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).

	🕼 🗖 🕼 Connexion - VMware ESXi 🛛 🗙 🍫 Coffre-fort - Coffre	ss-forts - Aucum × +	-	0	×
\leftarrow	C Non sécurisé https://192.168.10.204/ui/#/login	ゆ ☆ 1000	3 €		9
	Vmware [.]				
	ESXi Host Client™				
	root				
	CONNEXION				
۵	Duvrir la documentation de VMware Host Client				

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".

mor	n - Statu	Nagios: nagios.syr	ne 회 Ressources Humain	() IPSYLON (L'AIGLE) (C 💠 Cockpit
	D105535				
	🕞 Obten	ir vCenter Server	+ B Créer/Enregistrer	une VM 🕛 Arrêter	C Redém
		D105535			
		Version :	8.0 Update 3		
		État :	Normal (non cor	nnecté à vCenter Server)	
	0	Temps de foncti	ionne 15,84 jours		
	🛕 Le p	ériphérique TPM 2.0	a été détecté, mais impossil	ble d'établir une connexior	ı.
	1 You	are running Dell Cust	tomized version of VMware	ESXI Image. If you have Do	ell Inc. support,
	1 Vou	s utilisez actuellemen	t ESXi en mode d'évaluation	n. Cette licence expirera da	ans 45 jours.

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.

← C (⊗ Non sécurisé https://192.168.9.75		(} ☆	•	· 🧑
	A			
	A			
	Votre connexion n'est pas privée			
	Les utilisateurs malveillants essaient peut-être de voler vos informations de 192.168.9.75 (par			
	exemple, les mots de passe, les messages ou les cartes de crédit). En savoir plus à propos de cet avertissement			
	NET::ERR_CERT_AUTHORITY_INVALID			
	Avancé			

• 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.

\leftarrow	С	Non sécurisé	https://192.168.9.75/restgui/start.html	P	☆ 	ଓ ମ≊	۲	
			Integrated Dell Remote Access Controller 9					
			idrac-4S0RH04 PowerEdge R740 Enterprise					
			Saisissez le nom d'utilisateur et le mot de passe, puis cliquez sur Ouvrir une session.					
			Nom d'utilisateur: Mot de passe: 🛈					
			root					
			Domaine:					
			Cet iDRAC 🗸					
			V Avis de sécurité: By accessing this computer, you confirm that such access complies with your organization's se	ecurity	policy.			

5. Modification du paramètre TPM dans le BIOS

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

← C (❷ Non sécurisé https://192.168.9.75/re	stgui/index.html?08fb084484e2ab	of2493c3fbec6fa8aab#/		☆ 🗷 C C 🖉		0
iDRAC9 Enterprise			Recherche	Q 🔒	4 0	Î
🗌 Tableau de bord 🛛 🗏 Système 🗠 🛢 Stocka	ge \checkmark ttt Configuration \checkmark	🖾 Entretien 🗠 🛛 🍓 Paramètres de l'iD	RAC	8 Ouvrir Group Manager	- 1	•
Configuration						
Gestion de l'alimentation Console virtuelle M	édia virtuel Licences Pa	ramètres du système Suivi des actifs	Paramètres du BIOS	Profil de configuration de serveur C ⁴	r Actualise	er -
O Contrôle de l'alimentation						.
Contrôle de l'alimentation	Mettre hors tension le sy	rstème 🗸				
	Appliquer					
Pàpe de seuil éperaétique						
						1
Règle de seuil énergétique active	333 Watts; 1137 BTU/H					
Seuil énergétique	Désactivé 🗸					
Limites du seuil énergétique	333	Watts (plage recommandée : 468 - 658 watts)			
	1137	BTU/H				
	0	% maximum de la limite supérieure				

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

	Appliquer et redemanne Au prochain redemaringe Bupprimer Tout en strente	ł
>	Miscellaneous Settings	
>	Redundant OS Control	
>	System Security	
>	System Profile Settings	
>	Serial Communication	
>	Integrated Devices	
>	Network Settings	Û
>	Boot Settings	
>	NVMe Settings	
>	SATA Settings	
>	Processor Settings	
	i Tableau de bord 📱 Système 🗸 🛢 Stockage 🗸 Till Configuration 🗸 🐻 Entretien 🗸 🍕 Paramètres de TIDPAC V 🔒 David Sauge Vannage 🔹 🖈	
B	10FAC9 Enterprise Recherche Q 🏊 🖬 🔿	
\leftarrow	C 💿 Non skurité https://182.163.875/restgu/index.htm/?00h.06465462abf2493c3thee66fa8aabe/ 😒 🕱 C 🎓 🔹	٥

• Faites défiler jusqu'à TPM Advanced Settings.

✓ System Security

	Valeur actuelle	Valeur en attente
CPU AES-NI	Enabled	
System Password		
Confirm System Password		
Setup Password		
Confirm Setup Password		
Password Status	Unlocked V	
SHA256 hash of the System password		
Salt string appended to the System password prior to hash		
SHA256 hash of the Setup password		
Salt string appended to the Setup password prior to hash		
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**.

\leftarrow	C Non sécurisé https://192.168.9.75/restgui/ind	lex.html?08fb084484e2ab	of2493c3fbec6fa8aab#	<i>#/</i>	☆	# ()	£≞			Ø
	iDRAC9 Enterprise				Recherche		Q 1		?	•
Â	Tableau de bord 📱 Système 🗸 🛢 Stockage 🗸	†∔† Configuration ∽	Entretien 🗠	🎭 Paramètres de l'iDRAC 🗸		🔏 Ouvrir Gr	oup Manaç	ger 👻	*	
	TPM Security	On 🛩								
	TPM Information	Type: 2.0 NTC								
	TPM Firmware	7.2.2.0								
	TPM Hierarchy	Enabled ¥								
	✓ TPM Advanced Settings									
		Valeur actuelle			Valeur en attente					
	TPM PPI Bypass Provision	Disabled 🗸								
	TPM PPI Bypass Clear	Disabled 🗸								
	TPM2 Algorithm Selection	SHA256 V SHA1								
	Intel(R) TXT	Off • SHA256								
	SGX Launch Control Policy	SHA384 Unlouxeu								
	Power Button	Enabled 🛩								
	AC Power Recovery	Last 🛩								
	A.C. Devier Receiver / Belev	Immediate as								Ŧ

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

← C O Non sécurisé https://192.168.9.75/restgui/ind	ochtml?08fb084484e2abf2493c3fbec6fa8aab#/			\$P	N G	¢ 🙁		-
iDRAC9 Enterprise			Recherche			a 🕤 🛛	•	^
🏦 Tableau de bord 🛛 🗏 Système 🗸 🛢 Stockage 🗸	# Configuration \checkmark $\ $ Entretien \checkmark	9. Paramètres de l'IDRAC 🗸			8 Ouvrir Gro	p Manager	1	
AC Power Recovery	Last ¥							
AC Power Recovery Delay	Immediate 👻							
User Defined Delay (60s to 600s)	60							
UEFI Variable Access	Standard 🛩							
In-Band Manageability Interface	Enabled 🛩							
Secure Boot	Enabled ¥							0
Secure Boot Policy	Standard 🛩							
Secure Boot Mode	Deployed Mode 🛩							
Authorize Device Firmware	Disabled							
	Appliquer Supprimer							
> Redundant OS Control								
> Miscellaneous Settings								
Appliquer et redémarrer Au prochain redémarrage Supprin	er Tout en attente							ļ

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.