The Security Division of EMC

SA Kerberos, WinRM and Identity Setup

Revision 1.2 Updated 08/27/14

Michael Gotham

Chris Ahearn

Jay Kisner

Contents

Overview

The steps below are designed to assist with Windows Server 2008 Application, Security and Event log collection into a RSA Security Analytics 10.3 SP1 Log Collector using Kerberos and a domain account with administrative permissions. Finally this document will go over setting up the Identity Feed to add Active Directory Domains, Workstations and Usernames to packet and non Windows sessions.

This document has three distinct parts. The first is setting up Kerberos for Active Directory authentication of service accounts (Broker, Concentrator, etc) as well as other accounts used for various purposes. Please note these steps do not set up Active Directory integration into the GUI. This is a separate process configured in the SA GUI under **Administration -> System.** Setting up Kerberos on all boxes is essential for authenticating service accounts for Security Analytics use.

The second piece is setting up Windows Collection on Security Analytics and setting up WinRM via a GPO for log collection. Since domain controllers do not have local accounts an authenticated user and GPO must be used. Identity leverages Windows messages (Win2K8 =4624, 4769, 4770, 4773 Win2K3= 528, 540, 673, 674) which are typically found on domain controllers in the Security channel. This guide will only go over setup for Win2K8 using WinRM. However Win2K3 is similar.

The third piece is configuring the Log Collector for Identity and setting up the Identity feed.

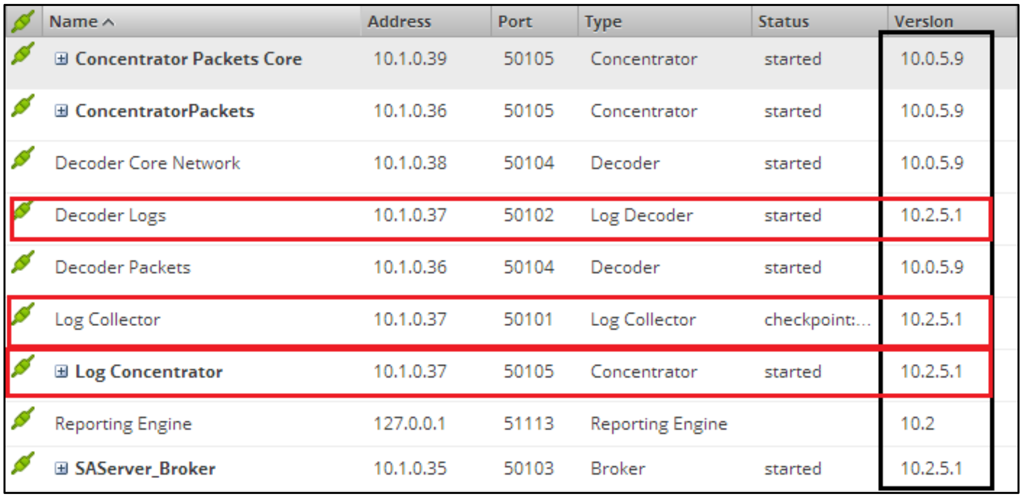
Windows Remote Management (WinRM) is the Microsoft implementation of WS-Management Protocol, a standard SOAP-based, firewall-friendly protocol that provides a common way for systems to access and exchange management information. WinRM is capable of many things, including remote execution of commands and scripts and the security implications of WinRM are beyond the scope of this paper. More information about WinRM can be found at: http://msdn.microsoft.com/en-us/library/windows/desktop/aa384426%28v=vs.85%29.aspx

(The WinRM version used for testing / configuration in this document is WinRM 2.0.)

https://knowledge.rsasecurity.com/docs/rsa_env/device_config/Windows_Eventing_deployment_overview.pdf

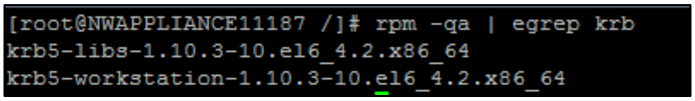
Prerequisites

1. Navigate to Administration->Devices to verify that log collector, log decoder and concentrator are running 10.2 SP1 (10.2.5.1) or higher



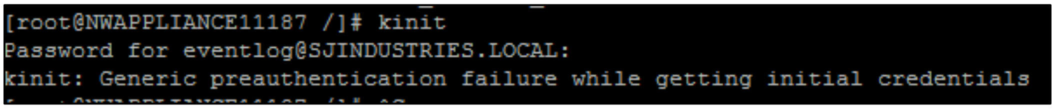
Name ^	Address	Port	Type	Status	Version
⊞ Concentrator Packets Core	10.1.0.39	50105	Concentrator	started	10.0.5.9
⊞ ConcentratorPackets	10.1.0.36	50105	Concentrator	started	10.0.5.9
Decoder Core Network	10.1.0.38	50104	Decoder	started	10.0.5.9
Decoder Logs	10.1.0.37	50102	Log Decoder	started	10.2.5.1
Decoder Packets	10.1.0.36	50104	Decoder	started	10.0.5.9
Log Collector	10.1.0.37	50101	Log Collector	checkpoint:...	10.2.5.1
⊞ Log Concentrator	10.1.0.37	50105	Concentrator	started	10.2.5.1
Reporting Engine	127.0.0.1	51113	Reporting Engine		10.2
⊞ SAServer_Broker	10.1.0.35	50103	Broker	started	10.2.5.1

2. Verify that proper Kerberos packages are installed



```
[root@NWAPPLIANCE11187 /]# rpm -qa | egrep krb
krb5-libs-1.10.3-10.el6_4.2.x86_64
krb5-workstation-1.10.3-10.el6_4.2.x86_64
```

3. Verify kinit is installed



```
[root@NWAPPLIANCE11187 /]# kinit
Password for eventlog@SJINDUSTRIES.LOCAL:
kinit: Generic preauthentication failure while getting initial credentials
```

Configure Kerberos Authentication

****Please note the following steps must be done on the log decoder or log collector appliances used to pull WinRM security logs. However if external Kerberos authentication for users is required on the appliances, the following steps will be used to set up Kerberos.**

1. Make sure that you have upgraded all your Log Collection services to at least Security Analytics 10.2.5.1 (using the **nwlogcollectorcontent-10.2.5.1-1.noarch.rpm)**.

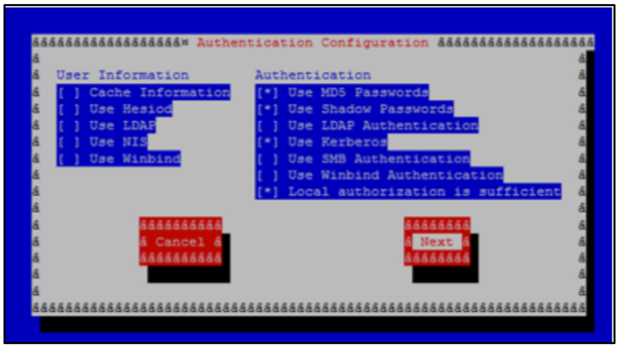
2. Make sure that DNS can resolve fully qualified domain names to addresses and the addresses to the fully qualified domain names. If this is not working check your /etc/resolv.conf file.

3. Security Analytics supports a single Kerberos principal per Kerberos domain. This means that all Windows collection aliases that correspond to a Windows Active Directory domain must use the same domain account. You must:
   a. Use domain accounts **exclusively**.
   b. Make sure that each domain account has the appropriate access for collection so that all channels work.

4. Use the Kerberos principal name as the **User Name**.
   When you configure an alias with the **Negotiate** authentication method under Windows Event Source Configuration Parameters, you must:
   a. Specify the Kerberos principal name for the **User Name** parameter in the format ***username@KERBEROSREALM***.
   Example: logcollector@LAB30.LOCAL.
   (Use all UPPER CASE letters to define a Kerberos realm name.)
   b. Use fully qualified domain names for event sources. (Do not use an IP address.)

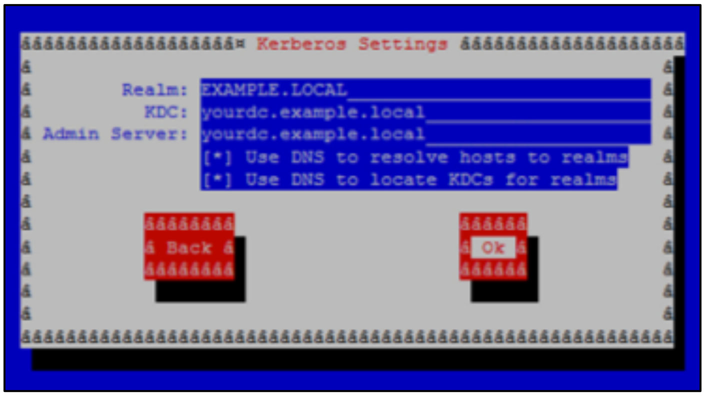
5. Install all the following RPM's from yum (This can be performed by running the following commands:
   a. yum install krb5-libs
   b. yum install pam_krb5
   c. yum install krb5-workstation

6. Run authconfig-tui from the command line.
   a. Select "Use Kerberos"
   b. Select "Local authorization is sufficient"



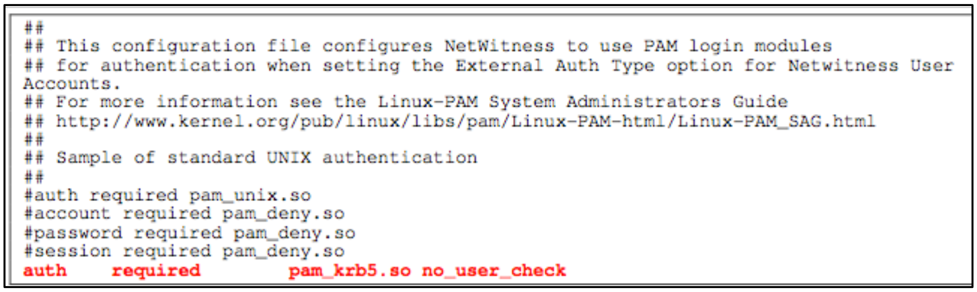
```
Authentication Configuration

User Information             Authentication
[ ] Cache Information        [*] Use MD5 Passwords
[ ] Use Hesiod               [*] Use Shadow Passwords
[ ] Use LDAP                 [ ] Use LDAP Authentication
[ ] Use NIS                  [*] Use Kerberos
[ ] Use Winbind              [ ] Use SMB Authentication
                             [ ] Use Winbind Authentication
                             [*] Local authorization is sufficient
```

7. Select Next
    a. Enter your Kerberos realm which should be your active directory domain name in **ALL CAPS.**
    b. Set your KDC and admin server to your AD domain controller
    c. Check "Use DNS to resolve hosts to realms" and "Use DNS to locate KDC's for realms"



```
       Realm: EXAMPLE.LOCAL
         KDC: yourdc.example.local
Admin Server: yourdc.example.local
              [*] Use DNS to resolve hosts to realms
              [*] Use DNS to locate KDCs for realms
```

8. Select Ok. You should now be back at the command line.
    a. Run "*kinit <youradusername>*" to test Kerberos authentication.
    b. Enter your AD password when prompted. This command will produce no output if successful, but will generate an error if it fails.
9. Run "**vi /etc/pam.d/netwitness**" to open the netwitness file in vi editor
    a. Comment out all lines in the Netwitness file and add the following to the end of the line "auth required pam_krb5.so no_user_check"



```
##
## This configuration file configures NetWitness to use PAM login modules
## for authentication when setting the External Auth Type option for Netwitness User
Accounts.
## For more information see the Linux-PAM System Administrators Guide
## http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/Linux-PAM_SAG.html
##
## Sample of standard UNIX authentication
##
#auth required pam_unix.so
#account required pam_deny.so
#password required pam_deny.so
#session required pam_deny.so
auth     required        pam_krb5.so no_user_check
```

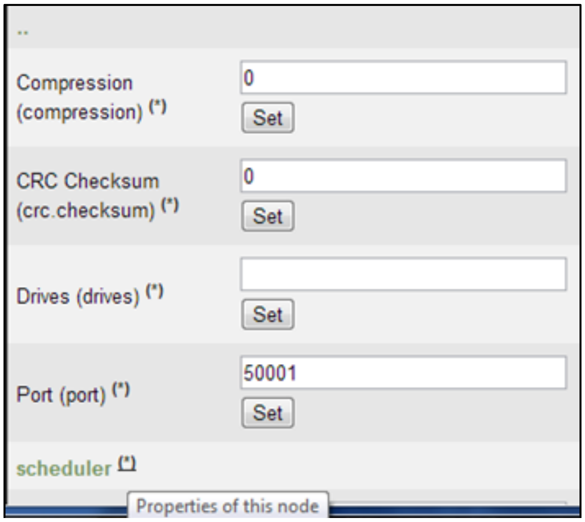
10. Run "**vi /etc/krb5.conf"** to open the krb5.conf file in editor.
    a. Set the **ticket_lifetime** parameter.
    b. Windows collection does not renew tickets. Set the **ticket_lifetime** parameter to the largest value that is supported in your Windows environment. 10h would represent 10 hours which is the Windows Active Directory Domain default setting.

Schedule Windows collection to restart

You can restart Windows collection automatically using the Task Scheduler. On a start and restart, Windows collection retrieves and lists Kerberos TGTs for the principals. Before the TGTs expire, you must restart the Windows collection. Please make sure that the restart interval you choose is lower than the lifetime of TGTs. Windows collection does not renew TGTs because the TGTs may expire before the requested ticket lifetime.

Complete the following steps to schedule a Windows collection restart using the Task Scheduler:

1. In the REST API, click **sys** > **config**.
   The system configuration parameters are displayed below.



..

Compression (compression) (*) — 0 — Set

CRC Checksum (crc.checksum) (*) — 0 — Set

Drives (drives) (*) — Set

Port (port) (*) — 50001 — Set

scheduler (*)

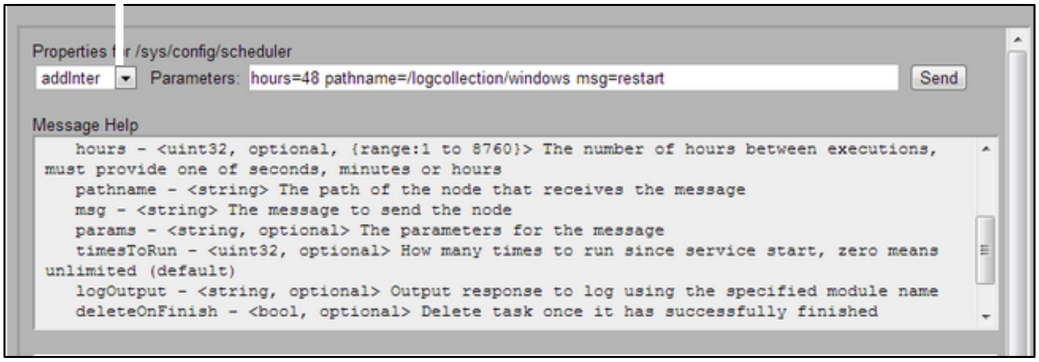
2. Click **(*)** to the right of **scheduler**. The **Properties for the/sys/config/scheduler** are displayed.

   .

3. Select **addInter** from the drop-down list to schedule an action at an interval.

4. Enter the following string in Parameters:
   ***durationtype=value* pathname=/logcollection/windows msg=restart**

   durationtype can be seconds, minutes or hours. For example, **hours=8** schedules Windows collection to restart every 48 hours.



Properties f r /sys/config/scheduler

addInter — Parameters: hours=48 pathname=/logcollection/windows msg=restart — Send

Message Help

```
   hours - <uint32, optional, {range:1 to 8760}> The number of hours between executions,
must provide one of seconds, minutes or hours
   pathname - <string> The path of the node that receives the message
   msg - <string> The message to send the node
   params - <string, optional> The parameters for the message
   timesToRun - <uint32, optional> How many times to run since service start, zero means
unlimited (default)
   logOutput - <string, optional> Output response to log using the specified module name
   deleteOnFinish - <bool, optional> Delete task once it has successfully finished
```

5. Click **Send** and review the **sys/config/scheduler** to confirm that the Security Analytics scheduled Windows Log Collection to restart.

6. If you need to change the interval of the scheduled restart task, you need to delete the task and specify a new one:
   - Click **(*)** to the right of **scheduler** and select **print** from the drop-down list to display the scheduled tasks under **Output**.
   - Note the task-id, select **delSched** from the drop-down list message, enter the **id=*task-id*** string in **Parameters**, and click**Send**.
   - Repeat the steps above for adding the new scheduled restart task.

Review Kerberos-Related Logs at Windows Collection Restart

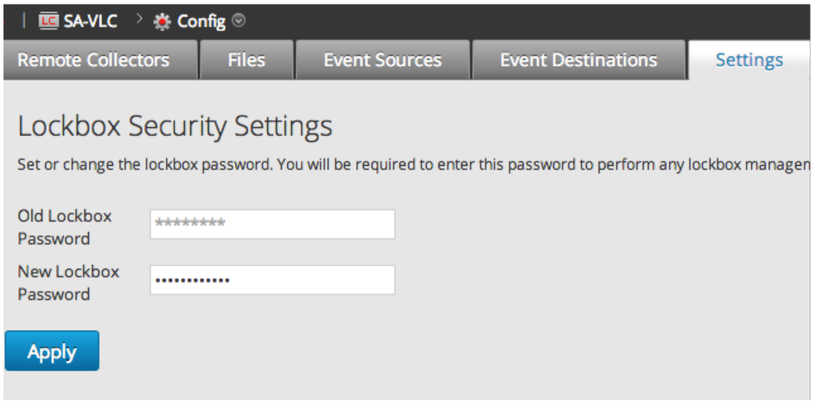
A Windows Collection restart generates log messages on the status of Kerberos TGT acquisition and other details, for example:

```
Apr 26 16:57:38 localhost nw[28119]: [WindowsCollection] [info] Refreshed Kerberos ticket
cache for account : logcollector@LAB30.LOCAL
Apr 26 16:57:38 localhost nw[28119]: [WindowsCollection] [info] Kerberos
ticket cache:
Ticket cache: DIR::/var/netwitness/logcollector/runtime/krb5_ccache_dir/
tktvl5iTI
Default principal: logcollector@LAB30.LOCAL
Valid starting Expires Service principal
2013-Apr-26 20:57:37 2013-Apr-26 21:12:37 krbtgt/LAB30.LOCAL@LAB30
.LOCAL
renew until 2013-Apr-26 21:12:37, Etype (skey, tkt): arcfour
-hmac, arcfour-hmac
```

Configure Windows Event Sources

Set up the Lockbox

1. Prior to setting up any Windows Devices on a Log Collector you will need to setup its Lockbox. You can do this by going to **Administration -> Devices -> Select Log Collector -> Config -> Settings**
   a. Enter a Lockbox password in **New Lockbox Password** that consists of atleast 1 of the following: Uppercase, Lowercase, Number, Special Character
   b. Click **Apply**



Lockbox Security Settings

Set or change the lockbox password. You will be required to enter this password to perform any lockbox managen

Old Lockbox Password: ********

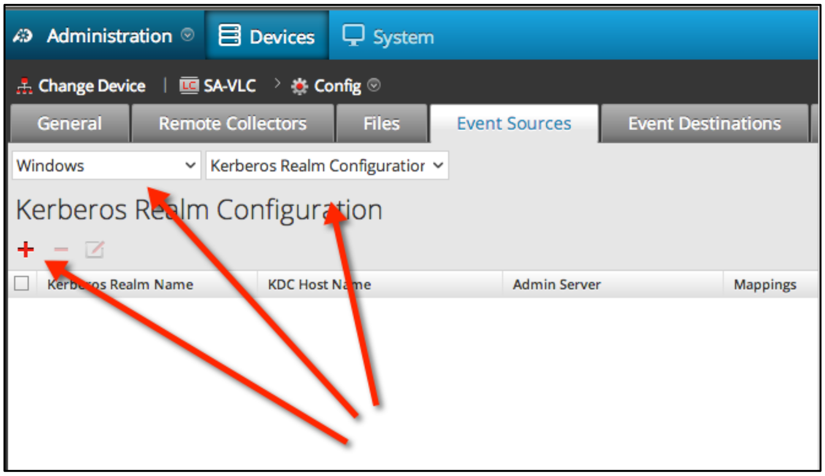
New Lockbox Password: ••••••••••••

Add Windows Event Sources

1. Go to **Administration → Devices → Select Log Collector → Config → Event Sources**
   a. Select **Windows** from the drop down menu and **Kerberos Realm Configuration** from the drop down next to it. Only perform this step if the Kerberos Realm you set up at the beginning of this document is **NOT** already populated.
   ***Note:** If you are running 10.2 SP2 or earlier this step is not necessary. Move to step 2

   b. Click the plus button to add a new Kerberos Realm Configuration

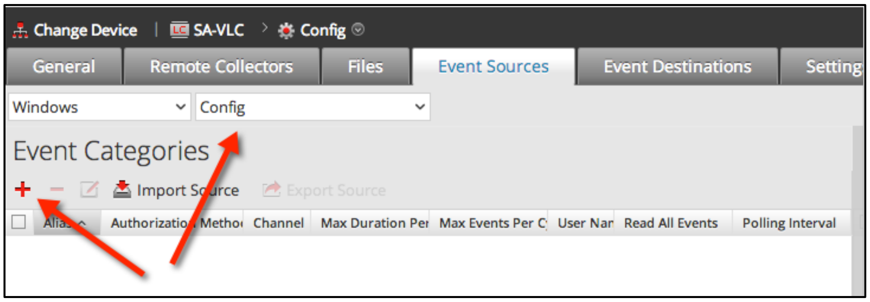
   c. Enter the same information you provided in the authconfig-tui wizard in the Configuring Kerberos Authentication section. Note Kerberos realm name must be in **ALL CAPS**

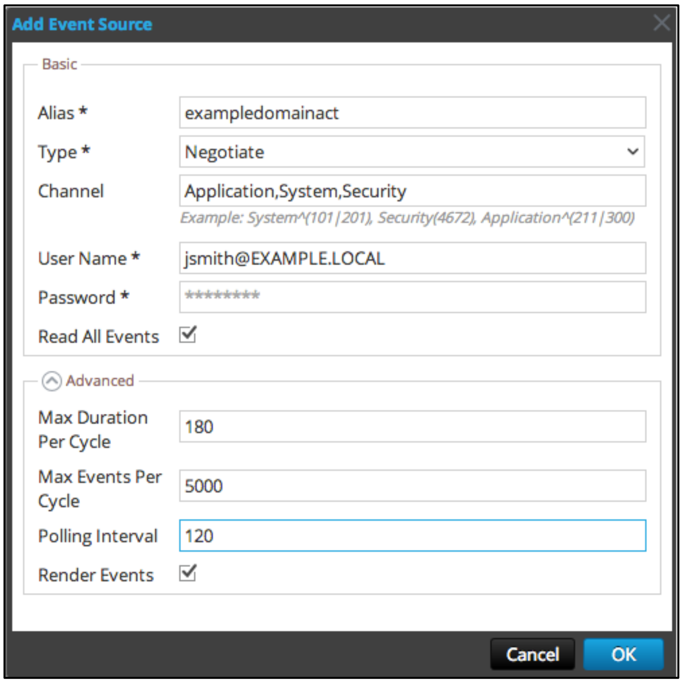


Kerberos Realm Configuration

□	Kerberos Realm Name	KDC Host Name	Admin Server	Mappings

2. Change the dropdown from **Kerberos Realm Configuration** to **Config** and click the plus button to add an event category.
   a. Give the event source an **Alias**.
      It is recommend to keep the alias alphanumeric and to not use special characters.
   b. Change **Type** to **Negotiate**
   c. For **Channel** enter **"Application,System,Security"**
   d. **Username** will be the username with administrative rights in the domain used to collect the logs from Windows Domain Controllers. Note the format of username@DOMAIN
      Capital letters are important for the domain suffix.
   e. Enter password for this account
   f. Check **Read All Events**
   g. From the advanced drop down set **Max Duration Per Cycle** to **180**
   h. **Max Events Per Cycle 5000**
   i. **Polling Interval 120**
   j. Check **Render Events**
   k. Click **OK**




Add Event Source

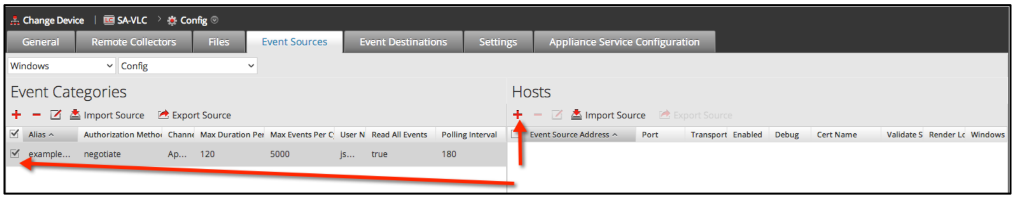
Basic

Alias *	exampledomainact
Type *	Negotiate
Channel	Application,System,Security *Example: System^(101|201), Security(4672), Application^(211|300)*
User Name *	jsmith@EXAMPLE.LOCAL
Password *	*********
Read All Events	☑

Advanced

Max Duration Per Cycle	180
Max Events Per Cycle	5000
Polling Interval	120
Render Events	☑

3. Check your newly added event category.



Event Categories

☑	Alias	Authorization Metho	Chann	Max Duration Pe	Max Events Per C	User N	Read All Events	Polling Interval
☑	example...	negotiate	Ap...	120	5000	js...	true	180

Hosts

□	Event Source Address	Port	Transport	Enabled	Debug	Cert Name	Validate S	Render Lc	Windows

a. To the right of event category click the plus under **Hosts** to add a new host

b. In the **Event Source Address** list the IP of your first domain controller.

c. If using http leave the port at **5985**

d. Set **Tansport Mode** to **http**

e. Check **Enabled**

f. Under Advanced select the appropriate type. In this case it will be **Domain Controller** however configuration for non domain controllers is the same with the exception of selecting **Non-Domain Controller**

g. Do not check **Validate Server**

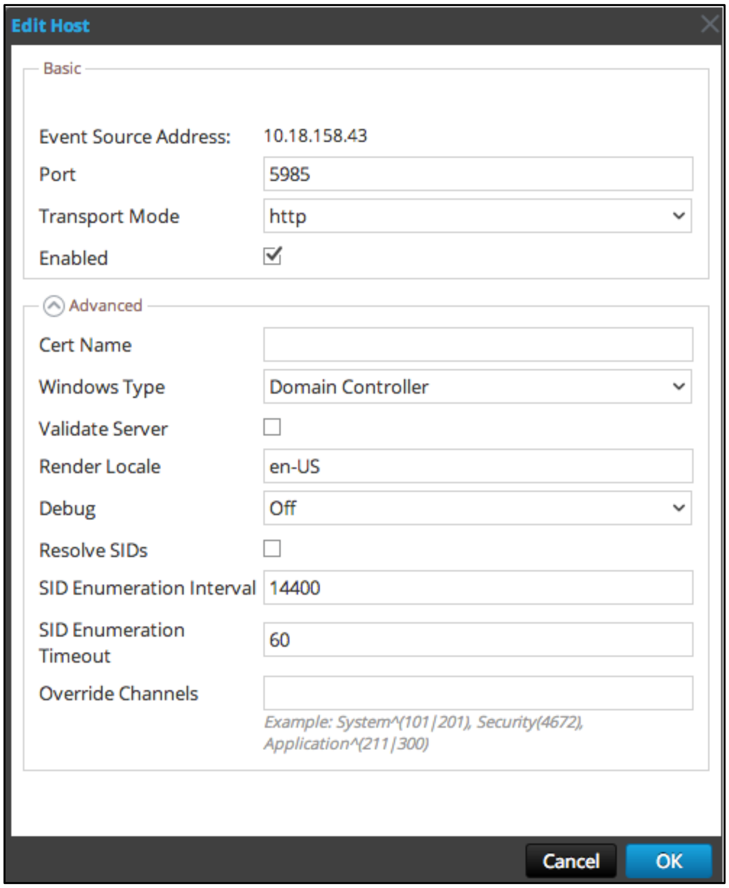
h. Enter your appropriate local language for the domain controller under **Render Locale**. US English is **en-US**

i. Select **Off** for **Debug**

j. Do not check **Resolve SIDs**

k. Click **OK**

l. Enter any remaining domain controllers or Windows servers. You can do a bulk import using a csv by clicking the **Import Source** button in the host section.



Edit Host

Basic

Event Source Address: 10.18.158.43

Port: 5985

Transport Mode: http

Enabled: ☑

Advanced

Cert Name:

Windows Type: Domain Controller

Validate Server: □

Render Locale: en-US

Debug: Off

Resolve SIDs: □

SID Enumeration Interval: 14400

SID Enumeration Timeout: 60

Override Channels:

Example: System^(101|201), Security(4672), Application^(211|300)

4. From the **General** tab scroll down to **Windows Collection** and select **Start Collection of Service Startup**

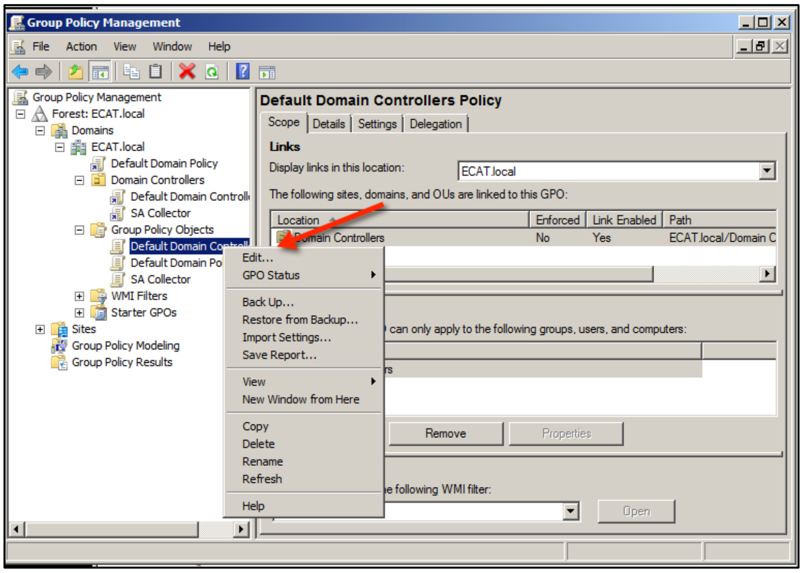
5. Restart the Log Collector Service.

WinRM Configuration with Active Directory Group Policy:

In cases where many computers need to be configured, or in cases where the target log source is a domain controller, it is necessary to enable WinRM via GPO.

To configure unsecured communication using a GPO:

1. Open the Group Policy Management Console on the domain controller, click **Start > Administrative Tools > Group Policy Management.** In the left hand tree, browse to the Group Policy Objects folder for your domain.
2. Right click on the **Default Domain Controller Policy** and click edit. If you create a new GPO please ensure Authenticated Users and the user name you will be using for pulling the logs are added to User, Groups and Computers the GPO applies to.



Default Domain Controllers Policy

Links

Display links in this location: ECAT.local

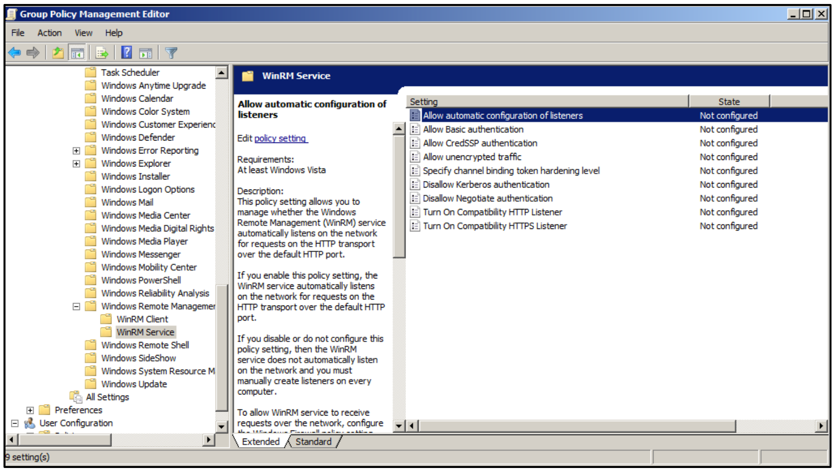
The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
Domain Controllers	No	Yes	ECAT.local/Domain C

can only apply to the following groups, users, and computers:

e following WMI filter:

a. Expand **Computer Configuration > Policies > Administrative Tempates > Windows Components > Windows Remote Management (WinRM),** and click **WinRM Service.**



Allow automatic configuration of listeners

Edit policy setting

Requirements:
At least Windows Vista

Description:
This policy setting allows you to manage whether the Windows Remote Management (WinRM) service automatically listens on the network for requests on the HTTP transport over the default HTTP port.

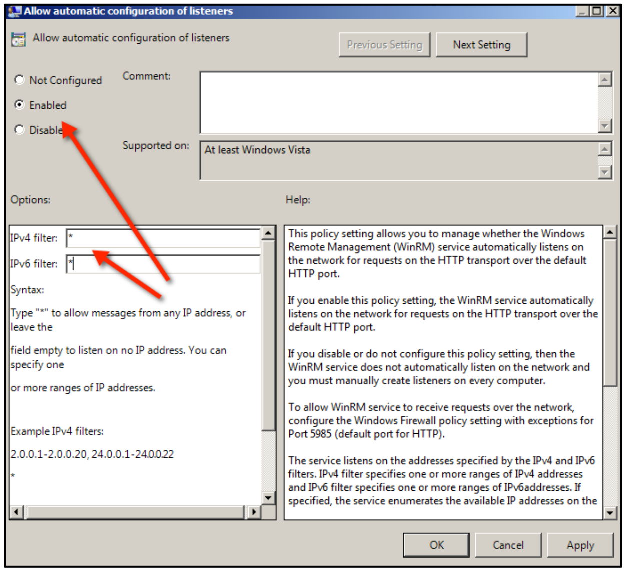
If you enable this policy setting, the WinRM service automatically listens on the network for requests on the HTTP transport over the default HTTP port.

If you disable or do not configure this policy setting, then the WinRM service does not automatically listen on the network and you must manually create listeners on every computer.

To allow WinRM service to receive requests over the network, configure

Setting	State
Allow automatic configuration of listeners	Not configured
Allow Basic authentication	Not configured
Allow CredSSP authentication	Not configured
Allow unencrypted traffic	Not configured
Specify channel binding token hardening level	Not configured
Disallow Kerberos authentication	Not configured
Disallow Negotiate authentication	Not configured
Turn On Compatibility HTTP Listener	Not configured
Turn On Compatibility HTTPS Listener	Not configured

b. In the right-hand pane, double-click **Allow automatic configuration for listeners** to open the Properties dialog box. Select **Enabled**, and in both **IPv4** filters and **IPv6** filter fields type * to allow for listener service on all interfaces.



Allow automatic configuration of listeners

Allow automatic configuration of listeners

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

IPv4 filter: *

IPv6 filter: *

Syntax:

Type "*" to allow messages from any IP address, or leave the

field empty to listen on no IP address. You can specify one

or more ranges of IP addresses.

Example IPv4 filters:

2.0.0.1-2.0.0.20, 24.0.0.1-24.0.0.22

*

Help:

This policy setting allows you to manage whether the Windows Remote Management (WinRM) service automatically listens on the network for requests on the HTTP transport over the default HTTP port.

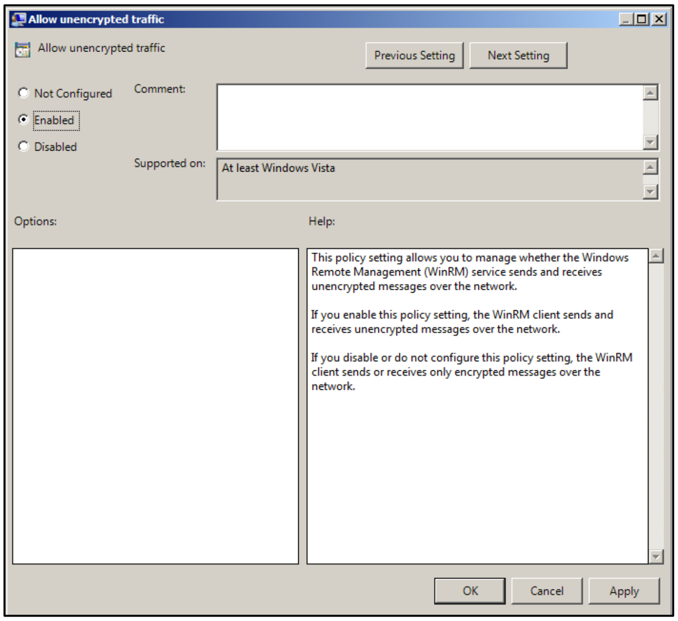
If you enable this policy setting, the WinRM service automatically listens on the network for requests on the HTTP transport over the default HTTP port.

If you disable or do not configure this policy setting, then the WinRM service does not automatically listen on the network and you must manually create listeners on every computer.

To allow WinRM service to receive requests over the network, configure the Windows Firewall policy setting with exceptions for Port 5985 (default port for HTTP).

The service listens on the addresses specified by the IPv4 and IPv6 filters. IPv4 filter specifies one or more ranges of IPv4 addresses and IPv6 filter specifies one or more ranges of IPv6addresses. If specified, the service enumerates the available IP addresses on the

c. Click **Next Setting** three times and in ***Allow unencrypted traffic*** properties dialog box ,select **Enabled then click** OK**.**



Allow unencrypted traffic

Allow unencrypted traffic

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

Help:

This policy setting allows you to manage whether the Windows Remote Management (WinRM) service sends and receives unencrypted messages over the network.

If you enable this policy setting, the WinRM client sends and receives unencrypted messages over the network.

If you disable or do not configure this policy setting, the WinRM client sends or receives only encrypted messages over the network.

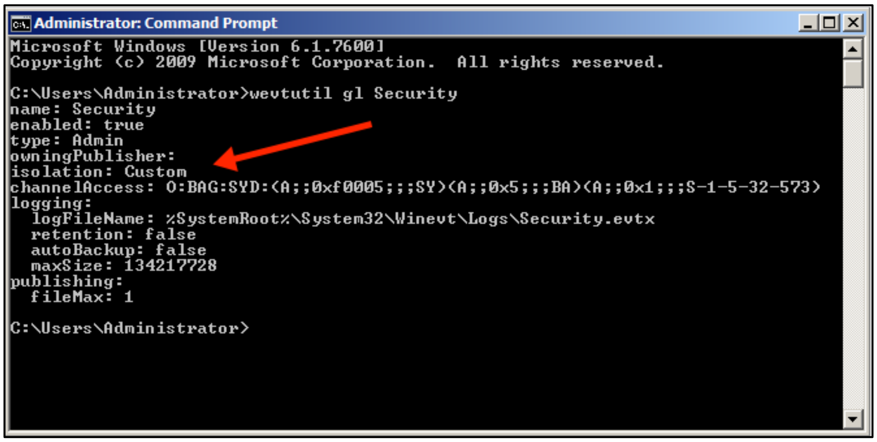
3. To allow WinRM service access to the Security log channel, follow these steps:

Note: The WinRM service requires explicit access to read events from the Security log channel. Access to Windows log channels are controlled using Security Descriptor Definition Language (SDDL) strings. For the WinRM service to gain read access, you must append the string **(A;;0x1;;;s-1-5-20)** to the existing SDDL strings for the Security channel.

a. Without closing the Group Policy Management Editor window, click **Start > Run** and type **cmd**.

b. Right click **cmd** in the search list and select ***Run as Admininstrator***. Elevated privileges are required when running the following commands.

c. To obtain the existing SDDL string from the domain controller, type: **wevtutil gl Security**

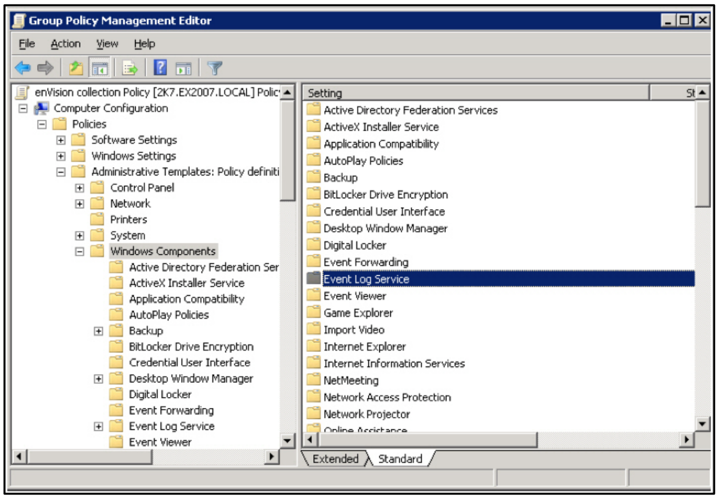


```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>wevtutil gl Security
name: Security
enabled: true
type: Admin
owningPublisher:
isolation: Custom
channelAccess: O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)
logging:
  logFileName: %SystemRoot%\System32\Winevt\Logs\Security.evtx
  retention: false
  autoBackup: false
  maxSize: 134217728
publishing:
  fileMax: 1

C:\Users\Administrator>
```

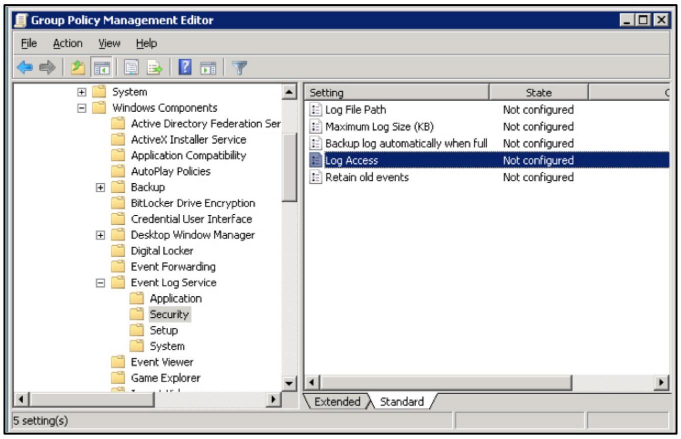
d. Copy the **channelAccess** string to the clipboard

e. In the Group Policy Management Editor, expand **Computer Configuration > Policies > Administrative Templates > Windows Component**

f. In the right-hand pane, double-click **Event Log Source**.



g. In the left-hand pane, expand **Security** in the right-hand pane double-click **Log Access**

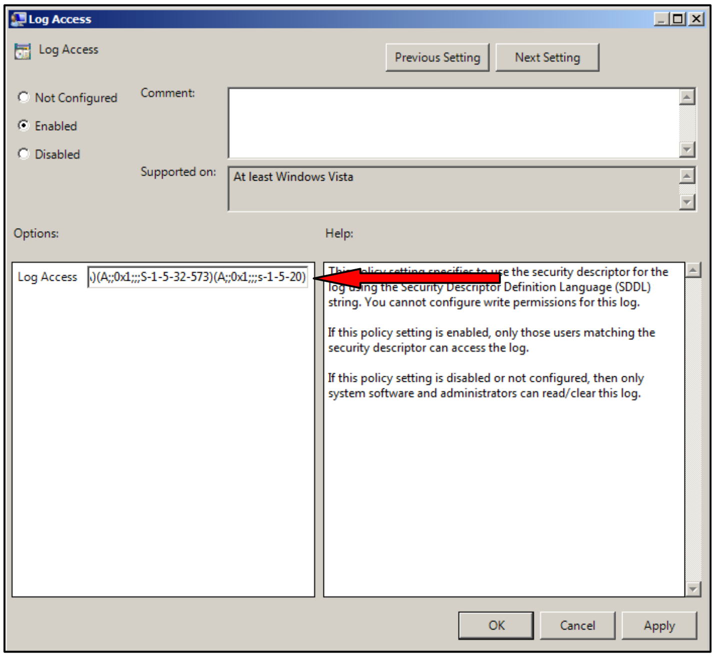


- System
- Windows Components
  - Active Directory Federation Ser
  - ActiveX Installer Service
  - Application Compatibility
  - AutoPlay Policies
  - Backup
  - BitLocker Drive Encryption
  - Credential User Interface
  - Desktop Window Manager
  - Digital Locker
  - Event Forwarding
  - Event Log Service
    - Application
    - Security
    - Setup
    - System
  - Event Viewer
  - Game Explorer

Setting	State
Log File Path	Not configured
Maximum Log Size (KB)	Not configured
Backup log automatically when full	Not configured
Log Access	Not configured
Retain old events	Not configured

5 setting(s)

h. Select **Enabled** and in the **Log Access** field paste the security SDDL string that you copied previously and append the following string: **(A;;0x1;;;S-1-5-20). Click** OK **to continue.**



○ Not Configured

● Enabled

○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

Log Access `)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;s-1-5-20)`

Help:

This policy setting specifies to use the security descriptor for the log using the Security Descriptor Definition Language (SDDL) string. You cannot configure write permissions for this log.

If this policy setting is enabled, only those users matching the security descriptor can access the log.

If this policy setting is disabled or not configured, then only system software and administrators can read/clear this log.

Note: By appending the string to the existing SDDL string, you gain read access to the Security log channel, and avoid overwriting your existing settings.

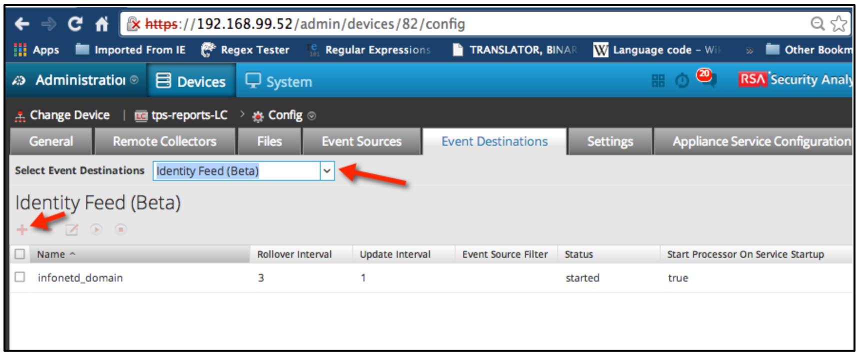
Once all options are enabled, execute the following command to update the group policy on the target computers:
C:\> gpupdate /force

Environment Credentials:

An account with administrative group membership is required, such as Domain Admins. It is possible to set up a non administrator member with rights to view the event security logs. These steps and are outside the scope of this document.

Configuring Identity

1. Go to the **Event Destinations** Tab. Select "***Identity Feed (Beta)***" from the **Select Event Destinations** box.

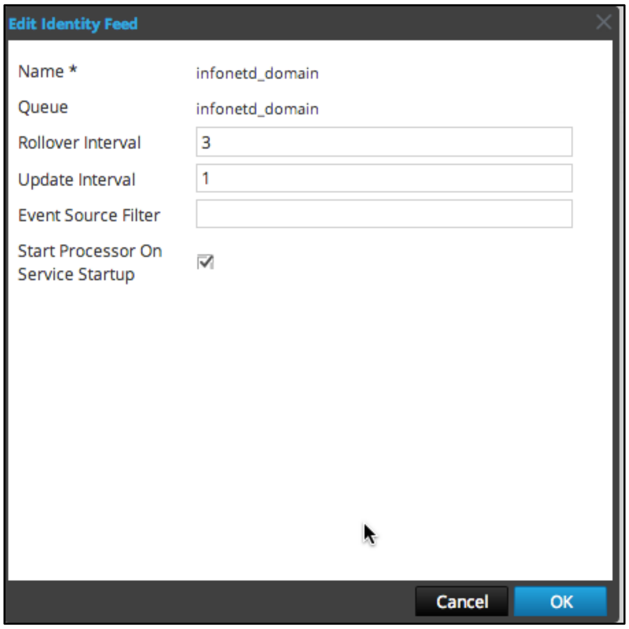


Select Event Destinations: Identity Feed (Beta)

Identity Feed (Beta)

□	Name	Rollover Interval	Update Interval	Event Source Filter	Status	Start Processor On Service Startup
□	infonetd_domain	3	1		started	true

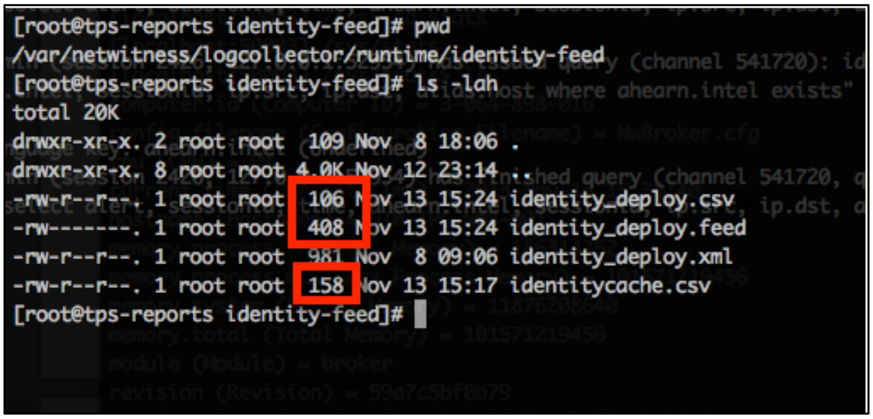
2. Click the red "**+**" sign and enter a unique name for the feed. The Queue name is to identify the feed within the log collector. Simply use the name of the feed for the Queue.



Name *	infonetd_domain
Queue	infonetd_domain
Rollover Interval	3
Update Interval	1
Event Source Filter	
Start Processor On Service Startup	☑

3. Have users log into Windows boxes on the domain to generate the appropriate log messages on the domain controllers for testing.

4. Verify that data is written to the feed files. SSH to the Log Decoder/Collector or Virtual Log Collector being configured. Navigate to /var/netwitness/logcollector/runtime/identity-feed and verify that the Identity_deploy files are getting populated with data.



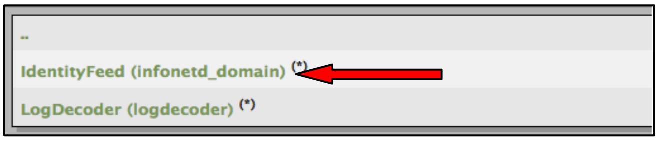
```
[root@tps-reports identity-feed]# pwd
/var/netwitness/logcollector/runtime/identity-feed
[root@tps-reports identity-feed]# ls -lah
total 20K
drwxr-xr-x. 2 root root  109 Nov  8 18:06 .
drwxr-xr-x. 8 root root 4.0K Nov 12 23:14 ..
-rw-r--r--. 1 root root  106 Nov 13 15:24 identity_deploy.csv
-rw-------. 1 root root  408 Nov 13 15:24 identity_deploy.feed
-rw-r--r--. 1 root root  981 Nov  8 09:06 identity_deploy.xml
-rw-r--r--. 1 root root  158 Nov 13 15:17 identitycache.csv
[root@tps-reports identity-feed]#
```

5. Open up a web browser (Non-Internet Explore browsers preferred) and log in to the REST interface of the Log Collector. Use administrative credentials when logging in. The default admin password is netwitness.

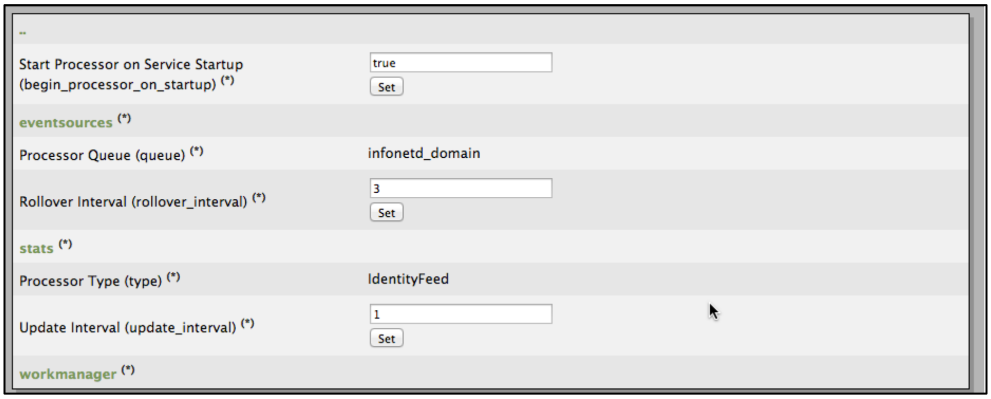
   Example:
   (SSL Not Enabled)
   http://192.168.99.66:50101/event-processors

   (SSL Enabled)
   https://192.168.99.65:50101/event-processors

6. Click IdentityFeed. The identity feed name created previously will appear in parentheses. Make a note of the URL.



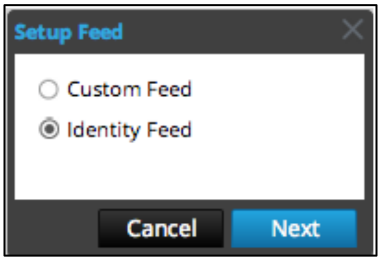
..
IdentityFeed (infonetd_domain) (*)
LogDecoder (logdecoder) (*)



..	
Start Processor on Service Startup (begin_processor_on_startup) (*)	true Set
eventsources (*)	
Processor Queue (queue) (*)	infonetd_domain
Rollover Interval (rollover_interval) (*)	3 Set
stats (*)	
Processor Type (type) (*)	IdentityFeed
Update Interval (update_interval) (*)	1 Set
workmanager (*)	

7. Open up Security Analytics and navigate to Live → Feeds

8. Create a new feed and choose Identity feed, then click **Next**



Setup Feed

○ Custom Feed

● Identity Feed

9. Name the feed, no special characters or spaces allowed.

10. In the URL field enter the url from the REST step above then append the following to the URL.

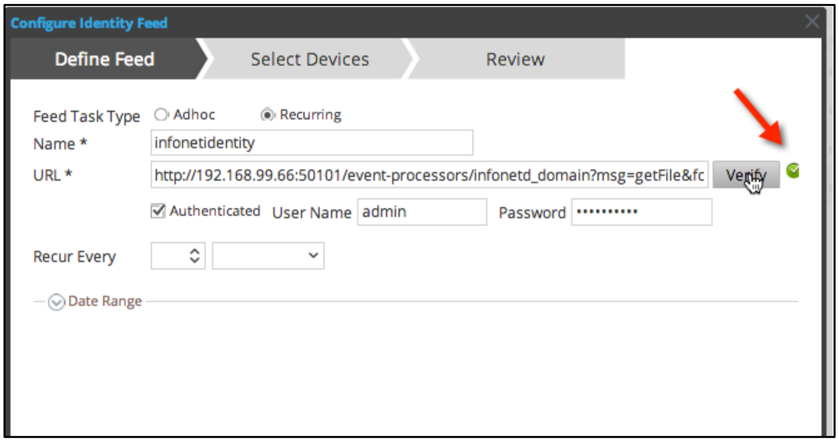
    ?msg=getFile&force-content-type=application/octet-stream&expiry=600

    The complete example URL should be: *http://192.168.99.66:50101/event-processors/infonetd_domain?msg=getFile&force-content-type=application/octet-stream&expiry=600*

    NOTE: *Replace the IP address in the example above with the CN name from the SSL certificate when using SSL.*

11. Check the **Authenticated** box and provide the credentials used to access the REST interface previously.

12. Click the verify button and look for the green checkmark next to the end of the URL box. If the identity feed source, the Log Collector, uses SSL please see the **Importing SSL Certificate** section.



Configure Identity Feed

Define Feed | Select Devices | Review

Feed Task Type ○ Adhoc ● Recurring

Name * infonetidentity

URL * http://192.168.99.66:50101/event-processors/infonetd_domain?msg=getFile&fc

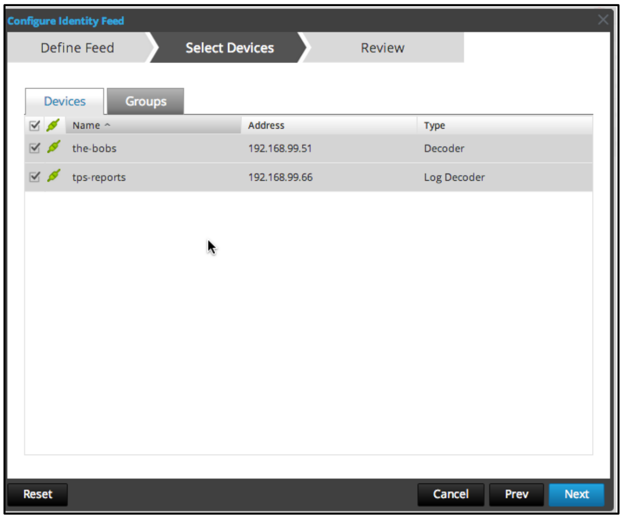
☑ Authenticated User Name admin Password ••••••••••

Recur Every

Date Range

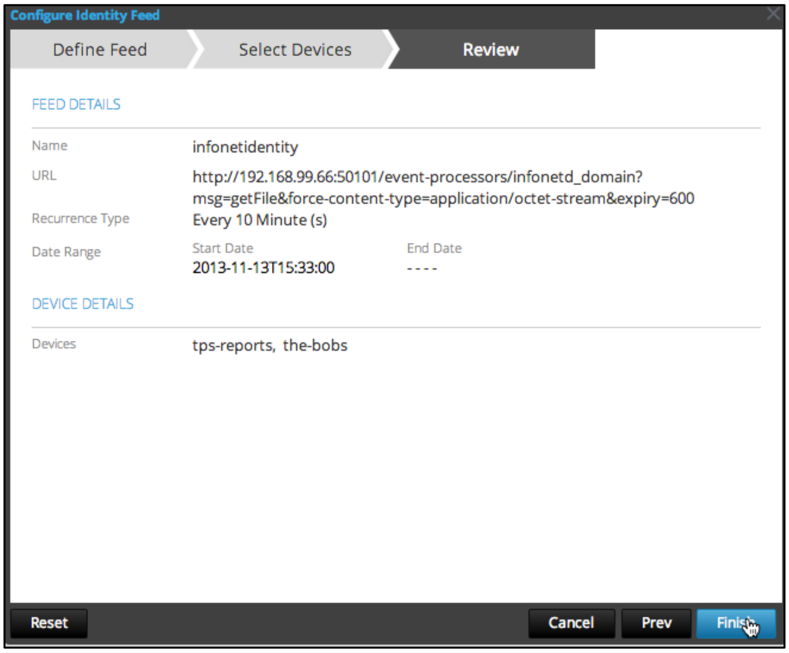
13. Once verified, configure the interval this feed will use for deployment. For this feed to work properly, all feeds will be forced to reload on the decoders. In production environments consider setting this to 30 minutes or more. Click **Next** to continue.

14. Select the Devices that this feed should be deployed to (typically all decoders). Click Next



	Name ^	Address	Type
☑	the-bobs	192.168.99.51	Decoder
☑	tps-reports	192.168.99.66	Log Decoder

15. Lastly, review it and click **Finish**



FEED DETAILS

Name infonetidentity

URL http://192.168.99.66:50101/event-processors/infonetd_domain?msg=getFile&force-content-type=application/octet-stream&expiry=600

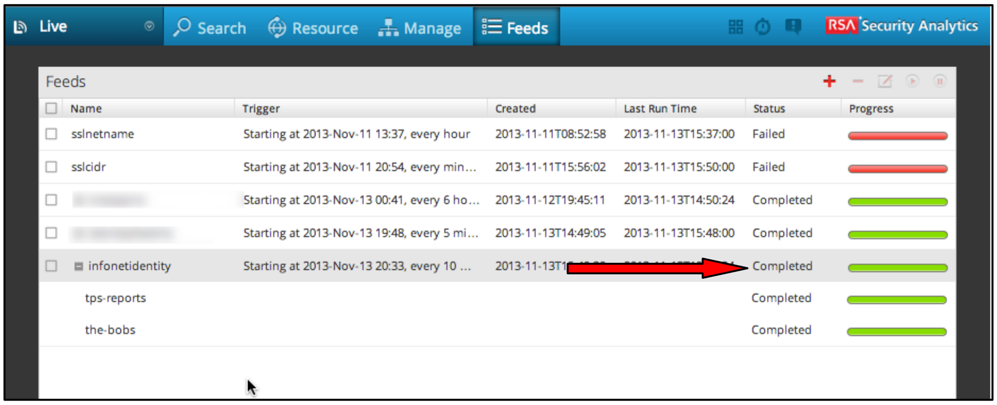
Recurrence Type Every 10 Minute (s)

Date Range Start Date 2013-11-13T15:33:00 End Date ----

DEVICE DETAILS

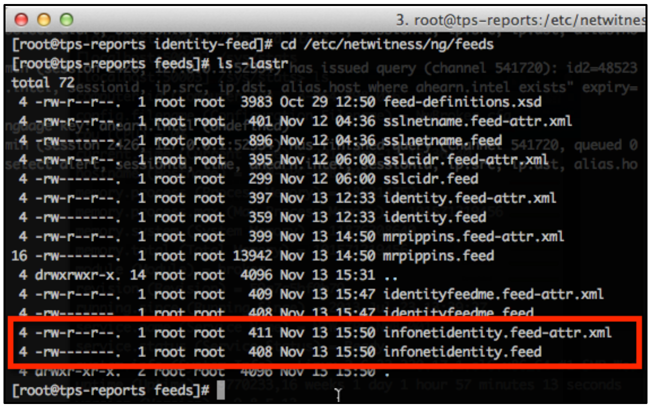
Devices tps-reports, the-bobs

16. The Progress bar will show the status of the deployment. It may be required to refresh the page before the status will change from Running to Completed/Failed.



□	Name	Trigger	Created	Last Run Time	Status	Progress
□	sslnetname	Starting at 2013-Nov-11 13:37, every hour	2013-11-11T08:52:58	2013-11-13T15:37:00	Failed	🟥
□	sslcidr	Starting at 2013-Nov-11 20:54, every min…	2013-11-11T15:56:02	2013-11-13T15:50:00	Failed	🟥
□	[redacted]	Starting at 2013-Nov-13 00:41, every 6 ho…	2013-11-12T19:45:11	2013-11-13T14:50:24	Completed	🟩
□	[redacted]	Starting at 2013-Nov-13 19:48, every 5 mi…	2013-11-13T14:49:05	2013-11-13T15:48:00	Completed	🟩
□	⊟ infonetidentity	Starting at 2013-Nov-13 20:33, every 10 …	2013-11-13T1		Completed	🟩
	tps-reports				Completed	🟩
	the-bobs				Completed	🟩

17. To verify the feed was deployed, SSH into the decoder's feed directory, */etc/netwitness/ng/feeds*, and checking for the identityfeed file.



```
[root@tps-reports identity-feed]# cd /etc/netwitness/ng/feeds
[root@tps-reports feeds]# ls -lastr
total 72
 4 -rw-r--r--.  1 root root  3983 Oct 29 12:50 feed-definitions.xsd
 4 -rw-r--r--.  1 root root   401 Nov 12 04:36 sslnetname.feed-attr.xml
 4 -rw-------.  1 root root   896 Nov 12 04:36 sslnetname.feed
 4 -rw-r--r--.  1 root root   395 Nov 12 06:00 sslcidr.feed-attr.xml
 4 -rw-------.  1 root root   299 Nov 12 06:00 sslcidr.feed
 4 -rw-r--r--.  1 root root   397 Nov 13 12:33 identity.feed-attr.xml
 4 -rw-------.  1 root root   359 Nov 13 12:33 identity.feed
 4 -rw-r--r--.  1 root root   399 Nov 13 14:50 mrpippins.feed-attr.xml
16 -rw-------.  1 root root 13942 Nov 13 14:50 mrpippins.feed
 4 drwxrwxr-x. 14 root root  4096 Nov 13 15:31 ..
 4 -rw-r--r--.  1 root root   409 Nov 13 15:47 identityfeedme.feed-attr.xml
 4 -rw-------.  1 root root   408 Nov 13 15:47 identityfeedme.feed
 4 -rw-r--r--.  1 root root   411 Nov 13 15:50 infonetidentity.feed-attr.xml
 4 -rw-------.  1 root root   408 Nov 13 15:50 infonetidentity.feed
 4 drwxr-xr-x.  2 root root  4096 Nov 13 15:50 .
[root@tps-reports feeds]#
```

Importing SSL Certificate

If SSL is configured on the Identity feed's Log Collector, follow these steps to import the Log Collector's SSL certificate into the Security Analytics UI server key store. If this certificate is not imported, the Security Analytics UI server will be unable to pull the Identify feed file from the Log Collector.

1. To pull the SSL certificate off the log collector, SSH into the Security Analytics UI server and run the following.
   echo -n | openssl s_client -connect ***<HOST>****:****<PORT>*** *| sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > /tmp****/<SERVERNAME>****.cert*

   Example:

   ```
   echo -n | openssl s_client -connect 192.168.99.66:50101 | sed -ne
   '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' >
   /tmp/logcollector.cert
   ```

2. The above command saves the SSL certificate to /tmp/<SERVERNAME>.cert

3. To import SSL certificate into the Security Analytics UI server, while SSHed into the UI server perform the following.
   keytool -importcert -alias ***<name an alias for the cert>*** *-file* ***<the cert file pathname>*** *-keystore /etc/pki/java/cacerts*

   Example:

   ```
   keytool -importcert -alias logcollector01 -file
   /tmp/logcollector.cert  -keystore /etc/pki/java/cacerts
   ```

4. A password will be requested. This password is for the keystore on the Security Analytics UI server, this is not the jetty keystore. The default password is ***changeit***.

5. Restart jettysrv to allow jetty to read the new certificate in the store.

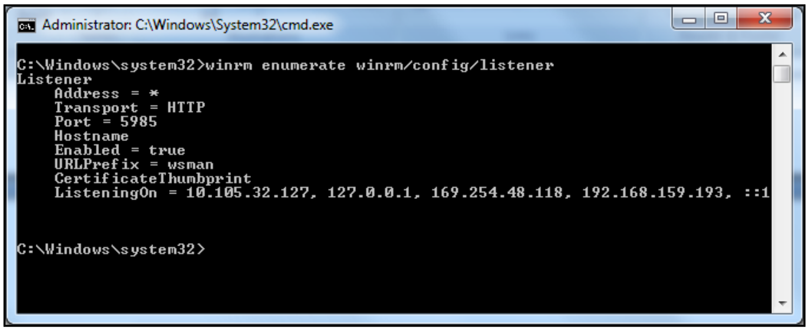
Troubleshooting

Not Pulling Logs from Event Source

1. Check to make sure the Log Collector service is running properly.

2. Check that the Windows account has the correct password and administrative permissions for the event source.

3. Determine that the event source has the proper WinRM settings.
   Open an elevated command prompt on the event source and run the following.
   winrm enumerate winrm/config/listener

   ```
   C:\Windows\system32>winrm enumerate winrm/config/listener
   Listener
       Address = *
       Transport = HTTP
       Port = 5985
       Hostname
       Enabled = true
       URLPrefix = wsman
       CertificateThumbprint
       ListeningOn = 10.105.32.127, 127.0.0.1, 169.254.48.118, 192.168.159.193, ::1


   C:\Windows\system32>
   ```

4. If still having issues add the Log Collector’s IP address as a trusted host within WinRM

Identity Feed URL Will Not Verify

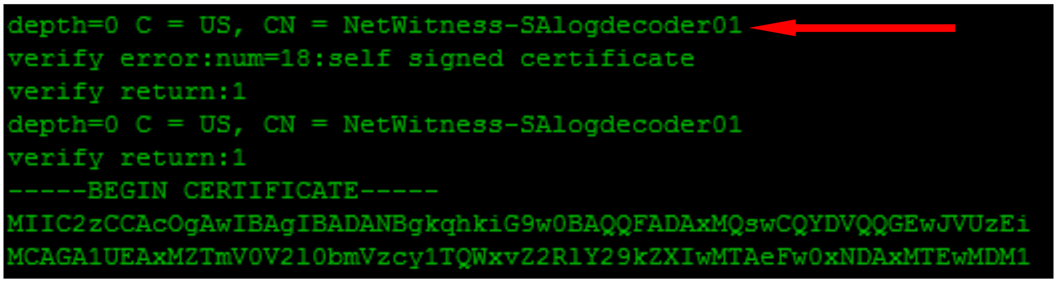
If the Identity feed url will not verify and SSL is being used. Make sure the section for Importing SSL Certificate was followed. If there are still issues it is possible that the internal name of the certificate does not match the hostname of the log collector.

1. SSH in to the Security Analytics UI server

2. Run the following to output the CN name of the SSL cert.

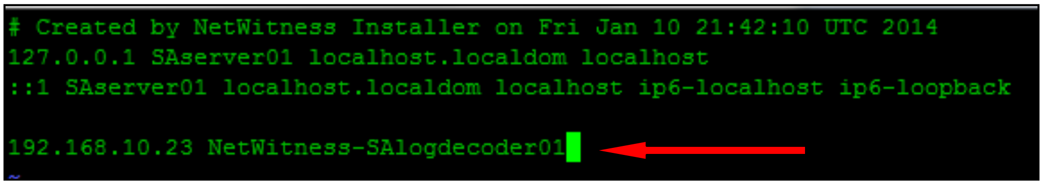
   ```
   echo -n | openssl s_client -connect <log decoder>:50101 | sed -ne '/BEGIN
   CERTIFICATE-/,/-END CERTIFICATE-/p'

   Example:
   echo -n | openssl s_client -connect salogdecoder01:50101 | sed -ne '/BEGIN
   CERTIFICATE-/,/-END CERTIFICATE-/p'
   ```

3. Retrieve the CN name of the SSL Certificate.



```
depth=0 C = US, CN = NetWitness-SAlogdecoder01
verify error:num=18:self signed certificate
verify return:1
depth=0 C = US, CN = NetWitness-SAlogdecoder01
verify return:1
-----BEGIN CERTIFICATE-----
MIIC2zCCAcOgAwIBAgIBADANBgkqhkiG9w0BAQQFADAxMQswCQYDVQQGEwJVUzEi
MCAGA1UEAxMZTmV0V2l0bmVzcy1TQWxvZ2RlY29kZXIwMTAeFw0xNDAxMTEwMDM1
```

4. Edit the /etc/hosts file and add the IP address and CN name to the file



```
# Created by NetWitness Installer on Fri Jan 10 21:42:10 UTC 2014
127.0.0.1 SAserver01 localhost.localdom localhost
::1 SAserver01 localhost.localdom localhost ip6-localhost ip6-loopback

192.168.10.23 NetWitness-SAlogdecoder01
```

5. Restart the network service on the appliance

   # service network restart

6. Confirm that the name placed in the /etc/hosts file is used instead of the FQDN or IP address in the Identity feed URL.

7. Re-verify the Identity feed URL