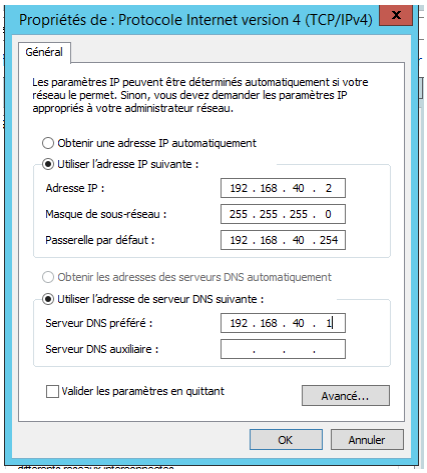
Serveur :

- **IP :** 192.168.40.1 (Classe C), masque 255.255.255.0.
- **DNS :** Auto-référencé (192.168.40.1).
- **Passerelle :** 192.168.40.254 (pour la communication externe).



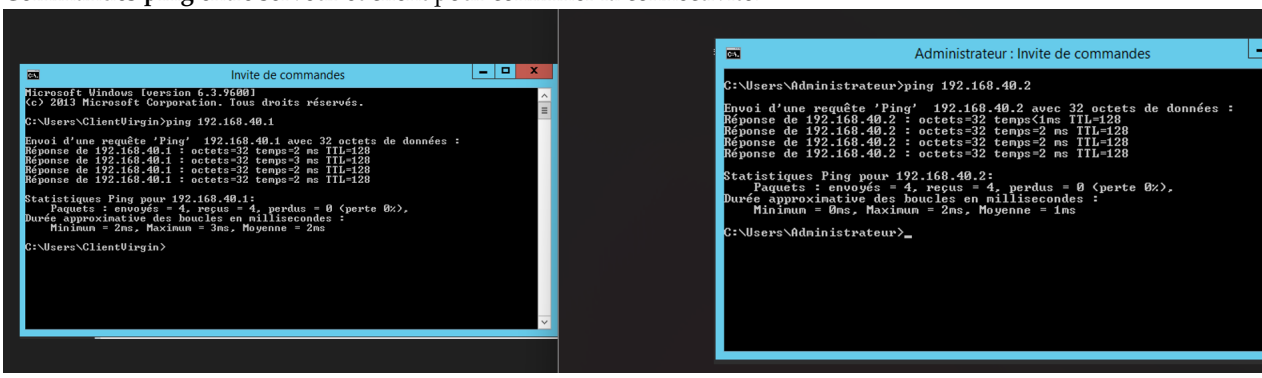
Client :

- **IP :** 192.168.40.2, même masque et passerelle.
- **DNS :** Pointé vers le serveur.



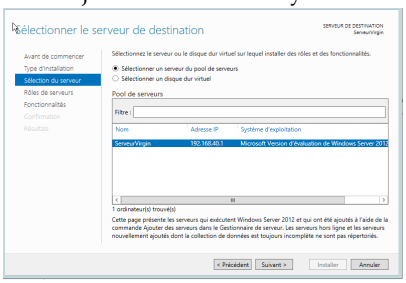
Vérification :

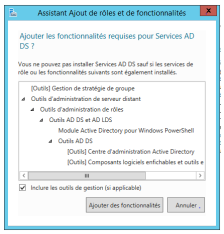
- Commandes **ping** entre serveur et client pour confirmer la connectivité.

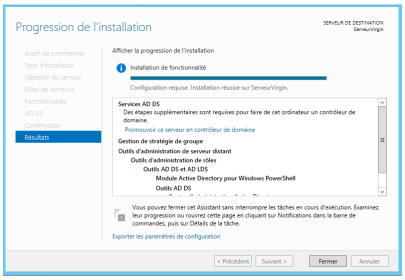


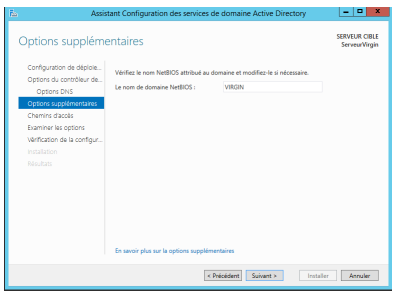
B. Configuration active directory dans la machine serveur

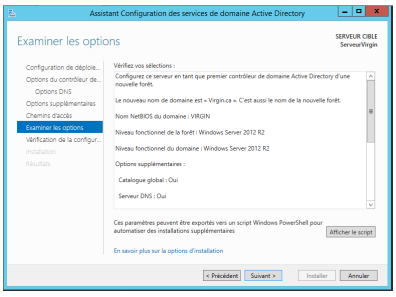
Pour conjurer active directory dans la machine serveur les étapes suivantes ont été effectués:

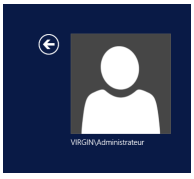












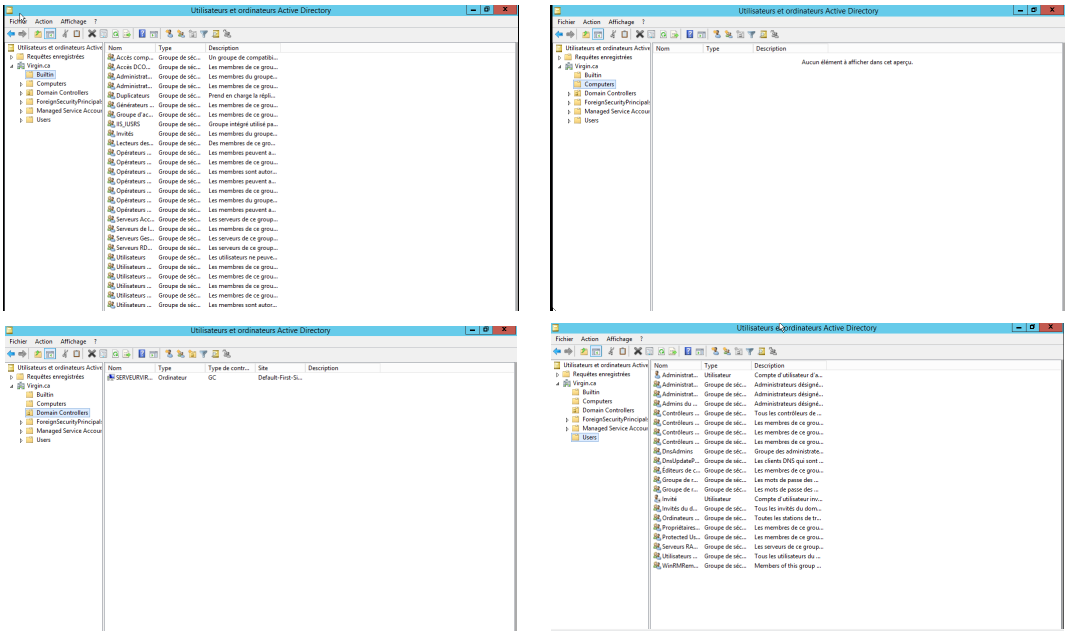
- **Nom de domaine :** Virgin.ca.
- **Niveaux fonctionnels :** Forêt et Domaine en Windows Server 2012 R2.
- **Mot de passe DSRM** (ex : P@ssw0rd123).

Après configuration nous avons lancé l'outil permettant à la machine serveur de faire l'administration cet outil s'appelle Utilisateurs et ordinateurs Active Directory. Cet outil possède une interface permettant à l'administrateur de gérer le réseau dans le serveur .

C. Présentation de l'interface d'administration AD DS

Sur cette interface est représenté le domaine du réseau nommé Virgin.ca. Dans ce domaine est représenté plusieurs conteneur :

- **Builtin :** Groupes système (ex : Administrateurs).
- **Computers :** Machines jointes au domaine (ex : ClientVirgin). Dans le conteneur Computer nous aurons toutes les machines qui viendront joindre le domaine pour le moment nous avons rien dedans parce que à l'instant T aucune machine n'a joint le domaine du réseau.
- **Domain Controllers :** Contrôleurs de domaine (ex : ServeurVirgin). Dans le conteneur Domain Controllers sont représentés les contrôleurs de domaine, raison pour laquelle notre machine serveur appelée serveurVirgin y est affichée.
- **Users:** Dans le conteneur Users nous aurons toutes les comptes d'utilisateurs administrateur et système tout ceci pour être capable d'administrer ces comptes .

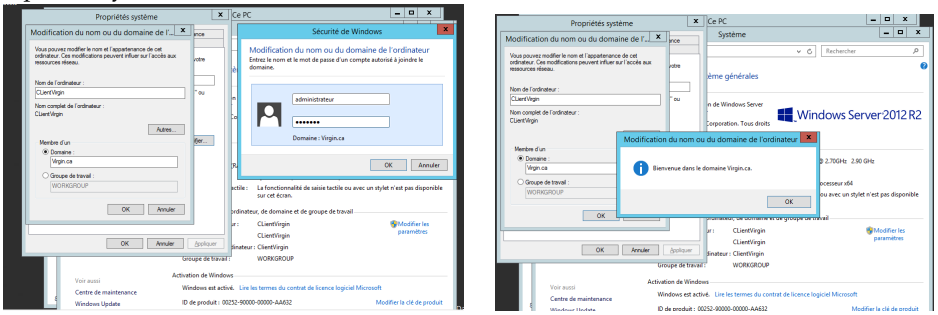


Après avoir fini de configurer le contrôleur de domaine, la prochaine étape serait donc de joindre toutes les machines au domaine pour permettre à la machine serveur de pouvoir les reconnaître afin de pouvoir les gérer.

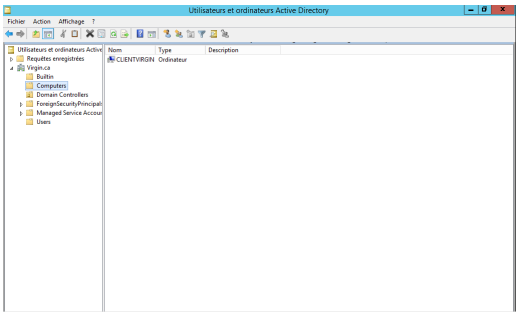
D. Jonction au domaine

D.1. Exemple d'une machine utilisateur qui rejoint le domaine Virgin.ca via :

- Propriétés système > Modifier le domaine, avec authentification administrateur.



D.2. Validation dans Utilisateurs et ordinateurs Active Directory > Conteneur Computers.



Une fois la jonction des machines au domaine est réalisée lorsque l'on partent dans la machine serveur tout en actualisant l'outil Utilisateurs et ordinateurs Active Directory nous verrons dans le conteneur computers du domaine Virgin.ca la jonction du machine Clientvirgin qui s'est bien fait et prêt pour être administrer par le contrôleur de domaine ou machine serveur . Essayons de créer une autre machine client depuis le contrôleur de domaine pour avoir au moins deux machines à administrer .

E. Création des utilisateurs et groupes

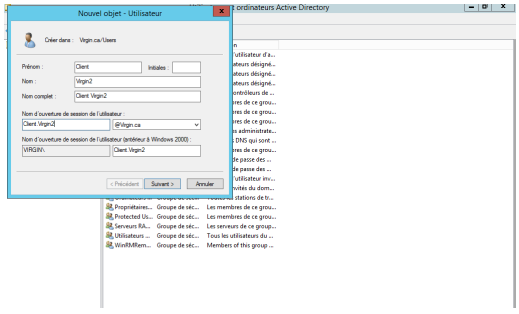
E.1. Utilisateurs :

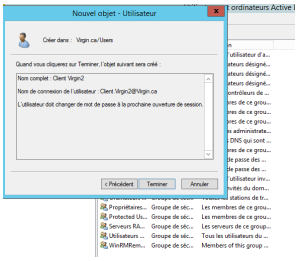
- **ClientVirgin1** (Membre du groupe IT).
- **ClientVirgin2** (Membre du groupe RH).

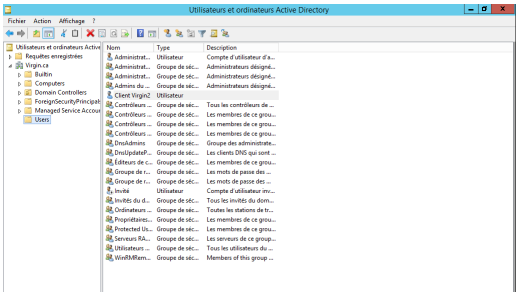
E.2. Stratégies :

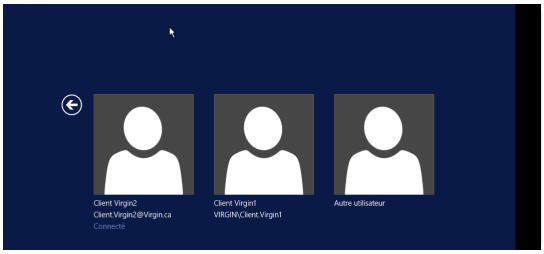
- Restrictions par défaut (groupe "Utilisateurs du domaine").
- Horaires d'accès et tentatives de connexion limitées.

E.3. Pratique concernant la création d'utilisateur :

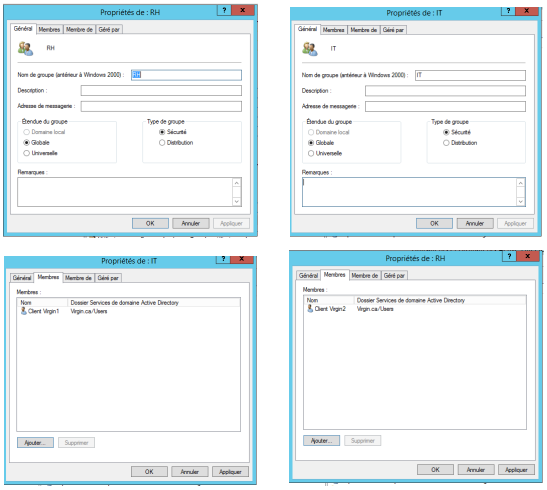








E.4. Pratique concernant la création et laffectation d'un groupe à un utilisateur :

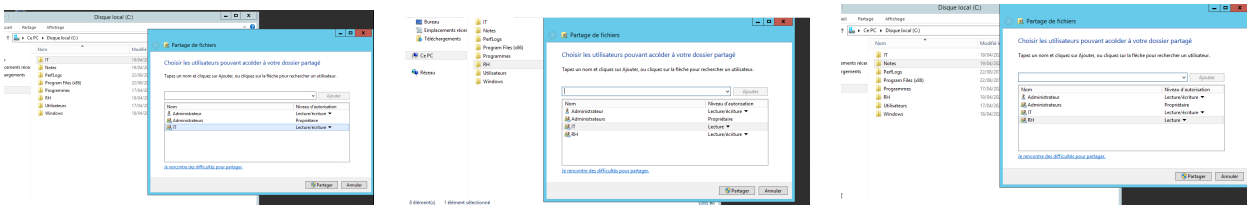


F. Partage des dossiers

Dossier	Groupe	Permissions
`IT`	IT	Lecture/Écriture/Exécution
`RH`	RH	Lecture/Écriture
`Notes`	RH	Lecture seule

Table S1. Permissions des dossiers partagés dans le domaine `Virgin.ca`

F.1. Pratique concernant le partage d'objet entre utilisateurs



5. SIMPLIFICATION ADMINISTRATIVE APPORTÉE PAR LE CONCEPT DE HIÉRARCHIE

A. Gestion des groupes (RBAC) ou Gestion de la Hiérarchie des permissions

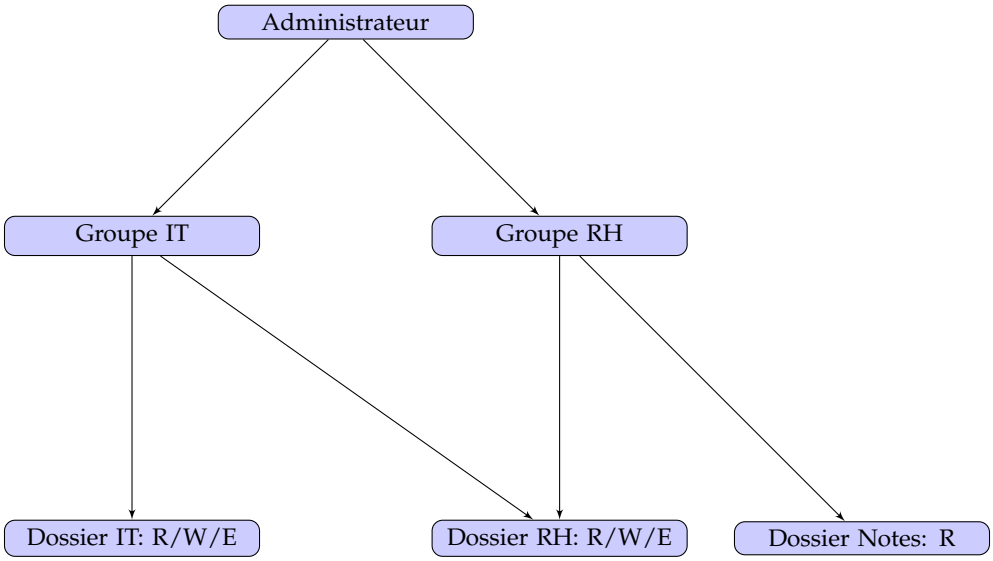


Fig. S1. Hiérarchie des permissions (RBAC)

B. Diagramme de classes d'équivalence entre utilisateurs et objets, Matrice des permissions et Étiquetage des accès

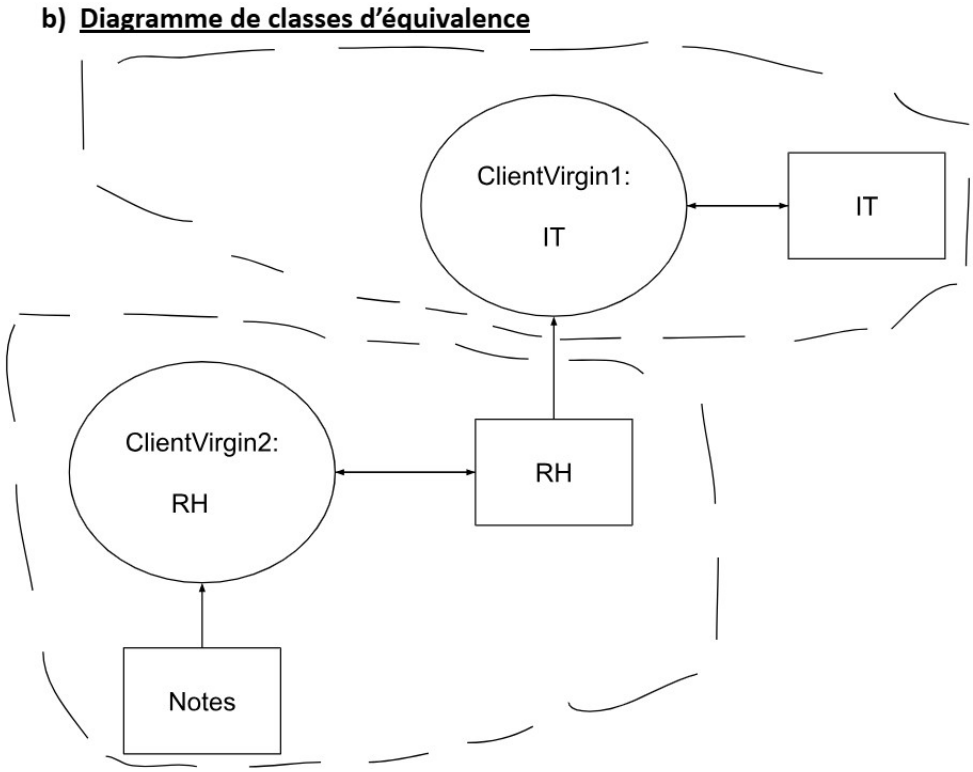


Table S2. Matrice des permissions RBAC

	Droits d'accès		
Utilisateur	IT	RH	Notes
ClientVirgin1	R/W	R	–
ClientVirgin2	–	R/W	R

- R/W : Lecture + Écriture
- R : Lecture seule
- – : Aucun accès

Table S3. Tableau des étiquettes d'accès RBAC

Utilisateur	Dossiers accessibles	Droits
ClientVirgin1	IT, RH	IT: R/W RH: R
ClientVirgin2	RH, Notes	RH: R/W Notes: R

Légende : R = Lecture, W = Écriture

6. CONCLUSION

A. Synthèse :

- Le déploiement d'AD DS a permis une gestion centralisée des utilisateurs et des ressources avec des permissions RBAC.

B. Apprentissages :

- L'importance des niveaux fonctionnels pour la compatibilité.
- La flexibilité des stratégies de groupe pour appliquer des restrictions.

C. Perspectives :

- Étendre l'architecture à des sites distants avec des contrôleurs de domaine secondaires.
- Implémenter des stratégies de chiffrement (BitLocker) pour les dossiers sensibles.

- Implémenter des stratégies de groupe (GPO) pour des contrôles plus fins.

REFERENCES

1. R. Sandhu et al., "Role-Based Access Control Models," IEEE Computer, vol. 29, no. 2, pp. 38–47, 1996.
2. Microsoft, "Best Practices for Active Directory Functional Levels," Microsoft Docs, 2012.
3. E. Bertino et al., "Secure Data Flow in Distributed Systems," ACM Transactions on Information and System Security, vol. 4, no. 3, pp. 254–291, 2001.