ManageEngine

非管理员域用户的 WMI 日志收集



概要

- 1. 在 Active Directory 中创建一个非管理员域用户。
- 2. 将创建的用户添加到必要的 AD 用户组。
- 3. 在组策略管理控制台中创建一个新的组策略。
- 4. 指派权限给创建的用户。
- 5. 强制创建的组策略。
- 6. 在 WMi 客户端和服务器中更新组策略。
- 7. 授予 WMI 命名空间安全权限给创建的用户。
- 8. 授予 COM 权限给创建的用户。
- 9. 在 EventLog Analyzer 的 web 控制台使用该非管理域用户的凭证进行日志收集。

步骤

1. 在 Active Directory 中创建一个非管理员用户

- a. 打开 Active Directory 用户和计算机。
- b. 点击 用户>新建>用户。
- c. 在弹出的窗口中输入指定的详细信息,并创建用户。

(23)	
🤏 Creat	e in: EVENTLOG1.COM/Users
First name:	WMINDA Initials:
Last name:	
Full name:	WMINDA
User logon name	
WMINDA	@EVENTLOG1.COM V
User logon name	(pre-Windows 2000)
EVENTLOG1\	WMINDA

2. 将创建的用户添加到必要的 AD 用户组

在创建的用户上点击右键并选择添加到组。.用户需要添加到以下组中。

- Performance Log Users
- Distributed COM Users

Security	6	vironment	Sessions		Remot	Remote control	
Remote	Deaktop Se	aktop Services Profile		DM+	Attrib.	te E	ditor
General	Address	Account	Profile	Telephone	es C	Irgan	ization
Published C	ertificates	Member Of	Passwon	d Replication	Dial	in	Object
Member of	£1						
Name			Active I	Directory Dor	nain Se	rvice	e Fc
Distribute	d COM Use	ers	EVENT	LOG1 COM	Builtin		
Domain	Jeere		EVENT	LOG1 COM/	Users		
renorma	HCC LOG LC	cia	EVENUE	LOGICOM	Buildh		
<							2
< Add .		ш Зеточе					>
Add . Primary gro	. f	III Remove					>
Add . Primary gro	. f nup: D nary Group	III Remove omain Users There is n you have application	o need to Macintosh ns.	change Prim cliente or PC	any grou JSIX-co	ip uni mplia) ess int

3. 在组策略管理控制台中创建一个新的组策略。

4. 指派权限给创建的用户

- a. 右键点击创建的组策略, 然后点击编辑。
- b. 打开组策略管理编辑器, 打开计算机配置 > 策略> Windows 设置 > 安全设置> 本地策略> 用户权限分配。
- c. 右键点击指定的权限然后点击属性,授予创建的用户以下权限。
- d. 启用定义这些策略设置,点击添加用户和组,选择创建的用户然后点击应用权限。

Copyright © 2018 ManageEngine

ManageEngine EventLog Analyzer

权限

- 以操作系统的方式执行 •
- 作为批处理作业登录 .
- 作为服务登录 .
- 替换一个进程级令牌
- 管理审核和安全日志



El] Access Credential Manager as a trusted caller Not Defined Not Defined CAccess this computer from the network Act as part of the operating system Add workstations to domain Not Defined Adjust memory guotas for a process Not Defined Allow log on locally Not Defined C Allow log on through Remote Desktop Services Not Defined Back up files and directories Not Defined Bypass traverse checking Not Defined Change the system time Not Defined Change the time zone Not Defined Create a pagefile Not Defined Create a token object Not Defined Create global objects Not Defined Not Defined Create permanent shared objects Create symbolic links Not Defined Not Defined Debug programs Deny access to this computer from the network Not Defined Deny log on as a batch job Not Defined Deny log on as a service Not Defined Deny log on locally Not Defined Deny log on through Remote Desktop Senices Not Defined Enable computer and user accounts to be trusted for delega.. Not Defined E Force shutdown from a remote system Not Defined Constants security audits Not Defined Impersonate a client after authentication Not Defined Increase a process working set Not Defined Increase scheduling priority Not Defined Load and unload device drivers Not Defined El Lock pages in memory Not Defined Log on as a batch job Log on as a service Manage auditing and security log C Modify an object label Not Defined R Modify firmware environment values Not Defined Perform volume maintenance tasks Not Defined Profile single process Not Defined Profile system performance Not Defined Not Defined Remove computer from docking station Replace a process level token Not Defined Restore files and directories Shut down the system Not Defined Synchronize directory service data Not Defined Take ownership of files or other objects Not Defined

EVENTLOG!\WWINDA EVENTLOGINWMINDA EVENTLOGI\WWINDA EVENTLOG!\WMINDA EVENTLOG!\WWINDA

5. 强制创建的组策略

在左窗格中,右键单击创建的组策略并单击强制。

6. 在 WMI 客户端和服务器中更新组策略

在客户端和服务器中以管理员的方式打开命令提示符,并运行以下命令。



7. 授予 WMI 命名空间安全权限给创建的用户

a. 在要收集日志的域控制器中,打开 WIN+R,输入 wmimgmt.msc 打开 WMI 管理控制台。

a	wmimgmt - [Console Root\WMI Control (Local)]	- 0	×
File Action View Favorit	es Window Help	-	@ ×
••• 200 0 0 0 0	¥		
Console Root	A	Actions	
	Windows Management Instrumentation (WMD	WMI Control (Local)	
	Configure WMI Control (Local) Properties 7	Mole Actions	10
	Deneral Backup/Penton Security Advanced		
	Samespace ravigation allows you to set mensapace specific security.		
	H 😲 Ret		
	Security		
	OK Genoel Apply		
			-

- b. 右击 WMI 控件(本地),点击属性。
- c. 在 WMI 控件属性窗口中,点击安全页签。
- d. 在安全页签中,展开 Root 命名空间,选择 CIMV2 命名空间。

ManageEngine

LOCAL SERVICE	8	_
Anix (Anix@EVENTLO	G1.COM) EVENTI OG1.COM	=
Administrators (EVENT	LOG1\Administrators) ~
<u> </u>	Add	Remove
ermissions for WMINDA	Allow	w Deny
Execute Methods	✓	
Full Write		
Partial Write		
Provider Write		
Enable Account	~	
	Lawrence of the Marcola	

- e. 点击右下角的安全设置按钮,打开 ROOT\CIMV2 的安全设置。
- f. 点击**添加**并选择创建的用户。
- g. 用户现在需要被授予权限。点击用户,勾选以下权限的允许选框。
 - i. 执行方法
 - ii. 启用账户
 - iii. 远程启用
 - iv. 读取
- h. 应用变更并点击确定,退出 WMI 管理控制台。

8. 授予 COM 权限给创建的用户

a. 在要收集日志的域控制器中,打开开始>管理工具>组件服务。

- B-	Compo	nent Services	- 0 ×
 File Action View Wind ◆● ● 2 □ □ □ □ □ □ 	ew Help [11] 11] 12] 24 18 18 18 18		_ # ×
Console Root		Actions	
b R Component Services	Computers	Component Services	*
p 🤤 Services (Local)		More Actions	

- b. 打开**计算机文件夹;**进入我的电脑> 属性> COM 安全。
- 在访问权限中,点击编辑限制,点击添加,添加创建的用户。授予所有的权限,然后点击确定。

General	Options	Defa	ault Properties
Default Protocols	COM Sec	unty	MSDTC
Access Permissions			
You may edit who is also set limts on app Caution: Mo of applications securely	allowed default according to the second default according to the second default according to start, connect according to start, connect according to start, connect according to start, connect according to start.	ase to applic ine their ow issions can function ar	ations. You ma n permissions. affect the ability nd/or run
	Edit Limits	E	dt Defaut
aunch and Activation	Permissions		
Tournuy car who is	allowed by default to	launch app	dications or
determine their own determine their own Affect the a and/or run	allowed by default to umay also set limits o permissions. odfying launch and a shifty of applications t securely.	o launch app on applicatio activation pe to start, con	olications or ons that emissions can nect, function
activate objects. Yo determine their own Caution: M affect the a and/or run	allowed by default to u may also set limits (permissions, odfying launch and a shifty of applications t securely, Edit Limits	o launch apj an applicatio activation pe to start, con	elications or ons thet amissions can nect, function idt Defaut
activate objects. Yo determine their own affect the a and/or run	allowed by default to u may also set limits (permissions, odfying launch and a bitty of applications : securely, Edit Limits	s lounch app an application activation pr to start, con	olications or ans that emissions can nect, function idt Defaut

● 在启用和激活权限,点击编辑限制,点击添加,添加创建的用户。授予所有的权限,然后点击确定。

Administrators (EVENTLOG1V	Administrators)		^
Performance Lo Distributed COI WMINDA (WM)	og Users (EVEN 14 Users (EVEN 11NDA@EVEN1	TLOG1\Perform TLOG1\Distribut [LOG1.COM]	ed COM I	Jee =
			TI	2
	[Add	Remo	ve
rmissions for WMI	NDA	Alow	Den	у
Local Launch Remote Launch Local Activation Remote Activation	1	NNN		

您授予上述所有权限之后,创建的非管理员用户就能够从域控制器中收集日志了。

9. 在 EventLog Analyzer 的 web 控制台使用该非管理域用户的凭证进行日志收集。