

Connexion TPM d'un serveur sur un esxi via IDRAC

HISTORIQUE DES MODIFICATIONS			
Version	Date	Description des modifications	Rédacteur / Fonction
0.1	25/02/25	Création du document	Rania Aboubakar Mohamed

APPROBATION DU DOCUMENT		
Entité	Nom / fonction	Date

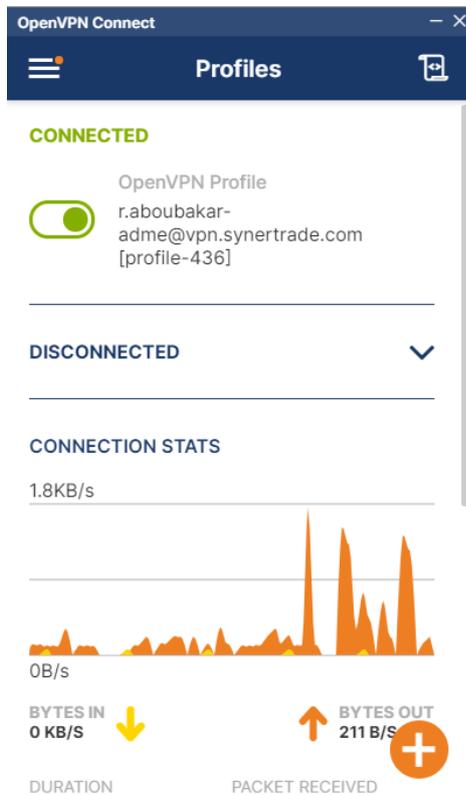
DATE DE RELECTURE - TABLEAU A RETIRER APRÈS L'APPROBATION		
Entité	Nom / fonction	Date

Table des matières

- 1. **Connexion au VPN** 3
 - 2. **Accès à l'interface de gestion de l'hôte ESXI** 3
 - 3. **Vérification de l'état du TPM** 4
 - 4. **Connexion à l'iDRAC** 4
 - 5. **Modification du paramètre TPM dans le BIOS** 6
 - 6. ***Vérification***
- Conclusion** Error! Bookmark not defined.

1. Connexion au VPN

- Assurez-vous d'être connecté au VPN OpenVPN pour accéder à l'interface de gestion de l'hôte ESXi.

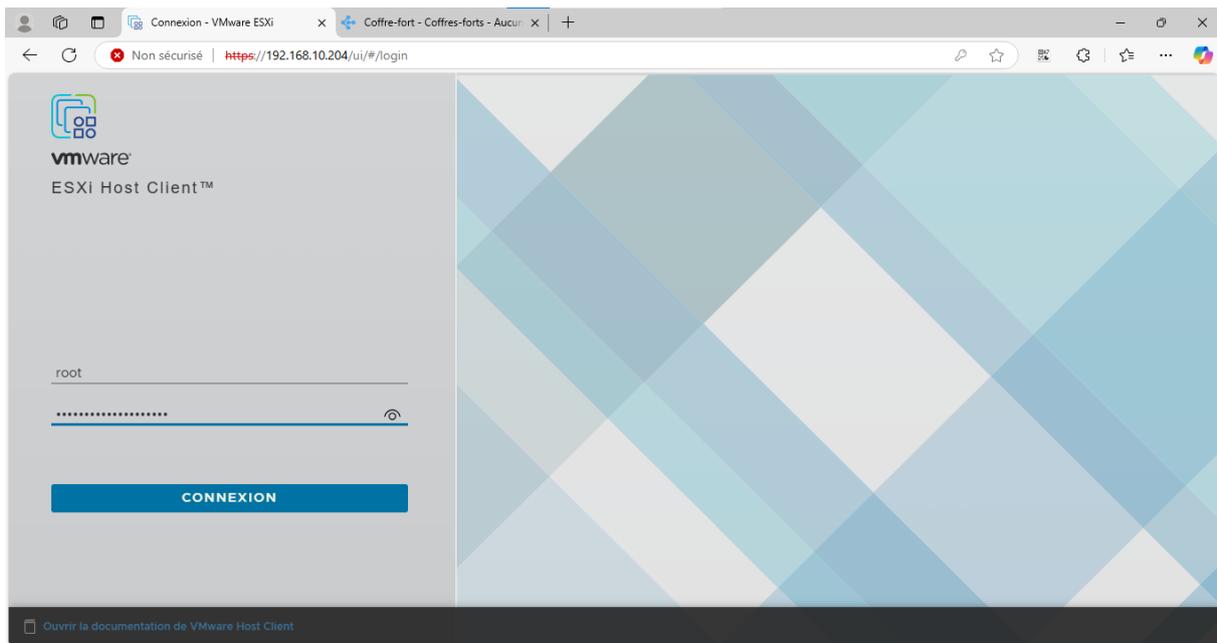


2. Accès à l'interface de gestion de l'hôte ESXi

- Ouvrez un navigateur web puis saisissez l'adresse IP de l'hôte ESXi concerné dans la barre d'adresse.



- Dans l'interface qui s'ouvre, saisissez vos identifiants et connectez-vous à l'hôte ESXi (vous trouverez les identifiants sur Cockpit dans Coffre-fort).



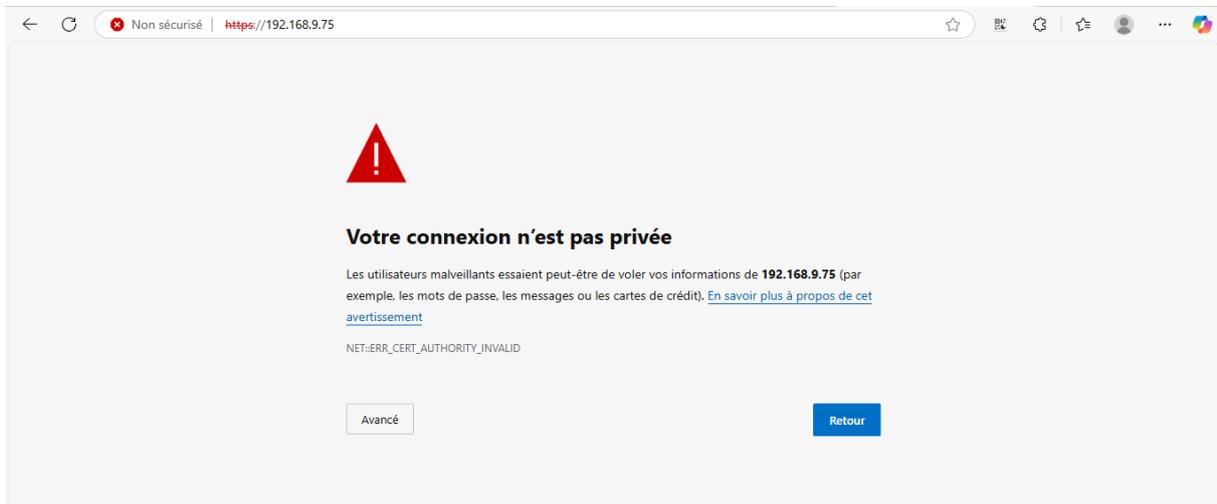
3. Vérification de l'état du TPM

- Une fois connecté à l'interface, on remarque une alerte indiquant **"Le périphérique TPM 2.0 a été détecté, mais impossible d'établir une connexion"**.

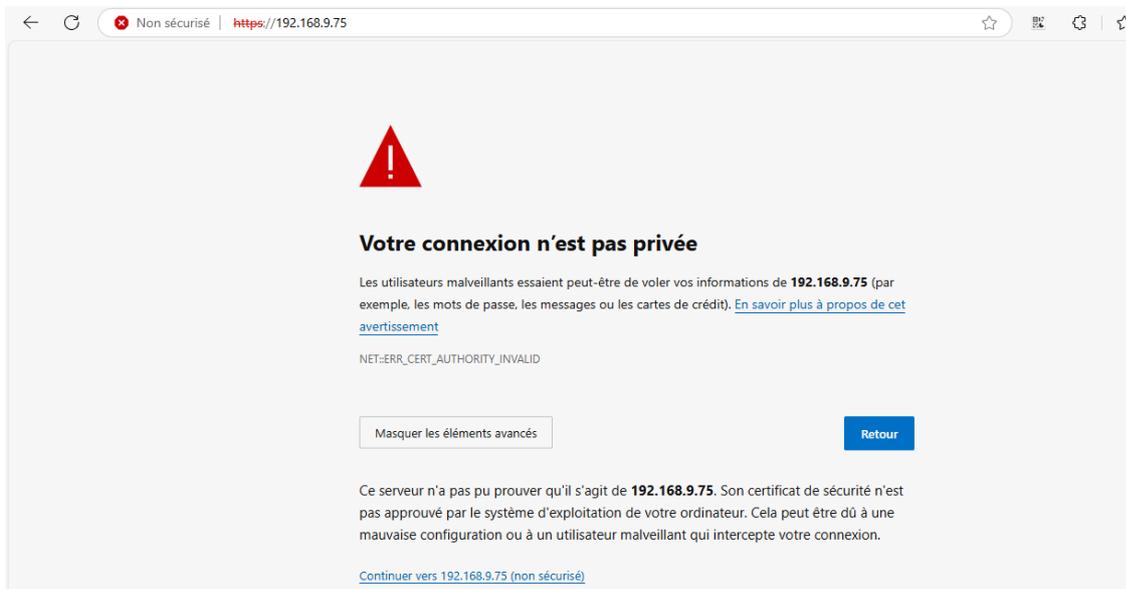


4. Connexion à l'iDRAC

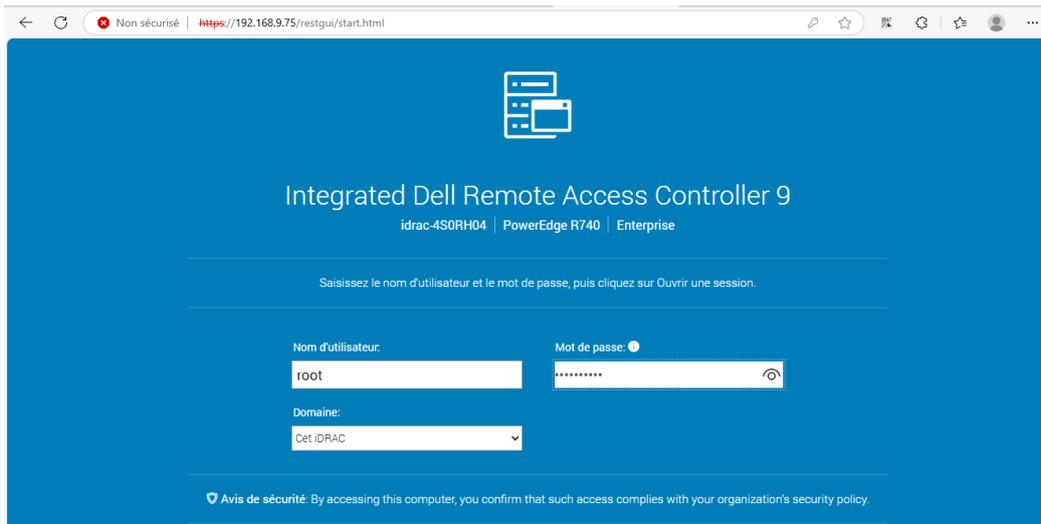
- Après analyse du message d’alerte sur l’interface ESXi, nous allons procéder à une vérification via l’interface iDRAC du serveur concerné. Pour se faire, Ouvrez votre navigateur web et saisissez l’adresse IP de l’iDRAC : 192.168.9.75.



- Une fenêtre d’avertissement s’ouvre : cliquez sur **"Avancé"**, puis sur **"Continuer vers 192.168.9.75 (non sécurisé)"**

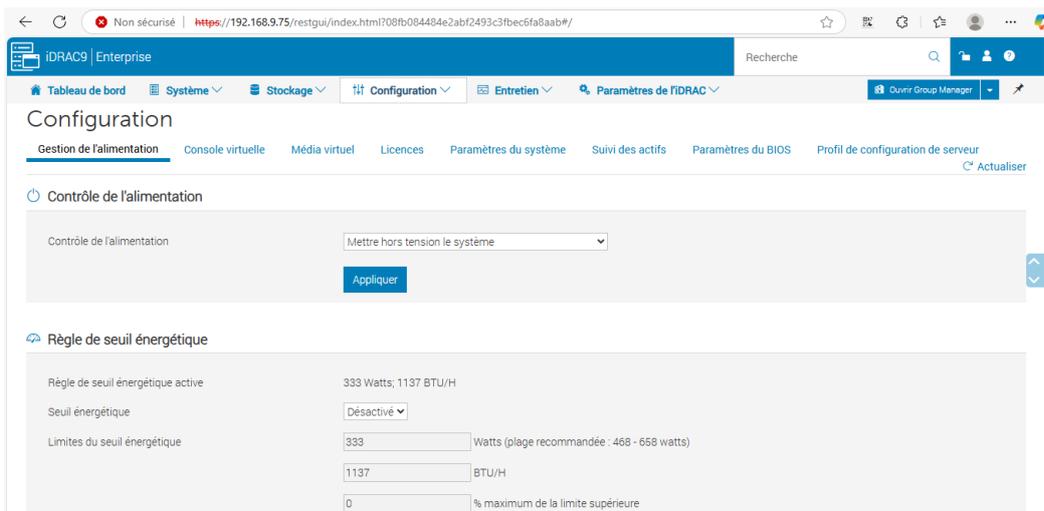


- Connectez-vous avec les identifiants suivants :
- **Nom d'utilisateur** : root
- **Mot de passe** : récupérable depuis l’interface Cockpit.



5. Modification du paramètre TPM dans le BIOS

- Une fois connecté à l'iDRAC, cliquez sur l'onglet **Configuration**, puis sur **Paramètres du BIOS**.



- Dans la fenêtre qui s'ouvre, sélectionnez l'option **System Security**



- Faites défiler jusqu'à **TPM Advanced Settings**.

System Security

	Valeur actuelle	Valeur en attente
CPU AES-NI	Enabled	
System Password	<input type="text"/>	
Confirm System Password	<input type="text"/>	
Setup Password	<input type="text"/>	
Confirm Setup Password	<input type="text"/>	
Password Status	Unlocked ▾	
SHA256 hash of the System password	<input type="text"/>	
Salt string appended to the System password prior to hash	<input type="text"/>	
SHA256 hash of the Setup password	<input type="text"/>	
Salt string appended to the Setup password prior to hash	<input type="text"/>	
TPM Security	On ▾	
TPM Information	Type: 2.0 NTC	
TPM Firmware	7.2.2.0	

- Modifiez la valeur de **TPM Algorithm Selection** en la remplaçant par **SHA-256**.

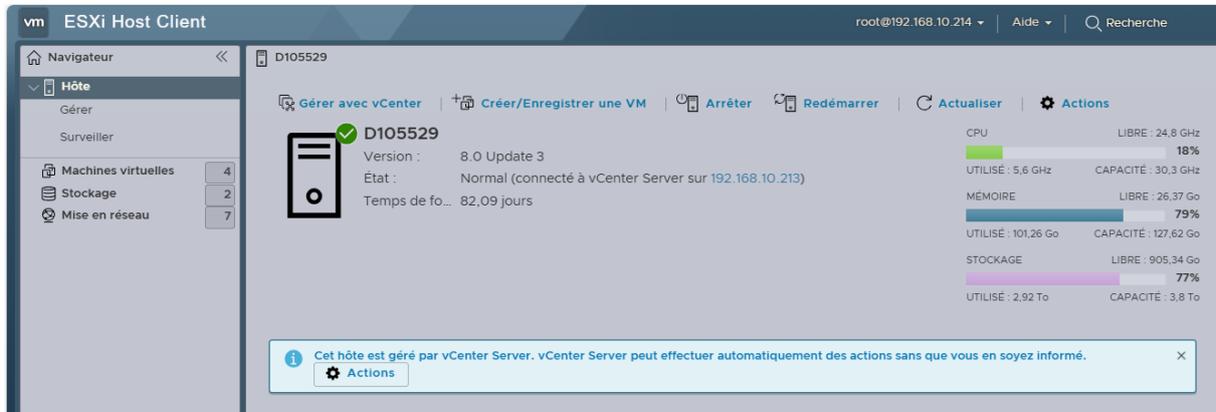
The screenshot shows the iDRAC9 Enterprise configuration interface. The 'TPM Advanced Settings' section is expanded, showing a table with columns for 'Valeur actuelle' and 'Valeur en attente'. The 'TPM2 Algorithm Selection' dropdown menu is open, showing options: Off, SHA256 (selected), SHA1, SHA384, and Unlocked. Other settings include TPM PPI Bypass Provision (Disabled), TPM PPI Bypass Clear (Disabled), Intel(R) TXT (Off), SGX Launch Control Policy (Unlocked), Power Button (Enabled), and AC Power Recovery (Last).

- Cliquez ensuite sur **Appliquer et redémarrer** en bas de la page.

The screenshot shows the bottom of the iDRAC9 Enterprise configuration page. The 'APpliquer et redémarrer' button is visible at the bottom left, along with other buttons: 'Au prochain redémarrage' and 'Supprimer Tout en attente'. The 'AC Power Recovery Delay' dropdown is set to 'Immediate'.

6. Vérification

- Après le redémarrage du serveur, retournez sur l'interface ESXi, vous constaterez que le message d'erreur a disparu.



Conclusion

Grâce à cette intervention via l'interface iDRAC, nous avons pu modifier les paramètres de sécurité TPM du BIOS, en sélectionnant l'algorithme de hachage SHA-256. Après redémarrage du serveur, l'alerte précédemment affichée sur l'interface ESXi a disparu, confirmant que le problème était bien lié à la configuration du module TPM. La situation est désormais résolue et le serveur fonctionne normalement.