



RAPPORT D'AUDIT EXTERNE

Référence : AU-EX-001-V1

<u>Destinataires</u>	<u>Champ d'audit</u> : Deux hyperviseur ESXI <u>Référentiel d'audit</u> : <u>Personnes ayant participé à l'audit</u> : <u>Audit réalisé par</u> : <ul style="list-style-type: none">• <u>Cyril</u>• <u>Maxime</u>• <u>Gregory</u>• <u>Tristan</u> <u>Date(s) de l'audit</u> : Les 25/08/2023 et 28/08/2023 <u>Rapport établi le</u> : 28/08/2023
-----------------------------	--

RAPPEL : Ce rapport fait l'objet de :

- **NON-CONFORMITES** : Il s'agit de déviations par rapport à des exigences spécifiées. Les non-conformités doivent obligatoirement faire l'objet d'une action corrective.
- **REMARQUES** : Il s'agit de constats qui ne sont pas des lacunes graves du système mais qui pourraient donner lieu à une action d'amélioration (préventive ou de progrès). Ces remarques font l'objet de recommandations.
- **OBSERVATIONS** : Il s'agit de commentaires suite à erreur, oubli ou autre point mineur.



RAPPORT D'AUDIT EXTERNE

Référence : AU-EX-001-V1

1. CONSTATS D'AUDIT

Constatations de l'Audit de l'Active Directory :

1. **Capacité physique de la machine** : La capacité physique des machines est considérablement basse, ce qui pourrait affecter les performances globales du système.
2. **RDP et SSH activés** : Bien que RDP et SSH soient activés, l'accès au RDP est restreint aux comptes administrateurs et aucun compte n'est autorisé sur le RDP.
3. **Connexion à Internet** : L'Active Directory est connectée à Internet, ce qui peut présenter des risques de sécurité.
4. **GPO (Stratégies de groupe)** : Aucune stratégie de groupe (GPO) n'est en place.
5. **Accès à Internet Explorer** : L'accès à Internet Explorer est activé, ce qui pourrait poser des problèmes de sécurité.
6. **Contrôle des comptes** : Le compte "Fabian" possède des droits excessifs sur les comptes administrateurs, y compris les droits d'Hyper-V et de Schéma.
7. **Comptes utilisateurs dans le groupe administrateur** : Des comptes d'utilisateurs sont présents dans le groupe administrateur, ce qui peut augmenter les risques de sécurité.
8. **Compte Administrateur** : Le compte "Administrateur" est activé et non renommé.
9. **Sauvegarde de l'AD** : Aucune sauvegarde de l'Active Directory n'a été effectuée ni programmée.
10. **Licence Windows** : Aucune licence Windows n'a été identifiée.
11. **Distribution des services** : Tous les services sont hébergés sur la même machine virtuelle, ce qui pourrait entraîner des problèmes de performances et de disponibilité.
12. **Réplication** : L'accès à la réplication est inexistant ou restreint.
13. **Accès aux partages** : Le compte "David" n'a pas accès au partage.
14. **Stockage du volume "commun"** : Le volume "commun" est stocké sur l'Active Directory, ce qui peut affecter les performances.
15. **Port 55** : Le port 55 est ouvert, mais son objectif n'est pas clairement identifié.
16. **Certificats SSL** : Aucun certificat SSL n'est en place, ce qui peut entraîner des problèmes de sécurité lors des communications.
17. **Répartition des droits** : Il y a des problèmes de répartition des droits entre les comptes, ce qui peut causer des problèmes d'accès et de sécurité.



RAPPORT D'AUDIT EXTERNE

Référence : AU-EX-001-V1

2. CONCLUSION DE L'AUDIT

En résumé, notre audit de l'Active Directory du collège a révélé des points importants nécessitant une attention. Les bonnes pratiques de sécurité, telles que les politiques de mot de passe et la configuration des comptes administrateurs, ont été respectées. Cependant, des zones de préoccupation ont été identifiées, notamment la connexion à Internet et l'absence de sauvegardes régulières. Des améliorations sont recommandées pour renforcer la sécurité, optimiser les performances et garantir une gestion efficace de l'Active Directory. En prenant des mesures pour résoudre ces problèmes, améliorer la sécurité et créer un environnement informatique plus robuste et fiable.



RAPPORT D'AUDIT EXTERNE

Référence : AU-EX-001-V1

FICHE DE REMARQUE N°001

Constat / recommandation :

Optimisation des performances : Évaluer les besoins en ressources système en fonction de la charge de travail et envisager une mise à niveau matérielle si nécessaire.

Nom de l'auditeur : Tristan Onquiert

Date : 28/08/2023

ACTION D'AMELIORATION

PROPOSITION :

Évaluez la capacité matérielle des machines pour améliorer les performances.

Vu que plusieurs service tourne sur la même machine, il est impératif d'augmenter la capacité RAM et la performance du processeur, la capacité du disque dur est aussi à augmenter.

Une capacité mémoire de 16 go et de 1 to de mémoire peut convenir à l'heure actuel, une évaluation des capacités est a revoir régulièrement en fonction de l'évolution du parc

Date à laquelle les propositions seront appliquées :

Nom du Responsable :

Visa :

Date :

APPROBATION RESPONSABLE QUALITE :

M.

Visa :

Date :

VERIFICATION DE L'EFFICACITE :

Fiche soldée

M.

Visa :

Date :



RAPPORT D'AUDIT EXTERNE

Référence : AU-EX-001-V1

FICHE DE REMARQUE N°002

Constat / recommandation :

Restriction des accès RDP et SSH : Revoir et restreindre les accès RDP et SSH aux comptes strictement nécessaires. Examiner les exigences de sécurité, y compris l'authentification à deux facteurs.

Nom de l'auditeur : Tristan Onquiert

Date : 28/08/2023

ACTION D'AMELIORATION

PROPOSITION :

Mettre en œuvre une politique d'accès distant pour l'accès, et limité les comptes autorisés

Date à laquelle les propositions seront appliquées :

Nom du Responsable :

Visa :

Date :

APPROBATION RESPONSABLE QUALITE :

M.

Visa :

Date :

VERIFICATION DE L'EFFICACITE :

Fiche soldée

M.

Visa :

Date :



RAPPORT D'AUDIT EXTERNE

Référence : AU-EX-001-V1

FICHE DE REMARQUE N°003

Constat / recommandation :

- **Connexion à Internet**
- Accès à Internet Explorer activé : limitez l'accès à Internet Explorer

Nom de l'auditeur : Tristan Onquiert

Date : 28/08/2023

ACTION D'AMELIORATION

PROPOSITION :

L'active directory ne doit pas être connecter à internet, connecter l'AD à Internet peut augmenter les risques de sécurité

Déconnecter l'AD d'internet et de supprimer la redirection DNS vers google si le DNS local est fonctionnel

Date à laquelle les propositions seront appliquées :

Nom du Responsable :

Visa :

Date :

APPROBATION RESPONSABLE QUALITE :

M.

Visa :

Date :

VERIFICATION DE L'EFFICACITE :

Fiche soldée

M.

Visa :

Date :



RAPPORT D'AUDIT EXTERNE

Référence : AU-EX-001-V1

FICHE DE REMARQUE N°004

Constat / recommandation :

Implémentation de stratégies de groupe (GPO) : Implémentez des stratégies de groupe (GPO) pour renforcer la sécurité et la configuration.

Nom de l'auditeur : Tristan Onquiert

Date : 28/08/2023

ACTION D'AMELIORATION

PROPOSITION :

Identifiez les paramètres de sécurité, les configurations et les préférences à appliquer.
Créez et déployez des GPO qui correspondent au besoin de l'entreprise

Date à laquelle les propositions seront appliquées :

Nom du Responsable :

Visa :

Date :

APPROBATION RESPONSABLE QUALITE :

M.

Visa :

Date :

VERIFICATION DE L'EFFICACITE :

Fiche soldée

M.

Visa :

Date :



RAPPORT D'AUDIT EXTERNE

Référence : AU-EX-001-V1

FICHE DE REMARQUE N°005

Constat / recommandation :

Gestion des comptes administrateur : Limitez les droits excessifs des comptes administrateurs

Nom de l'auditeur : Tristan Onquiert

Date : 28/08/2023

ACTION D'AMELIORATION

PROPOSITION :

Restreindre les droits des comptes administrateurs, donnez les droits qui correspond au rôle

Date à laquelle les propositions seront appliquées :

Nom du Responsable :

Visa :

Date :

APPROBATION RESPONSABLE QUALITE :

M.

Visa :

Date :

VERIFICATION DE L'EFFICACITE :

Fiche soldée

M.

Visa :

Date :



RAPPORT D'AUDIT EXTERNE

Référence : AU-EX-001-V1

FICHE DE REMARQUE N°006

Constat / recommandation :

Sauvegarde régulière de l'AD : Mettez en place un plan de sauvegarde régulière de l'Active Directory pour éviter la perte de données.

Nom de l'auditeur : Tristan Onquiert

Date : 28/08/2023

ACTION D'AMELIORATION

PROPOSITION :

Planifiez des sauvegardes régulières pour garantir la disponibilité et éviter les pertes des données à des intervalles réguliers

Exemple : 1 sauvegarde toutes les nuits, puis sur toutes les semaines, puis tous les mois sur des DD ou des bandes séparées

Date à laquelle les propositions seront appliquées :

Nom du Responsable :

Visa :

Date :

APPROBATION RESPONSABLE QUALITE :

M.

Visa :

Date :

VERIFICATION DE L'EFFICACITE :

Fiche soldée

M.

Visa :

Date :



RAPPORT D'AUDIT EXTERNE

Référence : AU-EX-001-V1

FICHE DE REMARQUE N°007

Constat / recommandation :

License Windows : Assurez-vous que toutes les instances Windows sont correctement licenciées pour éviter des problèmes de conformité

Nom de l'auditeur : Tristan Onquiert

Date : 28/08/2023

ACTION D'AMELIORATION

PROPOSITION :

Activer Windows serveur avec une clé conforme et officiel et effectuer un inventaire complet

Date à laquelle les propositions seront appliquées :

Nom du Responsable :

Visa :

Date :

APPROBATION RESPONSABLE QUALITE :

M.

Visa :

Date :

VERIFICATION DE L'EFFICACITE :

Fiche soldée

M.

Visa :

Date :



RAPPORT D'AUDIT EXTERNE

Référence : AU-EX-001-V1

FICHE DE REMARQUE N°008

Constat / recommandation :

Répartition des services : la répartition des services pour améliorer la performance.

Nom de l'auditeur : Tristan Onquiert

Date : 28/08/2023

ACTION D'AMELIORATION

PROPOSITION :

Identifiez les services essentiels actuellement exécutés sur une seule machine ou une seule VM. Répartissez ces services sur plusieurs machines ou VMs pour réduire les goulots d'étranglement et garantir la disponibilité. Idem pour leur réplication

Date à laquelle les propositions seront appliquées :

Nom du Responsable :

Visa :

Date :

APPROBATION RESPONSABLE QUALITE :

M.

Visa :

Date :

VERIFICATION DE L'EFFICACITE :

Fiche soldée

M.

Visa :

Date :



RAPPORT D'AUDIT EXTERNE

Référence : AU-EX-001-V1

FICHE DE REMARQUE N°009

Constat / recommandation :

Réplication : Renforcez la sécurité de la réplication pour protéger les données sensibles.

Nom de l'auditeur : Tristan Onquiert

Date : 28/08/2023

ACTION D'AMELIORATION

PROPOSITION :

Chaque service a sa réplication sur un serveur dédié pour la réplication

Date à laquelle les propositions seront appliquées :

Nom du Responsable :

Visa :

Date :

APPROBATION RESPONSABLE QUALITE :

M.

Visa :

Date :

VERIFICATION DE L'EFFICACITE :

Fiche soldée

M.

Visa :

Date :



RAPPORT D'AUDIT EXTERNE

Référence : AU-EX-001-V1

FICHE DE REMARQUE N°010

Constat / recommandation :

Stockage des volumes : déplacer le volume "commun" vers un emplacement dédié pour optimiser l'utilisation des ressources.

Nom de l'auditeur : Tristan Onquiert

Date : 28/08/2023

ACTION D'AMELIORATION

PROPOSITION :

Déplacer le volume "commun" vers un emplacement dédié.

Date à laquelle les propositions seront appliquées :

Nom du Responsable :

Visa :

Date :

APPROBATION RESPONSABLE QUALITE :

M.

Visa :

Date :

VERIFICATION DE L'EFFICACITE :

Fiche soldée

M.

Visa :

Date :



RAPPORT D'AUDIT EXTERNE

Référence : AU-EX-001-V1

FICHE DE REMARQUE N°012

Constat / recommandation :

Examen du port 55 : Identifiez et clarifiez l'utilisation du port 55.

Nom de l'auditeur : Tristan Onquiert

Date : 28/08/2023

ACTION D'AMELIORATION

PROPOSITION :

Ecrire en description, l'utilisateur du port

Date à laquelle les propositions seront appliquées :

Nom du Responsable :

Visa :

Date :

APPROBATION RESPONSABLE QUALITE :

M.

Visa :

Date :

VERIFICATION DE L'EFFICACITE :

Fiche soldée

M.

Visa :

Date :



RAPPORT D'AUDIT EXTERNE

Référence : AU-EX-001-V1

FICHE DE REMARQUE N°013

Constat / recommandation :

Implémentation de certificats SSL : Évaluez l'opportunité d'utiliser des certificats SSL pour renforcer la sécurité.

Nom de l'auditeur : Tristan Onquiert

Date : 28/08/2023

ACTION D'AMELIORATION

PROPOSITION :

Identifiez les flux de données sensibles qui nécessitent une protection. Si nécessaire, envisagez de mettre en place des certificats SSL pour chiffrer ces communications et renforcer la sécurité.

Date à laquelle les propositions seront appliquées :

Nom du Responsable :

Visa :

Date :

APPROBATION RESPONSABLE QUALITE :

M.

Visa :

Date :

VERIFICATION DE L'EFFICACITE :

Fiche soldée

M.

Visa :

Date :



RAPPORT D'AUDIT EXTERNE

Référence : AU-EX-001-V1

FICHE DE REMARQUE N°014

Constat / recommandation :

Répartition des droits : Répartir les droits pour éviter les conflits et assurer un accès approprié.

Nom de l'auditeur : Tristan Onquiert

Date : 28/08/2023

ACTION D'AMELIORATION

PROPOSITION :

Assurez-vous que les droits sont attribués en fonction des responsabilités spécifiques de chaque utilisateur. Surveillez régulièrement les modifications pour éviter les accumulations de droits non nécessaires.

Date à laquelle les propositions seront appliquées :

Nom du Responsable :

Visa :

Date :

APPROBATION RESPONSABLE QUALITE :

M.

Visa :

Date :

VERIFICATION DE L'EFFICACITE :

Fiche soldée

M.

Visa :

Date :



RAPPORT D'AUDIT EXTERNE

Référence : AU-EX-001-V1

FICHE COLLECTIVE D'OBSERVATIONS

N° d'OBS.	OBSERVATION