

N- Partner N-REPORTER

WMI syslog management of Windows AD Server V 1.1.2 (English)



Preface

This document introduces how to use WMI to manage the syslog of Windows AD Server for N-Reporter.

Contents :

1.Configuration of WMI in Windows AD Server	2
1-1 Configuration of WMI in Windows 2003 AD Server	2
1-1-1 Add a new WMI remote login user to Active Directory	2
1-1-2 Windows 2003 AD Server Audit Configuration	7
1-1-3 Windows 2003 AD Server Firewall configuration	7
1-2 Windows 2008 AD Server Configuration	10
1-2-1 Add new WMI Remote login Domain User	10
1-2-2 Windows 2008 AD Server Audit Configuration	15
1-3 Windows 2012 AD Server Configuration	15
1-3-1 Add new WMI Remote login Domain User	15
1-3-2 Windows 2012 AD Server Audit Configuration	20
2. Add Windows AD Server WMI Device on N-Reporter	21
2-1 Add Windows AD Server WMI device	21
2-2 Setting NTP Server	24
Contact	25

1.Configuration of WMI in Windows AD Server

1-1 Configuration of WMI in Windows 2003 AD Server

1-1-1 Add a new WMI remote login user to Active Directory

Logon Windows AD server by administrator. Then click [Start / All Programs /

Administrative Tools / Active Directory Users and Computers].



Click forest root domain. It is win2k3eng.local in this example. Right click [Users] and left

click [New => User].

Kara Active Directory Users and Computers			
G Eile Action View Window Help			_B×
	7 📆 🛍 💎 🍕 🕯	<u>s</u> i	
Active Directory Users and Computer Users 23 objects		-	
E Saved Oueries			
Name Name	Туре	Description	
🗄 👘 Builtin	User	Built-in account for admini	
🕀 🧰 Computers	Security Group	Members of this group are	
🗄 🤕 Domain Controllers 🛛 🕺 💯 DHCP Administrators	Security Group	Members who have admini	
EoreignSecurityPrincipals	Security Group	Members who have view	
User User	Security Group	DNS Administrators Group	
Delegate Control hsUpdateProxy	Security Group	DNS clients who are permi	
Final pmain Admins	Security Group	Designated administrators	
New Computer	curity Group	All workstations and serve	
All Tasks Contact	curity Group	All domain controllers in th	
Group	curity Group	All domain guests	
View InetOraPerson	curity Group	All domain users	
New Window from Here	lias curity Group	Designated administrators	
Refresh Printer	curity Group	Members in this group can	
Export List	er	Built-in account for guest	
Shared Folder	curity Group		
Properties pippervicesgroup	Security Group	Group for the Help and Su	
Help	User		
AS and IAS Server:	s Security Group	Servers in this group can	
Schema Admins	Security Group	Designated administrators	
50 SUPPORT_388945a0) User	This is a vendor's account	
TelnetClients	Security Group	Members of this group ha	
🖸 🕵 user1	User		
▼	1 User		
Creates a new item in this container.			

Type the Last name "npartner" and type User logon name as "npartner", then click [Next].

New Object - User	<u>×</u>
Create in: win2k3eng	local/Users
<u>F</u> irst name:	
Last name: npartner	
Full name: npartner	1
User logon name: npartner	@win2k3eng.local
User logon name (pre- <u>W</u> indows 200	10):
JWIN2K3ENG\	npartner
	< <u>B</u> ack <u>N</u> ext > Cancel

Check [Password never expires] after fill in the password. Click [Next] =>[Finish].

New Object - User	
Create in: win2k3eng.local/Users	
Password: •••••• Confirm password: ••••••	
 User <u>m</u>ust change password at new logon User cannot change password Password never expires Account is disabled 	
< <u>B</u> ack <u>N</u> ext > Cancel	
New Object - User	×
Create in: win2k3eng.local/Users	
When you click Finish, the following object will be created:	
Full name: npartner	
User logon name: npartner@win2k3eng.local	
The password never expires.	-
< <u>B</u> ack Finish Cance	el

Click [Users]. Right click "npartner", then click [Add to a group].

Image: Solution of the second computer Help Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer Image: Solution of the second computer <th></th>	
← → E Image: Computer of the second se	A
Active Directory Users and Computer Users 24 objects Saved Queries Win2k3eng.local Queries Queries	A
Active Directory Users and Computer Users 24 objects Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Queries Image: Saved Que	A
Name Type Description Image: Solution win2k3eng.local Image: Solution win2k3eng.local Image: Solution win2k3eng.local Image: Solution win2k3eng.local Image: Solution win2k3eng.local Image: Solution win2k3eng.local Image: Solution win2k3eng.local Image: Solution win2k3eng.local Image: Solution win2k3eng.local Image: Solution win2k3eng.local Image: Solution win2k3eng.local Image: Solution win2k3eng.local	<u> </u>
🛛 📅 🦳 Built-in account for admini	
🗄 💼 Computers 🦉 Cert Publishers Security Group Members of this group are	
🕀 😥 Domain Controllers 🛛 🙀 DHCP Administrators 🦳 Security Group Members who have admini	
ForeignSecurityPrincipals	
Users Security Group DNS Administrators Group	
Market Security Group DNS clients who are permi	
Security Group Designated administrators	
MDomain Computers Security Group All workstations and serve	
Benerale Cueste Security Group All domain controllers in th	
Bergin Guests Security Group All domain guests	
Security Group All dollarin users Security Group Decignated administrators	
Cherce prise Administration Security Group Members in this group can	
Guest User Built-in account for quest	
Welleli ibrary Indaters Security Group	
Relin Bervices Group Security Group Group for the Help and Su	
G iris User	
npartner <u>liser</u>	
RAS and IAS Serve ⊆opy Servers in this group can	
Schema Admins Add to a group Designated administrators	
SUPPORT_388945. Disable Account This is a vendor's account	
TelnetClients Reset Password Members of this group ha	
✓ Move	-
Disables the account for the current selection.	
Send Mail	
All Tas <u>k</u> s 🕨	
Cu <u>t</u>	
Delete	
Rena <u>m</u> e	
P <u>r</u> operties	

Click [Advance/ Find Now/ Domain Admins/ OK], add the WMI remote user npartner into

the Domain Admins group.

Select Group	<u>? ×</u>	Select Group	<u>? ×</u>
Select this object type:		Select this object type:	
Group or Built-in security principal	Object Types	Group or Built-in security principal	Object Types
From this location:		From this location:	
win2k3eng.local	Locations	win2k3eng.local	Locations
Enter the object name to select (examples):		Common Queries	
	Check Names		Columns
		Name: Starts with	
		Description: Starts with	Find Now
Advanced OK	Cancel	Disabled accounts	Stop
	//.	Non expiring password	
		Days since last logon.	≫∕
			K Cancel
		Search results:	
		Name (RDN) Description In Folder	<u> </u>
		Account Uperators win2k3eng.local/bailtin Win2k3eng.local/bailtin Win2k3eng.local/bailtin	n n
		Backup Operators win2k3engrocal/Builtin	n n
		Cert Publishers Members of this group ar win2k3eng.local/Users	s 🚽
		DHCP Administrators Members who have adm wipzk3eng.local/Users	s
		Members who have vie Win2k3eng.local/Users	s
		3 Distributed Lot Users win2k3eng.local/Builtin	n
		22 Dns IndateProxy DNS clients who are per win2k3eng local/Users	8
		Domain Admins Designated administrator win2k3eng.local/Users	s
		Domain Computers All workstations and ser win2k3eng.local/Users	5
		Jan second and second second second	

Click [OK]

Select Group		? ×
Select this object type:		
Group or Built-in security principal		<u>O</u> bject Types
Erom this location:		
win2k3eng.local		Locations
Enter the object name to select (<u>examples</u>):		
Domain Admins		<u>C</u> heck Names
Advanced	OK	Cancel

1-1-2 Windows 2003 AD Server Audit Configuration

Please refer to the chapter 2 [Windows 2003 AD Server Audit configuration] of the document [¬]Windows AD audit to syslog [¬] to setup audit policy of the Default Domain Controller.

1-1-3 Windows 2003 AD Server Firewall configuration

Clikc [Start/ All Programs/ Accessories/ Command Prompt].

administrato	ог			
Manage Your Server		😏 My Computer		
Command Pre	ompt	Control Panel	I	•
Windows Exp	🕸 Windows 🍓 Windows	Catalog Update	e Tools	•
🧭 Microsoft Visua	🗑 Accessor	ies	• 📾	Accessibility •
Notepad++	🖮 Administr 🖮 Startup	ative Tools	•	Communications
Event Viewer	 Internet Outlook E 	Explorer Express		System Tools Address Book
Notepad	Remote 4	Assistance Silverlight 3 SDK		Calculator Command Prompt
Active Directory Computers	Microsoft Microsoft	SQL Server 2008 Sync Framework	• •	Notepad Paint
Computer Mana	WinRAR	Visual Studio 2010	• 🥹	Program Compatibility Wizard Synchronize
All <u>P</u> rograms 🕨	m InterSect	: Alliance ++	• 🔄	Windows Explorer WordPad
1		💋 Log Off	0 5	hut Down
🍂 Start 🛛 🚱 🥭]			

Type [®] gpedit.msc ^a and open the [Group Policy Object Editor] to setup the [Local Computer

Policy].



Double click [Computer Configuration/ Administrative Templates/Network/Network

Connections /Windows Firewall/Standard Profile]. Double click (Windows Firewall: Allow

remote administration exception)].



Check [Enabled]. Click[OK].

Windows Firewall: Allow remote administration exception Prop?
Setting Explain
😭 Windows Firewall: Allow remote administration exception
 ○ Not <u>C</u>onfigured ● Enabled ○ <u>D</u>isabled
Allow unsplicited incoming messages from: Syntax: Type ''*'' to allow messages from any network, or else type a commandeparated list that contains
any number or combination of these: IP addresses, such at 10.0.0.1 Subnet descriptions, such as 10.2.3.0/24 The string "localsubnet"
Supported on: At least Microsoft Windows XP Professional with SP2 Previous Setting No. at Setting
OK Cancel <u>A</u> pply

Remark : Please allow the Windows AD Server DCOM port TCP 135 on the firewall.

1-2 Windows 2008 AD Server Configuration

1-2-1 Add new WMI Remote login Domain User.

Logon the Windows AD server by domain administrator. Click [Start/All

Programs/Administrative Tools/Active Directory Users and Computers].



Click forest root domain, the npartnerwin2k8.local in this example. Right click[Users], then

left click [New] =>[User].

Active Directory Users and Con	puters				
File Action View Help					
🗢 🔿 🖄 📅 🖌 🛍 🕷	(= =) 2 📰 4 🗉 🗙 🖹 Q 🖦 🗹 🗊 % 🗞 😭 🍸 🧕 🍇				
Active Directory Users and Comput	Name	Type	Description		
🕀 🧮 Saved Queries	Administrator	User	Built-in account for admini		
Image:	Allowed RODC Password Replication Group	Security Group	Members in this group can		
🛨 🧮 Builtin	용 Cert Publishers	Security Group	Members of this group are		
Computers	🙎 cris	User			
Domain Controllers	용 Denied RODC Password Replication Group	Security Group	Members in this group can		
	Sector Administrators	Security Group	Members who have admini		
LostAndFound Managed Service Accounts	State of the second sec	Security Group	Members who have view		
Program Data	& DnsAdmins	Security Group	DNS Administrators Group		
E System	A DnsUpdateProxy	Security Group	DNS dients who are permi		
User	Bandomain Admins	Security Group	Designated administrators		
🕂 🦳 NTD: 📢 Delegate Control	Domain Computers	Security Group	All workstations and serve		
Find	Domain Controllers	Security Group	All domain controllers in th		
New	Computer	Security Group	All domain guests		
All Tasks	Contact	Security Group	All domain users		
	Group	Security Group	Designated administrators		
View	InetOrgPerson ain Controllers	Security Group	Members of this group are		
Pefresh	msImaging-PSPs Prs	Security Group	Members in this group can		
Evport List	MSMO Queue Alias	User	Built-in account for guest		
Export Lister	Printer	User	Key Distribution Center Se		
Properties	User	Security Group			
Help	Shared Folder	Security Group	Servers in this group can		
nep	read only bomain controlers	Security Group	Members of this group are		
	Schema Admins	Security Group	Designated administrators		
	👗 sherman	User	-		
	J K win3kRad one unor1	Lleor			
Creates a new item in this container.					

Type the Last name as "npartner". Type User logon name as "npartner" . Then click [Next].

New Object - User	×
Create in: npartnerwin2k	8.local/Users
First name:	Initials:
Last name: npartner	
Full name: npartner	
User logon name:	
npartner	@npartnerwin2k8.local
User logon name (pre-Windows 2000):	
NPARTNERWIN2K8\	opartner
	< Back Next > Cancel

Check [Password never expires] after fill in the password. Click [Next/Finish].

New Object - User	
Create in: npartnerwin2k8.local/Users	
Password:	
Confirm password:	
User must our password at next logon	
User cannot change password	
Account is disabled	
< Back Next > Cancel	
	V
New Object - User	<u> </u>
Create in: npartnerwin2k8.local/Users	
When you click Finish, the following object will be created:	
Full name: npartner	<u> </u>
User logon name: npartner@npartnerwin2k8.local	
The password never expires.	
	_
	▼
< Back Finish Cance	el

Click [Users]. Right click "npartner" name and click [Add to a group].

Active Directory Users and Com	nuters					
File Action View Help	puters					
	1 🛛 🖻 🚺 🖬	1 🔏 💐 🗊 🍸 🖉	1882			
Active Directory Users and Comput	Name		Type		Description	
🕀 🚞 Saved Queries	👗 Administrator		User		Built-in account for admini	
Image:	Allowed RODC F	assword Replication Group	Security Gr	oup	Members in this group can	
🕀 🛄 Builtin	& Cert Publishers		Security Gr	oup	Members of this group are	
Computers Controllers	👗 cris		User			
Domain Controllers	Benied RODC Pa	assword Replication Group	Security Gr	oup	Members in this group can	
	BHCP Administra	ators	Security Gr	oup	Members who have admini	
Costenar ound Managed Service Accounts	& DHCP Users		Security Gr	oup	Members who have view	
Program Data	Magazina Bang Ma		Security Gr	oup	DNS Administrators Group	
F System	& DnsUpdateProx	у	Security Gr	oup	DNS dients who are permi	
Users	Bomain Admins		Security Gr	oup	Designated administrators	
🗉 🧮 NTDS Quotas	Bomain Comput	ers	Security Gr	oup	All workstations and serve	
	Bomain Control	ers	Security Gr	oup	All domain controllers in th	
	Bomain Guests		Security Gr	oup	All domain guests	
	Somain Users		Security Gr	oup	All domain users	
	Enterprise Admi	ns	Security Gr	oup	Designated administrators	
	Enterprise Read	l-only Domain Controllers	Security Gr	oup	Members of this group are	
	Group Policy Cre	eator Owners	Security Gr	oup	Members in this group can	
	🛵 Guest		User		Built-in account for guest	
	krbtat		User		Key Distribution Center Se	
	npartner		User			
	CRA_DBA	Copy	Security Gr	oup		
	RAS and IAS S	Add to a group	Security Gr	oup	Servers in this group can	
	Read-only Don	Name Mappings	Security Gr	oup	Members of this group are	
	Schema Admin	Disable Account	Security Gr	oup	Designated administrators	-1
Mana and Santas for this second	- chormon	Reset Password	Hoor			
Maps certificates for this account.		Move				
		Open Home Page Send Mail				
		Seriu Mali				
		All Tasks 🔹 🕨				
		0.4				
		Delete				
		Delete				
		Properties				
		Help				

Click [Advanced/ Find now/Domain Admins/ok], add the WMI remote user npartner into

the Group of the Domain Administrators.

Select Groups	? ×	Select Groups			? ×
Select this object type:		Select this object type:			
Groups or Built-in security principals	Object Types	Groups or Built-in security princip	als	Obje	ect Types
From this location:		From this location:			
npartnerwin2k8.local	Locations	npartnerwin2k8.local		Lo	cations
Enter the object names to select (examples):		Common Queries			
	Check Names			1	Columna
		Name: Starts with 💌			Columns
		Description: Clarts with the			Find Now
Advanced OK	Cancel	Disabled accounts		1	Stop
		Non expiring password			
			_ /		0
		Days since last logon:			The second secon
				-	
		Search results:		OK	Cancel
		Name (RDN)	Description	In Folder	-
		A Backup Operators		npartnerwin2k	8.local/Builtin
		Cert Publishers	Members of this group are permit	npartnerwin2k	8.local/Users
		Certificate Service DCOM A		npartnerwin2k	8.local/Builtin
		Cryptographic Operators		npartnerwin2k	8.local/Builtin —
		Denied RODC Password R	Members in this group cannot ha	npartnerwin2k	8.local/Users
		DHCP Administrators	Members who have administrativ	npartnerwin2k	8.local/Users
		Distributed Call Lloom	rwempers who have view-only ac	npartnerwin2k	8.10cal/Users
		A Dos Admins	DNS Administrators Group	npartnerwin2k	8 local/Lisers
		A DnsUpdateProxy	DNS clients who are permitted to	npartnerwin2k	8.local/Users
		Domain Admins	Designated administrators of the	npartnerwin2k	8.local/Users
		dan in i	And the second second second second		

Click [OK].

? ×
Object Types
Locations
Check Names
-
Cancel

1-2-2 Windows 2008 AD Server Audit Configuration

Please refer to the Chapter 3 [Windows 2008 AD Server Audit configuration] of the document [[]<u>Windows AD audit to syslog</u>] to setup audit policy of the Default Domain Controller.

Remark : Please allow the Windows AD Server DCOM port TCP 135 on the firewall.

1-3 Windows 2012 AD Server Configuration

1-3-1 Add new WMI Remote login Domain User

Logon the Windows AD server by domain administrator. Click [Start/All

Programs/Administrative Tools/Active Directory Users and Computers].

9 🖲 - 🛧 🗟 🕨	Control Panel 🔸 System and Security 🔸 Administra	itive Tools 🔸	~ C	Search Administrative	Tools 🔎
	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	
	Active Directory Module for Windows Po	8/22/2013 2:55 PM	Shortcut	2 KB	
🜉 This PC	Ref 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	
	💦 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	
	👼 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 K'B	-
11 items					855

Click forest root domain, the NPWin2012r2cht.local in this example. Right click [Users] and

Click [New/User].

	Active Directory Users and Computers		_ 🗆 X
File Action View Help			
🗢 🔿 📶 🔏 🗊 🔏 🖨	🗟 🖬 📷 🗏 🐮 🗑 🖉 🚨 🕷		
Active Directory Users and Computers	Name	Туре	Description 🔨
Saved Queries	& Administrator	User	Built-in account f
⊿ in NPWin2012r2.local	Allowed RODC Password Replication Group	Security Group	Members in this g
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 g
▷ OreignSecurityPrincipals	A DrsAdmins	Security Group	DNS Administrate
Managed Service Accounts	See DnsUpdateProxy	Security Group	DNS clients who :
Delegate Control	main Admins	Security Group	Designated admii
eregate Control	main Computers	Security Group	All workstations a \equiv
Finda	imain Controllers	Security Group	All domain contro
New	Computer	Security Group	All domain guest
All Tasks	Contact	Security Group	All domain users
Manu	Group	Security Group	Designated admir
01200	InstOrgPerson	Security Group	Members of this
Refresh		Security Group	Members in this g
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
	S User	Security Group	Designated admii 🧹
< III >	< Shared Folder		>
Creates a new item in this container.			

Type "npartner" into the field "Last Name". Type "npartner" into the User Logon Name. After all click [Next].

1	New Object - User
Create in: NPw	/in2012r2.local/Users
First name:	Initials:
Last name: npartn	ier
Full name: / npartn	ier
User logon name:	
npartner	@NPWin2012r2.local
User logon name (pre-Window	ws 2000):
NPWIN2012R2	npartner
	(Back Next) Cancel

Check [Password never expires] after fill in the password. Click [Next/Finish].

🧏 Create in: N	New Object - User
Password: Confirm password:	•••••
User must change pas User cannot change p Password never expire Account is disabled	ssword at next logon bassword
	< Back Next > Cancel

Click [Users]. Right click "npartner", then click [Add to a group].

3	Active Directory Users and (Computers		_ 🗆 X		
File Action View Help						
🗢 🔿 🙋 📰 🔏 📋 🗙 🚍 🙆	🔒 🛛 🖬 🔧 🗞 🗑 🍸 💆	°86.				
Active Directory Users and Computers	Name		Туре	Description 🔥		
D Saved Queries	🙎 Administrator		User	Built-in account f		
⊿ 🚔 NPWin2012r2.local	용 Allowed RODC Password Replicati	on Group	Security Group	Members in this 🤉		
⊳ 🧰 Builtin	용 Cert Publishers		Security Group	Members of this		
Computers	🙈 Cloneable Domain Controllers		Security Group	Members of this		
▷ Domain Controllers	용 Denied RODC Password Replicatio	n Group	Security Group	Members in this ç		
Foreign Security Principals	용 DnsAdmins		Security Group	DNS Administrate		
Managed Service Accounts	😣 DnsUpdateProxy		Security Group	DNS clients who :		
Users	용 Domain Admins		Security Group	Designated admir		
	용 Domain Computers		Security Group	All workstations a 🗏		
	용 Domain Controllers		Security Group	All domain contr		
	용 Domain Guests		Security Group	All domain guest		
	😣 Domain Users		Security Group	All domain users		
	용 Enterprise Admins	Security Group	Designated admii			
	용 Enterprise Read-only Domain Con	trollers	Security Group	Members of this		
	Sroup Policy Creator Owners	Security Group	Members in this g			
	🐍 Guest		User	Built-in account f		
	npartner		Hear			
	Reprotected Users	Copy	oup	Members of this		
	💐 RAS and IAS Servers	Add to a group.	oup	Servers in this gro		
	🙈 Read-only Domain Controllers	Disable Accoun	t oup	Members of this 🗸 🧹		
< III >	<	Reset Password		>		
Allows you to add the selected objects to a	group you select.	Move				
	and and the	Onen Home Da				
		open nome Pa	96			
		Send Mail				
		All Tasks	•			
		Cut				
		Delete				
		Rename				
		Properties				
		Help				

Click [Advanced/ Find now/ Domain Admins/ OK], add the WMI remote user npartner into

the Group of the Domain Admins.

	Select Groups	×	
Select this object type:			
Groups or Built-in security princip	als Ob	ject Types	
From this location:			
NPWin2012r2.local		ocations	
-			
Enter the object names to select (examples):		
	_ Ch	eck Names	
	1		
Advanced		Cancel	
			Y
	Select Groups		^
Select this object type:			
Groups or Built-in security princip	als	Object Types	
Erom this location:			
NPWin2012r2.local		Locations	
		Locations	
Common Queries			
Name: Starts with 👻		Columns	
Description: Starts with 👻		Find Now	
Disabled accounts		Stop	
Non expiring password			
Days since last logon:	~	,	
Search results:		JK Cancel	
Name	Description	In Folder	~
Certificate Service DCOM Acc.		NPWin2012r2.lo	
Cloneable Domain Controllers	Members of this group that are domain	NPWin2012r2.lo	=
Cryptographic Operator Denied RODC Password Repl.	Members in this group cannot have the	NPWin2012r2.lo	
Real Distributed COM Users		NPWin2012r2.lo	
🕰 DnsAdmin	DNS Administrators Group	NPWin2012r2.lo	
Dost IndateProxy	DNS clients who are permitted to perfo	NPWin2012r2.lo	
Domain Admins	Designated administrators of the domain	NPWin2012r2.lo	
Comain Computers	All workstations and servers joined to t	NPWIn2012t2.lo	
Rests	All domain quests	NPW/in201212.10	~

Click [OK]

ips	×
0	bject Types
	Locations
,,	
C	heck Names
ОК	Cancel
	иря О С

1-3-2 Windows 2012 AD Server Audit Configuration

Please refer to the Chapter 4 [Windows 2012 AD Server Audit configuration] of the

document [Windows AD audit to syslog] to setup audit policy of the Default Domain

Controller.

Remark : Please allow Windows AD Server the DCOM port TCP 135 on the firewall

2. Add Windows AD Server WMI Device on N-Reporter

2-1 Add Windows AD Server WMI device

Login the N-Reporter by go to URL <u>http://\$N-Reporter IP</u>. For example, go to <u>http://192.168.2.56</u>. Input account name and password. The default username and password are admin/admin. Click [Login] to logon N-Reporter Web.



Click [Device / Syslog Device].

			-	-	-	-	-	-	-					
(<)(I 🔊 \land http	://192.168.2	2.56/event,	/event_qu	ery.ht 🔎 -	r C \land	¥ Event	t Query	×		-	Ast	fh ★ ₩
A) [Reporte	P										admin	•
fa		Event 🕨	Event Que	ry 🔽 Re	fresh (12	Seconds)							
		+	Basic	Adva	nced	Show	All		Reset					
<u> </u>		1	Fime Query	sele	ect period	in 5 Mins		Last	O Start Time			🗃 🤭 St	art Query	C
•	•	Device			log 🔿 Flo	w	1	Туре	Security	Traffic	Audit	Web	Other	
*		👱 Syslog	Device		l Number	: 0								
÷			Monitored	Devices		E	vent						Src IP	
		≚ Flow D	evice											
		≣ Interfac	ce List											
		🗆 Host												
		🛠 Alert Te	emplate											
		na Device	Abnormal	Alert										
		<											>	
		First	Last) i	Record per	page: 50	✓ Cur	rrent Pa	age: 0 of 0					
						Co	pyright ©	2009 N	I-Partner. All rig	hts reserved.				
														>

Click I to open a windows [Add or Edit Syslog Device]. Select the [Location] where the WMI device is belongs to. For example, the location here is Root. Type Name and Device IP of the WMI device. Select [Windows 2008/2012 AD Server (WMI)] in data type and [(13) log audit] in Facility and Locale as "UTF8". Type in login account, Login password and Confirm password of the WMI device and check [Activate] to start receiving log from the WMI device. Then select the "Device folder" and click [OK].

					-	-								
(C	A http://192.168.2.56/sysadm/logdevice.html?q=b%2FRn989xf3colcDqG0zr						\land Device - Sysl	og Device ×	8	Aut	20	Author sur-	ĥ★¤	1
ø	NHR	EPORTEP										👤 admin	₽.,	~
G		Device 🕨 Syslog [Device Refresh (12	0 Seconds)		Add or	r Edit Syslog	Device	×					
		Syslog Device	Facility			sten 1	Location:	Root						
<u> </u>			Q C	Search by 'lf	P' and 'De	>	Name:	win2k8 AD ENG 192.168.1.98	-					
۲		Device Folder:	All Devices	✓ ▲			Device IP:	192.168.1.98						
ö		Total Number: 2					Device Turney							
		Total Number, 2	Denies Falder	10			Device Type:	Windows 2009/2012 AD Server (MMI)				Davidla		
			Device Folder	IP	De		Data Type.	Windows 2006/2012 AD Server (WWI)	* e	.VII	VC	Rawfile		
		*	Others	192.168.10.14	TP 192		Facility:	(13) log audit	✓ 0	**	4	=		
							Locale:	UIF8	⊻ ¦	La				
		*	Others	192.168.2.80	192.16	step 2	Login		D	ta	4	=		
							account:	npartner	- 1					
							Login password:	•••••						
							Confirm	•••••						
							password.							
						step 2	Receive status:	Activate OPause						
							Device Folder:	Server[0]	~					
								OK Cancel						
									1					
													, j	٢
										_			>	_

Remark : Choose [BIG5] for Windows 2003 Traditional Chinese Version. Choose [GB2312]

for 2003 Simple Chinese Version. Choose [UTF8] for Windows 2003 English Version. For

Windows 2008/2012, please use [UTF8].

2-2 Setting NTP Server

Click [System / Network / System Time].

			-					
(\leftarrow)	Av http://192.168.2.56/sysac	dm/network.html?	q=b%2FRn9 🔎	🔻 🖒 😽 Network	c X	Aatt -	- Aat	↑★☆
1	N-REPORTEP						💄 admin	•
G	System Network							
	System Time Net P	arameter	Sysylog Relay	Flow Relay	Flow Receive Port	Configure Access List		
<u> </u>	Conton Time							
۲	System Time							
0	System	2016/04/29						
Ľ,		13 : 49 : 00						
•	Information	GMT+0800						
	🛠 Network				Get PC Time			
	② Database							
	🛓 User							
	💩 IP Name Mapping	2016/04/29						
	🙊 Port Name Mapping	13:48:18						
	Email Notification	GMT +8 🗸						
	🛊 Upload Logo							
	Ø Audit Log				Save Setting			
	Preference							
	Bashboard							
			Copyrigh	ht © 2009 N-Partner	All rights reserved.			
								>

Click [Use NTP]. Type NTP server IP or host name, for example "time.stdtime.gov.tw".

Click [Save Setting]. You can also type "tw.pool.ntp.org or internal NTP server IP.

System Network							
System Time	Net	Parameter	Sysylog Relay	Flow Relay	Flow Receive Port	Configure Access List	
System Time							
System Time:	t	2016/04/29					
	Θ	13:50:49					
	3	GMT+0800	GMT+0800				
					Get PC Time		
Manual Setting							
O Manual Setting:	Ħ	2016/04/29					
	Θ	13:48:18					
	3	GMT +8	\checkmark				
Use NTP:	IP	time.stdtim	ie.gov.tw				
					Save Setting		
						_	

Remark : If the time setting between WMI device and N-Reporter system is not the same, it

will cause WMI query data loss. After you add a WMI device, then set the NTP Server,

synchronize system time every day.



Contact

N-Partner : TEL: +886-4-23752865 FAX: +886-4-23757458 TAC Support : Email: support@npartnertech.com Skype : support@npartnertech.com

Sales Support :

Email: sales@npartnertech.com

