Activer WMI sur Windows 7, 8 & 10

Activer les accès distants à WMI (toujours nécessaire)

Il s'agit ici de donner les droits d'accès distants au compte utilisateur qui sera utilisé par ESIA afin d'accéder aux données WMI. Pour cela :

Rendez vous dans « Gestion de l'ordinateur » (ou saisissez la commande « wmimgmt.msc ». Puis, Déroulez « Services et applications » pour pouvoir faire un clic droit sur « Contrôle WMI » et cliquez sur « Propriétés ».



Dans l'onglet « Sécurité » des « Propriétés de : Contrôle WMI », sélectionnez le namespace « Root » et cliquez ensuite sur « Sécurité ».

Si vous souhaitez un réglage plus fin au niveau de la sécurité, les namespaces « Root→CIMV2 » et « Root→SecurityCenter2 » sont ceux utilisés par ESIA.

<u>₽</u>	Gestion de l'ordinateur	- 0	×
Fichier Action Affichage ?			
💠 🧼 🖄 📰 📰 📓 🖬			
 Gestion de l'ordinateur (local) Outils système Planificateur de tâches Observateur d'événeme Dossiers partagés Utilisateurs et groupes I Performance Gestionnaire de périphé Stockage Gestionnaire des service Services et applications Gestionnaire des service Services Contrôle WMI SQL Server Configuratic 	Cereferal Sauvegarder/Restaurer Sécurté Options avancées Ca navigation dans l'espace de noms vous permet de définir des options de sécurté spécifiques à l'espace de noms. Image: Control of the served de local d	Actions Contrôle WMI Autres actions	
- C 🚞		- 😼 🔁 🕕 10	:32

2025/05/04 22:29	3/10	Activer WMI sur Windows 7, 8 & 10
Fichier Action Affichage ?	Gestion de l'ordinateur	- 0 ×
← → 2 📰 🔛 🔢 🖬		
Sestion de l'ordinateur (local)		Actions
Outils système Planificateur de tâches	Propriétés de : Contrôle WMI ? ×	Contrôle WMI 🔺
Id Observateur d'événeme Id Dossiers partagés Id Utilisateurs et groupes I Id Parfamente	Co Général Sauvegarder/Restaurer Sécurité Options avancées La navigation dans l'espace de noms vous permet de définir des options de sécurité spécifiques à l'espace de noms.	Autres actions
 Performance Gestionnaire de périphé Stockage Services et applications Gestionnaire des service Services Contrôle WMI SQL Server Configuratic 	a l'espèce de noms. B-0 asprét B-0 Cli B-0 Cli B-0 DEFAULT B-0 directory B-0 Interop B-0 Interop B-0 Interop B-0 Microsoft B-0 Microsoft B-0 Microsoft B-0 Risop B-0 Security B-0 Security Commit Microsoft B-0 Security B-0 Security Commit Microsoft Sécurité OK Annuler Appliquer	
< >		
📢 🙆 🚞		▲ 10:38 ▲ 10:38 26-06-15

Sélectionnez le compte utilisateur qui sera utilisé pour l'accès distant et cochez les cases « Autoriser » pour «Activer le compte » et « Appel à distance autorisé» qui sont les 2 autorisations nécessaires.

£	Gestion de l'ordinateur	- ð ×
Fichier Action Affichage ?		
🗢 🔿 🙍 📰 📰 🖉 📷		
Fichier Action Affichage ?	Ce General Sauvegarder/R La navigation dans l'espa à l'espace de noma.	Actions Contrôle WMI Autres actions
< >>		
📫 😂 🚔		 ▲ 10:34 ▲ 10:34 26-06-15

Assurez-vous que les autorisations ont été appliquées au namespace sélectionné et à ses sous namespaces en cliquant sur « Avancé » pour vérifier la colonne « S'applique à ».

- C 📑

🥑 🛛 🖅

5/10

*		Gestio	on de l'ordinateur		- 8 ×
Fichier Action	Affichage ?				
🗢 🌩 🛛 🖻	PL P	aramètres de sécu	rité avancés pour Root	×	
🜆 Gestion de l'e					15
a 👔 Outils sys		and descinization of the	to SE		rôle WMI 🔺
Plann B B Obser	Proprietaire : Administrateurs (winov	monoministrateurs)	roamer		utres actions
Dossi	Autorisations Audit				
b 🔊 Utilisa	Pour obtenir des informations suppléments	ires double cliques su	r une entrée d'autorisation. Pour	modifier une entrée d'autorisation	
Gestic	sélectionnez l'entrée et cliquez sur Modifier	(si disponible).	r une entree à autorisation. Pour	mouner une entree à autonsation,	
🖌 📇 Stockage	Entrées d'autorisations :				
Gestic	Type Principal	Accès	Hérité de	S'applique à	ot ×
Services b Struces Gestic	& Auto Utilisateurs authentifiés	Spéciale	Aucun	Cet espace de noms et les sou	
🔍 Servic	& Auto SERVICE LOCAL	Spéciale	Aucun	Cet espace de noms et les sou	
Contr	Auto SERVICE RÉSEAU	Spéciale	Aucun	Cet espace de noms et les sou	
D Sdr s	Auto Administrateurs (uin@um) Ad	P Speciale	Aucun	Cet espace de non set les sou	
	Ajouter Supprimer Moo Désactiver l'héritage	lifier) ter Supprimer utoriser Refuser
			OK	Annuler Appliquer	
				Autorisations spéciales	
				Pour les autorisations spéciales et les pa avancés, cliquez sur Avancé.	aramètres Avancé
				Informations sur le contrôle d'accès et le	es autorisations
				ОК	Annuler Appliquer
•					
					10.75

Permettre l'accès à travers le pare-feu (Si vous utilisez un pare-feu)

Afin d'éviter que le pare feu ne bloque les requêtes WMI, le plus simple est d'exécuter la ligne de commande suivante en tant qu'Administrateur : « netsh firewall set service RemoteAdmin enable » Vous pouvez aussi le faire via la page de configuration du pare-feu windows :

Applications autorisées – 🗗						× ۵
(e) → ↑ Panneau de configuration → Système et sécurité → Pare-feu Windows → Applicatio	ns autorisées		v	Ċ	Rechercher	Q,
(→ ↑ ▲ Panneau de configuration → Système et sécurité → Pare-feu Windows → Application Autoriser les applications à communiquer à travers le Pa Pour ajouter, modifier ou supprimer des applications et des ports autorisé paramètres. Quels sont les risques si une application est autorisée à communiquer ? Applications et fonctionnalités autorisées : Nom Gestion de carte à puce virtuelle TPM Gestion des services à distance Groupement résidentiel ✓ HP All-in-One Printer Remote ✓ Infrastructure de gestion Windows (WMI) Interruption SNMP	ns autorisées are-feu Wi is, cliquez sur ® Ma Domaine	Modifie difier le Privé	S er les is paramètr Public	¢	Rechercher	Ą
 ✓ Jeux ☐ Journaux et alertes de performance ✓ JuniperNetworks.JunosPulseVpn □ Lecteur Windows Media ✓ Liste de lettures Windows 	♥ □ ♥ Détails		Supprime	v		
	Autoriser un	e autre	application	h		
	(DK	Annul	ler		
🛋 ⋵ 🚞 🖻 🙋 🐺 💣 👘					- 🍺 🔁 🕪	15:09 26-06-15

Ajouter l'utilisateur dans un groupe qui a les permissions d'accès à distance

Pour pouvoir accéder à WMI à distance, il faut que WMI fasse partie du groupe « Administrateur ».

Activer les accès DCOM (si nécessaire)

Exécutez l'application « dcomcnfg »

ð.	Services d	e composants		×
🥺 Fichier 🛛 Actio	n Afficher Fenêtre 🔀 📴 🖸	? <u>1</u> <u>1</u> :	-	8×
 Racine de la co Services de Ordinate Observateu Services (loo 	nsole composants eurs r d'événements (Local) cal)	Poste de trava	Actions Ordinat Actualiser tous le Affichage	
			Proprietes	

Dans « **Racine de la console → Service de composant → ordinateurs** », faites un clic droit sur « Poste de travail » puis cliquez sur « Propriétés ».

Rendez-vous dans l'onglet « Sécurité DCOM » et, dans « Autorisations d'exécution et d'activation », cliquez sur le bouton « Modifier les limites ».

Général	Options		Propriété	s par défaut	
Protocoles par d	éfaut	Sécurité CO	М	MSDTC	
Autorisations d'ac	cès				
Vous pouvez m à des applicatio applications qui	odifier les personn ns. Vous pouvez déterminent leurs	nes autorisée également d propres aut	es par déf léfinir des orisations	aut à accéde limites sur les	
Attention : la modification des autorisations d'accès peut affecter la capacité des applications à démarrer, se connecter, fonctionner et/ou s'exécuter de manière sécurisée.					
	Madification	been en	M		
Autorisations d'exe Vous pouvez m exécuter des ap également défir propres autories	écution et d'activa odifier les personr oplications ou à ac ir des limites sur le tions	ation nes autorisée ctiver des ob es applicatio	es par déf jets. Vou: ns qui déf	aut à s pouvez terminent leur	
Autorisations d'exe Vous pouvez m exécuter des ap également défir propres autorisa Attenti d'activ démain	écution et d'activa odifier les personn oplications ou à ac ir des limites sur le stions. on : la modification ration peut affecte rer, se connecter, s sécurisée	ation nes autorisée ctiver des ob es applicatio n des autoris r la capacité fonctionner	es par déf jets. Vou: ns qui déf ations d'é é des app et/ou s'e	aut à s pouvez terminent leur exécution et lications à xécuter de	
Autorisations d'exe Vous pouvez m exécuter des ar également défir propres autorisa viennes Attenti d'activ déman manièr	écution et d'activa odifier les personn oplications ou à ac ir des limites sur le ations. on : la modification ration peut affecte rer, se connecter, re sécurisée. Modifier les	ation nes autorisée ctiver des ob es applicatio n des autoris fonctionner	es par déf ijets. Vou: ns qui déf sations d'é é des app et/ou s'es	aut à s pouvez terminent leur exécution et lications à xécuter de	
Autorisations d'exe Vous pouvez m exécuter des ap également défir propres autorisa Attenti d'activ déman manièr	écution et d'activa odifier les personn oplications ou à ac nir des limites sur le ations. on : la modification ration peut affecte rer, se connecter, re sécurisée. Modifier les	imites ation nes autorisée ctiver des ob es applicatio n des autoris r la capacité fonctionner limites propriétés.	es par déf ijets. Vou: ns qui déf sations d'é é des app et/ou s'e	aut à s pouvez terminent leur lications à xécuter de	

Ajoutez l'utilisateur pour WMI dans la liste et activez les autorisations distantes :

Autorisation d'exécution e	et d'activation	?	×				
Limites de sécurité							
Noms de groupes ou d'utilisateurs :							
Tout le monde TOUS LES PACKAGES D'APPLICATION Administrateurs (win8vm\Administrateurs) Utilisateurs du journal de performances (win8vm\Utilisateurs du Utilisateurs du modèle COM distribué (win8vm\Utilisateurs du							
	Ajouter Supprimer						
Autorisations pour Tout le monde	Autoriser	Refuser					
Exécution locale Image: Construction locale Exécution à distance Image: Construction locale Activation locale Image: Construction locale Activation à distance Image: Construction locale							
Informations sur le contrôle d'accès et les autorisations							
	ОК	Annule	er -				

<u>Remarque</u> : Si cela ne fonctionne pas, essayez toujours l'autre bouton « Modifier limites » et les 2 autres boutons. (« Modifier »).

Groupe de performance

Si vous obtenez une sortie inconnue du type avec un message contenant "2 WMI samples%". Il faut ajouter l'utilisateur dans le groupe local "Journal de Performance" s'il n'est pas administrateur de la machine

Renseigner les credentials WMI sur le boitier ESIA Unity

L'ensemble des manipulations ci-dessus étant faites, il ne reste plus qu'à renseigner les credentials WMI sur le boitier Unity.

Pour cela, rendez vous sur l'interface web du boitier Unity via son adresse IP et entrez les identifiants. (Comment configurer l'IP d'une Unity ?).



- Le nom d'utilisateur par défaut est : esia
- Mot de passe : gesa

Ensuite, rendez vous dans l'onglet WMI. Vous pouvez alors renseigner l'utilisateur, le mot de passe et le domaine avec lequel requêter en WMI :

Accueil	WMI	
IPMI	Nom d'utilisateur	esia
WMI	Mot de passe Domaine	WORKGROUP
JINTERFACE (IF-MIB)		Valider
Opdates		
Esia SA © copyright 2011 www.esia- network.com		
W3C 1.1 W3C css		

From: https://wiki.esia-sa.com/ - **Esia Wiki**

Permanent link: https://wiki.esia-sa.com/advanced/wmi_win_7_8



Last update: 2023/02/10 10:58