RSA NetWitness Logs

Event Source Log Configuration Guide

VMware vCenter Server

Last Modified: Thursday, November 30, 2017

Event Source Product Information:

Vendor: VMware
Event Source: VirtualCenter Server, vCenter Server
Versions:

- vCenter Server: 4.1, 5.0, 5.1, 5.5, 6.x

> **Note:** RSA is qualifying support for the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case and we will add support for it.

- VirtualCenter Server: 2.0.2, 2.5

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Type: vmware_vc
Collection Method: VMware collection
Event Source Class.Subclass: Host.Virtualization

To configure VMware vCenter Server/VirtualCenter Server, perform the following tasks:

I. Configure the VMware event source

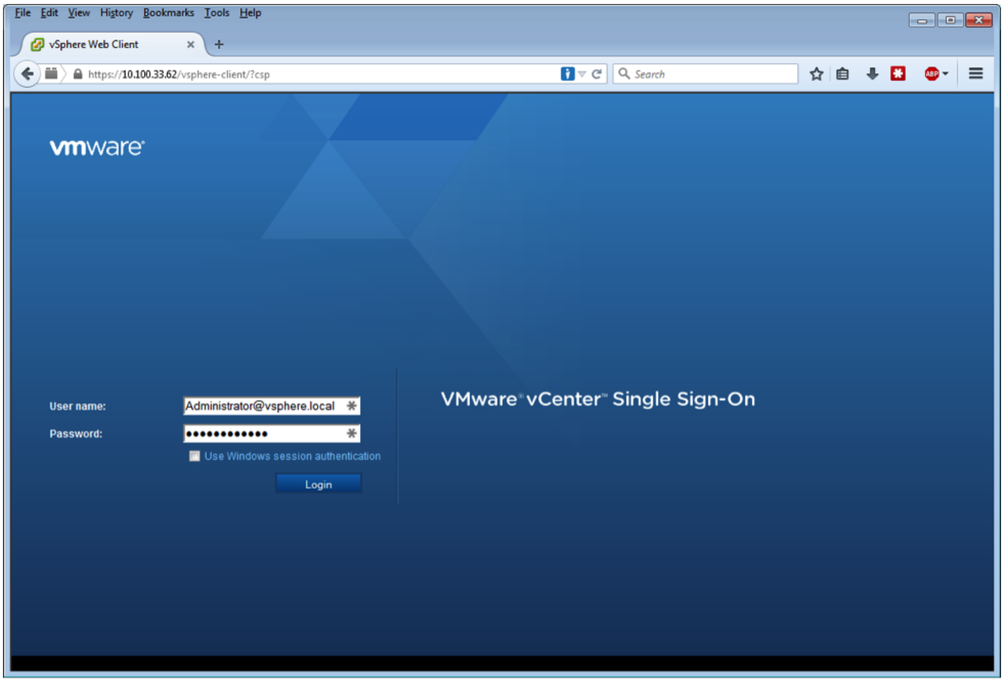
II. Configure the RSA NetWitness Suite Log Collector for VMware Collection

Configure the VMware vCenter Server or VirtualCenter Server

This section describes how to create a least privilege User to extract logs from a vCenter Server host. You first create the user, then you create a role, and finally, you assign the role to the user.

1. Create a user as follows:

   a. Log onto the Single Sign-On Server. A popular credential is **administrator@vsphere.local**.



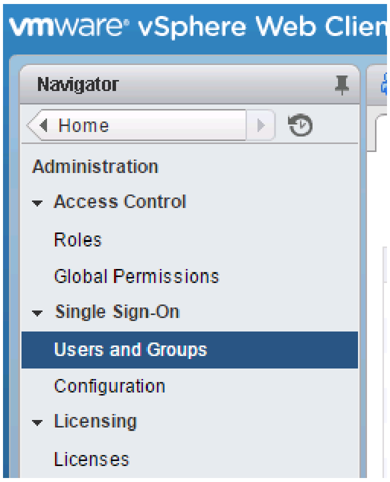
https://10.100.33.62/vsphere-client/?csp

User name: Administrator@vsphere.local

Password: ••••••••••••

File Edit View History Bookmarks Tools Help
vSphere Web Client
Search
vmware
VMware vCenter Single Sign-On
Use Windows session authentication
Login

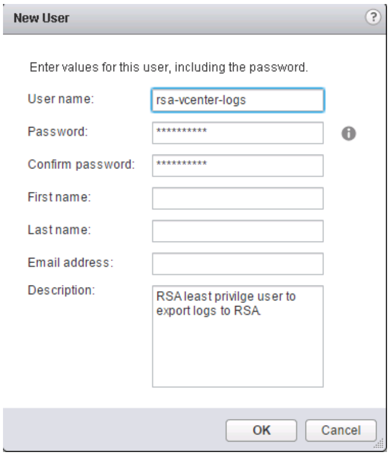
   b. Click on **Home** > **Administration** > **Users and Groups**.



c. On the **Users** tab, click + and add a user.

The New User dialog box is displayed.

d. Enter **rsa-vcenter-logs** as the user, and choose a strong password:


New User

Enter values for this user, including the password.

User name: rsa-vcenter-logs

Password: **********

Confirm password: **********

First name:

Last name:

Email address:

Description: RSA least privilge user to export logs to RSA

e. Click **OK** to add the user and close the dialog box.

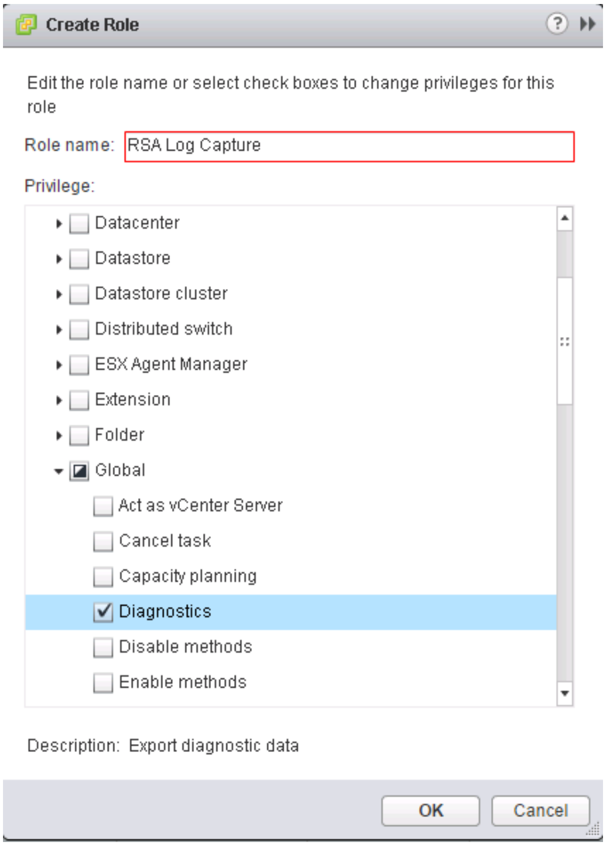
2. Create a role as follows:

a. From the Left navigation pane, under **Access Control**, select **Roles** and click + to create a new Role.

The Create Role dialog box is displayed.

b. Enter **RSA Log Capture** as the name of the Role.

c. Select **Global** > **Diagnostics** to assign the correct privileges.



Edit the role name or select check boxes to change privileges for this role

Role name: RSA Log Capture

Privilege:

- □ Datacenter
- □ Datastore
- □ Datastore cluster
- □ Distributed switch
- □ ESX Agent Manager
- □ Extension
- □ Folder
- ▪ Global
  - □ Act as vCenter Server
  - □ Cancel task
  - □ Capacity planning
  - ☑ Diagnostics
  - □ Disable methods
  - □ Enable methods

Description: Export diagnostic data

d. Click **OK**.

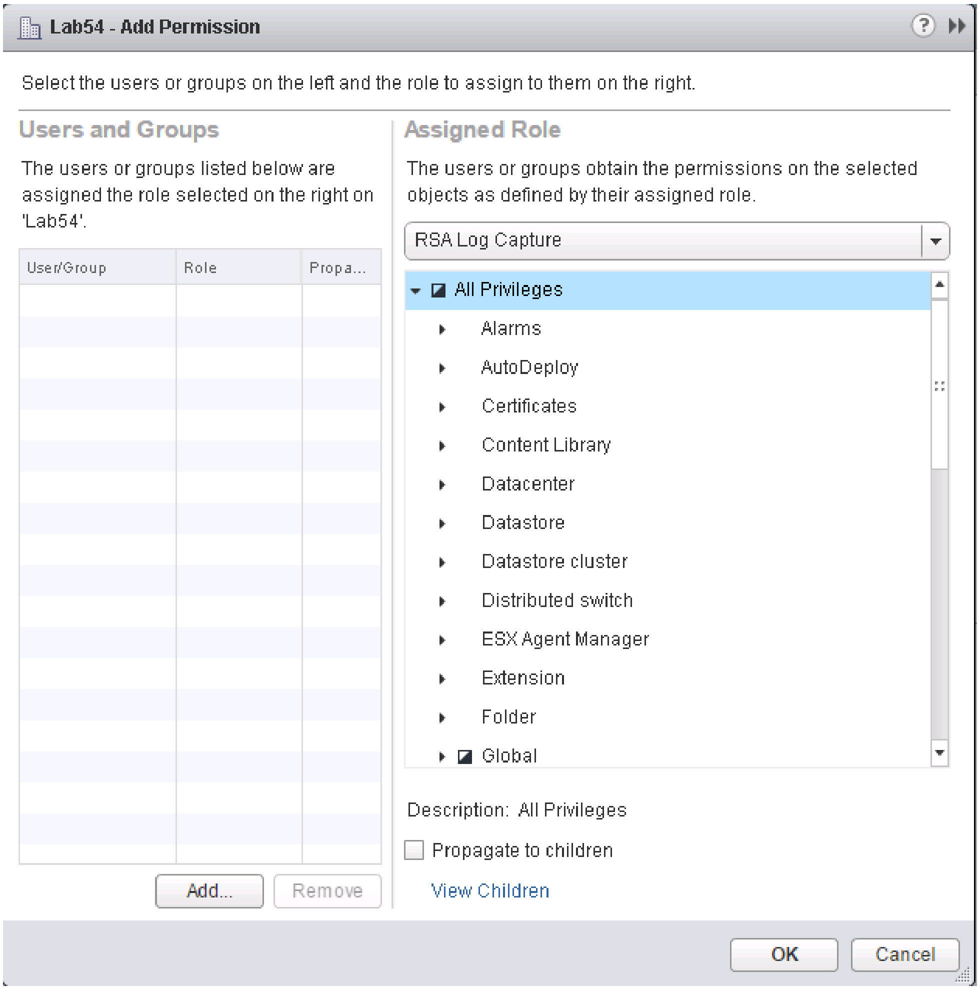
3. Assign a role to the user as follows:

   1. From the Left navigation pane, select **Home** > **Hosts and Clusters**.

   2. To add the user account to the VirtualCenter, right click the VirtualCenter Server in the VirtualCenter client, and select **Add Permission**.

      The Add Permission dialog box is displayed.

   3. From the **Assigned Role** section, select the **RSA Log Capture** role, and click **Add**.



Lab54 - Add Permission

Select the users or groups on the left and the role to assign to them on the right.

Users and Groups

The users or groups listed below are assigned the role selected on the right on 'Lab54'.

User/Group	Role	Propa...

Assigned Role

The users or groups obtain the permissions on the selected objects as defined by their assigned role.

RSA Log Capture

- ☒ All Privileges
  - Alarms
  - AutoDeploy
  - Certificates
  - Content Library
  - Datacenter
  - Datastore
  - Datastore cluster
  - Distributed switch
  - ESX Agent Manager
  - Extension
  - Folder
  - ☒ Global

Description: All Privileges

□ Propagate to children

View Children

4. To select the **rsa-vcenter-logs** user that you created, do one of the following:
   - If you created the user in the domain, select **Single Sign On** from the menu.
   - If you created the user locally on the VirtualCenter Server, select that system from the **Domain** drop-down menu.
5. Click **OK**.

This completes the process of adding a least privilege user. When you configure the Log Collector for VMware collection in RSA NetWitness Suite, make sure to enter the credentials for this user in the **Add Source** dialog box.

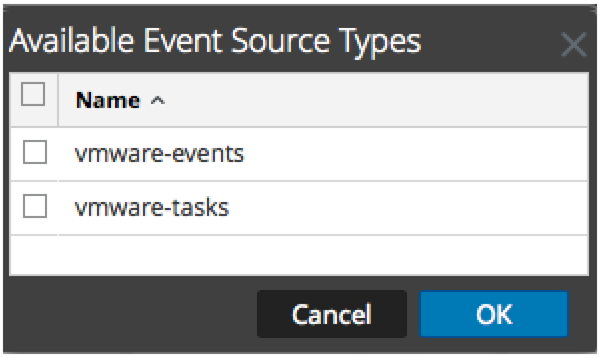
Configure the RSA NetWitness Log Collector for VMware Collection

Perform the following steps to configure the Log Collector for VMware collection.

Add the VMware Event Source Type:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the Services grid, select a Log Collector service.
3. Click ⚙ under **Actions** and select **View** > **Config**.
4. In the Log Collector **Event Sources** tab, select **VMware/Config** from the drop-down menu.

   The Event Categories panel displays the VMware event sources that are configured, if any.
5. Click + to open the **Available Event Source Types** dialog.

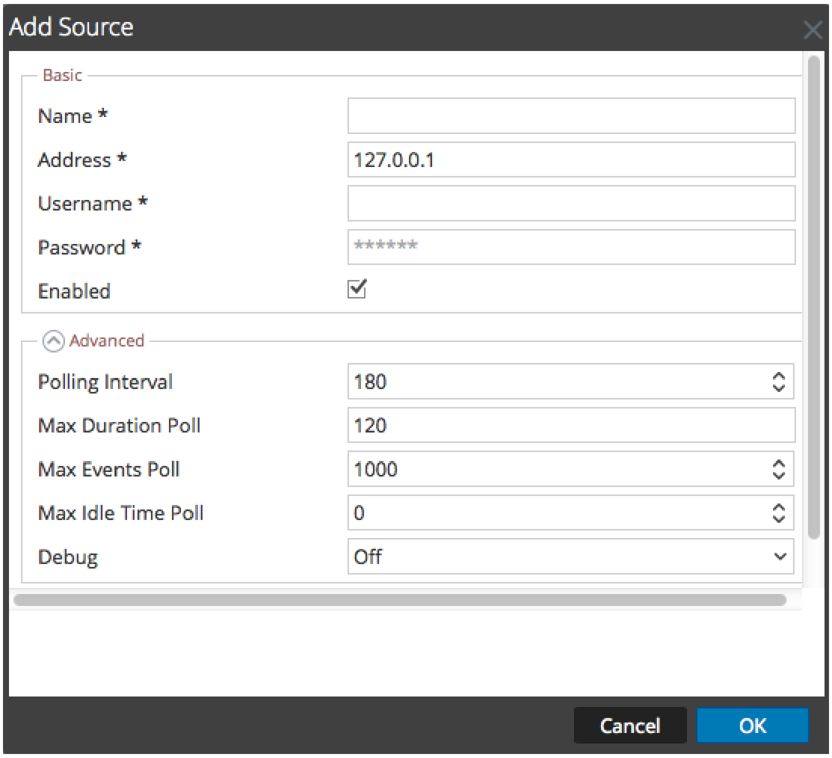
   

6. Select **vmware-events** or **vmware-tasks** from the Available Event Source Types dialog and click **OK**.

   The VMware available event source types are as follows:

   - **vmware-events:** Setup vmware-events to collect events from vCenter Servers and ESX/ESXi servers.
   - **vmware-tasks:** (Optional) Setup vmware-tasks to collect tasks from vCenter Servers.
7. Select the new type in the Event Categories panel, and click + in the Sources toolbar.
8. Add a Name, Username and Password, and modify any other parameters that require

changes.



Name *	
Address *	127.0.0.1
Username *	
Password *	******
Enabled	☑
Polling Interval	180
Max Duration Poll	120
Max Events Poll	1000
Max Idle Time Poll	0
Debug	Off

> **Caution:** If you need to enter the domain name as part of the Username, you must use a double-backslash as a separator. For example, if the domain|username is corp\smithj, you must specify **corp\\\\smithj**.

9. Click **OK** to save your changes.

Trademarks