Enabling WMI on Windows Server 2012 via GPO

Here's how to enable WMI via GPOs on an Active Directory

User & group creation

Create a user (here: "wmiesia") with the password : Wmic2015 (in this tutorial). Don't forget to select "the password never expires" and "the user cannot change the password".

	welchist Utilization	t ordinateurs Active Directory	_ 0 ×
INO	uvel objet - Othisateur		
🕺 Créer dans : esia	local/Users	n Sallinakur d'a	
Prénom : esia	Initiales :	ateurs désigné ateurs désigné	
Nom :		ateurs désigné	
Nom complet : esia		ontrôleurs de	
		ves de ce grou	
Nom d'ouverture de session	de l'utilisateur :	res de ce grou	
wmiesia	@esia.local V	s administrate	
Nom d'ouverture de session	de l'utilisateur (antérieur à Windows 2000) :	DNS gui sont	
ESIA\	wmiesia	pres de ce grou	
		de passe des	
		de passe des	
	- Defendent Columnity Annular	'utilisateur inv	
	< Precedent Survant > Annuer	rvités du dom	
		stations de tr	
	Repriétaires Groupe de séc Les men	nbres de ce grou	
	Serveurs RA Groupe de séc Les serv	eurs de ce group	
	Utilisateurs Groupe de séc Tous les	utilisateurs du	
	& WinRMRem Groupe de séc Membe	rs of this group	
<			
	R		
			14:20
		G	08-07-15



Create a "WMIUSER" group with a global domain and "security" as the group type.

Utilisateurs et ordinateurs Active Directory	-	0	x
Fichier Action Affichage ?			
← ⇒ ≥ 📷 🗈 🗟 🕞 🛛 🗊 😤 🤽 🗑 🍸 💆 🤽			
Utilisateurs et ordinateurs Active Requêtes enregistrées Builtin Builtin Computers Computers Computers Computers Computers Computers Computers Computers Computers Computers Computers Créer dans : esia.local/Users Nom du groupe : WMILUSER Nom de groupe (antérieur à Windows 2000) : WMILUSER Ètendue du groupe Créer dans : Type de groupe Sécurité			
OK Annuler			
< III >			
	6	07: 09-0	14 7-15

Right-click on the Esia user and go to the "Member of" tab and add it to the WMIUSER group. Set the WMIUSER group as the main group and delete it from the "Domain user" group.

2025/05/03 00:57

3/22

	Utilisateurs et ordinateurs Active Directory	- 0	x
Fichier Action Affichage ?			
🕈 🕈 🔝 🖌 🖬 🔛 🖬	n 🐮 📚 🗑 🐨 🚨 📚		
Utilisateurs et ordinateurs Active Nom	Type Description		
Image: Service Accourt Image: Service Accourt Image: Serve Image: Ser	Propriétés de : esia 2 X vivormement Sessions Contrôle à distance Profil des services Bureau à distance COM+ énéral Adresse Compte Profil Téléphones Organisation Membre de Appel entrant Membre de :: Nom Dossier Services de domaine Active Directory Ubisateurs du do esia local/Users Vidiadeurs du do esia local/Users Vidiadeurs du do esia local/Users Vidiadeurs Vidiadeurs Ajouter Supprimer Stroupe principal : Utisateurs du domaine Définir le groupe principal In'est pas utile de modifier le groupe principal, saul si vous dignoser de cleints Macintosh ou d'applicatione compatibles POSIX. OK Annuler Appliquer		
		. 14	24
	19.13	08-0	7-15

You should now have :

	Utilisateurs et ordinateurs Active Directory	_ 0 ×
Fichier Action Affichage ?		
🗢 🔿 🙍 📅 🤞 🖬	2 🖬 🖬 🐮 🐮 🗑 🍸 🚨 🐮	
Utilisateurs et ordinateurs Active Nom	Type Description	
Requêtes enregistrées 4 Ad Builtin Ad Computers Ad Computers Ad Computers Ad Computers Co Comain Controllers Co	Propriétés de : esia ? Ermitornement Sessioni: Compte Général Addesse Compte Membre de : Membre de : Nom Dossier Services de domaine Active Directory MMIUSER esia.local/Users	
🔚 🛛 📋 🚿	2 Re 19	(b 14:25 08-07-15

You now have 2 options. Add the WMIUSER group to the "**Domain Admins**Add the WMIUSER group to the "Domain Admins" group, but this is not secure, or perform a manipulation on each machine to authorise a non-administrator user to connect.

Adding the WMIUSER group as an administrator

To add the WMIUSER group to the "Domain Admins" group, right-click on it and go to "Properties". Then go to the "Member of" tab and click "Add".

Type "admin" then click on "Check names".

	Utilisateurs et ordinateurs Active Directory	= 0 ×
Fichier Action Affichage ?		
← ⇒ ≥ □ 4 □ × □	a 🖦 🖬 📷 🗏 🐮 🐨 🧝 🍇	
Utilisateurs et ordinateurs Active	Nom Type Description	
a ∰ esia.local	Admir Propriétés de : WMIUSER ? X	
b Builtin g b Computers da	Admir Sélectionnez des groupes ? X	
Domain Controllers	Contre Sélectionnez le type de cet objet :	
ForeignsecurityPrincipal: Managed Service Accourting Managed Service Ac	Contre des groupes ou Principaux de sécurité intégrés Types d'objets	
C Users	Contro esia Jocal Emplacement.	
8	DnsAc Entrez les noms des objets à sélectionner (exemples) :	
8	& Éditeu admin Vérifier les noms	
8	Sesia B. Group	
8	& Group Avancé OK Annuler	
	R Invite Ayouter Supprmer	
8	Ordin Cette liste n'affiche que les groupes du domaine actuel et les groupes gérés dans le Catalogue	
8	global, tels que des groupes universels.	
8	R. Utilisa R. WinRA	
8	R WMU	
	OK Annuler Appliquer	
< III >		

Select "domain admin" and click OK.



Finally, click OK.

3	Utilisateurs et ordinateurs Active Directory	_	٥	x
Fichier Action Affichage ?				
🗢 🔶 🙇 🚾 🤞 🖾				
Utilisateurs et ordinateurs Active	Nom Type Description			
 Requetes enregistrees A A esia.local 	S Admin Propriétés de : WMIUSER ? X			
Builtin	& Admir Général Membre de Géné par			
Domain Controllers	Admin SR. Contra Membre de :			
ForeignSecurityPrincipal:	& Contre Nom Dossier Services de domaine Active Directory			
Managed Service Accourt Users	Admins du domaine esia Jocal/Users			
	8 Contre			
	A DISAC			
	88. Éditeu			
	sia come			
	Stoup			
	🐍 Invité			
	& Invités Ajouter Supprimer			
	Ordini Cette liste n'affiche que les groupes du domaine actuel et les groupes gérés dans le Catalogue Cette liste n'affiche que les groupes du domaine actuel et les groupes gérés dans le Catalogue			
	& Server			
	器 Utilisa ドロ Re weight			
	as wink			
	OK Annuler Appliquer			
< = >				

Creating the GPO (Groups Policies Objects)

Open the "Group Policy Manager" of your Active Directory. Right-click on your domain and create a new GPO (here: WMIACCESS)



In the security filters, delete "authenticated users" and add "domain computers".

<u>E</u>		Gestion de stratégie de groupe	_ 0 X
📓 Fichier Action Affichage	Fenétre ?		_ 8 ×
🗢 🔿 🙍 🖬 🖬			
Gestion de stratégie de groupe	WMIACCESS		
🔺 🛕 Forêt : esia.local	Étendue Détails Paramètres Délégati		
a 📸 Domaines	Liaisons		
a pa esia.local	Afficher les liaisons à cet emplacement :	sia local	
WMIACCESS	Les stes domaines et unités d'organisatio	e ivante cont liés à cet chiet GPD -	
⊿ 🗐 Domain Contro	Les sites, domanes el unites d'organisato	survants sort lies a cet objet diru .	
🛒 Default Dorr	Emplacement -	Appliqué Lien activé Chemin d'	80085
a 🌅 Objets de straté	geg esia local	Non Gui esia.ioda	
📑 Default Dorr			
Default Dom			
WMIACCES			
Filtres WMI			
🛅 Objets GPO Star			
iii Sites			
Modélisation de stratéc	Filtrage de sécurité		
Résultats de stratégie d	Les paramètres de cet obiet GPO ne s'app	quent qu'à ces groupes, utilisateurs et ordinateurs :	
	Nom		
	8 Ordinateurs du domaine (ESIA/Ordina	eurs du domaine)	
	Ajouter Supprimer	Propriétés	
	Filtrage WMI		
	Cet objet de stratégie de groupe est lié au	tre WMI suivant :	
	<aucun></aucun>	✓ Ouvrir	
< III >			
			De 6m de 08:50
			NO 169 NO 09-07-15

In the settings tab, right-click and then select "modify settings". In Computer configuration \rightarrow Policies \rightarrow Windows settings \rightarrow Security settings \rightarrow Local policies \rightarrow Security option

g .	Éditeur de gestion des stratégies de groupe	Ŀ	- 0 X
Fichier Action Affichage ?			
💠 🔶 🙍 💥 🔛 🔛 🔛			
Stratégie WMIACCESS [WIN-R70LAI1L3KU.ESIA.LOC ^	Stratégie	Paramètre	s de stratégie \land
a 🛃 Configuration ordinateur	Sécurité réseau : conditions requises pour la signature de client LDAP	Non défini	
🛛 🚞 Stratégies	Périphériques : permettre le formatage et l'éjection des médias amovibles	Non défini	
Paramètres du logiciel	Périphériques : ne permettre l'accès aux disquettes qu'aux utilisateurs connectés localement	Non défini	1
a 🔛 Paramètres Windows	Périphériques : empêcher les utilisateurs d'installer des pilotes d'imprimante	Non défini	
Stratégie de résolution de noms	Périphériques : autoriser le retrait sans ouverture de session préalable	Non défini	
Scripts (démarrage/arrêt)	B Périphériques : autoriser l'accès au CD-ROM uniquement aux utilisateurs ayant ouvert une session	Non défini	
Paramètres de sécurité	Paramètres système : utiliser les règles de certificat avec les exécutables Windows pour les stratégi	Non défini	
Stratégies de comptes	Deramètres système : Sous-systèmes optionnels	Non défini	
⊿ Strategies locales	B Ouvertures de sessions interactives : nombre d'ouvertures de sessions précédentes réalisées en util	Non défini	
Strategie d audit	B Ouverture de session interactive : seuil de verrouillage du compte d'ordinateur	Non défini	
Attribution des droits utilisater Ontions de sécurité	Duverture de session interactive : limite d'inactivité de l'ordinateur	Non défini	
lournal das événements	Duverture de session interactive : titre du message pour les utilisateurs essayant de se connecter	Non défini	_
b Groupes restreints	Duverture de session interactive : prévenir l'utilisateur qu'il doit changer son mot de passe avant q	Non défini	-
h Services système	Duverture de session interactive : nécessite l'authentification par le contrôleur de domaine pour le	Non défini	1
b 🙃 Registre	Duverture de session interactive : ne pas demander la combinaison de touches Ctrl+Alt+Suppr.	Non défini	1
Système de fichiers	Ouverture de session interactive : ne pas afficher le dernier nom d'utilisateur	Non défini	
b Stratégies de réseau filaire (IEEE 80)	Ouverture de session interactive : contenu du message pour les utilisateurs essayant de se connec	Non défini	
Pare-feu Windows avec fonctions	Ouverture de session interactive : comportement lorsque la carte à puce est retirée	Non défini	
Stratégies du gestionnaire de liste	Duverture de session interactive : carte à puce nécessaire	Non défini	1
þ 🚂 Stratégies de réseau sans fil (IEEE (Dijets système : renforcer les autorisations par défaut des objets système internes (comme les lie	Non défini	
Stratégies de clé publique	Dijets système : les différences entre majuscules et minuscules ne doivent pas être prises en com	Non défini	
b 🧮 Stratégies de restriction logicielle	Membre de domaine : signer numériquement les données des canaux sécurisés (lorsque cela est p	Non défini	
Protection d'accès réseau	Membre de domaine : nécessite une clé de session forte (Windows 2000 ou ultérieur)	Non défini	
Stratégies de contrôle de l'applica	Membre de domaine : désactive les modifications de mot de passe du compte ordinateur	Non défini	
þ 👼 Stratégies de sécurité IP sur Active	Membre de domaine : chiffrer ou signer numériquement les données des canaux sécurisés (toujo	Non défini	
Configuration avancée de la strate	Membre de domaine : chiffrer numériquement les données des canaux sécurisés (lorsque cela est	Non défini	
QoS basée sur la stratégie	Membre de domaine : ancienneté maximale du mot de passe du compte ordinateur	Non défini	
Modèles d'administration : définitions de De contraction : de contraction : définitions de De contraction : de contraction : définitions de De contraction : de contr	DCOM : Restrictions de démarrage d'ordinateur au format du langage SDDL (Security Descriptor D	O:BAG:BA	D:(A::CCDCSv
Preferences	DCOM : Restrictions d'accès à un ordinateur au format du langage SDDL (Security Descriptor Defi	O:BAG:BA	D:(A::CCDCLC
a no configuration utilisateur	Cryptographie système : force une protection forte des clés utilisateur enregistrées sur l'ordinateur	Non défini	
p Dréférences	Contrôleur de domaine : refuser les modifications de mot de passe du compte ordinateur	Non défini	~
<	< III		>
占 🛛 📋 🛷 📕		Re 19 (e	08:48 09-07-15

Double-click on "DCOM: Computer start-up restrictions in SDDL format". Then select the "Define this security parameter" box and click on "Modify security".



Click on "Add", type WMIUSER (the name of your WMI management group). Then click OK.

Tick the "Local execution" and "Remote execution" boxes. Click OK and then OK again.

B	Éditeur de gestion des stratégies de groupe		. 0 X	-
Fichier Action Affichage ?				
← ⇒ 🖄 📷 🗙 🖾 🕞 📓 🖬				
Stratégie WMIACCESS [WIN-R70LAI1L3KU.ESIA.LO	∧ Stratégie ▼	Paramètres r	de stratégie	~
4 🛃 Configuration ordinateur	El Sécurité réceau : forcer la fermeture de secsion quand les boraires de connexion expirent	Non défini	, , , , , , , , , , , , , , , , , , , ,	
4 🧮 Stratégies	Propriétés de : DCOM : Restrictions de démarrage ? X	Non défini		
Paramètres du logiciel		Non défini		
🛥 🧮 Paramètres Windows	Paramètre de stratégie de sécurité du modèle Expliquer	Non défini		
Stratégie de résolution de noms	the pool of the first statement	Non défini		
Scripts (démarrage/arrêt)	Autorisation d'exécution et d'activation ? ×	Non défini		
🔺 📠 Paramètres de sécurité	avant ouvert une session	Non défini		
b j Stratégies de comptes	findows nour les stratégi	Non défini		
a 📓 Stratégies locales	Nons de munes ou d'utilisateurs :	Non défini		
D 📓 Stratégie d'audit	g Reins de groupes de la manadara :	Non défini		
Attribution des droits utilisation	Administrateure (ESIA) Administrateure)	Nen diffici		
Options de sécurité		Non défini		_
Journal des événements	8. Utilisateurs du modèle CDM distribué (ESIA\Utilisateurs du mo	Nex 466-1		=
Groupes restreints	sayaric de se conneccer	Non defini		
b Services système b	on mot de passe avant q	Non defini		
Registre	Ajouter Supprimer pieur de domaine pour le	Non defini		
Système de fichiers	uches Cb1+Alt+Suppr.	Non défini		
b iii Strategies de réseau filaire (IEEE 8	Autorisations pour WMIUSER Autoriser Refuser	Non défini		
Pare-feu Windows avec fonction	rs essayant de se connec	Non défini		
Strategies du gestionnaire de list	Exécution locale	Non défini		
b and Strategies de reseau sans fil (IEEE Strategies de als aubliques)	Exécution à distance	Non défini		
b Strategies de cle publique b Stratégies de rectriction la sisielle	Activation locale	Non défini		
p Strategies de restriction logicielle b Deste ation d'anale sécond	Activation à distanceit pas être prises en com	Non défini		
p Protection d'acces reseau	curisés (lorsque cela est p	Non défini		
p Stratégies de controle de l'applic	ju ultérieur)	Non défini		
p Stategies de securite la strategies de la strategies	mpte ordinateur	Non défini		
p Configuration avancee de la stra b. Ju OoS basée sur la stratégie	Informations sur le contrôle d'accès et les autorisations Canaux sécurisés (toujo	Non défini		
 Madàlas d'administration : définitions d 	Ecurisés (lorsque cela est	Non défini		
p Préférences	OK. Annuler grow ordinateur	Non défini		
A Configuration utilisateur	SDDL (Security Descriptor D	Non défini		
b Stratégies	📓 DCOM : Restrictions d'accès à un ordinateur au format du langage SDDL (Security Descriptor Defi	Non défini		
Préférences	🗸 🗟 Cryptographie système : force une protection forte des clés utilisateur enregistrées sur l'ordinateur	Non défini		¥
< = >	K		>	
	f =f	2.82.4	07:49	
		0.6.0	09-07-15	

Double-click on "DCOM: Restrictions on access to a computer in the SDDL language format". Then select the "Define this security parameter" box and click on "Modify security".

Click on "Add", type WMIUSER (the name of your WMI management group). Click on OK.

Tick the "Local Access" and "Remote Access" boxes. Click OK and then OK again.



Don't forget to run gpupdate /force

Configuring the Windows firewall

<HTML>

</HTML> In your GPO, go to Computer Configuration \rightarrow Policies \rightarrow Windows Settings \rightarrow Security Settings \rightarrow Windows Firewall with Advanced Security Features \rightarrow Windows Firewall with Advanced Security Features \rightarrow Incoming Traffic Rules.

Right-click to create a "New rule ... ".



Select "Predefined" and choose "WMI Management Infrastructure". Click Next.



3 basic rules will be created, click next.

3	Éditeur de gestion des stratégies de groupe				- 0	x
Fic	Assistant Nouvelle règle de trafic entrant					
4	Règles prédéfinies Sélectionner les règles à créer pour cette utilisation.	rofil	Activée	Action	Remplacer	Pro
4	Etapes: Queles règles voulez-vous créer ? • Règles prédéfinies Les règles suivantes définissent les besoins en connectivité réseau pour le groupe prédéfini stéentormé. Les règles qui cont cochées seront créées. Si une règle cochée existe déjà, son contenu sera remplacé. • Action Règles : • Windows Management Instrumentation (JASyn Non Tout Règis Windows Management Instrumentation (JASyn Non Tout Règis Windows Management Instrumentation (DCD Non Tout Règis Configuration utilisateur) • Précédent Suivent > Annulet	erçu.				>
				R 😨	09:1 09-07-	7 -15

Leave "Allow connection" selected and click Finish.

17/22



Don't forget to run gpupdate /force

Add the WMIUSER group as a single user

<HTML>

```
<style>
    #ajout_du_groupe_wmiuser_en_tant_que_simple_utilisateur:after
{content:" (OPTION)"; font-size:.75em; font-weight:500;}
    </style>
```

</HTML> (! To be used on all machines)

This involves giving remote access rights to the user account that will be used by ESIA to access the WMI data. This operation must be carried out on each of the machines to be interrogated.

To do this :

Go to "Computer Management" (or enter the command "wmimgmt.msc". Then scroll down to "Services and Applications" so that you can right-click on "WMI Control" and click on "Properties".



In the "Security" tab of the "WMI Control Properties", select the "Root" namespace and then click on "Security": WMI Control", select the "Root" namespace and then click on "Security".

If you want to fine-tune security, the namespaces 'Root \rightarrow CIMV2' and 'Root \rightarrow SecurityCenter2' are those used by ESIA.



Appliquer

<

e

>

Ê.

🛃 🔕

Last update: 2023/11/09 18:0	07 en:advanced:wmi_win_serveur_2012 https://wiki.esia-sa.com/en/adva	nced/wmi_win_serveur_2012
Fichier Action Affichage ?	Gestion de l'ordinateur	- ð ×
Sestion de l'ordinateur (local)	-	Actions
Outils système Oliver de ticher	Propriétés de : Contrôle WMI ? ×	Contrôle WMI
 Planificateur de tâches Observateur d'événeme Dossiers partagés Utilisateurs et groupes I Performance Gestionnaire de périphé Stockage Stockage Gestionnaire des service Services et applications Gestionnaire des service Services Contrôle WMI SQL Server Configuratic 	Co Sénéral Sauvegarder/Restaurer Sécurté Options avancées La navigation dans l'espace de noms vous permet de définir des options de sécurté spécifiques à l'espace de noms. Root Co Root Co Clive DEFAULT Co	Autres actions
< >>		
🖬 🙆 🚞 🖻		- 🍡 🔁 🕼 10:38
		20-00-13

Select the user account that will be used for remote access and tick the "Authorise" boxes for "Enable account" and "Remote call authorised", which are the 2 authorisations required.



Check that the authorisations have been applied to the selected namespace and its sub-namespaces by clicking on "Advanced" to check the "Applies to" column.

<u>*</u>	Gestion de l'ordinateur				- 8 ×
Fichier Action	Affichage ?				
🗢 🏟 🖄 📴	T. Par	amètres de sécurit	é avancés pour Root	– 🗆 🗙	
Gestion de l' Gutils sys Dutils sys De Planif De Conse Dessibility Dessibilit	Propriétaire : Administrateurs (win8vm\Administrateurs) Modifier Autorisations Audit Pour obtenir des informations supplémentaires, double-cliquez sur une entrée d'autorisation. Pour modifier une entrée d'autorisation, sélectionnez l'entrée et cliquez sur Modifier (si disponible). Entrées d'autorisations : Tuno Principal				s rôle WMI
 Services ↓ ♥ Gestic Gestic Gestic	Auto Utilisateurs authentifiés Auto SERVICE LOCAL Auto SERVICE RÉSEAU Auto Julien George (, Auto Administrateurs (win&vm\Ad Ajouter Supprimer Modifie Désactiver l'héritage	spéciale Aucun Spéciale Aucun Spéciale Aucun Spéciale Aucun Spéciale Aucun	Aucun Aucun Aucun Aucun Aucun	Cet espace de noms et les sou Cet espace de noms et les sou Cet espace de noms et les sou Cet espace de nom <u>et les sou</u> Cet espace de nom <u>s</u> et les sou)))) ter Supprimer utoriser Refuser
٤	>		OK	Annuler Appliquer Autorisations spéciales Pour les autorisations spéciales et les parar avancés, cliquez aur Avancé. Informations sur le contrôle d'accès et les a OK	Netres Avancé utorisations Annuler Appliquer
- To Table					

That's it, WMI is now activated.

