

N- Partner N-REPORTER

用户如何使用 WMI 管理配置 Windows AD Server 日志 V 1.1.2 (简体)



前言

本文件描述 N-Reporter 用户如何使用 WMI 管理配置 Windows AD Server 日志。

文件章节如下:	
1. 配置 Windows AD Server	2
1-1 配置 Windows 2003 AD Server	2
1-1-1 新增 WMI 远程登录的域用户	2
1-1-2 Windows 2003 AD Server 审核配置	6
1-1-3 Windows 2003 AD Server 防火墙配置	6
1-2 配置 Windows 2008 AD Server	9
1-2-1 新增 WMI 远程登录的域用户	9
1-2-2 Windows 2008 AD Server 审核配置	
1-3 配置 Windows 2012 AD Server	
1-3-1 新增 WMI 远程登录的域用户	14
1-3-2 Windows 2012 AD Server 审核配置	
2.新增 Windows AD Server WMI 设备	
2-1 新增 Windows AD Server WMI 设备	
2-2 设定 NTP Server	21
連絡資訊	

1. 配置 Windows AD Server

1-1 配置 Windows 2003 AD Server

1-1-1 新增 WMI 远程登录的域用户

以域管理员账号 administrator 登录Windows AD server, 鼠标左点 [开始 / 所有程序 / 管理

工具 / Active Directory 用户和计算器]。



鼠标左点根域(forest root domain),本例为 NPWin2k3chs.local。右点[Users],左点[新建 / 用



名输入"npartner",用户登录名输入"npartner",左点[下一步]。

新建对象 - 用户	×
创建在: NFWin2k3chs.local/Users	
姓(止):	
名 (E):	
姓名(A): npartner	
用户登录名(10):	
npartner @NPWin2k3chs.local 💌	
用户登录名 (Windows 2000 以前版本) (W):	
NPWIN2K3CHS\ npartner	
< 上一步 (B) 下一步 (B) > 取消	

输入密码。只勾选[密码永不过期]。左点[下一步]。左点[完成]。

新建对	象 - 用户		×
<u></u>	く 创建在: NPW;	in2k3chs.local/Users	
strT	1 m	· · · · · · ·	_
2014	9(£):	******	_
确i	人密码(C):	****	
	用户下次登录时须更改	(密码 (M)	
Г	用户不能更改密码(<u>S</u>)		
V	密码永不过期(2)		
_			
		〈上一步®)下一步®)〉	取消

鼠标左点 [Users]。右点 WMI 远程登录用户 npartner, 左点[添加到组]。

≪∮Active Directory 用户和计算机				
<и>✓ 文件(12) 操作(4) 查看(2) 窗口(32) 帮助(4)				_ Ð ×
← → 🗈 🖬 🗼 🛍 🗙 📽 🖻 🗟 😢 💷 🦉 🖉 🚵	7 🍕 📴			
Active Directory 用户和计算机 [win2003ADchs. NPWin2k3chs.loce	Users 18 个对象			
	名称	类型	描述	
Entranzkochs. Local	🕵 ad_user1	用户		
	🛃 Administrator	用户	管理计算机(域)的	讷置
Domain Controllers	🕵Cert Publishers	安全组 - 本	此组的成员被允许	f发行
F. ForeignSecurityPrincipals	🚮 DnsAdmins	安全组 - 本	DNS 管理员组	
	🕵 DnsUpdateProxy	安全组 - 全局	允许替其他客户端	₩დე⊡
	🕵 Domain Admins	安全组 - 全局	指定的域管理员	
🕀 💼 Program Data	🕵 Domain Computers	安全组 - 全局	加入到域中的所有	「工作
<u>∓ Svstem</u>	🕵 Domain Controllers	安全组 - 全局	域中所有域控制器	<u>}</u>
Sers Vsers	🕵 Domain Guests	安全组 - 全局	域的所有来宾	
	🕵 Domain Users	安全组 - 全局	所有域用户	
	🕵 Enterprise Admins	安全组 - 全局	企业的指定系统管	理员
	🕵 Group Policy Creator	安全组 - 全局	这个组中的成员可	f以修
	🥵 Guest	用户	供来宾访问计算机	【或访
	👧 krbtgt	用户	密钥发行中心服务	9帐户
	🕵 npartner	用户		1
	💯 RAS and IAS Servers	安全統一本	复制(C)	可以
	🕵 Schema Admins	安全组 - 全	添加到组(G)	理员
	🕵 win2k3ad_chs_user1	用户	名称映射(P)	
			禁用帐户(S)	
			重设密码(E)	
			移动(V)	
			打开主页 (0)	
为当前选择重设密码。			剪切(I)	
			囲ぼ(D)	
			重命名(20)	
			雇性 (B)	
			帮助 (Y)	

鼠标左点[高级 / 立即查找 / Domain Admins / 确定]。将 WMI 远程登录用户 npartner 加入 到域管理员组中。

选择组	?×
选择对象类型 (S):	
组或内置安全主体	
, 查找位置 (E):	
NPWin2k3chs.local	位置(L)
~ 输入要选择的对象名称(例如)(B):	
	检查名称(C)
高级 (A)	确定 取消
选择组	<u>?×</u>
选择此对象类型 (S):	
组或内置安全主体	対象类型 (0)
查找位置 (2):	
NPW1n2k3chs.local	位査(L)
一般性查询	
名称 (4): 开始 🔻	列(C)
描述 印): 王治 🔽	
	停止(四)
□ 宗市的限户 (b) □ 不过期密码 (x)	
	确定 取消
捜索结果(U):	
名称 (RDN) 描述 住又件夹	T locel/Bui
Administrators NPWingk3	chs. local/Bui
Backup Operators	chs.local/Bui
@Cert Publishers 此组的成员, NPWin2k3	chs.local/Users
Distributed CO NPWin2k3	chs.local/Bui
🚺 👧 DnsAdmins 🖌 🐹 管理员组 NPWin2k3	chs.local/Users
ngunsUpdateProxy	chs.local/Users
👔 Domain Admins 指定的域管理员 NPWin2k3	chs.local/Users
1 🕵 Domain Computers 加人到域中 NPWin2k3	chs.local/Users
II Omain Control 域中所有域 NFWin2k3	chs.local/Users

左点[确定]。

选择组	<u>?×</u>
选择对象类型 (S):	
组或内置安全主体	对象类型 (0)
查找位置 (2):	
NFWin2k3chs.local	位置(L)
输入要选择的对象名称(例如)(图):	
Domain Admins	检查名称 (C)
局級 (A)	

1-1-2 Windows 2003 AD Server 审核配置

请依照文件「Windows AD audit to syslog」第2章「Windows 2003 AD Server 审核配置」,

配置默认域控制站(Default Domain Controller)的审核策略(Policy)。

1-1-3 Windows 2003 AD Server 防火墙配置

鼠标左点[开始 / 所有程序 / 附件 / 命令提示符]。



输入『gpedit.msc』,开启[组策略对象编辑器]设定[本机计算器原则(Local Computer Policy)]。



鼠标双击 [计算器配置 / 管理模板 / 网络 / 网络连接 / Windows 防火墙 / 标准配置文件]。

双击[Windows 防火墙: 允许远程管理例外(Windows Firewall: Allow remote administration

exception)].



勾选[己启用], 左点[确定]。



注1:若用户环境有防火墙设备,请开放 Windows AD Server 的 DCOM port TCP 135。

1-2 配置 Windows 2008 AD Server

1-2-1 新增 WMI 远程登录的域用户

以域管理员账号 administrator 登录 Windows AD server, 鼠标左点 [开始 / 所有程序 / 管理

工具 / Active Directory 用户和计算器]。



鼠标左点根域(forest root domain),本例为 NPwin2k8chs.local。右点[Users],左点[新建 / 用

户]。

🧧 Active Directory 用户和计算机						
文件(F) 操作(A) 查看(V) 帮助(H)						
A A						
📃 Active Directory 用户和计算机 [win2k8s	名称		类型	描述		
🖸 🛄 保存的查询	💧 ad_user:	1	用户			
🖃 🏥 NPwin2k8chs.local	📕 🤱 Adminis	& Administrator		管理计算机(域)的内置		
🕀 🛄 Builtin	Allowed	RODC Password Rep	安全组 - 本	允许将此组中成员的密		
- mputers	🥵 Cert Pul	blishers	安全组 - 本	此组的成员被允许发布		
+ 🔤 Domain Controllers	👫 Denied 1	RODC Password Repl	安全组 - 本	不允许将此组中成员的		
+ ForeignSecurityfrincipals	📲 DnsAdmin	ns	安全组 - 本	DNS Administrators 组		
▲ 0580-5-5 ● 季派控制 (R)	👫 DnsUpda	teProxy	安全组一全	局 允许替其他客户端 如		
音楽(II)	Bomain J	Admins	安全组一全	局指定的域管理员		
	Bomain (Computers	安全组一全	局 加入到域中的所有工作		
新建 (ヌ) 计算机	η,	ontrollers	安全组一全点	局 域中所有域控制器		
所有任务 🕰 🕨 联系/		luests	安全组一全点	同 域的所有来兵		
(本手の) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1		sers	安全组一全	同所有域用户		
旦目(V) Inet(rgPerson	se Admins	安全组一通	用 企业的指定系统管理页		
刷新(F) MSMQ	队列别名	se Kead-only Doma	安全组一通	用 该组的成页是企业中的		
导出列表 (L) 打印相	t	licy Creator Uwners	安全组一全	同 这个组甲的成贝可以修		
用户			用户	供米兵功问计昇机或功		
	て件実	710.0	用户	泣來如古的眼冬眼耳미		
帮助(H)	de P l	JIAD Dervers	女王组 - 本	··· 这个组中的服务器可以··· 目前,此组点的武器目标中口		
	Acad-on	Ly Domain Controllers	女王组 二王. 安公祖 二语!	问 既组甲的购贝定缴甲只 田 加扬的指令系统管理号		
	Chema J	Admins J 1	女王组 一 通	用 采钩的相连系统管理风		
	winzkoa	a_cns_user1	щР			
在此容器中创建一新的项目。						

名输入"npartner",用户登录名输入"npartner",左点[下一步]。

新建对象 - 用户		×
2 创建于	: NFwin2k8chs.local/Users	
姓(L):		
名():	npartner 英文缩写(I):	
姓名(A):	nparimer	
用户登录名(10):		
npartner	@NPwin2k8chs.local 💌	
用户登录名(Wind	ows 2000 以前版本)(W):	
NPWIN2K8CHS\	npartner	
	<上一步 (B) 下一步 (M) > 取消	

输入密码。只勾选[密码永不过期]。左点[下一步 / 完成]。

新建对象 - 用户	×
创建于: NPwin2k8chs.local/Users	
密码 (P):●●●●●●●●●确认密码 (C):	
 □ 用户下次登录时须更改密码(M) □ 用户不能更改密码(S) ☑ 密码永不过期(W) 	
□ 帐户已禁用 (0)	
< 上一步 (B) 下一步 (B)) 取消	

鼠标左点 [Users]。右点 WMI 远程登录用户 npartner, 左点[添加到组]。

■ Active Directory 用户和计算机							
文件(F) 操作(A) 查看(V) 帮助(H)							
(= =) 2 📅 4 📋 🗙 🖹 Q 📑 🛛 🖬 🔧 🐮 🔻 🗵 🖉							
 Active Directory 用户和计算机 [win2k8e ● 保存的查询 ■ Wwin2k8chs.local ● Duiltin ● Computers ● Domain Controllers ● ForeignSecurityPrincipals ● Users 	名称 ad_user1 Administrator Administrator Cert Publishers Denied RODC Password Repl Donain & RoDC Password Repl Do	<u>类型</u> 用用安全全全全全全全全全全全全全全全全全全全全全全全全全全全全全全全全全全全	描述 管理计算机(域)的内置 允许将此组中成员的密 此组的成员被允许发布 不允许将此组中成员的 DNS Administrators 组 允许替其他客户端做口 指定的域管理员 加入到域中的所有工作 域中所有域控制器 域的所有来宾 所有域用户 企业的指定系统管理员 该组的成员是企业中的 这个组中的成员可以修	· · · · · · · · · · · · · · · · · · ·			
▲ ▲ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	A Guest Inpartner RAS and IAS Servers Read-only Domain Controllers Schema Admins win2k8ad_chs_user1	用户 用户 安全组 - 全局 安全组 - 通用 用户	供来兵访问计算机或访 夏制(C) 添加到组(G) 禁用帐户(S) 重置密码(C) 移动(V) 打开主页(D) 发送邮件(A) 所有任务(C) 開切(T) 開除(D) デーク(C)	• • •			
			里市召 (M) 属性 (R) 帮助 (H)				

鼠标左点[高级 / 立即查找 / Domain Admins / 确定]。将 WMI 远程登录用户 npartner 加入 到域管理员组中。

选择组				<u>?×</u>
选择此对象类型(S):				
组或内置安全主体			对象类型	(0)
查找位置(1):				
NPwin2k8chs.local			查找范围	(L)
输入对象名称来选择(示例))(E):			
			检查名和	尔(C)
高級(A)		确定		消
进报 相				2 2
及件组				<u> </u>
选择此对象类型(S):				a ** #1(0)
组験内立文主主体 本状常同ない			X73	x央型(0)
NPwin2k8chs.local				立帯 (エ)
一般注意问				Til (c)
名称(A): 起始为	•			
描述 (D): 起始为	-			立即查找()()
□ 禁用的帐户(B)				停止(T)
■ 不过期密码(X)				
自上次登录后的天数 (I)	:			- 77
搜索结果(V):			确定	
名称 (RDN)	描述	在文件夹		<u> </u>
Backup Operators	Y细的成员	NPwin2k8chs.loc	al/Builtir al/Neers	L
Certificate Servic	FC-TH DAYS	NPwin2k8chs.loc	al/Builtir	
Cryptographic Over	25.45.11	NPwin2k8chs.loc	al/Builtir	۰ – – – – – – – – – – – – – – – – – – –
Denied RODC Passwo	不元讦将此	NPwin2k8chs.loc	al/Users al/Builtir	
DisAdrins	DNS Adminis	NPwin2k8chs.loc	al/Users	
A DnsUpdateProxy	允许替其他	NPwin2k8chs.loc	al/Users	-
Domain Admins	指定的域管理员	NPwin2k8chs.loc	al/Users	
Domain computers	加入主印教中中	MIWINZROCHS, 100	aryosers	-

左点[确定]。

选择组	<u>?</u> ×
选择此对象类型(S):	
组或内置安全主体	对象类型(0)
查找位置(#):	
NPwin2k8chs.local	查找范围(L)
输入对象名称来选择(<u>示例</u>)(2):	
Domain Admins	 检查名称(C)
高级(A)	

1-2-2 Windows 2008 AD Server 审核配置

请依照文件「Windows AD audit to syslog」第3章「Windows 2008 AD Server 审核配置」,

配置默认域控制站(Default Domain Controller)的审核策略(Policy)。

注2:若用户环境有防火墙设备,请开放此 Windows AD Server 的 DCOM port TCP 135。

1-3 配置 Windows 2012 AD Server

1-3-1 新增 WMI 远程登录的域用户

以域管理员账号 administrator 登录 Windows AD server, 鼠标左点 [Start(开始)/

Adminitratives Tools(管理工具) / Active Directory Users and Computers(Active Directory 用

户和计算器)]。

) 💿 - 🛧 🔞 • !	Control Panel 🔸 System and Security 🔸 Administra	tive Tools 🕨	~ C	Search Administrative	Tools 🔎
Favorites	Name	Date modified	Туре	Size	
Desktop	Terminal Services	8/22/2013 11:39 PM	File folder		
📜 Downloads	Active Directory Administrative Center	8/22/2013 7:50 AM	Shortcut	2 KB	
📃 Recent places	Active Directory Domains and Trusts	8/22/2013 2:55 PM	Shortcut	2 KB	
30-5-5 3-1	Active Directory Module for Windows Po	8/22/2013 2:55 PM	Shortcut	2 KB	
🖳 This PC	Active Directory Sites and Services	8/22/2013 2:55 PM	Shortcut	2 KB	
	Active Directory Users and Computers	8/22/2013 2:55 PM	Shortcut	2. KB	
📮 Network	ADSI Edit	8/22/2013 2:55 PM	Shortcut	2 KB	
	Component Services	8/22/2013 2:57 PM	Shortcut	2 KB	
	💦 Computer Management	8/22/2013 2:54 PM	Shortcut	2 KB	
	📸 Defragment and Optimize Drives	8/22/2013 2:47 PM	Shortcut	2 KB	
	A DNS	8/22/2013 2:55 PM	Shortcut	2 KB	
	🔚 Event Viewer	8/22/2013 2:55 PM	Shortcut	2 KB	
	🚟 Group Policy Management	8/22/2013 2:56 PM	Shortcut	2 KB	
	🙈 iSCSI Initiator	8/22/2013 2:57 PM	Shortcut	2. KB	
	ᡖ Local Security Policy	8/22/2013 2:54 PM	Shortcut	2 KB	
	📆 ODBC Data Sources (32-bit)	8/22/2013 7:56 AM	Shortcut	2 KB	
	📆 ODBC Data Sources (64-bit)	8/22/2013 2:59 PM	Shortcut	2 KB	
	Performance Monitor	8/22/2013 2:52 PM	Shortcut	2 KB	
	B Resource Monitor	8/22/2013 2-52 PM	Shortcut	2 KB	
items					833

鼠标左点根域(forest root domain),本例为 NPWin2012r2.local。右点[Users],左点[New/

User]。

	Active Directory Users and Computers		_ 0 X
File Action View Help			
🗢 🔿 📶 🔏 🗊 🔏 🖨	🗟 🖬 🖬 % 🎕 🛅 🍸 🚨 🗞		
Active Directory Users and Computers	Name	Туре	Description 🔥
Saved Queries	🚴 Administrator	User	Built-in account f
⊿ 🚔 NPWin2012r2.local	Allowed RODC Password Replication Group	Security Group	Members in this 🤉
▷ Builtin	Sert Publishers	Security Group	Members of this
Computers	🙈 Cloneable Domain Controllers	Security Group	Members of this
Domain Controllers	💐 Denied RODC Password Replication Group	Security Group	Members in this 🤇
▷ OreignSecurityPrincipals	A DnsAdmins	Security Group	DNS Administrate
Managed Service Accounts	🎎 DnsUpdateProxy	Security Group	DNS clients who
Delegate Control	main Admins	Security Group	Designated admir
eregate condoin.	imain Computers	Security Group	All workstations a \equiv
Finda	main Controllers	Security Group	All domain contr
New	Computer	Security Group	All domain guest
All Tasks	Contact	Security Group	All domain users
Manu	Group	Security Group	Designated admir
01200		Security Group	Members of this
Refresh		Security Group	Members in this 🤉
Export List	msDS-ResourcePropertyList	User	Built-in account f
Properties	msImaging-PSPs	Security Group	Members of this
	MSMQ Queue Alias	Security Group	Servers in this gro
Help	Printer	Security Group	Members of this
12 SP 02 01 - 22	S User	Security Group	Designated admii 🧹
<	Shared Folder		>
Creates a new item in this container.			

名(Last name)输入"npartner",用户登录名(User logon name)输入"npartner",左点[下一步

(Next)]。

cal/Users	Initials:	
	Initials:	
NPWin2012	2r2.local	~
artner		
-		
-		1
		partner

输入密码(password)。只勾选[密码永不过期(Password never expires)]。左点[下一步(Next)/

完成(Finish)]。

Password:		•••••	 1
Confirm passwor	rd:	•••••	1
User cannot	change ever expir	password ass	

鼠标左点 [Users]。右点 WMI 远程登录用户 npartner, 左点[添加到组(Add to a group)]。

3	Active Directory Users and (Computers		×
File Action View Help				
🗢 🔿 📶 🔏 🗈 🔀 🖬 🧔	🗟 🛛 🖬 🗏 🐮 🍞 🗕	8		
Active Directory Users and Computers Saved Queries Saved Queries Builtin Computers Computers Solution Managed Service Accounts Users	Name Administrator Administrator Cert Publishers Cloneable Domain Controllers Denied RODC Password Replicatio Donsid RODC Password Replicatio DnsAdmins DosUpdateProxy Domain Admins Domain Computers Domain Computers Domain Controllers Domain Guests Domain Users Enterprise Read-only Domain Control Group Policy Creator Owners	on Group n Group trollers	Type User Security Group Security Group	Description Built-in account f Members in this c Members of this Members of this Members of this DNS Administrate DNS clients who Designated admin All workstations a All domain contre All domain guest All domain users Designated admin Members of this Members in this c
III > Allows you to add the selected objects to a	Guest Protected Users RAS and IAS Servers Read-only Domain Controllers c group you select.	Copy Add to a group. Disable Account Reset Password. Move Open Home Pay Send Mail All Tasks Cut Delete Rename Properties	User oup t ge	Built-in account f
		Help		

鼠标左点[高级(Advanced) / 立即查找(Find Now) / Domain Admins / 确定(OK)]。将 WMI 远

程登录用户 npartner 加入到域管理员组中。

	Select Groups	×	<u>.</u>	
Select this object type:				
Groups or Built-in security principa	ls Ot	oject Types	6	
From this location:	1			
NPWin2012r2.local	1	Locations		
Color the object access to color t (
Enter the object names to select (e	xamples).	Last Massa	te la la	
		neck Mames	6.	
Advanced		Cancel		
Auvanceu		Cancer	41	
	Select Groups			x
	Selectoroups			_
Select this object type:				
Groups or Built-in security principa	ls	Object Type	əs	
From this location:				
NPWin2012r2.local		Locations		
Common Queries				
				-
Name: Starts with 🗸	-		Jolumns	4
Description: Starts with 🐱			Find Now	1
			Shap	
Disabled accounts			Stop	4
ivon expiring password			~	
Days since last logon:	~		PI	
1				
		ок	Cancel	
Name	Description	In Folder		
Certificate Service DCOM Acc.	Description	NPWin2012	2r2.lo	-
🕂 Cloneable Domain Controllers	Members of this group that are domain	NPWin2012	2r2.lo	14124
Cryptographic Operator		NPWin2012	2r2.lo	≡
Denied RODC Password Repl	Members in this group cannot have the	. NPWin2012	2r2.lo	
Distributed CULTUSers	DNS Administrators Group	NPWin2012	212.10 2•2.1a	
Drisedmin Drisedmin	DNS clients who are permitted to perform	NPWIN2012	212.10 212.10	
Domain Admins	Designated administrators of the domain	NPWin2012	2r2.lo	
Domain Computers	All workstations and servers joined to t	NPWin2012	2r2.lo	
🕂 Domain Controllers	All domain controllers in the domain	NPWin2012	2r2.lo	-
🚉 Domain Guests	All domain quests	NPM/in2010	2r2 lo	Y

左点[确定(OK)]。

Select Grou	ups
Select this object type:	
Groups or Built-in security principals	Object Types.
From this location:	100
NPWin2012r2.local	Locations
Enter the object names to select (<u>examples)</u> :	
Domain Admins	Check Name
Domain Admins	Check Name
Domain Admins	Check Name

1-3-2 Windows 2012 AD Server 审核配置

请依照文件「Windows AD audit to syslog」第4章「Windows 2012 AD Server 审核配置」,

配置默认域控制站(Default Domain Controller)的审核策略(Policy)。

注3:若用户环境有防火墙设备,请开放此 Windows AD Server 的 DCOM port TCP 135。

2.新增 Windows AD Server WMI 设备

2-1 新增 Windows AD Server WMI 设备

浏览器 URL 输入 http://\$N-Reporter_IP,本例输入"http://192.168.2.7"。输入 N-Reporter 管理

	the April and				
() @ http://192.168.2.7/event/event_query.html?q=1441262454448	5 - Q	🧉 192.168.2.7	×	-	n 🛧 🔅
	k	V			
	1C				
	N-REP	orter			
	admin				
	P				
	Logi	'n			
	Remember Me	Forget Password			
	Copyright © 2009 №	I-Partner. All rights reserved			
<					>

员账号/密码,默认 admin/admin,鼠标左点 [Login],登录 N-Reporter Web。

鼠标左点[接收设备 / Syslog 设备]。

				1 1 1			_			×		
E	9	AV http://192	2.168.2.7/sysadm	n/logdevice	.html?q=b0ynIiInhYRureTSD	№ 🔎 🕈 😋 🔊 接收设备 - Syslog 设备	×		ŵ	大 22		
	NR		elog 沿条 □ T	后面白动面如	(120秒)			💄 admin	*	^		
G		Syslog i #4	siogig marging marging to the side of the	以回口初史和	(120(5))							
ш.	▲ Q C P F H対 *IPa 及 *设备名称。进行搜寻											
•												
-												
	-	SNMP 收纳	32		1.6.1.1	汎な力が	27. 47 Stat Ht (Facilitat)	Action III WAS	2 17 4.	10.42		
?		SINNE MED	¢Ш	-	исл	设备名称	设备种尖 (Facility)	Action 阻挡设备	道奈	反音		
	×	Flow设备			192.168.2.252	192.168.2.252	Auto-Detection		UTF8	暂停 接收		
	Ξ	接口协议								暫停		
	Q	主机			192.168.2.80	192.168.2.80	Auto-Detection		UTF8	接收		
	*	告警样版			102 168 2 82	102168282	Auto-Detection		LITER	暂停		
	កៅ	设备异常告警			152.100.2.02	152.100.2.02	Auto Detection		0110	接收		
		*	其他		192.168.0.10	TP 192.168.0.10	TippingPoint	Action 阻挡 设备	UTF8	暂无 数据		
		%	其他		192.168.10.14	TP 192.168.10.14	TippingPoint	Action 阻挡 设备	UTF8	暂无 数据		
		%	其他		192.168.4.1	Debian 192.168.4.1	Unix/Linux/Solaris		UTF8	暂无 数据		
		% ŵ	其他		192.168.2.73	Win2k3 AD chs 192.168.2.73	Windows AD		UTF8	暂无 数据		
					Copyrigh	t © 2009 N-Partner. All rights reserved.				\sim		
<										>		

左点[+],开启[新增或编辑 Syslog 设备]。区域选择此 WMI 设备所在位置,本例为 Root。输入设备名称。输入 WMI 设备 IP。数据格式选[Windows 2003 AD (WMI)],本例为 Windows 2003 AD Server。语系选[GB2312](注4)。输入 WMI 设备远程登录账号与密码。设备状态勾选[启动接收]。选择所属活页夹。鼠标左点[确定]。

注4: Windows 2003 繁体版语系选[BIG5]; Windows 2003 简体版语系选[GB2312]; Windows 2003 英文版语系选[UTF8]。Windows 2008/2012 请选[UTF8] 编码。

										×
(→ 👌 🕸 http://19	92.168.2.7/sysadm/logdevic	e.html?q=b0ynIilnł	nYRureTSDp 🔎	▼ C	×	_	_	ŵ	* 🌣
۵ 📎	Reporter							👤 admii	n 🖡	^
G	接收设备 ▶ S	yslog 设备 🗌 页面自动更	新 (120秒)							_
њ	Syslog 18	A Facility	•	1 PID TE P./L. 47	女华 进行检查					
•	所属文件夹:	All Devices		『P』及・设备 聞Syslog设备	·右你』进行授守	×				
•	总笔数:9		step 1	区域:	Root	~				
?	操作	所属文件夹 ▲		名称: 设备IP·	Win2k3 AD CHS 192.168.2.82		y)	Action 阻挡设备	语系	设备
≣⇒	1	未知设备	:	设备种类:	 Action 设备 	\checkmark			UTF8	暂停
		土和沿东		数据格式:	Windows 2003 AD Server (WMI)	~			LITER	暂停
	18 1	小和设置		Facility:		 Image: A start of the start of			UIPo	接收
	*€	未知设备	:	增杂;	GB2312				UTF8	暂停 接收
	\$ m	其他	step 2	登录帐号: 登录杰码:	npartner			Action 阻挡	UTF8	暂无
	6.J W			登录密码: 确认密码:	•••••			设备		数提
	*	其他	:					Action 阻挡 设备	UTF8	暂无 数据
	\$ ŵ	其他	step 2	接收状态:	● 启动接收 ○ 暂停接收		ris		UTF8	暂无
				所属文件夹:	vvmiloj					数据
	*	其他	:			确定 取消			UTF8	当 尤
				Copyright © 20	009 N-Partner. All rights reserved.					~
<										>
<u> </u>										

2-2 设定 NTP Server

鼠标左点[系统管理 / 网络参数设置 / 系统时间]。

	A http://192.168.2.7/sv	adm/network.html?a=b0.nfilnhYRureTSDpK(0 - c) 約 网络泰斯培莱	
	N-Reporter	A NORMAL A	L admin
G	系统管理 ▶ 网络参数设置		
	条统时间 基本制	数 日志转发 Flow转发 Flow接收Port 设置Access List	
	条统时间		
		2016/02/3	
Ľ	条统管理	4 : 20 : 15	
?	□ 系统信息	5MT+0800	
	☆ 网络参数设置	同步电脑时间	
	◎ 数据库管理		
	▲ 用户管理		
	圖 名称解析	016/02/03	
	g Port 名称解析	4:19:45	
	⊠ 告警通报设置	MT +8 💟	
	會 报表图标上传		
	◎ 操作历程	体存成五	
	e)偏好设置		
	❷ 仪表盘		
		Copyright © 2009 N-Partner. All rights reserved.	
<			>

勾选[使用 NTP], IP 输入 NTP server IP 或 host name,可输入"cn.pool.ntp.org 或是公司内部

的 NTP server IP。本例子输入"cn.pool.ntp.org "。左点[储存设置]。

(←)⊖) \land http://192.168.2	2.7/sysa	dm/network.ht	ml?q=b0ynIilnhYRur	eTSDp 🔎 🕈 🖒 🖄	网络参数设置	×	∩ ★ 🕸
a 🔊	REPORTER							💄 admin 🛛 💱
G	系统管理 ▶ 网络参数	设置						
	系统时间	基本參数	日志转发	t Flow转发	Flow接收Port	设置Access List		
	系统时间							
	系统时间	:	2016/02/3					
•		Θ	14:25:15					
?		3	GMT+0800					
						同步电脑时间		
	使用手动设置							
	○ 使用手动设置:	Ħ	2016/02/03					
		Θ	14:19:45					
		\$	GMT +8	~				
	 使用NTP: 	IP	cn.pool.ntp.	org		×		
						保存设置		
•								
				Co	pyright © 2009 N-Partn	er. All rights reserved.		
<								>

注 5:如果 WMI 设备与 N-Reporter 时间不一致,将导致 WMI query 数据遗失。新增 WMI 设

备后,请再设定 NTP Server,每日定时做时间校正。



連絡資訊 N-Partner 公司連絡方式: TEL: +886-4-23752865 FAX: +886-4-23757458 有關技術問題請洽: Email: support@npartnertech.com Skype : support@npartnertech.com 有關業務相關問題請洽:

Email: sales@npartnertech.com

