Overview
This document describes the configuration of Dell AppAssure Core to Core Replication for use with Silver Peak VRX software. When Silver Peak VRX software is deployed with Dell AppAssure Core to Core Replication, a static route will be used to direct replication traffic to the VRX software for acceleration.

Prerequisites
• Silver Peak VXOA version 6.2.4 or later with licenses
• Please read this entire document before beginning configuration
• Install the VRX software using the Quick Start Guide for your hypervisor
• AppAssure Version 5 or later already configured for replication

This document uses Windows Server 2012 for all configuration examples. Links are supplied to Windows 2008 steps, where available, on page 12.

Configuration Steps
The tasks in the deployment guide should not be performed until the Silver Peak VRX software has been configured using the Velocity Quick Start Guide and the tunnel is listed as up.

• Create an application definition for AppAssure
• Change the VRX software tunnel mode to IPSEC
• Create an SSL optimization map for AppAssure in each VRX software instance
• Export the AppAssure server certificate from the replication target
• Load the server certificate into each VRX software instance
• Add a static route to each AppAssure server using the VRX software as a next hop
• Restart the AppAssure service on the replication target
• Verify acceleration
Contents

Overview .................................................................................................................................................. 1
Prerequisites .......................................................................................................................................... 1
Configuration Steps ............................................................................................................................... 1
Topology Diagram ................................................................................................................................. 3
Create an Application Definition for AppAssure .................................................................................. 4
Changing the VRX tunnel mode to IPSEC ............................................................................................ 4
Creating an SSL Optimization Policy for AppAssure ......................................................................... 5
Exporting the AppAssure Server Certificate ......................................................................................... 6
Set the Cipher Order on the Windows Server ...................................................................................... 8
Loading the Certificate into the VRX Software ..................................................................................... 9
Add A Static Route to the Windows Server ........................................................................................... 9
Restart the AppAssure Service on the Replication Target .................................................................... 10
Am I Accelerated? ............................................................................................................................... 11
Links .................................................................................................................................................... 12
Create an Application Definition for AppAssure

These steps must be completed on the source and destination Silver Peak VRX software instances.

Completing this section will provide better detail when viewing reports.

1. Select Configuration>Application>User-Defined.

2. Click Add Rule.

3. Use the following settings in the Add Application Rule dialog box. Unspecified fields do not need to be edited.
   - Application: AppAssure
   - Protocol: tcp
   - Destination Port: 8006

4. Click Apply.

5. Create a second rule with the following settings.
   Unspecified fields do not need to be edited.
   - Application: AppAssure
   - Protocol: tcp
   - Source Port: 8006

<table>
<thead>
<tr>
<th>Priority</th>
<th>Application</th>
<th>Protocol</th>
<th>Source IP/Subnet</th>
<th>Source Port/Range</th>
<th>Destination IP/Subnet</th>
<th>Destination Port/Range</th>
<th>DSCP</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>AppAssure</td>
<td>tcp</td>
<td>0.0.0.0/0</td>
<td>8006</td>
<td>0.0.0.0/0</td>
<td>0</td>
<td>any</td>
<td>any</td>
</tr>
<tr>
<td>20</td>
<td>AppAssure</td>
<td>tcp</td>
<td>0.0.0.0/0</td>
<td>0</td>
<td>0.0.0.0/0</td>
<td>8006</td>
<td>any</td>
<td>any</td>
</tr>
</tbody>
</table>

Changing the VRX tunnel mode to IPSEC

These steps must be completed on the source and destination Silver Peak VRX software instances.

The use of IPSEC between Silver Peak VRX instances ensures the security of AppAssure replication data sent across the network.

1. Login to the Silver Peak VRX software instance using a web browser.
2. Select Configuration>Tunnels

3. Click on the name of the Tunnel that will be used to accelerate AppAssure replication.

4. Change the Mode to IPSEC.

5. Set a pre-shared key. (this must be the same at both sites)

6. Click Apply.

7. Click the Save Changes button.

Creating an SSL Optimization Policy for AppAssure

These steps must be completed on the source and destination Silver Peak VRX software instances.

1. Login to the VRX software instance using a web browser.

2. Select Configuration>Optimization Policy.

3. Click the Add Rule button for the active map.

4. Use the following settings for the new optimization policy.
   Protocol: tcp
   Source:Dest Port: 0:8006
Protocol Acceleration: ssl

5. Verify that the new optimization policy is shown.
6. Click the Save Changes button.

Exporting the AppAssure Server Certificate

This step must be performed on the Windows Server that is the AppAssure Core replication target.

The certificate from the Core replication source server is not needed.

1. Log into the Windows Server that is running the AppAssure Core software and is the replication target.
2. Start the Windows Certificate Manager.
3. Expand Trusted Root Certification Authorities and select Certificates.
4. Select the first entry that matches the Windows Server name. In this example the Windows Server is named AACORE.
   a. Double click on the entry
   b. Select the Details tab
   c. Select Subject
d. Verify that $T = \text{AppAssureServerCertificate}$

```
O = Root
CN = AACORE
T = AppAssureServerCertificate
```

e. If $T$ = anything other than AppAssureServerCertificate, select each certificate that matches the Windows Server name until Subject $T = \text{AppAssureServerCertificate}$

5. After identifying the correct certificate select it and then go to Action> All Tasks> Export

6. Complete the steps in the Certificate Export Wizard with the following options:
   a. Yes, export the private key
      Do you want to export the private key with the certificate?
      
      ☑ Yes, export the private key
   b. Verify that Include all certificates in the certification path if possible is checked
      ☑ Personal Information Exchange - PKCS #12 (.PFX)
      ☑ Include all certificates in the certification path if possible
   c. Enter the same password into both fields. This password will be used during the import process in the VRX software.
      
      ✔ Password:  
      
      ☑ Confirm password:
      
      ✔ Password:
   d. Choose a file name and location for the exported certificate. Also, to make the exported certificate easier to click Browse and save the file to the desktop.
      
      File name:  
      
      C:\\Users\\Administrator\\Desktop\\aacore.pfx
Set the Cipher Order on the Windows Server

This step must be completed on the replication target core server.

1. Open the Group Policy Object Editor.
3. Double click SSL Cipher Suite Order.
4. Set SSL Cipher Suite Order to Enabled.
5. Enter TLS_RSA_WITH_AES_256_CBC_SHA into the SSL Cipher Suites field.
6. Click Apply and then OK.
Loading the Certificate into the VRX Software

Note that these steps must be completed on each Silver Peak VRX software instance that will be accelerating AppAssure replication.

1. Select Configuration>SSL Certificates.
2. Select Add Certificate.
3. Check the box for PFX Certificate File.
4. Click on Choose File for the Certificate File and browse to the file stored in the previous step.
5. Type in the password that was set in the previous step.
6. Click Add.
7. The new certificate will be displayed in the SSL Certificates window. Verify that the Issuer and Issued To fields display the server name for the replication target core.

Add A Static Route to the Windows Server

Note that the following steps need to be performed on each Windows Server that is part of AppAssure replication.

A static route needs to be added to each Windows Server in order to direct the AppAssure replication traffic to the VRX software. A default gateway change can also be made, but is not recommended due to the potential effects on other traffic. By using a static route, any traffic that is not between the two AppAssure Core instances will not be sent to the VRX software.

For more information on Windows static routes use this link: http://technet.microsoft.com/en-us/library/cc757323(v=ws.10).aspx

1. Open a command prompt on the Windows Server.
2. Enter the following command replacing XXX.XXX.XXX.XXX with the IP Address of the remote Windows Server running AppAssure Core and YYY.YYY.YYY.YYY with the IP Address of the Silver Peak VRX software:
   
   ```
   route add XXX.XXX.XXX.XXX mask 255.255.255.255 YYY.YYY.YYY.YYY -p
   ```
   
   Note that the IP Addresses will be different at each site

**Restart the AppAssure Service on the Replication Target**

The final step is to restart the AppAssure Core Service on the replication target server. Restarting the service allows the Silver Peak software to accelerate the AppAssure replication traffic.

1. Open the Windows services manager
2. Right click the AppAssure Core Service and select restart
3. Check the AppAssure service console to verify that the service restarted
Am I Accelerated?

To determine if the Silver Peak software is working, login to the source side VRX software and select the Data View. For each replication pair there will be an entry under Top Flows listing the IP Addresses of the filer pair. This entry displays the Up Time for the connection, the status (it should read OPTIMIZED), and also the effect of Network Memory. The light blue bar represents the data transmitted by the source filer, while the dark blue bar represents the data transmitted across the WAN by the VRX software accelerator after Network Memory has been applied.

### Top Flows

<table>
<thead>
<tr>
<th>Application</th>
<th>SP1 PORT1</th>
<th>SP2 PORT2</th>
<th>Status</th>
<th>Inbound Bytes</th>
<th>Reduction %</th>
<th>Outbound Bytes</th>
<th>Reduction %</th>
<th>Up Time</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliciple</td>
<td>10.0.2.143</td>
<td>129.168.0.154</td>
<td>8005</td>
<td>OPTIMIZED</td>
<td>0.0</td>
<td>4.8M</td>
<td>36.8</td>
<td>3m 26s</td>
<td>top</td>
</tr>
<tr>
<td>Appliciple</td>
<td>10.0.2.143</td>
<td>129.168.0.154</td>
<td>8006</td>
<td>OPTIMIZED</td>
<td>14.1</td>
<td>6.0M</td>
<td>37.7</td>
<td>3m 29s</td>
<td>top</td>
</tr>
<tr>
<td>Appliciple</td>
<td>10.0.2.143</td>
<td>129.168.0.154</td>
<td>8005</td>
<td>OPTIMIZED</td>
<td>16.8</td>
<td>6.0M</td>
<td>37.7</td>
<td>3m 29s</td>
<td>top</td>
</tr>
<tr>
<td>Appliciple</td>
<td>10.0.2.143</td>
<td>129.168.0.154</td>
<td>8006</td>
<td>OPTIMIZED</td>
<td>16.8</td>
<td>6.0M</td>
<td>37.7</td>
<td>3m 29s</td>
<td>top</td>
</tr>
<tr>
<td>Appliciple</td>
<td>10.0.2.143</td>
<td>129.168.0.154</td>
<td>8005</td>
<td>OPTIMIZED</td>
<td>16.8</td>
<td>6.0M</td>
<td>37.7</td>
<td>3m 29s</td>
<td>top</td>
</tr>
<tr>
<td>Appliciple</td>
<td>10.0.2.143</td>
<td>129.168.0.154</td>
<td>8006</td>
<td>OPTIMIZED</td>
<td>16.8</td>
<td>6.0M</td>
<td>37.7</td>
<td>3m 29s</td>
<td>top</td>
</tr>
<tr>
<td>Appliciple</td>
<td>10.0.2.143</td>
<td>129.168.0.154</td>
<td>8005</td>
<td>OPTIMIZED</td>
<td>16.8</td>
<td>6.0M</td>
<td>37.7</td>
<td>3m 29s</td>
<td>top</td>
</tr>
<tr>
<td>Appliciple</td>
<td>10.0.2.143</td>
<td>129.168.0.154</td>
<td>8006</td>
<td>OPTIMIZED</td>
<td>16.8</td>
<td>6.0M</td>
<td>37.7</td>
<td>3m 29s</td>
<td>top</td>
</tr>
<tr>
<td>Appliciple</td>
<td>10.0.2.143</td>
<td>129.168.0.154</td>
<td>8005</td>
<td>OPTIMIZED</td>
<td>16.8</td>
<td>6.0M</td>
<td>37.7</td>
<td>3m 29s</td>
<td>top</td>
</tr>
<tr>
<td>Appliciple</td>
<td>10.0.2.143</td>
<td>129.168.0.154</td>
<td>8006</td>
<td>OPTIMIZED</td>
<td>16.8</td>
<td>6.0M</td>
<td>37.7</td>
<td>3m 29s</td>
<td>top</td>
</tr>
</tbody>
</table>

Historic information is available per minute for the last 60 minutes, per hour for the last 24 hours, and per day for the last 10 days.
Links
Silver Peak documentation: http://silver-peak.com/Support/user_docs.asp

Dell AppAssure documentation: http://docs.appassure.com


Using Group Policy Editor: http://support.microsoft.com/kb/307882