RSA NetWitness Logs

Event Source Log Configuration Guide

VMware ESX/ESXi

Last Modified: Tuesday, November 7, 2017

Event Source Product Information:

Vendor: VMware
Event Source: ESX, ESXi, Embedded ESXi
Versions:

- ESX: 3.0.3, 3.5, 4.0, 4.1
- Embedded ESXi: 3.5, 4.0
- ESXi: 3.5, 4.0, 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.

RSA Product Information:

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

To configure VMware ESX/ESXi, perform the following tasks:

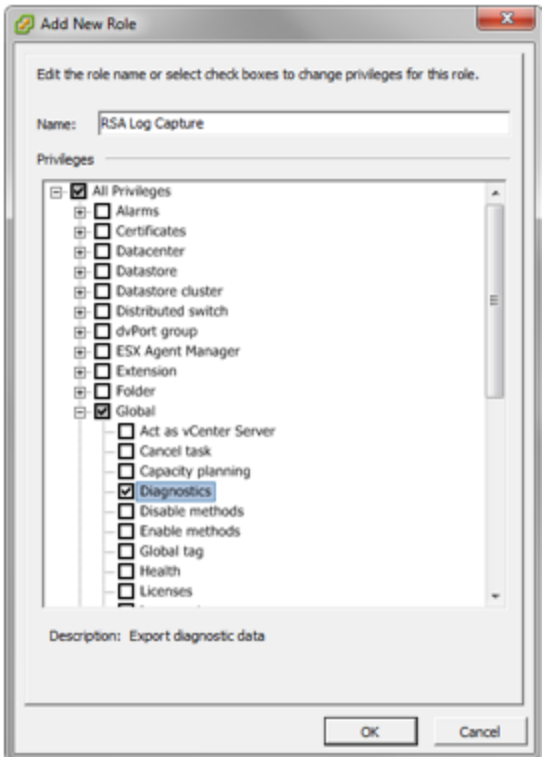
I. Configure the VMware event source

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

Configure the VMware ESX/ESXi Event Source

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

1. Create a role as follows:
   a. Log onto the ESXi host using the vSphere Client, with administrative privileges.
   b. Click on **Administration** > **Roles**.
   c. Click on **Add Role**.
   d. Enter **RSA Log Capture** as the name of the Role.
   e. Choose **All Privileges** > **Global** > **Diagnostics** as the only privilege for this role:

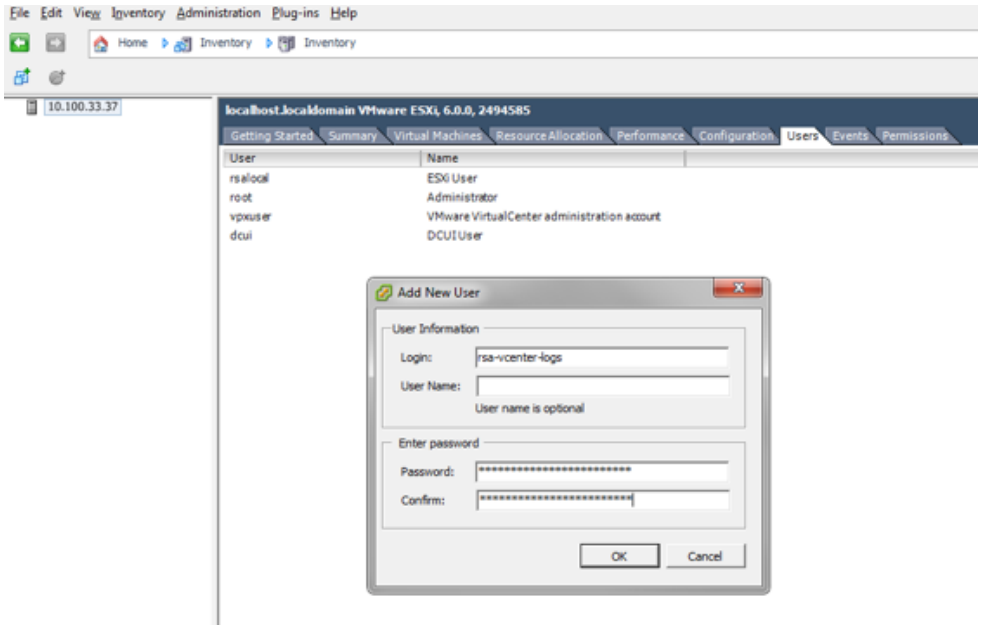


2. Create a local ESXi user as follows:

a. From the Left navigation pane, click on the ESXI host, then click the **Users** or **Local Users & Groups** tab. The name of the tab depends on the credentials you used to log onto the ESXi host.

b. Right click on the **Users** tab, then click **Add**.

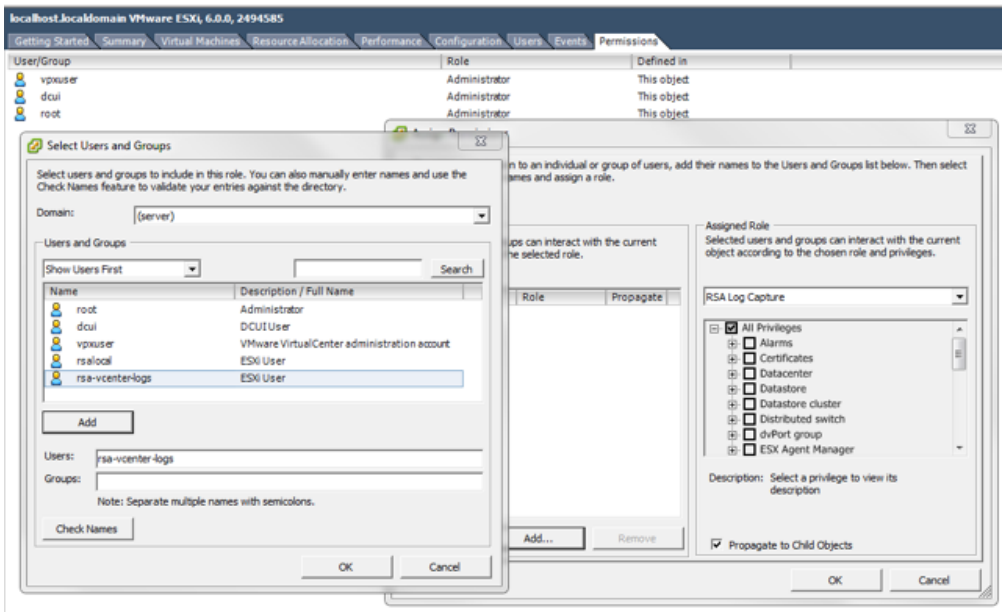
c. Enter **rsa-vcenter-logs** in the **Login** field, and choose a strong password:



3. Assign a role to the local user as follows:

   1. From the Left navigation pane, click on the ESXI host, then click the **Permissions** tab.
   2. Right click in the **Permissions** table, then click **Add Permission**.
   3. In the dialog box, under the **Assigned Role** drop-down menu, choose **RSA Log Capture**.
   4. Under **Users and Groups**, click **Add...**.

      The **Select Users and Groups** dialog box is displayed.
   5. In the dialog box, leave the Domain value as (server), and select the **rsa-vcenter-logs** user.



6. Click **Add**, then 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.

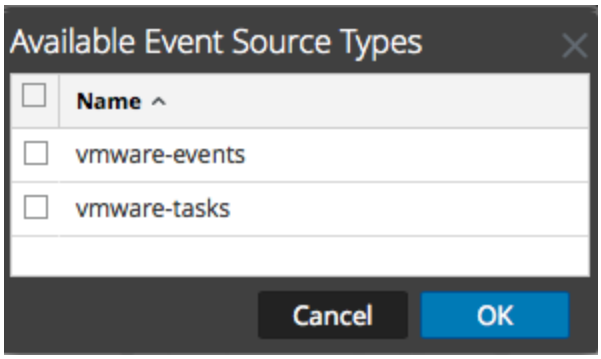
Configure the RSA NetWitness Log Collector for VMware Collection

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.

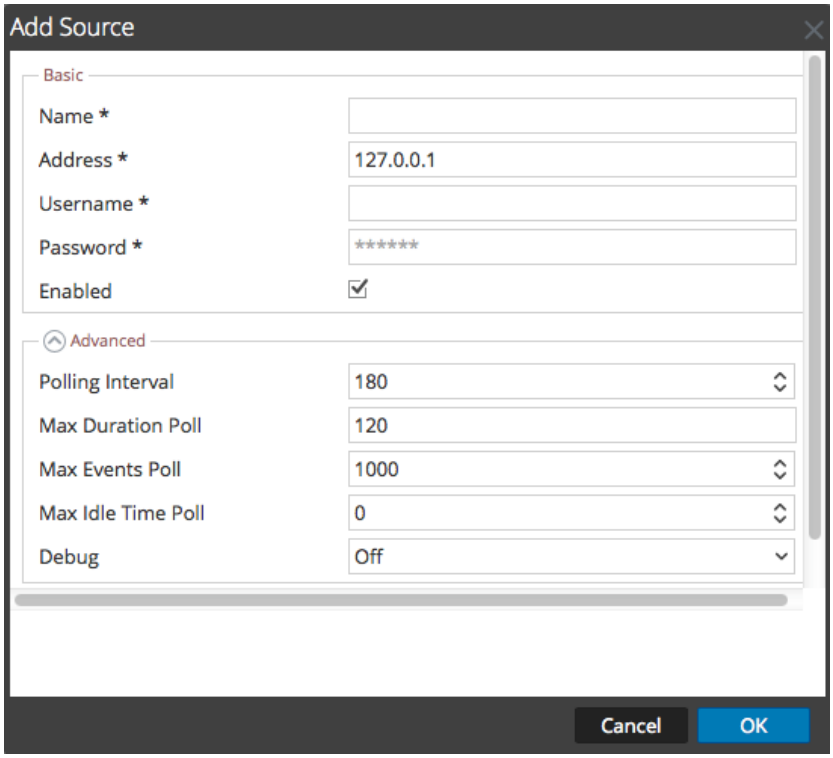


6. Select **vmware-events** or **vmware-tasks** from the Available Event Source Types dialog and click **OK**.

   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.



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