

Cloud Security at Scale with Trend Micro, Splunk and Chef

Launch and Learn

-
- » This Integrated stack is based on ARM template and intended for Microsoft Azure and Trend Micro customers and partners such as Solution Integrators (SI) partners and Cloud Solution Providers (CSP). This ARM template will help you launch a fully integrated stacks on Azure. The extensive automation and testing of these solutions will allow you to spin up pre-production environments with minimal manual steps and customization.



TABLE OF CONTENTS

TABLE OF CONTENTS.....	1
WHAT MAKES THIS INTEGRATED STACK?	3
<i>Deep Security Manager</i>	<i>3</i>
<i>Deep Security Agent.....</i>	<i>3</i>
<i>Splunk enterprise</i>	<i>3</i>
<i>Chef.....</i>	<i>3</i>
<i>Azure.....</i>	<i>3</i>
HOW TO BUILD THIS INTEGRATED STACK?.....	4
<i>Overview.....</i>	<i>4</i>
WHAT YOU WILL LEARN?	5
BEFORE WE START	6
<i>Tools and Information</i>	<i>6</i>
<i>Initial Steps</i>	<i>6</i>
DEPLOY STACK	9
<i>Overview.....</i>	<i>9</i>
<i>Launch Stack.....</i>	<i>10</i>
<i>Template Parameters</i>	<i>10</i>
<i>Protecting Azure Virtual Machine with Deep Security.....</i>	<i>12</i>
Trend Micro Azure Extension	12
Trend Micro Chef Cookbooks	12
<i>Add Protection to Test Azure Virtual Machines (Exercise)</i>	<i>12</i>
INTEGRATE	15
<i>Configure Trend Micro Deep Security For System event log forwarding (Exercise).....</i>	<i>15</i>
<i>Configure Trend Micro Deep Security For Security event log forwarding (Exercise)</i>	<i>15</i>
ANALYZE	17
<i>Generate Sample Events (Exercise)</i>	<i>17</i>
<i>Analyze Deep Security event data in Splunk's web console (Exercise)</i>	<i>18</i>
<i>Install Deep Security Agent to Test Azure Virtual Machine via Chef (Optional Exercise).....</i>	<i>21</i>

WHAT MAKES THIS INTEGRATED STACK?

The integrated stack consists of Trend Micro Deep Security platform, Splunk Enterprise and Chef automation platform.



DEEP SECURITY MANAGER This is the management component of the system and is responsible for sending rules and security settings to the Deep Security Agents. The DSM is controlled using the web-based management console. Using the console, the administrator can define security policies, manage deployed agents, query status of various managed instances, etc. The integration with Splunk is done using this interface and no additional component or software is required.

DEEP SECURITY AGENT This component provides all protection functionality. The nature of protection depends on the rules and security settings that each DSA receives from the Deep Security Manager.



SPLUNK ENTERPRISE The Splunk Enterprise on Azure is a high performance, scalable software server. It indexes and searches logs and other IT data in real time. Splunk works with data generated by any application, server or device. Deep Security will be integrated with Splunk to send security events to Splunk for further correlation and analytics using the Deep Security app for Splunk.



CHEF The Chef server is the highly scalable foundation of the Chef automation platform. The Chef Server integration with Chef Nodes (i.e. Azure VMs) is done using micro services, as a set of two Docker Containers for Node.js app and a database. This Chef platform can be used push Deep security agents to Azure Virtual Machine.



AZURE This integrated stack will be deployed on Azure using the provided ARM template.

HOW TO BUILD THIS INTEGRATED STACK?

OVERVIEW

This integrated stack is built using a JSON template, the template is based on Microsoft Azure Resource Manager (ARM) templates. Through, ARM templates, we can deploy topologies quickly, consistently with multiple services along with their dependencies. The figure below provides the overview of the end to end task required to completely build the stack. Each task is discussed in detail later in this document.

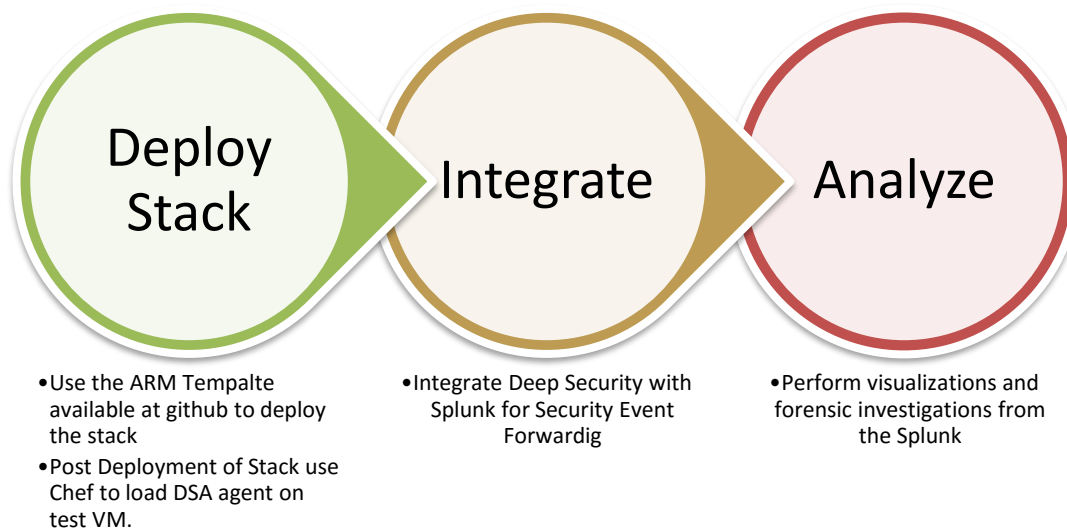


FIGURE 1 – HOW TO BUILD THIS INTEGRATED STACK?

WHAT YOU WILL LEARN?

In this launch and learn session, you will discover what makes an arm template and how this integrated stack was built. We will do a walk through of this fully automated stack as a way of managing security on existing as well as new cloud workloads with monitoring and continuous integration built in. In doing so, you will get a hands-on understanding of how Trend Micro's Deep Security Manager product can be integrated with various other cloud products to create a well-rounded cloud security solution. You will also learn how different components of this stack can be configured and how to add protection to the test Azure virtual machines that are provisioned as part of stack launch.

BEFORE WE START

Before we dive into the exercises, let's make sure that you have all of the tools and information that you will need.

TOOLS AND INFORMATION

To successfully complete some of the exercises in this launch and learn session, you will need the following:

- A reasonably up-to-date browser (IE 9+, Chrome, Firefox, Safari, etc.). You will use the browser to interact with the Deep Security Manager as well as with the Splunk web console.
- A username and password to access Azure Portal (<https://portal.azure.com>). These credentials are provided to you at the time of check-in to the session. For assistance please check with the session staff.
- Azure Resource Group Name that is created for you to deploy the stack.
- Trend Micro Deep Security and Splunk Web Console username and password provided to you.

INITIAL STEPS

- Launch a web browser of your choice and Go to <https://portal.azure.com>
- Log in with the lab Username and Password provided for you.
- Navigate the Azure Portal and select “All Resources” and then search for the **Resource Group** name that was provided to you that contains your stack deployment.
- Click on the Resource Group name that was given to you, for example “ignite”. Your resource group name will be different. For assistance please check with the session staff.

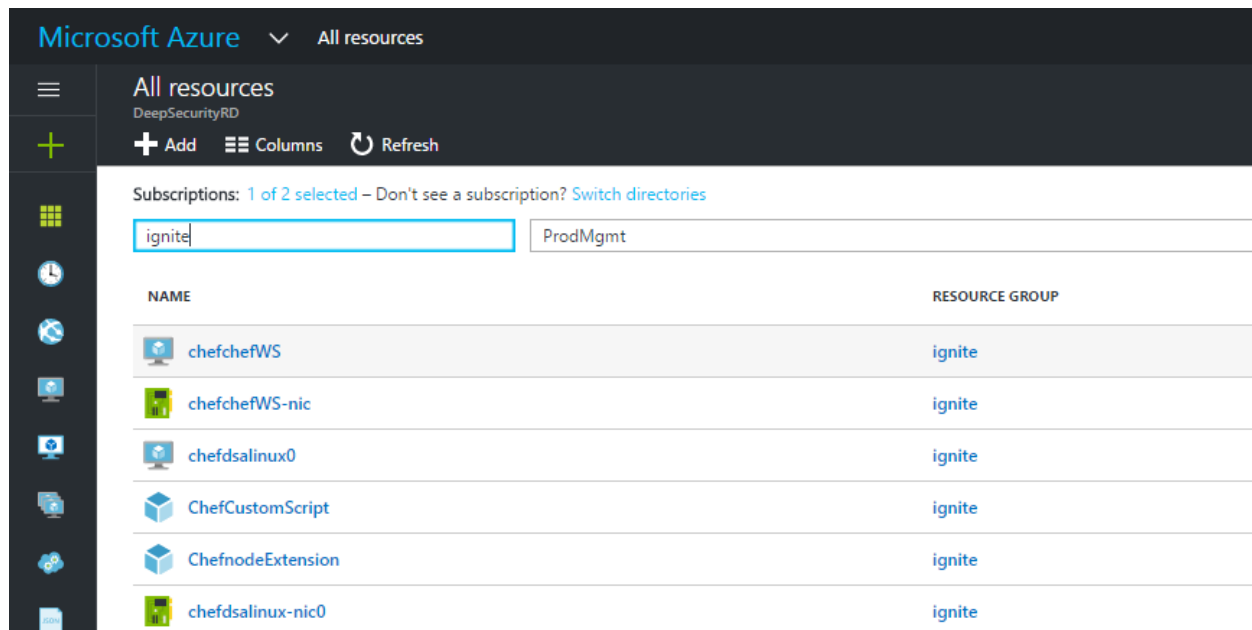
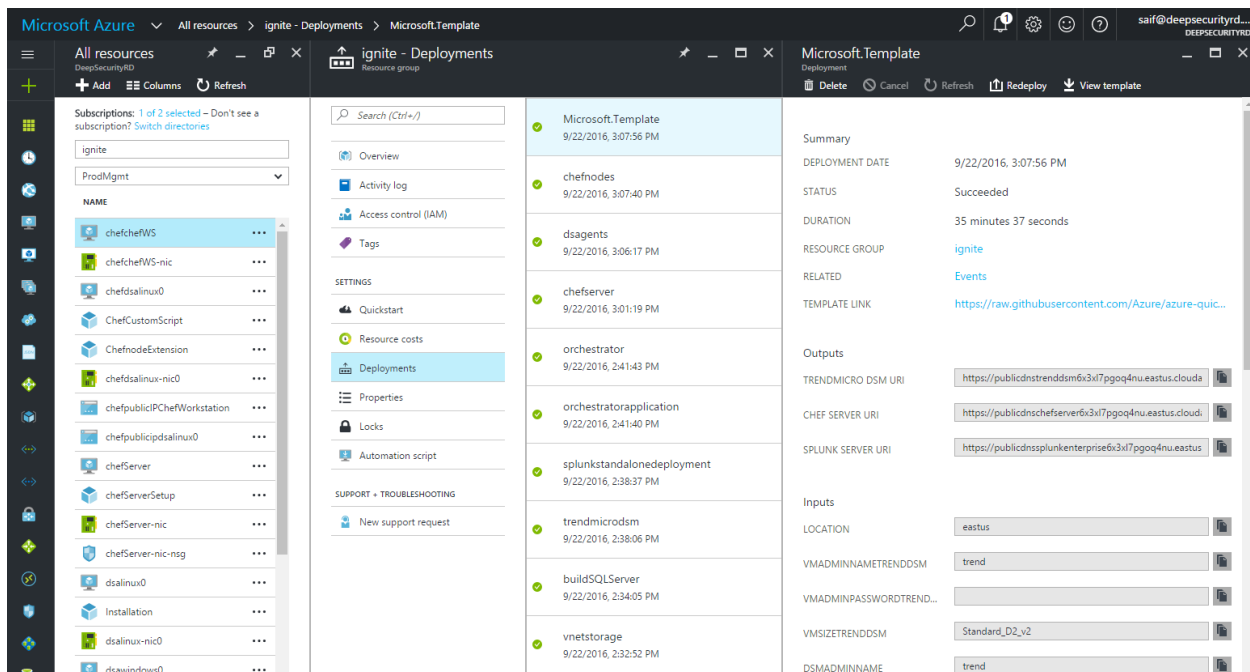


FIGURE 2 - RESOURCE GROUP FOR DEPLOYMENT

- Once the Resource Groups details are open, click on “**Deployments**” and select “**Microsoft.Template**” from the list of deployments.



Microsoft.Template

Deployment

Summary

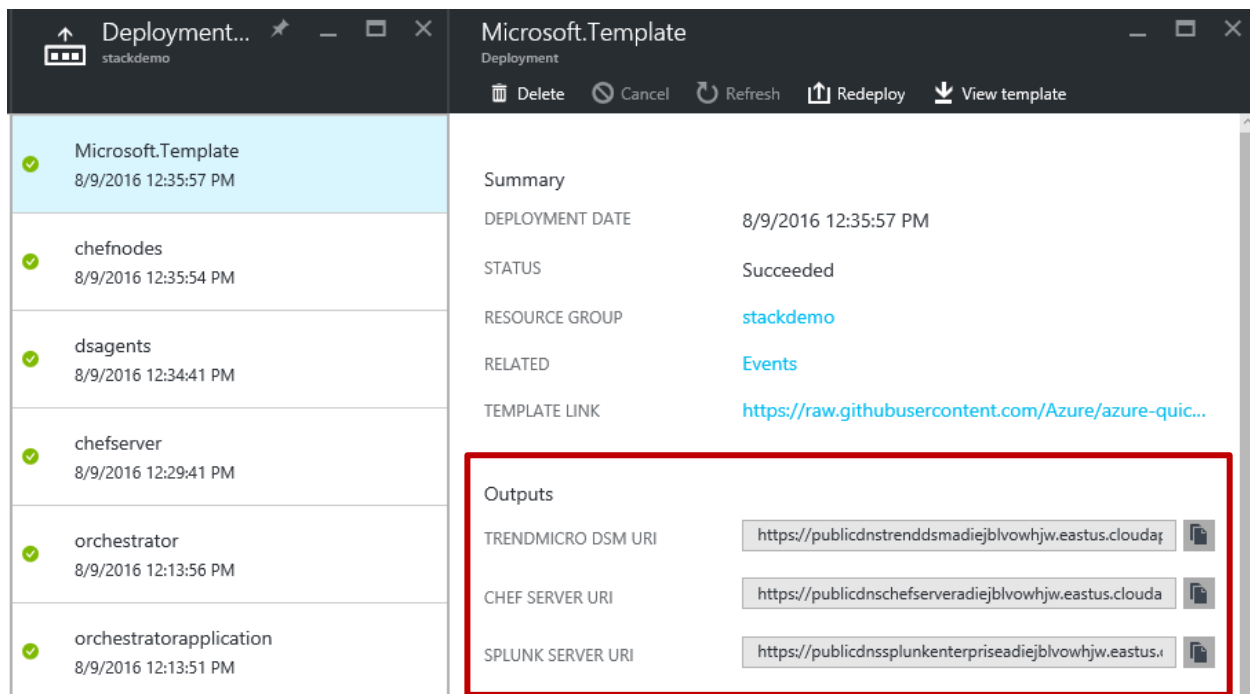
DEPLOYMENT DATE	9/22/2016, 3:07:56 PM
STATUS	Succeeded
DURATION	35 minutes 37 seconds
RESOURCE GROUP	ignite
RELATED	Events
TEMPLATE LINK	https://raw.githubusercontent.com/Azure/azure-quickstart-templates/master/101-terraform/101-terraform-ignite/azuredeploy.json

Outputs

TRENDMICRO DSM URI	https://publicdnstrenddsm63x17pgq4nu.eastus.cloudapp.azure.com/
CHEF SERVER URI	https://publicdnscchefserver63x17pgq4nu.eastus.cloudapp.azure.com/
SPLUNK SERVER URI	https://publicdnssplunkenterprise63x17pgq4nu.eastus.cloudapp.azure.com/

FIGURE 3 MICROSFOT.TEMPLATE UNDER DEPLOYMENT

- In the Outputs section of this ARM template, we specify values that are returned post stack deployment. The following output values are returned;
 - Trend Micro Deep Security Web Console URL
 - Splunk Enterprise Server Web Console URL
 - Chef Server Web Console URL



Microsoft.Template

Deployment

Summary

DEPLOYMENT DATE	8/9/2016 12:35:57 PM
STATUS	Succeeded
RESOURCE GROUP	stackdemo
RELATED	Events
TEMPLATE LINK	https://raw.githubusercontent.com/Azure/azure-quickstart-templates/master/101-terraform/101-terraform-ignite/azuredeploy.json

Outputs

TRENDMICRO DSM URI	https://publicdnstrenddsmadiejblvowhjw.eastus.cloudapp.azure.com/
CHEF SERVER URI	https://publicdnscchefserveradiejblvowhjw.eastus.cloudapp.azure.com/
SPLUNK SERVER URI	https://publicdnssplunkenterpriseadiejblvowhjw.eastus.cloudapp.azure.com/

FIGURE 4 ARM TEMPLATE OUTPUT

- Copy the URL's for Trend Micro Deep Security Web Console and Splunk Enterprise Server Web Console URL and bookmark them, or record them so that you can easily navigate to them later during the exercises.
- Login to Trend Micro Deep Security Web Console and Splunk Enterprise Server Web Console to ensure you have access to each application using the Trend Micro Deep Security and Splunk Web Console username and password provided earlier.

DEPLOY STACK

OVERVIEW

The template provides an automated provisioning, configuration and integration of Trend Micro's Deep Security product on Azure. The figure below depicts the stack details once it is deployed;

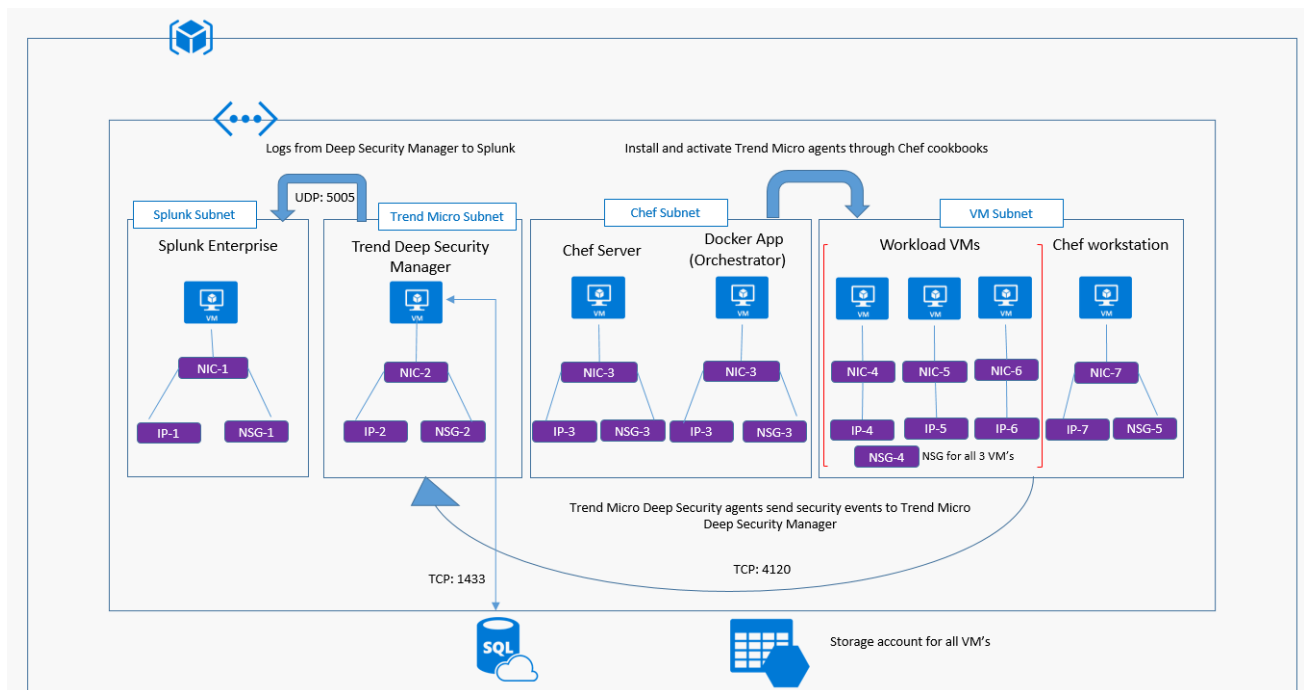


FIGURE 5 – INTEGRATED STACK ARCHITECTURE

As a part of stack deployment the template launches the following;

- A storage account in the resource group.
- A Virtual Network (vNet) with four subnets
- Virtual Machines to host solution components
- Network security groups to control what communication paths are allowed
- Azure SQL DB to host Deep Security persistent data
- Three test Virtual Machines; 2 VMs (Linux, Windows) with bootstrap scripts to install TrendMicro agents (through Azure VM extensions) and 1 VMs (Linux) with bootstrap scripts to install Chef Agents

LAUNCH STACK

The stack deployment can be started by accessing the ARM template at GitHub ([here](#)). You can simply click the "Deploy to Azure" button on this GitHub repository or use PowerShell, Azure CLI etc. to start the deployment. The deployment takes about 30-45 mins.



For this launch and learn session the stack is pre-launched for you. Review the instructions later in this document on how to access the pre-provisioned stack environment in Azure for this session.

TEMPLATE PARAMETERS

The template provides a list of parameters. Some parameters are defined with default values but some require your input during stack launch. In the parameters section of the template, we specify which values you can input when deploying this stack. These parameter values enable us to customize the stack deployment which is tailored to your particular requirements.

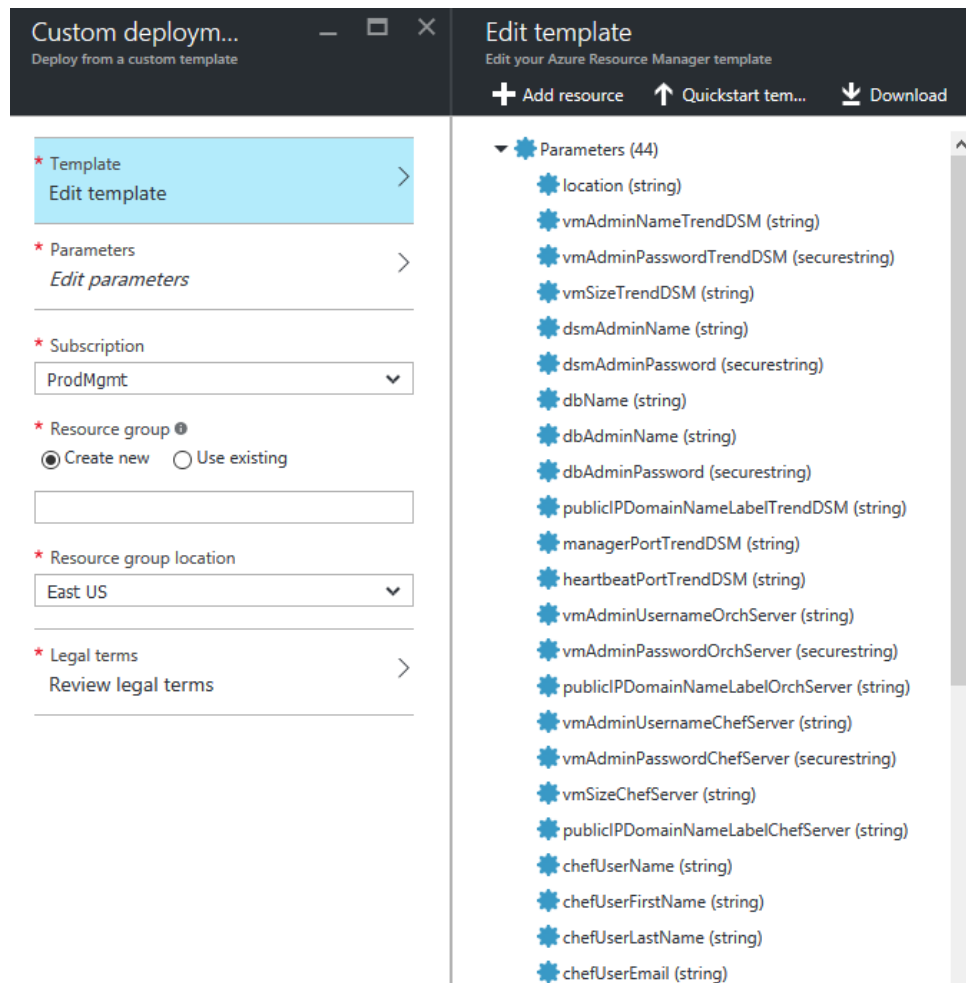


FIGURE 6 - ARM TEMPLATE - PARAMETERS

The parameters sections can be summarized into these logical areas;

- Where you want to deploy this stack.
- Web application administrators account and Virtual machine administrator account credentials for the various stack components.
- Communication ports for Deep Security
- Virtual machine size and number of test virtual machines

PROTECTING AZURE VIRTUAL MACHINE WITH DEEP SECURITY

This solution stack provides two ways of deploying deep security agents on Azure VM to add various security controls;

TREND MICRO AZURE EXTENSION Azure through VM Agent, a light weight process intended to bootstrap additional solutions, offered VM extensions both by Microsoft and its partners, for configuring and managing Azure Virtual Machines.

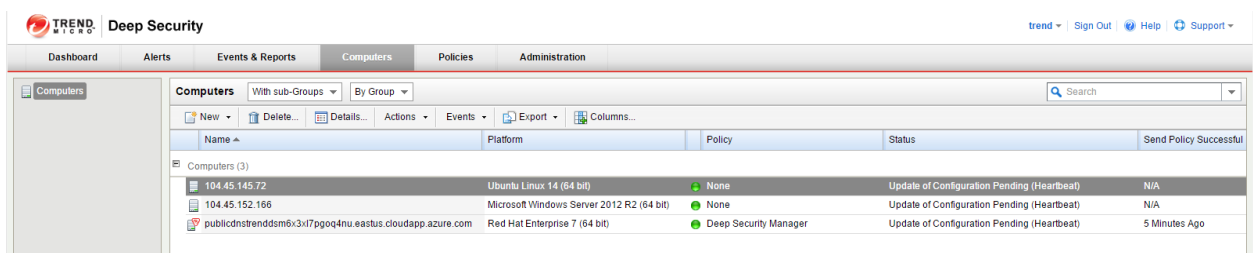
As a part of this stack deployment, we provide two test virtual machines (windows and Linux) that have Deep Security agent already installed via Trend Micro Deep Security VM extensions on Azure.

TREND MICRO CHEF COOKBOOKS Configuration Management is a key aspect in configuring servers, its applications and handling security. Chef can be used to install and configure Trend Micro agent. As a part of stack launch, we deploy a Chef Server and an automated framework that allows any VM's to bootstrap to chef Server when they get provisioned.

ADD PROTECTION TO TEST AZURE VIRTUAL MACHINES (EXERCISE)

The Deep Security Agent is already installed on these test Azure Virtual Machines as a part of stack launch, the next step is to enable protection and assign security policy to the Azure VM from Deep Security Manager. Deep Security provides out of the box security policies based on various Operating Systems. To assign policy to the test VM:

- Login to Deep Security Manager Web Console using the credential provided.
- Click on the “Computers” tab from the top main menu
- There should be two VM listed here. One Microsoft Windows based and the second one Linux ubuntu based.



Name	Platform	Policy	Status	Send Policy Successful
104.45.145.72	Ubuntu Linux 14 (64 bit)	None	Update of Configuration Pending (Heartbeat)	N/A
104.45.152.166	Microsoft Windows Server 2012 R2 (64 bit)	None	Update of Configuration Pending (Heartbeat)	N/A
publicdnstrendsm6ix17pgq4nu.eastus.cloudapp.azure.com	Red Hat Enterprise 7 (64 bit)	Deep Security Manager	Update of Configuration Pending (Heartbeat)	5 Minutes Ago

- Double click on the Windows test Azure VMs one by one and then Under “Overview” → “General” select Policy in the “Policy” dropdown list.
 - Linux ubuntu test VM: Select the Linux policy
 - Windows test VM: Select the Windows 2012 policy

Computer: 40.121.143.158

Help

Overview

Anti-Malware

Web Reputation

Firewall

Intrusion Prevention

Integrity Monitoring

Log Inspection

Interfaces

Settings

Updates

Overrides

General

Actions

Events

General

Hostname: 40.121.143.158 (Last IP Used: 40.121.143.158)

Display Name:

Description:

Platform: Microsoft Windows Server 2012 R2 (64 bit) Build 9600

Group: Computers

Policy: Base Policy ▶ Windows ▶ Windows Server 2012 Edit

Asset Importance: None Edit

Download Security Updates From: Default Relay Group Edit

Status

Agent

Status: Managed (Online)

Anti-Malware: Off, not installed, no configuration

Web Reputation: Off, not installed

Firewall: Off, not installed, no rules

Intrusion Prevention: Off, not installed, no rules

Integrity Monitoring: Off, not installed, no rules

Log Inspection: Off, not installed, no rules

Online: Yes

Save Close

FIGURE 7 - ASSIGN POLICY TO TEST AZURE VM



The Deep Security Agent and Deep Security Manager communicate with each other at a regular time interval, by default it is set to 10 minutes. If you notice the status of the VM is reported as “Update of Configuration Pending (heartbeat), that just means the agent has not performed heartbeat. There is no action required as the policy update will be pushed to agent once the heartbeat happened.

INTEGRATE

The majority of the integration steps are already handled by the stack template. The only integration step that is required to be performed post deployment is to configure Trend Micro Deep Security to send system and security events to Splunk.

CONFIGURE TREND MICRO DEEP SECURITY FOR SYSTEM EVENT LOG FORWARDING (EXERCISE)

The integration of Trend Micro Deep Security for system events forwarding to Splunk Enterprise is done via system setting (Administration → System Settings → SIEM) configuration as shown below;

- Login to Deep Security Manager Web Console using the credentials provided.
- Click Administration from the top menu.
- Click System Settings from the left pane.
- Click on SIEM tab under system settings and then specify the following details.
 - FQDN of the Splunk server. The FQDN for the Splunk can be retrieved from the stack Output that you recorded earlier.
 - “Forward System Events to a remote computer” is enabled
 - In UDP port textbox enter port **5005**
 - Syslog Format is set to “Common Event Format”

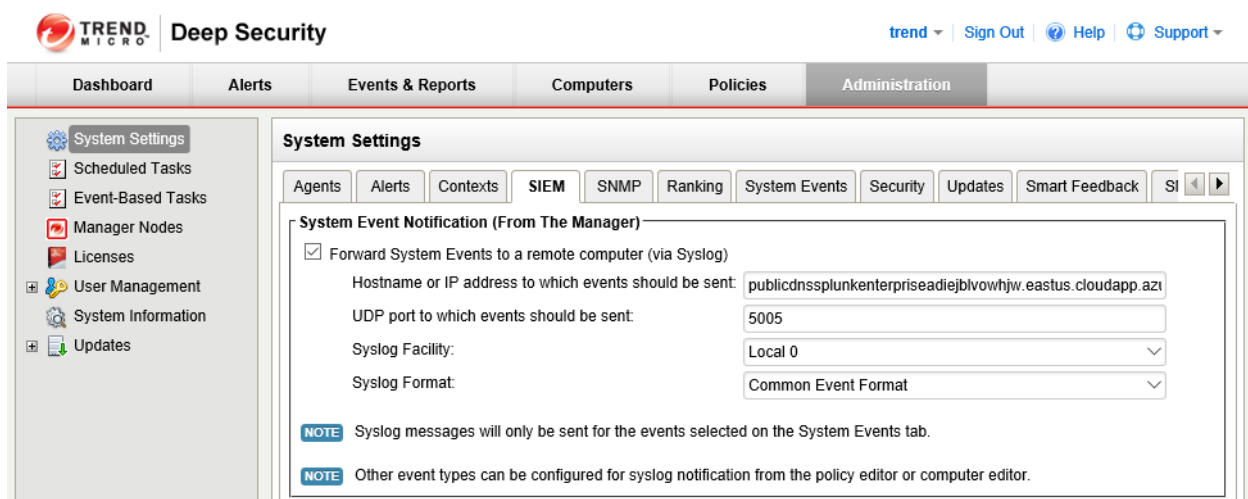


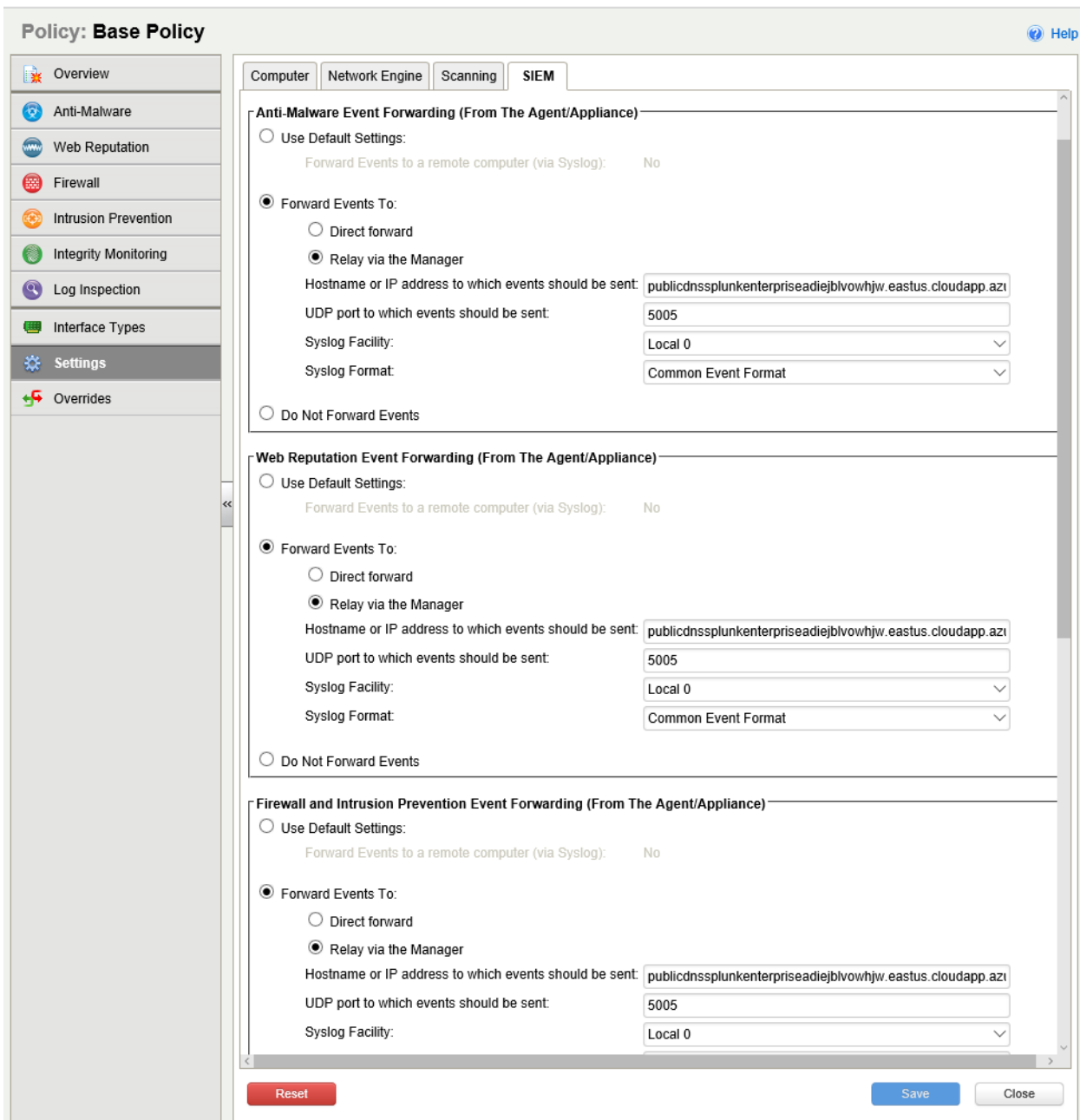
FIGURE 8 - SYSTEM EVENT FORWARDING TO SPLUNK

CONFIGURE TREND MICRO DEEP SECURITY FOR SECURITY EVENT LOG FORWARDING (EXERCISE)

The integration of Trend Micro Deep Security for security event forwarding to Splunk is done via Policy configuration. Deep Security allows Policy inheritance where child policies inherit their settings from their parent Policies. This way you can create a policy tree that begins with a top/base parent policy configured with settings and rules that will

apply to all computers. It is recommended to set the integration details at the Top (root/base) policy as shown below.

- Select “Policies” in the menu bar - Click on the “Base Policy” which opens a pop-up - In pop-up screen go to settings and select “SIEM” then specify the following details.
 - FQDN of the Splunk server. The FQDN for the Splunk can be retrieved from the stack Output that you recorded earlier.
 - Ensure “Forward Events to” and “Relay Via Manager” options are selected.
 - In UDP port textbox enter port **5005**
 - Syslog Format is set to “Common Event Format”



Policy: Base Policy

Computer | Network Engine | Scanning | **SIEM**

Anti-Malware Event Forwarding (From The Agent/Appliance)

☐ Use Default Settings:
Forward Events to a remote computer (via Syslog): No

☒ Forward Events To:

☐ Direct forward

☒ Relay via the Manager

Hostname or IP address to which events should be sent: publicdnssplunkenterpriseadiejblvowhjw.eastus.cloudapp.azure.com

UDP port to which events should be sent: 5005

Syslog Facility: Local 0

Syslog Format: Common Event Format

☐ Do Not Forward Events

Web Reputation Event Forwarding (From The Agent/Appliance)

☐ Use Default Settings:
Forward Events to a remote computer (via Syslog): No

☒ Forward Events To:

☐ Direct forward

☒ Relay via the Manager

Hostname or IP address to which events should be sent: publicdnssplunkenterpriseadiejblvowhjw.eastus.cloudapp.azure.com

UDP port to which events should be sent: 5005

Syslog Facility: Local 0

Syslog Format: Common Event Format

☐ Do Not Forward Events

Firewall and Intrusion Prevention Event Forwarding (From The Agent/Appliance)

☐ Use Default Settings:
Forward Events to a remote computer (via Syslog): No

☒ Forward Events To:

☐ Direct forward

☒ Relay via the Manager

Hostname or IP address to which events should be sent: publicdnssplunkenterpriseadiejblvowhjw.eastus.cloudapp.azure.com

UDP port to which events should be sent: 5005

Syslog Facility: Local 0

☐ Do Not Forward Events

Reset Save Close

FIGURE 9 - SECURITY EVENT FORWARDING TO SPLUNK

ANALYZE

GENERATE SAMPLE EVENTS (EXERCISE)

Now that the integration piece is completed we are all set to Analyze security events in Splunk Web Console. For this launch and learn session we will leverage Trend Micro Deep Security Demo mode setup to generate sample data for us.

- Login to Deep Security Manager Web Console using the credential provided.
- Click **Administration** from the top menu.
- Click **System Information** from the left pane.
- From the System Information page, click **Demo Mode** to start the wizard.

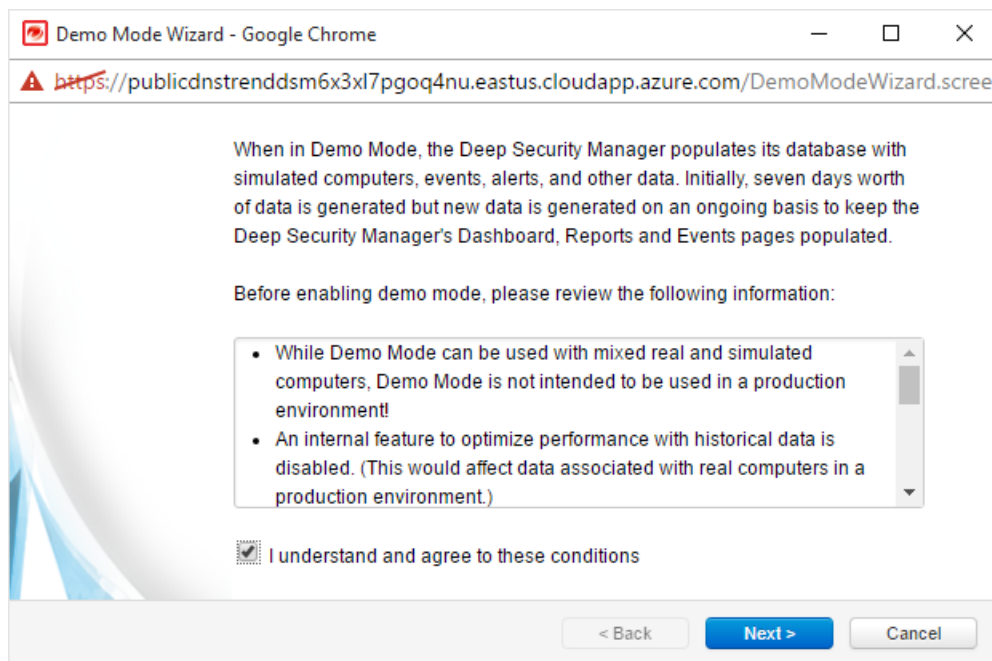


FIGURE 10 - DEEP SECURITY DEMO MODE

- Check **I understand and agree to these conditions** and Click Next

- Click **Finish**



The Demo mode will take roughly 20-30 minutes to complete but as the task is being completed you can still start visualizing the event data in Splunk.

ANALYZE DEEP SECURITY EVENT DATA IN SPLUNK'S WEB CONSOLE (**EXERCISE**)

Once the install and integration steps are done, you are all set to analyze Deep Security event data in Splunk's web console. You can run searches, identify anomalies and correlate events across your protected workloads. The Splunk platform offers many options for data analysis and visualization. As a part of stack launch, we will deploy Deep Security App for Splunk. This app contains parsing logic, saved searches, and dashboards for monitoring.

- Login to Splunk Web Console using the credential provided.
- From the Apps panel on the left, select **Trend Micro Deep Security for Splunk** app.

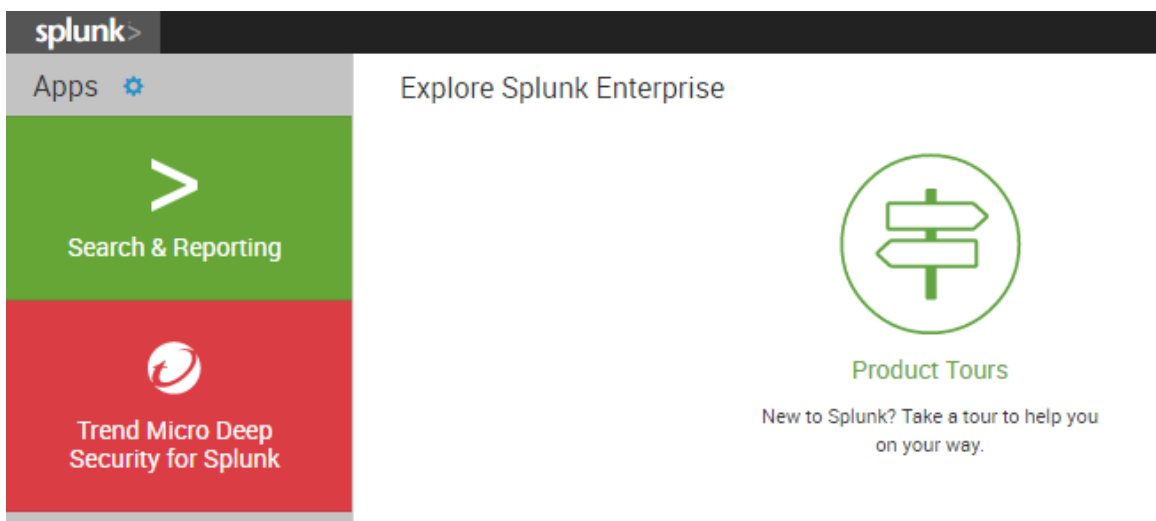
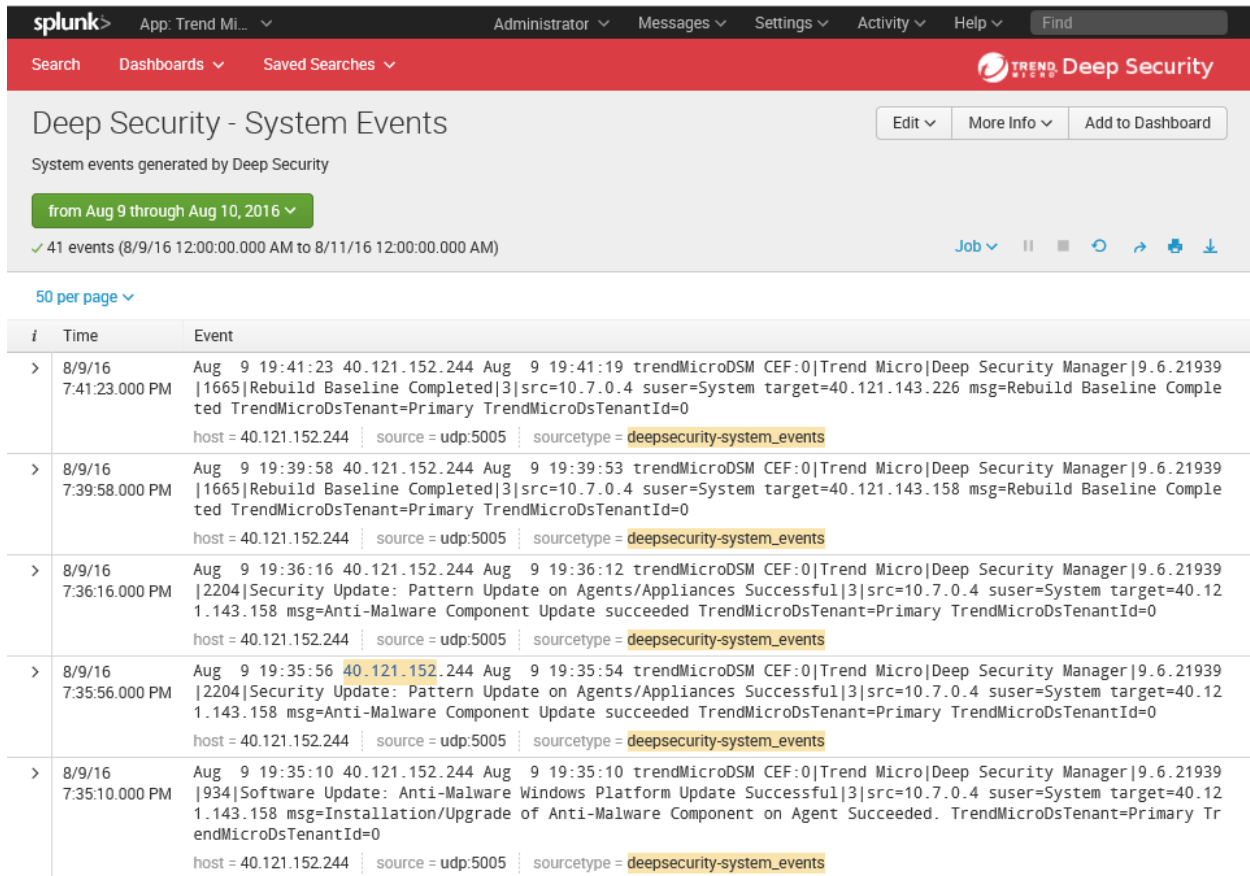


FIGURE 11 - TREND MICRO DEEP SECURITY FOR SPLUNK

- From the top menu bar, expand **Saved Searches** using the drop down option and then select **System Events** and search for "**Deep Security – System Events**" you will notice the raw data is coming through as part of the integration exercise we did previously.



Deep Security - System Events

System events generated by Deep Security

from Aug 9 through Aug 10, 2016

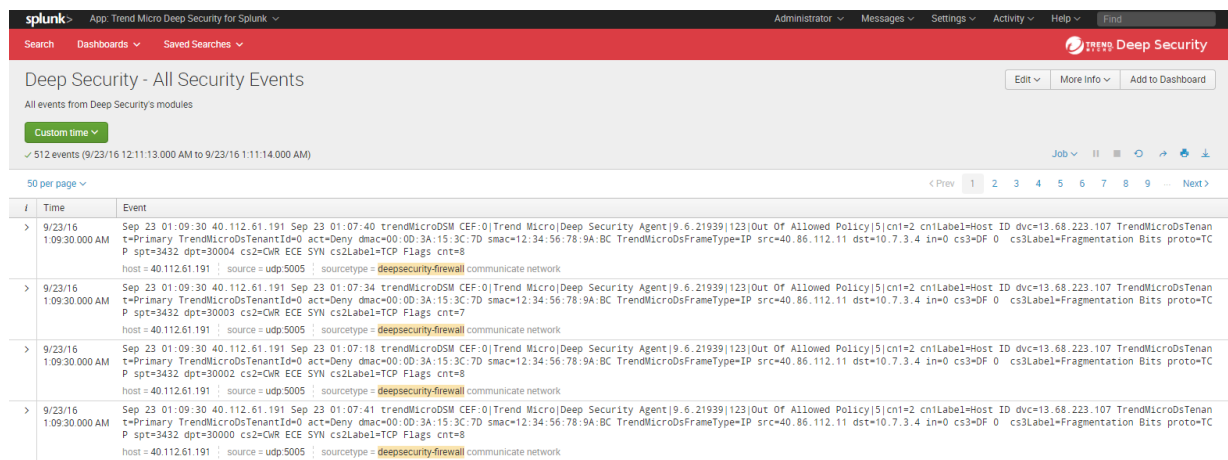
✓ 41 events (8/9/16 12:00:00.000 AM to 8/11/16 12:00:00.000 AM)

50 per page

i	Time	Event
>	8/9/16 7:41:23.000 PM	Aug 9 19:41:23 40.121.152.244 Aug 9 19:41:19 trendMicroDSM CEF:0 Trend Micro Deep Security Manager 9.6.21939 1665 Rebuild Baseline Completed 3 src=10.7.0.4 suser=System target=40.121.143.226 msg=Rebuild Baseline Completed TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 host = 40.121.152.244 source = udp:5005 sourcetype = deepsecurity-system_events
>	8/9/16 7:39:58.000 PM	Aug 9 19:39:58 40.121.152.244 Aug 9 19:39:53 trendMicroDSM CEF:0 Trend Micro Deep Security Manager 9.6.21939 1665 Rebuild Baseline Completed 3 src=10.7.0.4 suser=System target=40.121.143.158 msg=Rebuild Baseline Completed TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 host = 40.121.152.244 source = udp:5005 sourcetype = deepsecurity-system_events
>	8/9/16 7:36:16.000 PM	Aug 9 19:36:16 40.121.152.244 Aug 9 19:36:12 trendMicroDSM CEF:0 Trend Micro Deep Security Manager 9.6.21939 12204 Security Update: Pattern Update on Agents/Appliances Successful 3 src=10.7.0.4 suser=System target=40.121.143.158 msg=Anti-Malware Component Update succeeded TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 host = 40.121.152.244 source = udp:5005 sourcetype = deepsecurity-system_events
>	8/9/16 7:35:56.000 PM	Aug 9 19:35:56 40.121.152.244 Aug 9 19:35:54 trendMicroDSM CEF:0 Trend Micro Deep Security Manager 9.6.21939 12204 Security Update: Pattern Update on Agents/Appliances Successful 3 src=10.7.0.4 suser=System target=40.121.143.158 msg=Anti-Malware Component Update succeeded TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 host = 40.121.152.244 source = udp:5005 sourcetype = deepsecurity-system_events
>	8/9/16 7:35:10.000 PM	Aug 9 19:35:10 40.121.152.244 Aug 9 19:35:10 trendMicroDSM CEF:0 Trend Micro Deep Security Manager 9.6.21939 1934 Software Update: Anti-Malware Windows Platform Update Successful 3 src=10.7.0.4 suser=System target=40.121.143.158 msg=Installation/Upgrade of Anti-Malware Component on Agent Succeeded. TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 host = 40.121.152.244 source = udp:5005 sourcetype = deepsecurity-system_events

FIGURE 12 SPLUNK WEB CONSOLE WITH TREND MICRO DEEP SECURITY SYSTEM EVENTS

- Again from the top menu bar, expand **Saved Searches** using the drop down option and then select **Security Events** and search for “**Deep Security – All Security Events**” you will notice the raw data is coming through and there are various security events reported such as firewall traffic that is not allowed by our firewall policy set.



Deep Security - All Security Events

All events from Deep Security's modules

Custom time

✓ 512 events (9/23/16 12:11:13.000 AM to 9/23/16 1:11:14.000 AM)

50 per page

i	Time	Event
>	9/23/16 1:09:30.000 AM	Sep 23 01:09:30 40.112.61.191 Sep 23 01:07:40 trendMicroDSM CEF:0 Trend Micro Deep Security Agent 9.6.21939 123 Out Of Allowed Policy 5 cnt=2 cntLabel=Host ID dvc=13.68.223.107 TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 act=Deny dmac=00:0D:3A:15:3C:7D smac=12:34:56:78:9A:BC TrendMicroDsFrameType=IP src=40.86.112.11 dst=10.7.3.4 in=0 cs3=DF 0 cs3Label=Fragmentation Bits proto=TCP spt=3432 dpt=30004 cs2=QWR ECE SYN cs2Label=TCP Flags cnt=8 host = 40.112.61.191 source = udp:5005 sourcetype = deepsecurity-firewall communicate network
>	9/23/16 1:09:30.000 AM	Sep 23 01:09:30 40.112.61.191 Sep 23 01:07:34 trendMicroDSM CEF:0 Trend Micro Deep Security Agent 9.6.21939 123 Out Of Allowed Policy 5 cnt=2 cntLabel=Host ID dvc=13.68.223.107 TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 act=Deny dmac=00:0D:3A:15:3C:7D smac=12:34:56:78:9A:BC TrendMicroDsFrameType=IP src=40.86.112.11 dst=10.7.3.4 in=0 cs3=DF 0 cs3Label=Fragmentation Bits proto=TCP spt=3432 dpt=30003 cs2=QWR ECE SYN cs2Label=TCP Flags cnt=7 host = 40.112.61.191 source = udp:5005 sourcetype = deepsecurity-firewall communicate network
>	9/23/16 1:09:30.000 AM	Sep 23 01:09:30 40.112.61.191 Sep 23 01:07:18 trendMicroDSM CEF:0 Trend Micro Deep Security Agent 9.6.21939 123 Out Of Allowed Policy 5 cnt=2 cntLabel=Host ID dvc=13.68.223.107 TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 act=Deny dmac=00:0D:3A:15:3C:7D smac=12:34:56:78:9A:BC TrendMicroDsFrameType=IP src=40.86.112.11 dst=10.7.3.4 in=0 cs3=DF 0 cs3Label=Fragmentation Bits proto=TCP spt=3432 dpt=30002 cs2=QWR ECE SYN cs2Label=TCP Flags cnt=6 host = 40.112.61.191 source = udp:5005 sourcetype = deepsecurity-firewall communicate network
>	9/23/16 1:09:30.000 AM	Sep 23 01:09:30 40.112.61.191 Sep 23 01:07:41 trendMicroDSM CEF:0 Trend Micro Deep Security Agent 9.6.21939 123 Out Of Allowed Policy 5 cnt=2 cntLabel=Host ID dvc=13.68.223.107 TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 act=Deny dmac=00:0D:3A:15:3C:7D smac=12:34:56:78:9A:BC TrendMicroDsFrameType=IP src=40.86.112.11 dst=10.7.3.4 in=0 cs3=DF 0 cs3Label=Fragmentation Bits proto=TCP spt=3432 dpt=30000 cs2=QWR ECE SYN cs2Label=TCP Flags cnt=8 host = 40.112.61.191 source = udp:5005 sourcetype = deepsecurity-firewall communicate network

FIGURE 13 DEEP SECURITY – ALL SECURITY EVENTS



If you don't see any event data then try reloading the search from the refresh button on the right few times.

Now that you have the event data coming in Splunk it's time to observe some pre-built dashboards from the Trend Micro Deep security app for Splunk.

Dashboards are a powerful visualization tool to help accelerate the time to identify anomalies and indicators of compromise (IOC). The saved searches powering these dashboards can also be leverage for forensic investigations and to reduce the time it takes for root cause analysis and remediation.

- From the top menu bar, expand **Dashboards** using the drop down option and then pick available dashboard one by one to observe and analyse security data;

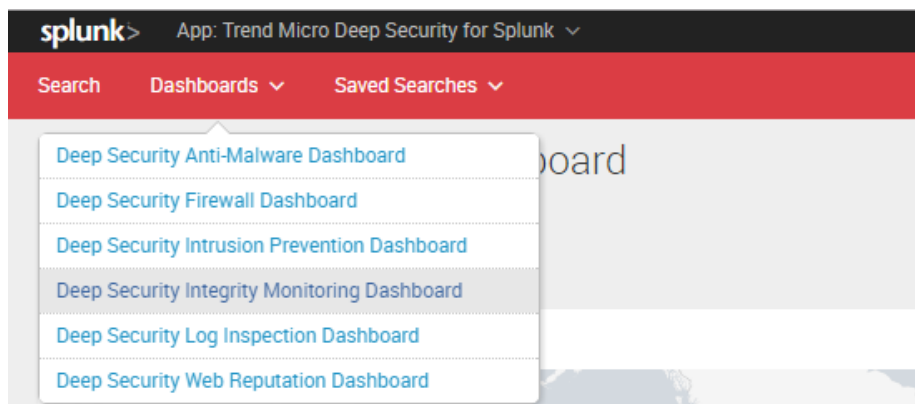


FIGURE 14 TREND MICRO DEEP SECURITY FOR SPLUNK DASHBOARD

For example, picking a firewall dashboard will show you that there are many “out of allowed policy” events are being generated. These are generated because our Azure VM's are being hit by traffic that is not specifically allowed. You can further click on the “Event Name” and start the search / query screen.

From this search screen you can easily expand your search criteria and start filtering data for your analyses etc. Expanding search filter is as easy as picking a data field in the search results by clicking on it and selecting add to the search such as “dpt” is 3389, now the search will filter all the events based on where destination port is RDP port.




List ▾ Format ▾ 20 Per Page ▾				< Prev 1 2 3 4 5 6 7 8 9 10 Next >											
ids	i	Time	Event												
	>	9/23/16 1:33:21.000 AM	Sep 23 01:33:21 40.112.61.191 Sep 16 23:43:42 trendMicroDSM CEF:0 Trend Micro Deep Security Agent 9.6.21939 21 Out Of Allowed Policy 5 cn1=47 cn1Lab=Host ID dvchost=laptop_mneil TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 act=Deny dmac=A6:5A:F7:00:E8:39 smac=49:8C:74:3B:72:34 TrendMicroDsFrameType=IP src=137.137.17.40 dst=10.0.123.137 in=398 cs3= cs3Label=Fragmentation Bits proto=TCP spt=20 dpt=3389 cs2= cs2Label=TCP Flags cnt=1 host = 40.112.61.191 source = udp:5005 sourcetype = deepsecurity-firewall communicate network												
	>	9/23/16 1:33:21.000 AM	Sep 23 01:33:21 40.112.61.191 Sep 16 23:53:46 trendMicroDSM CEF:0 Trend Micro Deep Security Agent 9.6.21939 21 Out Of Allowed Policy 5 cn1=47 cn1Lab=Host ID dvchost=hr_app TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 act=Deny dmac=5F:CD:E8:39 smac=49:8C:74:3B:72:34 TrendMicroDsFrameType=IP src=87.11.93.147 dst=10.0.5.166 in=391 cs3= cs3Label=Fragmentation Bits proto=TCP spt=20 dpt=3389 cs2= cs2Label=TCP Flags cnt=1 host = 40.112.61.191 source = udp:5005 sourcetype = deepsecurity-firewall communicate network	<div>Add to search  Exclude from search  New search </div>											
	>	9/23/16 1:33:21.000 AM	Sep 23 01:33:21 40.112.61.191 Sep 16 23:45:24 trendMicroDSM CEF:0 Trend Micro Deep Security Agent 9.6.21939 21 Out Of Allowed Policy 5 cn1=47 cn1Lab=Host ID dvchost=laptop_mneil TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 act=Deny dmac=A6:5A:F7:00:E8:39 smac=49:8C:74:3B:72:34 TrendMicroDsFrameType=IP src=137.137.17.40 dst=10.0.123.137 in=398 cs3= cs3Label=Fragmentation Bits proto=TCP spt=20 dpt=3389 cs2= cs2Label=TCP Flags cnt=1 host = 40.112.61.191 source = udp:5005 sourcetype = deepsecurity-firewall communicate network												

FIGURE 15 EXPANDING THE SEARCH

Similarly, you can observe other dashboards such as Log Inspection, the Log Inspection module lets you alert on specific log entries that are of concern from a security perspective. For example, it is useful to track specific user logins to a system. In the demo data under the you will find various activities such as;

Event Description	Event Count	Percent of Total
Successful login during weekend	101	1.219218
Detected an error in the protocol stream and has disconnected the client	101	1.219218
Successful login during non-business hours	84	1.014003
Exceeded maximum allowed failed logon attempts	83	1.001931
Multiple connection attempts from same source.	50	0.603573

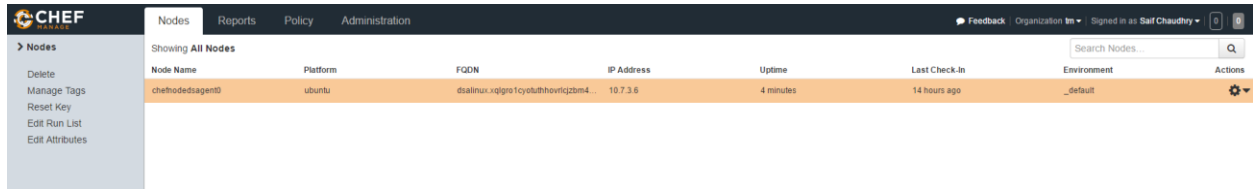
FIGURE 16 LOG INSPECTION EVENT

- Click any one of the event of your interest and observe the raw event data and spend some time with the search filters to do analyses and correlation with other security event data.

INSTALL DEEP SECURITY AGENT TO TEST AZURE VIRTUAL MACHINE VIA CHEF (OPTIONAL EXERCISE)

We have provisioned one test virtual machine as part of stack launch that is registered as a node to the Chef Server. As an additional exercise, if you are familiar with Chef orchestration tool, you can go ahead and install deep security agent via Chef on to a test Azure VM.

- Access the Chef Server Web Console, the URL to access the Chef Web Server console is provided in the output section of the ARM template. The instructions are provided earlier in the document on how to retrieve the output values from Azure Portal.
- Login to the Chef Server Web Console using the credentials provided to you. If asked about "Please enter your VM Name to continue to the web interface", type "ChefServer".
- Verify one node is registered in the web console



The screenshot shows the Chef web interface. At the top, there are tabs for 'Nodes', 'Reports', 'Policy', and 'Administration'. The 'Nodes' tab is selected. On the left, there is a sidebar with options: 'Nodes', 'Delete', 'Manage Tags', 'Reset Key', 'Edit Run List', and 'Edit Attributes'. The main content area shows 'Showing All Nodes' with a search bar. Below this is a table with one row of data.

Node Name	Platform	FQDN	IP Address	Uptime	Last Check-In	Environment	Actions
chefnode0agent0	ubuntu	dsaltnu-xqign1cyetabthoviqzdm4	10.7.3.6	4 minutes	14 hours ago	_default	

FIGURE 17 - REGISTERED NODE IN CHEF

- You can access the Chef recipe for Deep Security Agent [here](#) and install Deep Security agent on this test node.