RSA[®]Security Analytics

Security Analytics v10.3 Windows Legacy Collection Installation Instructions

Contents

Window Legacy Collection	2
SA Legacy Windows Collector Setup Requirements	3
Create a Non-Admin Domain User	4
Task 1 - Create Non-Admin Domain User on the Domain Controller	5
Task 2 - Set Event Log Security on Domain Controller	6
Task 3 - Add Non-Admin Domain User to WMI and DCOMCNFG on Each Windows Legacy Event Source	8
Task 4 - Add Non-Admin Domain User to Local Administrators and Remote Desktop Users Groups on	
Windows 2008 Server	. 13
Install the SA Legacy Windows Collector	14



Window Legacy Collection

The Security Analytics (SA) 10.3 Log Collector introduces Windows Legacy collection. With this feature, you can collect event data from:

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



SA Legacy Windows Collector Setup Requirements

To set up the SA Legacy Windows Collector, you need:

- Any physical or virtual Windows 2008 64-Bit Server located in the same domain as your Windows 2003 event sources.
- A minimum of 20% free disk space. For example, you need at least 20 GB of free space if your system drive is 100 GB in size.
- A non-admin domain user (see <u>Create a Non-Admin Domain User</u>) that has access to the event sources in the domain.
- To include the non-admin domain user in both the Local Administrator Group and the Remote Desktop User Group on Windows legacy collector system.







Create a Non-Admin Domain User

You must complete the following tasks to create a non-admin domain user for the **SA Legacy Windows Collector.**

Task 1 - Create a non-admin domain user (for example, sauser) on the Domain Controller.

Task 2 - Set Event Log Security on the Domain Controller.

Task 3 - Add a non-admin domain user to **WMI** and **DCOMCNFG** management on each Windows 2003 or earlier event source from which you want to collect event data.

Task 4 - Add non-admin domain user (for example, **sauser**) to the Local Administrators group and Remote Desktop Users group on Windows 2008 server.

You need to add a non-admin domain user in the Local Administrators group only on the
 Windows 2008 server on which the SA Legacy Windows Collection Service is installed. You do not need to add it to all event source machines.



Task 1 - Create Non-Admin Domain User on the Domain Controller

To create the SA domain user (for example, **sauser**) on the Domain Controller:

1. Log into the Domain Controller.



2. On Domain Controller create a non-admin domain user (for example, sauser).

Active Directory Users and Com	puters		
HIE Action View Help			
≥ 🗢 Z 🗔 🔏 🖬 👗 🛛		7 🔎 🎕	
Active Directory Users and Comput	Name	Туре	Description
🗄 🚞 Saved Queries	💄 Administrator	User	Built-in account for admini
∃ 🙀 lab30.local	& Allowed RODC Password Replicati	Security Group - Domai	Members in this group can
🗄 🛄 Builtin	& Cert Publishers	Security Group - Domai	Members of this group are
Computers	& Denied RODC Password Replicatio	Security Group - Domai	Members in this group can
Domain Controllers	& DnsAdmins	Security Group - Domai	DNS Administrators Group
	& DnsUpdateProxy	Security Group - Global	DNS clients who are permi
Intervice 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
	& 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
	& Group 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
	S RSA Log Collector	User	
	& sauser	User	
	Schema Admins	Security Group - Universal	Designated administrators
	-		-
	*		

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



Task 2 - Set Event Log Security on Domain Controller

To set Event Log Security on the Domain Controller:

- 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\System\CustomSD,1,%SysCustomSD%,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 **Sceregvl.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 pane, right click, and select **Enforce**.
 - e. Under Security Filtering, click Add.
 - f. Under Select User, Computer and Group, type Domain Computers, click on 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 pane.

📖 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
B Eventlog: Security descriptor for Security event log	Not Defined
📖 Eventlog: Security descriptor for System event log	Not Defined
📖 Interactive logon: Display user information when the session is lo	Not Defined
🔝 Interactive leader. Do not display last user name	Mat Defined

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

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:

Run following command in powershell. 1. Make sure that you change the user name accordingly (for example, change the user Note: 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 : S-1-5-21-3244245077-2111152846-3233386924-1114

If the security policy Settings box:

Value

• Is not empty, append the following string to the value in the box: (A;; 0x1;;; siz.

For example:

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

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;;0
x7;;;SO)(A;;0x3;;;IU)(A;;0x3;;;SU)(A;;0x3;;;S-1-5-3)(A;; 0x1;;;SID.
```

For example:

```
O:BAG:SYD:(D;;0xf0007;;;AN)(D;;0xf0007;;;BG)(A;;0xf0007;;;SY)(A;;0x7;;;BA)(A;;0
x7;;;SO)(A;;0x3;;;IU)(A;;0x3;;;SU)(A;;0x3;;;S-1-5-3)(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.



Task 3 - Add Non-Admin Domain User to WMI and DCOMCNFG on Each Windows Legacy Event Source

To add the SA user (for example, **sauser**) to the WMI and DCOMCNFG management on each Windows 2003 or earlier event source:

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



- 3. Add the SA 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

📸 wmimgmt - [Console Root\WMI Control (Local)]	
a File Action View Favorites Window Help ← → 2 c L L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L f c L	_ 8 ×
Console Root	Actions
WMI Control (Local) Windows Management Instrumentation (WMI)	WMI Control (Local)
WMI Control (Local) Properties	More Actions
General Backup/Restore Security Advanced	
Namespace navigation allows you to set namespace specific security.	
Root Image: Second Seco	
OK Cancel Apply	

- 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 ?X	
General Backup/Restore	Security Advanced	
N Security for ROOT\CI	M¥2 🔀	
Security		
Group or user names:		
& Authenticated U	sers	
& LOCAL SERVIC	E	
NETWORK SEP	RVICE	
👗 NextGen Log Co	ollector (nglogcollector@lab30.local)	
Administrators (F	(L-GULD \Administrators)	
, , , , , , , , , , , , , , , , , , ,		
D	Add Hemove	
Users	Allow Denv	
Execute Methods	Select Users, Computers, Service Accounts, or Groups	? ×
Full Write	Select this object type:	
Partial Write	Users Groups of Built-in security principals	Object Tupes
Provider Write		- Object Types
Enable Account	From this location:	
For special permissic	lab30.local	Locations
click Advanced.	Enter the object names to select (examples):	
Learn about access	sauser	Check Names
	Advanced OK	Cancel



ecurity for ROOT\CIMV2		×
Security		
Group or user names:		
& NETWORK SERVICE		
📃 🧸 NextGen Log Collector (nglog	jcollector@lab30.	local)
Administrators (RC-GOLD \Ad	ministrators)	
👗 sauser (sauser@lab30.local)		
•		
	Add	Remove
Permissions for sauser	Allow	Deny
Provider Write		
Enable Account		
Remote Enable		
Read Security		
Edit Security		
For special permissions or advance click Advanced.	ed settings,	Advanced
Learn about access control and pe	ermissions	
ОК	Cancel	Apply

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

Select Users, Computers, Service Accounts, or Groups	? ×
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>):	
sauser (sauser@lab30.local)	Check Names
Advanced OK	Cancel

- 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**.

Component Services			
💩 File Action View Window Help	3		_ B ×
🗢 🔿 🗾 🖬 🗶 🗐 🙆	〒 11 12 12 12 12 12 12 12 12 12 12 12 12 12		
 Console Root Component Services My Computer COM+ Applications DCOM Config DCOM Config DCOM Config E Contributed Transac E Services (Local) Services (Local) 		Actions Computers ? X MSDTC Default Properties	,
1	Learn more about <u>setting these properties</u> .	Cancel Apply	

- 5. Under Access Permissions:
 - a. Click Edit Limits
 - b. Add the SA 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 SA 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.

My Computer Proper	ties			1	? ×			'		
General) Opti	ions	Defaul	t Properties						
Default Protocol	s	COM Sec	urity	MSDTC						
Access Permission	15									
You may edit wh also set limits on	no is allowed Lapplications	default acce that determi	ess to applicat ne their own r	ions. You may ermissions.						
of appli secure	n: Modirying ications to st ly.	access perm art, connect,	function and	or run						
	Ed	it Limits	Edit	Default						
	Acces	ss Permissi	on			?	×			
Launch and Activa	ation Sec	urity Limits								
You may edit wh activate objects	nois :You Gi	oun or user r	ames:							
determine their o	own p	Everyone								
Caution	n: Moj 🛛 🖇	Renformar	ice Log Users	(RC-GOLD\Pe	rforma	ince Log Users)				
and/or	neat 👔 run s 📝	🔏 Distributei 🗽 ΔΝΠΝΥΜ	1 COM Users ALIS LAGAN	(RC-GOLD\Dis 	tribute	d COM Users)				
		_			Selec	t Users, Compu	ters, Service	Accounts, or	Groups	? ×
					Sele	ct this object type	:			
				Ad	Use	ers, Groups, or Bui	t-in security prir	ncipals		Object Types
	Pe	ermissions for	Everyone		From	n this location:				
		Local Acces	s		lab3	30.local				Locations
Learn more about <u>se</u>	<u>itting</u>	Remote Acc	ess		Ente	r the object name	s to select (<u>exa</u>	imples):		
					sau	ser				Check Names
					A	dvanced			OK	Cancel
	Le	arn about ac	cess control a	and permissions	1					
					ОК	Cancel				



Task 4 - Add Non-Admin Domain User to Local Administrators and Remote Desktop Users Groups on Windows 2008 Server

You only need to add non-admin domain user in the Local Administrators group on the
 Note: Windows 2008 server on which the SA Legacy Windows Collection Service is installed. You do not need to add it to all eventsource machines.

To add a non-admin user (for example, sauser) to local Administrators and Remote Desktop Users groups:

- 1. Log in as a local administrator to windows 2008 server.
- 2. Click Start >Administrative Tools>Computer Management.
- 3. Click Local Users and Groups.
- 4. Click Groups.
- 5. Add a non-admin user (for example, sauser) to the local Administrator group:
 - a. Click Administrators.
 - b. Add a non-admin user (for example, sauser) to the local Administrator group.
- 6. Add a non-admin user (for example, sauser) to the local Remote Desktop Users group:
 - a. From Administrative Tools>Computer Management>Local Users and Groups>Groups, click Remote Desktop Users.
 - b. Add a non-admin user (for example, sauser) to the local Remote Desktop Users group.





Install the SA Legacy Windows Collector

To install the SA Legacy Windows Collector on a Windows 2008 server:

- 1. Download the SALegacyWindowsCollector-version-number.exe from SecurCare Online (SCOL).
- Log on to a Windows 2008 machine using a non-admin domain user (or local administrator). Please refer to <u>Create a Non-Admin Domain User</u> if you need instructions on how to create a non-admin domain user.
- 3. Copy the SALegacyWindowsCollector-version-number.exe to the Windows 2008 server.
- 4. Right click on the SALegacyWindowsCollector-version-number.exe and select Run As Administrator.

The **Preparing to Install....** page of installation wizard displays.

Security Analytics Legacy	Windows Collector - InstallShield Wizard
	Preparing to Install
0	Security Analytics Legacy Windows Colector Setup is preparing the InstallShield Wizard, which will guide you through the program setup process. Please wait.
2	Extracting: Security Analytics Legacy Windows Colector.msi
	Cancel



After the installation program extracts SA Legacy Windows Collector installation files, the **Welcome...** page is displayed.

🖶 Security Analytics Legac	y Windows Collector
2	Welcome to installation wizard for Security Analytics Legacy Windows Collector
H	The Setup Wizard will install Securty Analytics Legacy Windows Collector on your computer. To continue, click Next.
	WARNING: This program is protected by copyright law and international treaties.
inscellonielo	< Back: Next > Cancel

5. Click Next.

The License Agreement page is displayed.

License Agreement Please read the following Icens	: agreement carefully.	
LICENSE AGREEMENT		A
** READ CAREFULLY **	• IMPORTANT INFORMAT •	ION PLEASE
Th programs and other information, the u expressly conditio License Agreement	is Software contains proprietary material se of which is subject ned upon acceptance o (the Agreement).	computer and t to and f this
 I accept the terms in the Icensi I do not accept the terms in the stallShield 	e agreement Llicense agreement	Print
	< Back Next :	> Cancel

6. Read the License agreement carefully, select the I accept the terms in the license agreement radio button, and click Next.



The Logon Information page is displayed.

Note: The example in this procedure uses the non-admin domain user "**sauser**" for a windows domain called "**mydomain**" along with the corresponding password for the user.

Logon	Information	2
Specify t user acco	he user name and password of the user account that will logon to use this a ount must be in the form DOMAIN(Username.	oplication. The
	User name:	1
	Password:	
	••••••]
nstallShie	eld .	1

7. Enter a user name and password and click **Next**.



The **Ready to Install the Program** page displays.

Note: If the credentials are not valid, **Invalid credentials message** is displayed.

The wizard is ready to begin installation.		
Click Install to begin the installation.		
stali5held	 	

8. Click Install.

The Installing SA Legacy Windows Collector page displays.

Security Installing The proc	Analytics Legacy Windows Collector g Security Analytics Legacy Windows Collector gram features you selected are being installed.	
1 1 1 1	Please wait while the Installation Wizard installs Security Analytics Legacy Windows Collector. This may take several minutes. Status:	
InstallShield -	< Back Next > Canc	el

After the installation completes, the **Next** button becomes active.



9. Click Next.

The Installation Completed page is displayed.

🔂 Security Analytics Legacy V	Windows Collector
	Installation Completed
2	The Installation Wizard has successfully installed Security Analytics Legacy Windows Collector, Click Finish to exit the wizard.
3	Show the Windows Installer log Collector Log: C:\Program Files\NwLogCollector\installlog.txt
	< Back Finish Cancel

- 10. (Optional) If you want to review a log of the Installation, select the **Show the Windows Installer log** check box.
- 11. Click Finish.

Refer to the following log files if you need to troubleshoot problems:

- Note:
- %systemDrive%\Netwitness\ng\logcollector\MessageBroker.log
- %systemDrive%\Program Files\NwLogCollector\installlog.txt