RSA NetWitness Logs

Event Source Log Configuration Guide



Microsoft Windows Legacy

Last Modified: Friday, September 8, 2017

Event Source Product Information:

Vendor: Microsoft Event Source: Windows Versions: Microsoft Windows Server versions 2003 and earlier

RSA Product Information::

Supported On: NetWitness Suite 10.0 and later

Collection Method: Windows Legacy

Event Source Log Parser: winevent_nic

Event Source Class.Subclass: Host.Windows

The RSA NetWitness Suite Legacy Windows collection collects event data from multiple Windows Event Source domains.

It supports collection from:

- Windows 2003 and earlier event sources
- NetApp ONTAP host evt files

You must complete these tasks to configure Windows Legacy collection:

- I. Create a Non-Admin Domain User for Each Domain
- II. Configure Legacy Collection on RSA NetWitness Suite

Prerequisite:

Before configuring a Windows Legacy event source, you must install the RSA NetWitness[®] Suite Legacy Windows Collector. Search the RSA Link NetWitness Suite space for "Legacy Windows Collection Update" and select the version that corresponds to your NetWitness version.

Create a Non-Admin Domain User for Each Domain

This section provides an overview of the end-to-end sequential configuration procedure for the Windows Legacy Collection protocol with a checklist that contains each configuration step.

Context

Configuration steps for the Windows Legacy collection protocol must occur in the specific sequence listed in the table below.

Create Non-Admin Domain User Checklist

Note: The steps in this list are in the order in which you must complete them.

Step	Description
1	Step 1 - Create a Non-Admin Domain User (for example, sauser) on the domain controller for each domain.
2	Step 2 - Set Event Log Security on the domain controller for each domain.
3	Step 3 - (Conditional) Disable Remote Registry Access Method)

Note: In the local Security policy on a Windows 2000 event source, you must assign the Manage auditing and security log user right that gives a non admin user access to the Event log.

Step 1 - Create a Non-Admin Domain User

To create the RSA NetWitness® Suite domain user (for example, **sauser**) on the domain controller for each domain:

1. Log on to the domain controller.



2. Create a non-admin domain user (for example, sauser).

🔿 🔼 📅 🔏 🗋 🗙 🕻	i 🗈 🖻 🖬 🕷 🗽 în 🦷	r 🖸 😹		
Active Directory Users and Comput	Name	Description		
🗵 🧰 Saved Queries 🖃 🏭 lab30.local	& Administrator	User	Built-in account for admini	
	Allowed RODC Password Replicati	Security Group - Domai	Members in this group can	
🗉 🧾 Bultin	& Cert Publishers	Security Group - Domai	Members of this group are	
E 🧮 Computers	Robert Robert Password Replicatio	Security Group - Domai	Members in this group can	
E 🗾 Domain Controllers	St. DnsAdmins	Security Group - Domai	DNS Administrators Group	
E ForeignSecurityPrincipals	DnsUpdateProxy	Security Group - Global	DNS clients who are permi	
Managed Service Accounts	& Domain Admins	Security Group - Global	Designated administrators	
Users	& Domain Computers	Security Group - Global	All workstations and serve	
	& Domain Controllers	Security Group - Global	All domain controllers in th	
	& Domain Guests	Security Group - Global	All domain guests	
	R Domain Users	Security Group - Global	All domain users	
	& Enterprise Admins	Security Group - Universal	Designated administrators	
	& Enterprise Read-only Domain Con	Security Group - Universal	Members of this group are	
	Scoup Policy Creator Owners	Security Group - Global	Members in this group can	
	🔓 Guest	User	Built-in account for guest	
	& IDFTest1	User		
	& IDFTest2	User		
	& NextGen Log Collector	User		
	RAS and IAS Servers	Security Group - Domai	Servers in this group can	
	Read-only Domain Controllers	Security Group - Global	Members of this group are	
	🙎 RSA Log Collector	User		
	🔱 sauser	User		
	Schema Admins	Security Group - Universal	Designated administrators	

3. Add the new user to the remote desktop user groups.

Step 2 - Set Event Log Security

This section tells you how to set event log security on the domain controller for a domain.

To set event log security on the domain controller for a domain:

- 1. Log on the Domain Controller.
- 2. Use a text editor such as Notepad to open the **Sceregvl.inf** in the **%Windir%****Inf folder**.
- 3. Add the following lines to the [Register Registry Values] section:

```
MACHINE\System\CurrentControlSet\Services\Eventlog\Application\
CustomSD,1,%AppCustomSD%,2
MACHINE\System\CurrentControlSet\Services\Eventlog\
Security\CustomSD,1,%SecCustomSD%,2
MACHINE\System\CurrentControlSet\ Services\Eventlog\Directory
Service\CustomSD,1,%DSCustomSD%,2
MACHINE\System\ CurrentControlSet\Services\Eventlog\DNS
Server\CustomSD,1,%DNSCustomSD%,2
MACHINE\ System\CurrentControlSet\Services\Eventlog\File
Replication Service\ CustomSD,1,%FRSCustomSD%,2
```

4. Add the following lines to the [Strings] section:

```
AppCustomSD="Eventlog: Security descriptor for Application event
log" SecCustomSD="Eventlog: Security descriptor for Security
event log" SysCustomSD="Eventlog: Security descriptor for System
event log"
DSCustomSD="Eventlog: Security descriptor for Directory Service
event log" DNSCustomSD="Eventlog: Security descriptor for DNS
Server event log" FRSCustomSD="Eventlog: Security descriptor for
File Replication Service event log"
```

- 5. Save the changes you made to the **Sceregyl.inf** file, and run the **regsvr32 scecli.dll** command.
- 6. Click Start > Administrator Tools > Group Policy Management and complete the following steps:
 - a. Expand the **Domains** tree, right click on the domain, and select the **Create a GPO** in this domain, and link it here option.

- b. Specify a name for the GPO policy and click **OK**.
- c. Select the newly created GPO policy.
- d. Select the domain in the right panel, right click, and select Enforce.
- e. Under Security Filtering, click Add.
- f. Under Select User, Computer and Group, type Domain Computers, click Check Names, and click OK.
- 7. Right-click on the newly created GPO policy and click Edit.
- 8. Double-click the following branches to expand them:
 - Computer Configuration
 - Windows Settings
 - Security Settings
 - Local Policies
 - Security Options
- 9. Find the new **Eventing** settings in the right panel.

Domain member: Digitally encrypt secure channel data (when pos	Not Defined
📖 Domain member: Digitally sign secure channel data (when possible)	Not Defined
Domain member: Disable machine account password changes	Not Defined
📖 Domain member: Maximum machine account password age	Not Defined
🖾 Domain member: Require strong (Windows 2000 or later) session	Not Defined
🛞 Eventlog: Security descriptor for Application event log	Not Defined
Eventlog: Security descriptor for Directory Service event log	Not Defined
📖 Eventlog: Security descriptor for DNS Server event log	Not Defined
Eventlog: Security descriptor for File Replication Service event log	Not Defined
Eventlog: Security descriptor for Security event log	Not Defined
🖏 Eventlog: Security descriptor for System event log	Not Defined

10. In right panel, double-click Event log: Security descriptor for Application event log and add SDDL string.

Note: Note: In the following steps, the *SID* (for example, S-1-5-21-3244245077-2111152846-3233386924-1114) is the SID for a particular non-admin domain user (for example, **sauser**). If you need to retrieve the SID, see <u>Retrieve the SID</u> below.

Depending on whether the security policy Settings box is empty or not, do one of the following:

Box is not empty: append the following string to the value in the box: (A;; 0x1;;;SID).

For example:

(A;; 0x1;;;S-1-5-21-3244245077-2111152846-3233386924-1114)

Box is empty: insert the following string in the box:

```
O:BAG:SYD:(D;;0xf0007;;;AN)(D;;0xf0007;;;BG)(A;;0xf0007;;;SY)
(A;;0x7;;;BA)(A;;0x7;;;SO)(A;;0x3;;;IU)(A; 0x1;;;SID)
```

For example:

```
O:BAG:SYD: (D;;0xf0007;;;AN) (D;;0xf0007;;;BG) (A;;0xf0007;;;SY) (A;;0x7;;;BA) (A;;0x7;;;SO) (A;;0x3;;;IU) (A; 0x1;;;S-1-5-21-3244245077-2111152846-3233386924-1114)
```

11. Repeat step 9 and 10 for Event log: Security descriptor for Security event log and Event log: Security descriptor for System event log.

Retrieve the SID

To retrieve the SID:

1. run the following command in PowerShell. Make sure that you change the user name accordingly (for example, change the user name to **sauser**).

```
([System.Security.Principal.NTAccount]'sauser').translate
([system. security.principal.securityidentifier]) | Format-List
```

2. Copy value field:

```
BinaryLength: 28
AccountDomainSid : S-1-5-21-3244245077-2111152846-3233386924
Value: S-1-5-21-3244245077-2111152846-3233386924-1114
```

Step 3 - (Conditional) Disable Remote Registry Access Method

The Remote Registry Access Method is enabled by default when you set up a Legacy Windows event source in RSA NetWitness® Suite. If you want to disable this method, you must uncheck the **Use Remote Registry Initialization** parameter.

For details on completing this procedure, see the "Configure Remote Registry Access" topic in the *Windows Legacy and NetApp Collection Configuration Guide* in the RSA NetWitness® Suite help.

To disable the Remote Registry Access Method:

- 1. Uncheck the Use Remote Registry Initialization parameter.
- 2. Add the RSA NetWitness® Suite user (for example, **sauser**) to the WMI and DCOMCNFG management on each Windows 2003 or earlier event source.
- 3. Add the Local Security Policy on each Windows 2000 event source.

You need to add non-admin domain user to WMI and DCOMCNFG on each Legacy Event Source. See the appropriate section, depending on the version of your event source:

- Add Non-Admin Domain User on Windows 2003 Event Source
- Add Non-Admin Domain User on Windows 2000 Event Source

Add Non-Admin Domain User on Windows 2003 Event Source

To add the RSA NetWitness® Suite user to the WMI and DCOMCNFG management on each Windows 2003 event source:

- 1. Log on the event source.
- 2. Run wmimgmt.msc.



3. Add the RSA NetWitness® Suite user under wmi\root\CIMV2 security option.

a. Right-click WMI Control and click Properties.



- b. Click Security tab and click on **Root\CIMV2**.
- c. Click Security

Control (Local)	Windows Management	Actions
	Instrumentation (WMI)	WMI Control (Local)
General Backup/Restore Secu Namespace navigation allows you Backup/Restore Secu Backup/Restore Secu Backup/Restore Secu Backup/Restore Security Backup/Restore Security Backup/Restore Security Backup/Restore Security Backup/Restore Security Backup/Restore SecurityCenter Backup/Restore SecurityCenter Backup/Restore SecurityCenter2	Advanced set namespace specific security.	

- d. In the Group or user names section, click Add... to create a user.
- e. Select the Enable Account and Remote Enable permissions for that user.
- f. Enter the user (for example, **sauser**).

WMI Control (Local) Prope	rties	? ×		
General Backup/Restore	Security Advanced			
N Security for ROOT\CL	M¥2	×		
Security				
Group or user names				
& Authenticated U & LOCAL SERVIC & NETWORK SEI & NextGen Log C & Administrators (F	lsers E RVICE ollector (nglogcollector@lab30.lc RC-GOLD\Administrators)	cal)		
Permissions for Authe	Add	Remove		
Execute Methods	Select Users, Computers, S	ervice Accounts, or G	roups	? ×
Full Write	Select this object type:			
Partial Write Provider Write	Users, Groups, or Built-in sec	urity principals		Object Types
Enable Account	From this location:			
For special permissic click Advanced.	Enter the object names to sel	ect (examples):		Locations
Learn about access	sause			Check Names
	Advanced		OK	Cancel
				11.
Security for ROOT\CIMV2	×			
Group or user names:				
Administrators (RC-GOLD \Administrators	Nab30.local)			
Sauser (sauser@lab30.local)				
Add.	. Remove			
Permissions for sauser A				
Enable Account Bemote Enable				
Read Security Edit Security				
For special permissions or advanced settings, click Advanced.	Advanced			
Learn about access control and permissions				
OK Ca	ncel Apply			
Click Check Names	to verify that the nev	v user was added	l correctly.	

g.

Select this object type:	
Users, Groups, or Built-in security principals	Object Types
From this location:	
lab30.local	Locations
nter the object names to select (<u>examples</u>):	
inter the object names to select (<u>examples)</u> : sauser (sauser@lab30.local)	Check Names
inter the object names to select (<u>examples)</u> : sauser (sauser@lab30.local)	Check Names
Enter the object names to select (<u>examples)</u> : sauser (sauser@lab30.local)	Check Names

- h. Click Apply, OK, and OK.
- 4. Add a user under **DCOMCNFG**:
 - a. Run **dcomcnfg**.
 - b. Click Root > Component Services > Computers > My Computer.
 - c. Right click My Computer and click properties.

Image: Second secon	-B×
← → 2 □ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
Console Root	-
E Computers	
My Computer My Computer Properties	•
COM+ Applications Default Protocole COM Security MSDTC	
Running Processes General Options Default Properties	
Jistributed Iransac Jistributed Iransac Jistributed Iransac	
The Services (Local)	
Description:	
Lean nivie doow <u>servici niese taopenies</u> .	
UK Cancel Apply	

- 5. Under Access Permissions:
 - a. Click Edit Limits.
 - b. Add the RSA NetWitness Suite user (for example, sauser).
 - c. Enable the Local Access and Remote Access permissions.
 - d. Click OK.
- 6. Under Launch and Access Permissions:
 - a. Click Edit Limits.
 - b. Add the RSA NetWitness Suite user (for example, sauser).
 - c. Enable Local Launch, Remote Launch, Local Activation, and Remote Activation permissions.
 - d. Click **OK** and click **OK** again to close the properties box.

General	Options	Default Properties		
Default Protocols	COM Secu	irity MSDTC		
Access Permissions You may edit who also set limits on ap Caution: N of applica securely.	is allowed default acce pplications that determin Modifying access permi tions to start, connect,	ss to applications. You may ne their own permissions. ssions can affect the ability function and/or run		
	Edit Limits	Edit Default		
You may edit who activate objects. Y determine their ow	on Security Limits is . 'ou Group or user n n p & Everyone	ames:		
Caution: t affect the and/or ru	Mo & Performan at & Distributed n s & ANONYM	ce Log Users (RC-GOLD\P I COM Users (RC-GOLD\Di DUS LOGON	erformance Log Users) stributed COM Users) Select Users, Computers, Service Accounts, or Groups	ľ
Caution: 1 affect the and/or ru	Mo & Performan at & Distributed n s & ANONYM	ce Log Users (RC-GOLD\P I COM Users (RC-GOLD\Di DUS LOGON	erformance Log Users) stributed COM Users) Select Users, Computers, Service Accounts, or Groups Select this object type:	1
Caution: 1 affect the and/or ru	Mo & Performan at & Distributed n s & ANONYMI	ce Log Users (RC-GOLD\P I COM Users (RC-GOLD\Di DUS LOGON Ad	erformance Log Users) stributed COM Users) Select Users, Computers, Service Accounts, or Groups Select this object type: Users, Groups, or Built-in security principals Object	Types
Caution: 1 affect the and/or ru	Mo & Performan at & Distributed & ANDNYM	ce Log Users (RC-GOLDVP I COM Users (RC-GOLDVDi DUS LOGON Ad	erformance Log Users) stributed COM Users) Select Users, Computers, Service Accounts, or Groups Select this object type: Users, Groups, or Built-in security principals Object From this location:	1 Types
Caution: 1 affect the and/or ru	No 82 Performan A at 82 Distributed ANDNYM	ce Log Users (RC-GOLDVP I COM Users (RC-GOLDVDi DUS LOGON Ad Everyone	erformance Log Users) stributed COM Users) Select Users, Computers, Service Accounts, or Groups Select this object type: Users, Groups, or Built-in security principals Diject From this location: Iab30.local Locat	Types.
Caution: 1 affect the and/or ru earn more about <u>settir</u>	Mo & Performan At At A	ce Log Users (RC-GOLDVP I COM Users (RC-GOLDVD) DUS LOGON Ad Everyone s ess	erformance Log Users) stributed COM Users) Select Users, Computers, Service Accounts, or Groups Select this object type: Users, Groups, or Built-in security principals Object From this location: [ab30.local Locat Enter the object names to select (examples):	Types
earn more about <u>settin</u>	Mo & Performan A Distributed ANDNYMI Permissions for Local Access Remote Acce	ce Log Users (RC-GOLDVP I COM Users (RC-GOLDVD) DUS LOGON Ad Everyone s ess	erformance Log Users) stributed COM Users) Select Users, Computers, Service Accounts, or Groups Select this object type: Users, Groups, or Built-in security principals From this location: [ab30.local Enter the object names to select (examples): Sause[Check	Types ions
earn more about <u>settin</u>	Mo & Performan A Distributed A ANONYMI Permissions for Local Access Remote Acce	ce Log Users (RC-GOLDVP I COM Users (RC-GOLDVD) DUS LOGON Ad Everyone s ess	erformance Log Users) stributed COM Users) Select Users, Computers, Service Accounts, or Groups Select this object type: Users, Groups, or Builtin security principals From this location: [ab30.local Enter the object names to select (<u>examples</u>): sause(Advanced OK C	Types ions Name

Add Non-Admin Domain User on Windows 2000 Event Source

For Windows 2000 Event Sources, you need to perform the following procedures:

- I. Add the sauser to WMI and DCOMCNFG Management
- II. Add Local Security Policy

To add the RSA NetWitness® Suite user to the WMI and DCOMCNFG management on each Windows 2000 event source:

- 1. Log on to the event source.
- 2. Run wmimgmt.msc.

📨 Run	
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	wmimgmt.msc 🗸
	OK Cancel Browse

- 3. Add the RSA NetWitness Suite user under wmi \root\CIMV2 security option.
 - a. Right click WMI Control and click Properties.

mimgmt - [Console Root\WMI	Control (Local)]		
File Action View Favorites	s Window Help		-
Console Root	· · · · · ·	Actions	
衡 WMI Control (Local)	Windows Management Instrumentation (WMI)	WMI Control (Local)	
WMI Control (Local) Prop General Backup/Restor Computer. Successfully Connec Processor : Intel(R) Operating System : OS Version : 61.76 Service Pack : 1.0 WMI Version : 7601 WMI Version : C/W	erties 2 2 X e Security Advanced alows you to get general information about the ted to: docal computer> Core(TM) 17-2640M CPU @ 2.80GHz Microsoft Windows 7 Enterprise 01 .17514 Windows'aystem 32'unbern	More Actions	
	OK Cancel Apply		

- b. Select the Security tab and click Root\CIMV2.
- c. Click Security

Root	200 A 20	Actions
Control (Local) Win	dows Management rumentation (WMI)	WMI Control (Local)
MI Control (Local) Properties General Backup/Restore Security Adv Namespace navigation allows you to set na	need nespace specific security.	MOREACTIONS

- d. In the Group or user names section, click Add... to create a user.
- e. Select the Enable Account and Remote Enable permissions for that user.
- f. Enter the user (for example, sauser).

WMI Co	ontrol (Local) Proper	ties		1	X		
Gene	ral Backup/Restore	Security Advance	ed				
		40.0	_				
NE	CONCY FOR ROUT (CL	172	_		-		
	Security						
	Group or user names: Authenticated Users CDCAL SERVICE NextGen Log Collector (nglogcollector@lab30.local) Administrators (RC-GOLD\Administrators)						
	Permissions for Auther Users	nticated	Add	Remove Denu			
	Execute Methods	Select Users, Co	mputers, S	ervice Accou	unts, or Gro	oups	? ×
	Full Write	Select this object	t type:				
	Partial Write	Users, Groups, o	or Built-in secu	urity principals			Object Types
	Enable Account	From this location	r.				
_		lab30.local					Locations
	For special permissic click Advanced.	, Enter the chirat		at (automatica)			
_	1	Enter the object	names to sele	ct (<u>examples</u>):			Charle Names 1
_	Learn about access	sausei					Lineck Names
- 7		Advanced				ОК	Cancel
							14
Security for	r ROOT\CIM¥2	×					
Group or Security Group or Security Nex Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security S	user names: TWORK SERVICE dien Log Collector (nglogcollector@ ninistrators (RC-GOLD V-dministrators ser (sauser@lab30.local) 	tab30.local)					
Permissio Panar Provid Enable Remot Read S Edit Se	ons for sauser Al vinne ler Write e Account E Enable Security ecurity						
For speci click Adv	ial permissions or advanced settings, vanced.	Advanced					
Learn ab	out access control and permissions						
	UK Ca	ncel Apply					

g. Click **Check Names** to verify that the new user was added correctly.

Select this object type:		
Users, Groups, or Built-in security principals	Object Types	
From this location:		
lab30.local	Locations	
Enter the object names to select (<u>examples</u>):		
Enter the object names to select (<u>examples</u>): sauser (sauser@lab30.local)	Check Name	s
Enter the object names to select (<u>examples</u>): sauser (sauser@lab30.local)	Check Name	s
Enter the object names to select <u>(examples)</u> : sauser (sauser@lab30.local)	Check Name	s

- h. Click Apply, OK, and OK.
- 4. Run dcomcnfg to add a user under DCOMCNFG.

Applications Default Properties Defaul Security Default Protocols	
Applications:	
{000C101C-0000-0000-C000-00000000046}	1
{1BE1F766-5536-11D1-B726-00C04FB926AF}	11
Automatic Updates	
COM+ Event System	
ComEvents.ComServiceEvents	
CustReg Class	
Defrag FAT engine	
Defrag NTFS engine	
HTML Application	
Image Document	
Internet Explorer(Ver 1.0)	
logagent	
Logical Disk Manager Administrative Service	
Media Plaver	
Microsoft Agent Server 2.0	
Microsoft WBEM Active Scripting Event Consumer Provider	- I
Properties	
OK Cancel Apply	

5. Select **Default Security** tab.



- 6. Click Edit Permissions.
- 7. Find sauser.

nd User or Group: sauser		Search
Couch All		
Search Only In:		
CHILDSSL		
DLPSSLDOMAIN		
	R	
arch Results:		
DLPSSLDOMAIN\sauser (sa u	ser)	

8. Click Add, select Allow Access in the Type of Access field from the drop-down list, and click OK.

ConsUpdateProxy	DNS clients who are permitted to perform
Domain Admins	Designated administrators of the domain
Domain Computers	All workstations and servers joined to the
Domain Controllers	All domain controllers in the domain
RDomain Guests	All domain guests
🕵 Domain Users	All domain users
REnterprise Admins	Designated administrators of the enterpri
REnterprise Read only Doma	in Cor Members of this group are Read-Only Do
REnterprise Read-only Doma	in Cor Members of this group are Read-Only Do
Centerprise Read-only Doma	in Cor Members of this group are Read-Only Do
Centerprise Read-only Doma	in Cor Members of this group are Read-Only Do
Add Show dd Names: DLPSSLDOMAIN\sauser	in Cor Members of this group are Read-Only Do

The Registry Value Permission page is displayed.

Registry Value Permissions	×
Registry Value: DefaultAccessPermission Owner: muditp Name:	
DLPSSLDOMAIN\sauser (sa user)	
R	
Type of Access: Allow Access	•
OK Cancel Add Remo	ve Help

9. Click OK.

To add the Local Security Policy on each Windows 2000 event source:

1. In a command prompt, run the secpol.msc command.

The Local Security Settings window is displayed.

2. In the Local Policies folder, select the User Rights Assignment folder.

Local Security Settings			-	
Action ⊻iew	🗈 🖪 🗡 🖪 🔮			
Tree	Policy A	Local Setting	Effective Setting	
Security Settings	Create a pagefile	Administrators	Administrators	
E G Account Policies	Create a token object			
E Ga Local Policies	Create global objects	Administrators, SER	Administrators, SER	
🕢 🧾 Audit Policy	Create permanent shared objects			
🕑 🤐 User Rights Assign	BB Debug programs	Administrators	Administrators	
E G Security Options	BDeny access to this computer from			
Public Key Policies	BDeny logon as a batch job			
IP Security Policies on	Deny logon as a service			
	BDeny logon locally			
	Enable computer and user account			
	Force shutdown from a remote sy	Administrators	Administrators	
	Generate security audits			
	Dimpersonate a client after authent	SERVICE, Administra	SERVICE, Administra	
	Concrease quotas	Administrators	Administrators	
	Contract and the second	Administrators	Administrators	
	BLoad and unload device drivers	Administrators	Administrators	
	BLock pages in memory			
	BLog on as a batch job			
	BLog on as a service			
	BLog on locally	Administrators, Back	Administrators, Back	
	Manage auditing and security log	DLPSSLDOMAIN(ne	DLPSSLDOMAINine	
	BModify firmware environment values	Administrators	Administrators	-
	ana			
🏂 Start 🛛 🕥 😂 🎲	Local Security Settings		5 🗳 9:39	MAR

3. Select Manage auditing and security log, right click, and select Security.

The Local Security Policy Setting dialog is displayed.

4. Click Add.

Local Security Policy Setting		?	×
Manage auditing and s	ecurity log		
Assigned To	Local Policy Setting	Effective Policy Setting	
DLPSSLDOMAIN\saadmin Administrators DLPSSLDOMAIN\newsa	N N N	2	-
R			
Add If domain-level policy settings are de	fined, they override	local policy settings.	
	OK	Cancel	

The Select Users or Groups dialog is displayed.

5. Enter the non admin username [for example, NetWitness (sauser@childssl.dlpssldomain.com) and click Check Names.

Name	In Folder	^
Everyone Authoratio at ad Llogra		
ANONYMOUS LOGON		1
BATCH		
CREATOR OWNER		
DIALUP		
	85	
ecurity Analytics (sauser@child	ssl. dlpssldomain.com)	

The Local Security Policy Setting dialog is displayed.

6. Click **OK** twice to update the local security policy setting.

Local Security Policy Setting		?	×
Manage auditing and se	ecurity log		
Assigned To	Local Policy Setting	Effective Policy Setting	200
DLPSSLDOMAIN\saadmin Administrators DLPSSLDOMAIN\newsa CHILDSSL\sauser	2 2 2	5	
Add If domain-level policy settings are def	ined, they override I	ocal policy settings.	
	0K	Cancel	

Configure Legacy Collection on RSA NetWitness Suite

This section describes the procedures you need to follow in RSA NetWitness Suite to complete the Windows Legacy event source configuration.

Add a Windows Legacy Event Source

- 1. Access the Services view by selecting Admin > Services from the NetWitness menu.
- 2. In the Services grid, select a Windows Legacy Log Collector service.
- Under Actions, select ^{SO} > View > Config to display the Log Collection configuration parameter tabs.
- 4. Click the Event Sources tab.
- 5. In the **Event Sources** tab, select one of the following options from the drop-down menu.
 - Windows Legacy/Windows.
 - Windows Legacy/NetApp.
- 6. Configure the alias:
 - a. Click ⁺ in the **Event Categories** panel toolbar.

The Add Source dialog is displayed.

b. Specify values for the parameters and click OK.

Add Source		×
Basic		
Alias *	Domain-Alias	
User Name *	user1@domain.com	
Password *	*****	
Advanced		
Use Remote Registry Initialization		
	Cancel	ОК
Note: Enter the creden	ntials you created during Step 1 - Create a Non-A	dmin_
Domain User.		

Note: By default, **Remote Registry Initialization** is selected. For details, see <u>Remote Registry Access</u> below.

The newly added windows event source type is displayed in the **Event Categories** panel.

- 7. Add the event source:
 - a. Select the new alias in the **Event Categories** panel and click + in the **Source** panel toolbar.

The Add Source dialog is displayed.

b. Specify values for the event source parameters and click **OK**.

Add Source			×
Basic			
Name *	Domainsource		
Event Source Address *			
Event Log Name *	Security		~
Enabled	\checkmark		
Advanced			
Event Buffer Size	100	Kilobyte	~
Event Too Large Result	fail		
Maximum Event Data	16	Kilobyte	~
Max Events Per Cycle	0		0
Polling Interval	180		\$
Debug	Off		~
		Cancel	ОК

For details, see Windows Legacy Configuration Parameters below.

The newly added Windows event source is displayed in the **Event Categories** panel.

Sc	Sources						
+	🛨 🗕 🗹 📥 Import Source 🛛 🖄 Export Source						
\checkmark	Name	Event Source Addr	Event Log Name	Event	Event Buffer S	Maximum Eve	
≤	Domainsource		Security	fail	100 KB	16 KB	

Remote Registry Access

Windows Legacy Collector performs an initial verification of the event source before collecting data. By default, Windows Legacy Collector uses Windows Management Instrumentation (WMI) method to perform this initial verification. If you enable Remote registry access method, Windows Legacy Collector performs a remote registry query to verify the event source.

Windows Legacy Configuration Parameters

The following table describes the parameters for a Windows Legacy event source.

Feature	Description		
Basic			
Name*	The name of the event source. Valid value is a name in the [_a-zA-Z] [_a-zA-Z0-9]* range. You can use a dash "-" as part of the name.		
Event Source Address*	IP address of the event source. Valid value is an IPv4 address, IPv6 address, or a hostname including a fully qualified domain name. NetWit- ness defaults to 127.0.0.1 . The Log Collector converts the hostname to lower-case letters to prevent duplicate entries.		
Event Log Name	 The name of the event log from which to collect event data (for example, System, Application, or Security). The following are examples of some of these channels: System - applications that run under system service accounts (installed system services), drivers, or a component or application that has events that relate to the health of the system. Application - all user-level applications. This channel is unsecured and it is open to any application. If an application has extensive information, you should define an application-specific channel for it. Security - the Windows Audit Log (event log) used exclusively for the Windows Local Security Authority. 		
Enabled	Select this checkbox to collect from this event source. If you do not check this checkbox, the Log Collector does not collect events from this event source.		

Feature	Description	
Event Dir- ectory Path	 NetApp .evt or .evtx files directory path. This must be the UNC path. The NetApp generates event data and saves it in .evt or .evtx files in a shareable directory on the NetApp appliance. In each polling cycle, the Log Collector browses the configured NetApp shared path for the .evt files that you identified with the Event Directory Path and Event File Prefix parameters. The Log Collector: sorts files that match the event-file-prefix.YYMMDDhhmmss.evt format in ascending order. uses the timestamp of the last file processed to determine the files that still need processing. If the Log Collector browses the configured NetApp shared path for the .evtx files that you identified with the Event Directory Path and Event File Prefix parameters. The Log Collector: sorts files that match the event-file-prefix.YYMMDDhhmmss.evt format in ascending order. uses the timestamp of the last file processed to determine the files that still need processing. If the Log Collector browses the configured NetApp shared path for the .evtx files that you identified with the Event Directory Path and Event File Prefix parameters. The Log Collector : sorts files that match the event-file-prefix.YYMMDDhhmmssms.evtx format in ascending order. 	
Event File Pre- fix	Prefix of the .evt files (for example, adtlog .) saved in the Event Dir ectory Path.	
Advanced		
Event Buffer Size	Maximum size of the data the Log Collector pulls from the event source for each request. Valid value is a number in 0 to 511 Kilobytes range. You specify this value in Kilobytes .	

Feature	Description
Event Too Large Result	Tells the Log Collector what to do if an event is too large for the event buf- fer.
Maximum Event Data	 Maximum size of event data to include in the output. Valid value is a number in 0 to 511Kilobytes range. You specify this value in Kilobytes or Megabytes. 1 Kilobyte - 100 Megabytes 0 = do not include event data in the output.
Max Events Per Cycle	The maximum number of events per polling cycle (how many events col- lected per polling cycle).
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is 180.For example, if you specify 180, the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, it will wait for it to finish that cycle. If you have a large number of event sources that you are polling, it may take longer than 180 seconds for the polling to start because the threads are busy.

Feature	Description
Debug	Caution: Only enable debugging (set this parameter to On or Verbose) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector .
	Enables or disables debug logging for the event source. Valid values are:
	• Off = (default) disabled
	• $On = enabled$
	• Verbose = enabled in verbose mode - adds thread information and source context information to the messages.
	This parameter is designed to debug and monitor isolated event source collection issues. If you change this value, the change takes effect immediately (no restart required). Limit the number of event sources for which you use Verbose debugging to minimize performance impact.
Cancel	Closes the dialog without adding the Windows Legacy event source.
OK	Adds the current parameter values as a new event source.

Copyright © 2017 EMC Corporation. All Rights Reserved.

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners.