ThreatTap (Network Threat Detection) Setup and Configuration

Before you begin

In order to install the ThreatTap virtual appliance, you must have the following prerequisites:

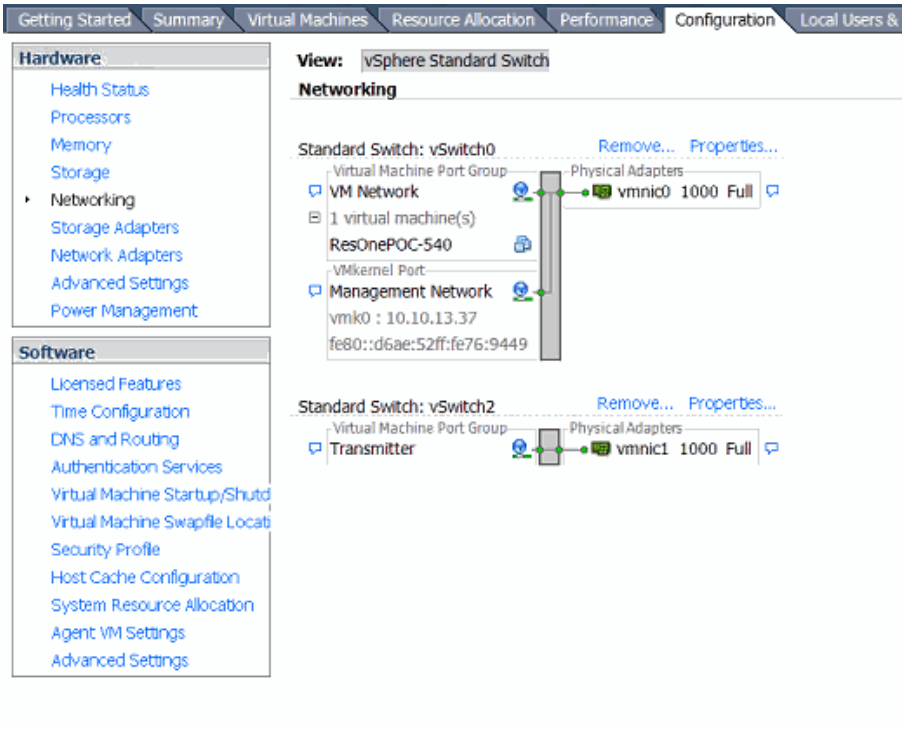
- A VM image of the ThreatTap Appliance. You can download the ThreatTap appliance or contact your AccessData sales rep to provide the image on media.
- A download of the OVF Template. You can obtain the template at the link above or through your sales rep.
- An active demo license for the ThreatTap Virtual appliance. Please contact your sales rep to obtain a virtual license key (dongle) for your ThreatTap 10 day demo at sales@accessdata.com.
- VMware ESXi server should be installed and configured with the correct datastores (Storage container for the VMware files). See hardware requirements above.

Creating a Network Collection SPAN/Mirror Port

To detect threats and potentially malicious activity, ThreatTap must be configured to connect to a SPAN port on your target network segment. The ThreatTap virtual appliance can analyze data on networks segments up to speeds of 1GBs. We suggest targeting a segment that has both internal and external network communication. The port, also known as a SPAN port or mirror port, allows you to collect and analyze network metadata.

To create a Collection Port

1. Physically connect to your **ESXi server** through the SPAN port on the switch. This is the connector port.
2. Connect to the **ESXi server** through the **vSphere client**.
3. Select the *Configuration* tab. The collector port should appear under the *Physical Adapters* heading in the main *Configuration* pane.



4. In the left column, click **Networking**.
5. At the top of the pane on the right side, click **Add Networking. . . .**
6. The *Add Network Wizard* window appears. **Virtual Machine** is selected as the default. Click **Next**.
7. Under the **Create a vSphere standard switch heading**, make sure that your collector port is selected. Click **Next**.
8. In the **Network Label field**, enter **Collector**. This changes the name of your collector port. Click **Next**.
9. Click **Finish**.

Editing Collector Properties

Once the collector port has been added, you need to edit the properties of both the vSwitch and Collector ports. By editing the properties of the Collector port, you ensure that the Collector port's properties mirror the properties in the vSwitch.

To edit the vSwitch port properties

1. In the Configuration tab, click *Properties* next to the virtual switch that you created named Collector.
2. In the *vSwitch1 Properties* window, select the vSwitch configuration. Click **Edit**.
3. Select the **Security** tab.
4. In the **Promiscuous Mode** dropdown, select **Accept**.
5. Click **OK**.

To edit the Collector port properties

1. In the Configuration tab, click *Properties* next to the virtual switch that you created named Collector.
2. In the *vSwitch1 Properties* window, select the Connector configuration. Click **Edit**.
3. Select the **Security** tab.
4. Check the box by **Accept** in the **Promiscuous Mode** dropdown.
5. Select the **Traffic Shaping** tab.
6. Click **OK**.
7. Check the box by **Disabled** in the **Status** dropdown.
8. Select the **NIC Teaming** tab.
9. Check the box by **Link Status only** in the **Network Fallover Detection** dropdown.
10. Click **Close**.

Editing Settings

Once the Collector has been attached and set up, you need to map the interface of the network adapter to the Collector.

To edit the settings

1. From the main window of the vSphere client, select your virtual machine (ThreatTap) and right click.
2. Select **Edit Settings**.
3. Select **Network adapter 2**. In the **Network label** dropdown under *Network Connection*, select **Collector**.

Deploying the OVF Template

Once the Collector is installed, you need to deploy the OVF template. You can find the template at the location with the VM ThreatTap.

To deploy the OVF Template

1. Log into the VMware vSphere client.
2. Go to **File > Deploy OVF Template**.

3. Browse to the location of the OVF Template on your hard drive. You should have previously downloaded the template before installation. Click **Next**.
4. In the *OVF Template Details* window, click **Next**.
5. In the *Name and Location* window, specify the name of the template. You will want to change the name of the file to avoid writing over the original template. Click **Next**.
6. In the *Storage* window, choose where to store the virtual machine files. Click **Next**.
7. In the *Disk Format* window, select **Thin Provision**. Click **Next**.
8. Select the VM Network to which to map the network. There are two networks listed in the Network Mapping window: VM Network and Collector Network. You should have previously created a destination network for the Collector network. See Creating a Network Collection SPAN/Mirror Port. Click **Next**.
9. In the *Ready to Complete* window, review the Deployment settings. Click **Back** to edit any of the deployment settings. Click **Finish** to finish the deployment.

Opening the VM Console

After configuring the virtual machine and deploying the OVF template, you need to open the console and license the product.

Opening the Console

To open the console

1. From the main window of the vSphere client, select your virtual machine (ThreatTap) and right click.
2. Select **Power > Power On**.
3. Right click the virtual machine and select **Open Console**. The virtual machine appears.
4. In the *Set Up Windows* window, click **Next**.
5. Enter your Windows product key. Click **Next**.
6. Accept the license terms and click **Start**.
7. After Windows has completed finalizing your settings, login as Administrator.
8. The system will request for you to change your password. Change the password for the Administrator account.

Creating a Local Virtual License CMStick (Dongle)

Once you have opened the virtual console, you need to activate your 10 day trial license of ThreatTap by creating a local Virtual CMStick. Before setting up a Virtual CMStick, you

need the confirmation code you should have requested from your sales representative detailed in the Before you Begin section

To create a local Virtual CMStick

1. Launch License Manager from the virtual desktop.
2. An error message appears, stating *No Security Device Found*. Because you are creating a virtual license, there is no need for a physical license dongle. Click **OK**.
3. Select **Create A Local Virtual CMStick**. Click **OK**.
4. Enter your confirmation code.
5. Click **OK**. AccessData License Manager automatically synchronizes with the License Server over the Internet.
6. Click **OK** when the update completes. License Manager creates the Virtual CMStick on your system.

After ThreatTap Setup and Configuration

After installing the virtual image, you can launch Resolution1 from the desktop and login to the console.

For instructions on use and function of the ThreatTap virtual appliance and network threat detection workflow, please see the ThreatTap User guide.