Dell AppAssure Core to Core Replication Configuration Guide for Silver Peak Velocity

Tech Note
Version 5
June 2014

Overview

This document describes the configuration of Dell AppAssure Core to Core Replication for use with Silver Peak Velocity Replication Acceleration (VRX). 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 VRX version 6.2 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 13.

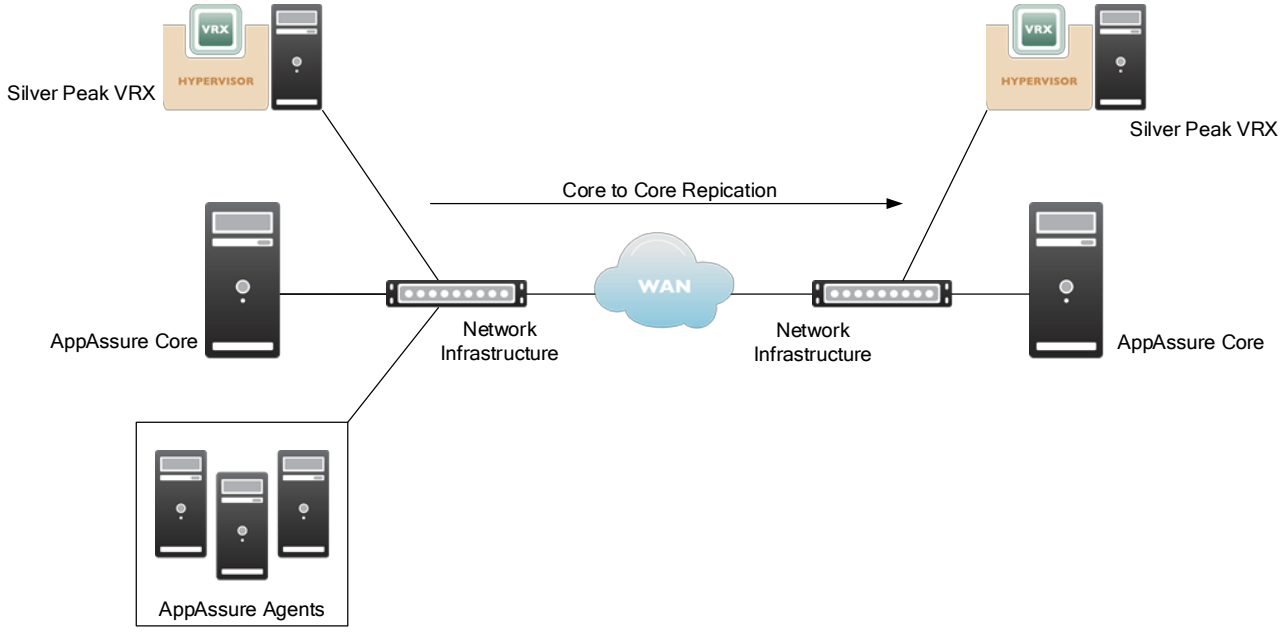
Configuration Steps

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

Topology Diagram

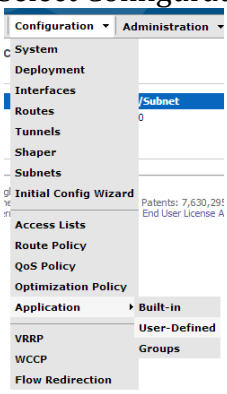


Create an Application Definition for AppAssure

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.



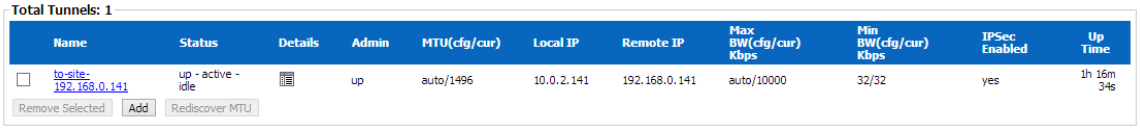
2. Click Add.
3. Use the following settings in the Add Application Rule dialog box. Unspecified fields do not need to be edited.
   Application: AppAssure
   Protocol: tcp
   Destination Port: 8006
4. Click Apply.

Changing the VRX tunnel mode to IPSEC

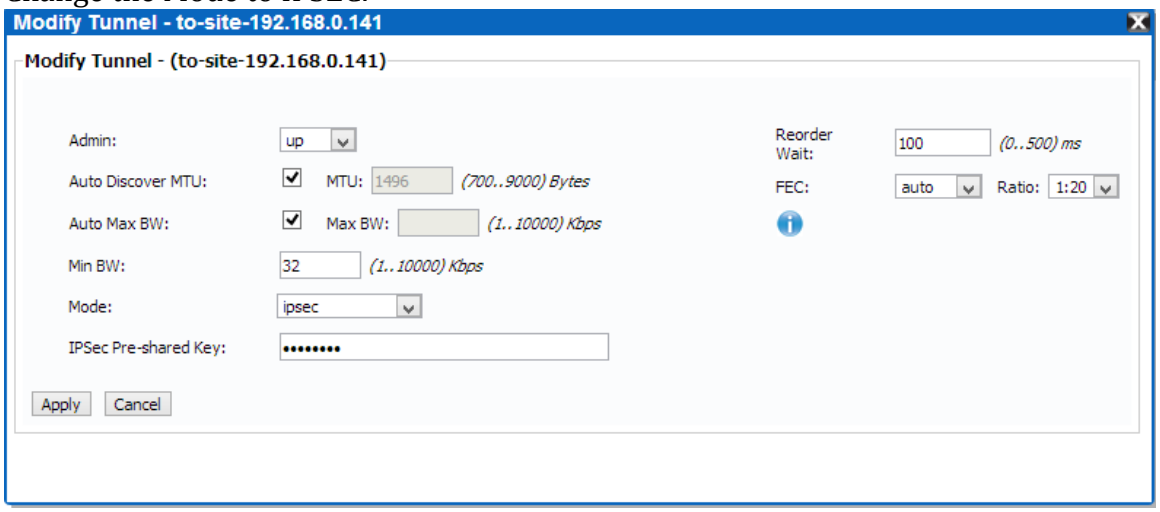
These steps must be completed on the source and destination Silver Peak VRX software instances.

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.

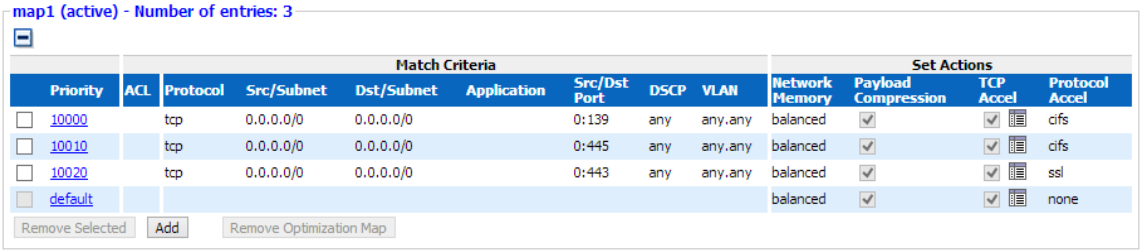


5. Set a pre-shared key. (this must be the same at both sites)
6. Click Apply.
7. Click the Save Changes button.

Creating an SSL Optimization Map for AppAssure

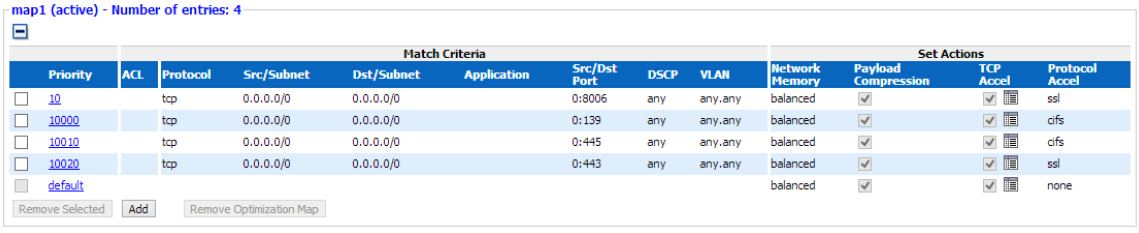
These steps must be completed on the source and destination Silver Peak VRX software instances.

1. Login to the VRX software instance using a web browser.
2. Select Configuration>Optimization Policy.
3. Click the Add button for the active map.



4. Use the following settings for the new optimization policy.

5. Verify that the new optimization policy is shown.

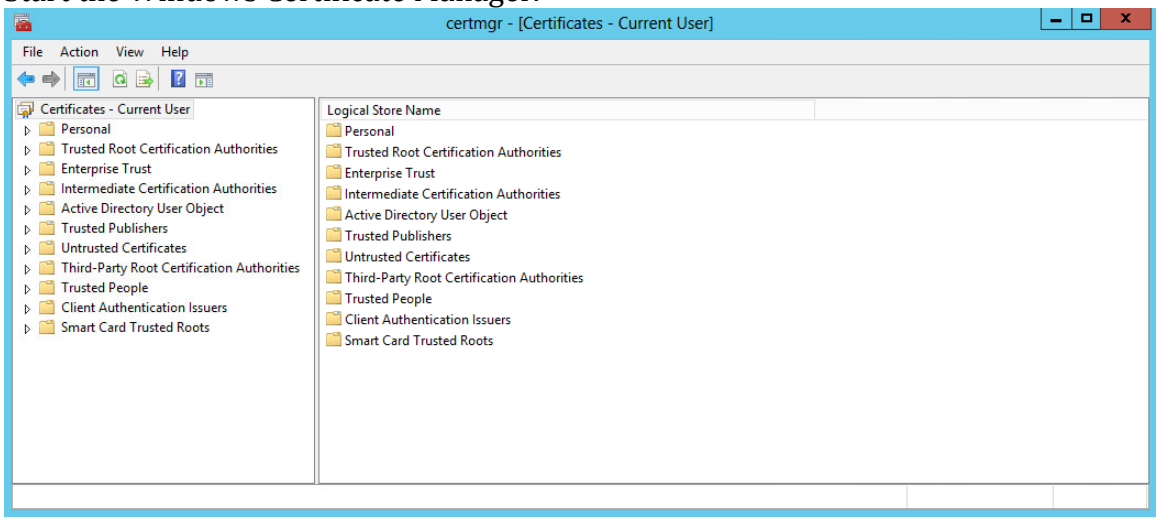


6. Click the Save Changes button.

Exporting the AppAssure Server Certificate

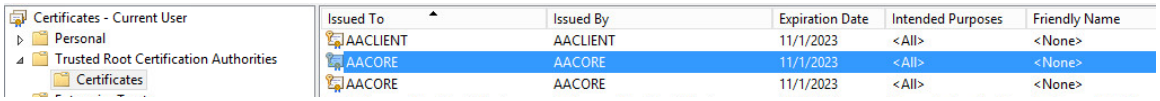
This step must be performed on the Windows Server that is the AppAssure Core replication target.

1. Log into the Windows Server that is running the AppAssure Core software.
2. Start the Windows Certificate Manager.

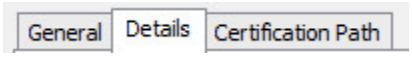


3. Expand Trusted Root Certification Authorities and select Certificates.

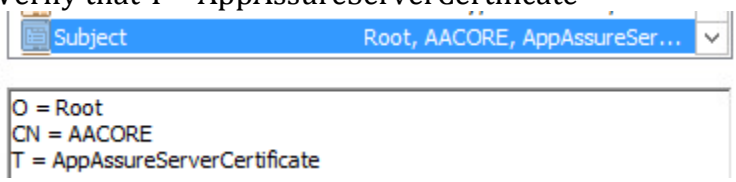
4. Select the first entry that matches the Windows Server name. In this example the Windows Server is named AACORE.



   a. Double click on the entry
   b. Select the Details tab

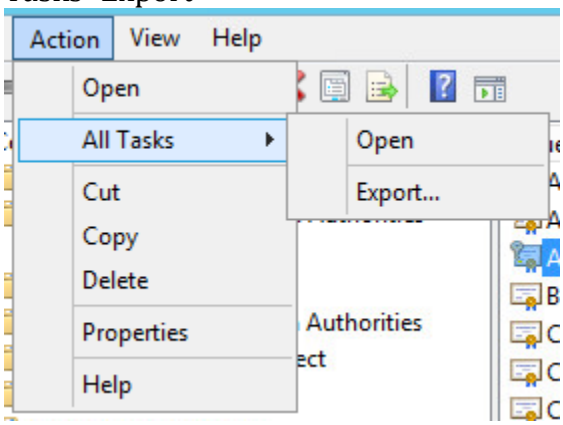


   c. Select Subject
   d. Verify that T = AppAssureServerCertificate

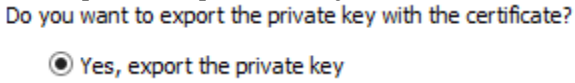


   e. If T = anything other than AppAssureServerCertificate, select each certificate that matches the Windows Server name until the Subject T = AppAssureServerCertificate

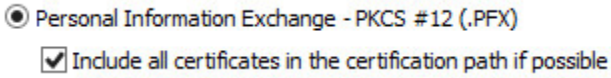
5. After identifying the correct certificate select it and then go to Action>All Tasks>Export



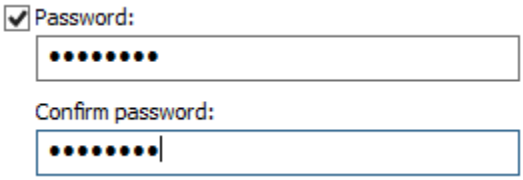
6. Complete the steps in the Certificate Export Wizard with the following options:
    a. Yes, export the private key



    b. Verify that Include all certificates in the certification path if possible is checked



    c. Enter the same password into both fields. This password will be used during the import process in the VRX software.



    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.

Loading the Certificate into the VRX Software

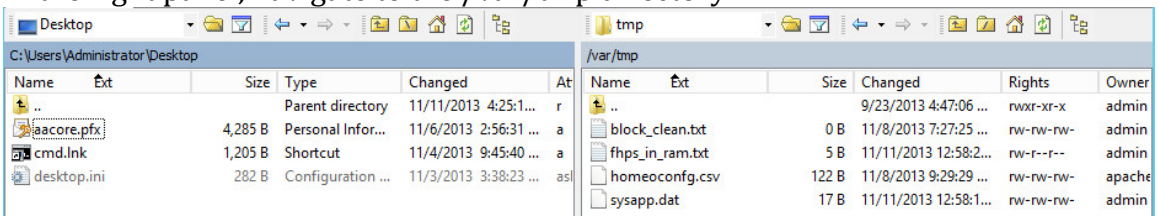
Note that these steps must be completed on each Silver Peak VRX software instance that will be accelerating AppAssure replication.

These steps also require the use of additional software tools to copy the certificates and load them into the VRX software. This guide uses WinSCP and PuTTY.

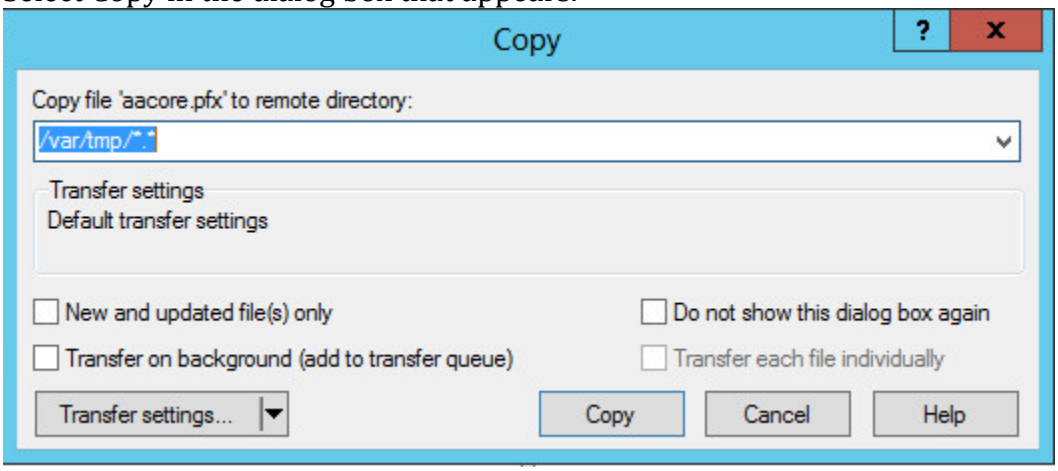
WinSCP can be downloaded from: http://winscp.net/eng/index.php

PuTTY can be downloaded from:
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

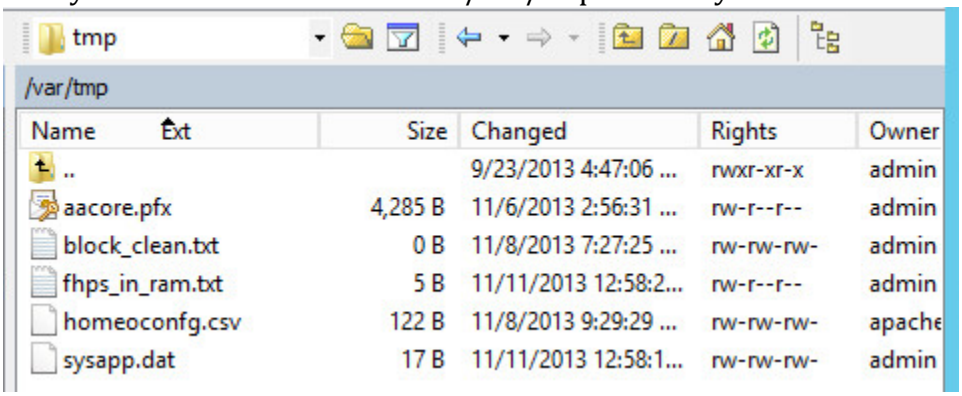
1. Use WinSCP to copy the certificate into the VRX software.
    1. Open WinSCP and select SFTP for the file protocol.
    2. Enter the IP Address of the VRX software into the Host name field.
    3. Enter the admin user name and password for the VRX software.
    4. Click Login.
    5. In the left panel, navigate to the location where the server certificate was saved in the previous step.
    6. In the right panel, navigate to the /var/tmp directory.



    7. To copy the certificate, drag it from the left panel to the right panel.
    8. Select Copy in the dialog box that appears.



9. Verify that the certificate is in the /var/tmp directory.



10. Close WinSCP.

2. Use PuTTY to load the certificate into the VRX software.
    1. Open PuTTY and select SSH for the connection type.
    2. Enter the IP Address of the VRX software into the Host Name field and click Open.
    3. Log in to the VRX software as Admin.
    4. Type `enable` at the command prompt and hit enter.
    5. Type `conf t` at the command prompt and hit enter.

```
Last login: Fri Nov  8 23:53:22 2013
VRX-2-Primary > enable
VRX-2-Primary # conf t
VRX-2-Primary (config) #
```

    6. Enter the following command at the command prompt replacing ***** with the password that was used to export the certificate from the Windows Server, aacore with the certificate name: `ssl host-certificate install pfx-file /car/tmp/aacore.pfx mac-password ***** crypt-password *****`
    7. Verify that the certificate loaded correctly with the following command: `ssl host-certificate list`

```
VRX-2-Primary (config) # ssl host-certificate list
Issuer: AACORE
Subject: AACORE
Valid from: Nov  1 21:24:41 2013 GMT
Valid to: Nov  1 21:24:41 2023 GMT
```

    8. Type exit and close PuTTY.

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.

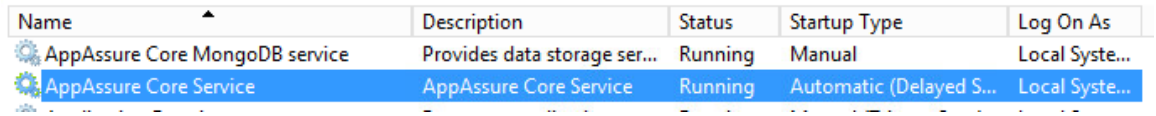
For more information on Windows static routes use this link:
http://technet.microsoft.com/en-us/library/cc757323(v=ws.10).aspx

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

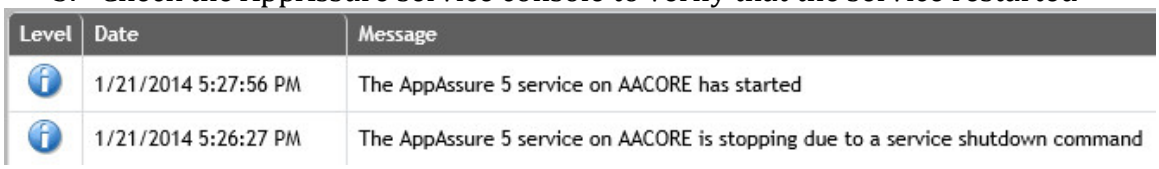
The final step is to restart the AppAssure Core Service on the replication target server. Restarting the service allows the Silver Peak software to accelerate the AppAssure replication traffic.

1. Open the services manager
2. Right click the AppAssure Core Service and select restart



Name	Description	Status	Startup Type	Log On As
AppAssure Core MongoDB service	Provides data storage ser...	Running	Manual	Local Syste...
AppAssure Core Service	AppAssure Core Service	Running	Automatic (Delayed S...	Local Syste...

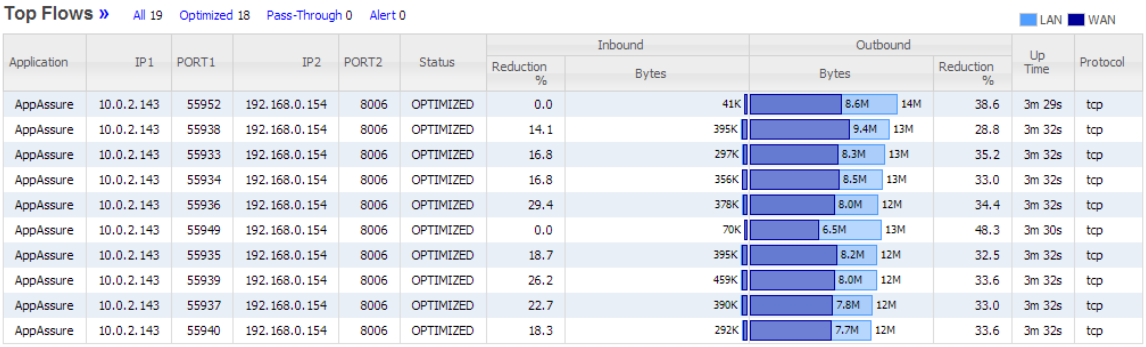
3. Check the AppAssure service console to verify that the service restarted



Level	Date	Message
	1/21/2014 5:27:56 PM	The AppAssure 5 service on AACORE has started
	1/21/2014 5:26:27 PM	The AppAssure 5 service on AACORE is stopping due to a service shutdown command

Am I Accelerated?

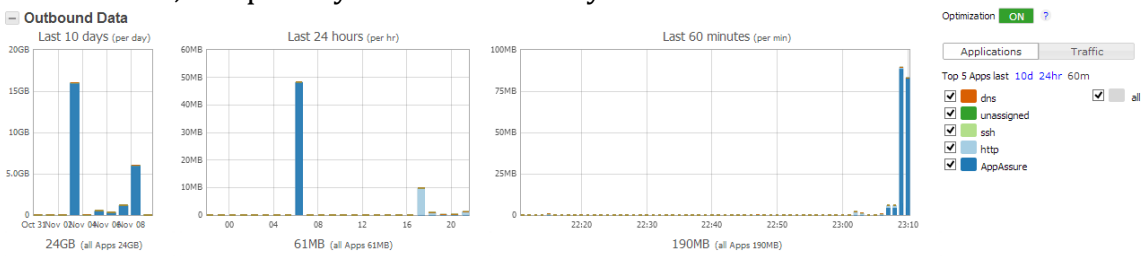
To determine if the Silver Peak software is working, login to the source side VRX software and select the Data View. For each replication pair there will be an entry under Top Flows listing the IP Addresses of the filer pair. This entry displays the Up Time for the connection, the status (it should read 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.

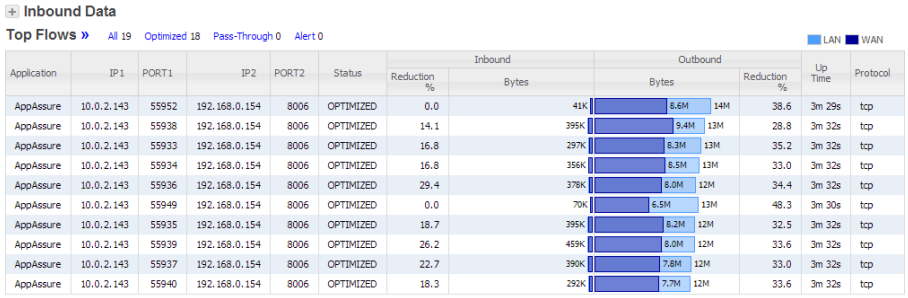


Top Flows » All 19 Optimized 18 Pass-Through 0 Alert 0 — LAN WAN

Application	IP1	PORT1	IP2	PORT2	Status	Inbound		Outbound		Up Time	Protocol
						Reduction %	Bytes	Bytes	Reduction %		
AppAssure	10.0.2.143	55952	192.168.0.154	8006	OPTIMIZED	0.0	41K	8.6M 14M	38.6	3m 29s	tcp
AppAssure	10.0.2.143	55938	192.168.0.154	8006	OPTIMIZED	14.1	395K	9.4M 13M	28.8	3m 32s	tcp
AppAssure	10.0.2.143	55933	192.168.0.154	8006	OPTIMIZED	16.8	297K	8.3M 13M	35.2	3m 32s	tcp
AppAssure	10.0.2.143	55934	192.168.0.154	8006	OPTIMIZED	16.8	356K	8.5M 13M	33.0	3m 32s	tcp
AppAssure	10.0.2.143	55936	192.168.0.154	8006	OPTIMIZED	29.4	378K	8.0M 12M	34.4	3m 32s	tcp
AppAssure	10.0.2.143	55949	192.168.0.154	8006	OPTIMIZED	0.0	70K	6.5M 13M	48.3	3m 30s	tcp
AppAssure	10.0.2.143	55935	192.168.0.154	8006	OPTIMIZED	18.7	395K	8.2M 12M	32.5	3m 32s	tcp
AppAssure	10.0.2.143	55939	192.168.0.154	8006	OPTIMIZED	26.2	459K	8.0M 12M	33.6	3m 32s	tcp
AppAssure	10.0.2.143	55937	192.168.0.154	8006	OPTIMIZED	22.7	390K	7.8M 12M	33.0	3m 32s	tcp
AppAssure	10.0.2.143	55940	192.168.0.154	8006	OPTIMIZED	18.3	292K	7.7M 12M	33.6	3m 32s	tcp

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.





Inbound Data

Top Flows » All 19 Optimized 18 Pass-Through 0 Alert 0 — LAN WAN

Application	IP1	PORT1	IP2	PORT2	Status	Inbound		Outbound		Up Time	Protocol
						Reduction %	Bytes	Bytes	Reduction %		
AppAssure	10.0.2.143	55952	192.168.0.154	8006	OPTIMIZED	0.0	41K	8.6M 14M	38.6	3m 29s	tcp
AppAssure	10.0.2.143	55938	192.168.0.154	8006	OPTIMIZED	14.1	395K	9.4M 13M	28.8	3m 32s	tcp
AppAssure	10.0.2.143	55933	192.168.0.154	8006	OPTIMIZED	16.8	297K	8.3M 13M	35.2	3m 32s	tcp
AppAssure	10.0.2.143	55934	192.168.0.154	8006	OPTIMIZED	16.8	356K	8.5M 13M	33.0	3m 32s	tcp
AppAssure	10.0.2.143	55936	192.168.0.154	8006	OPTIMIZED	29.4	378K	8.0M 12M	34.4	3m 32s	tcp
AppAssure	10.0.2.143	55949	192.168.0.154	8006	OPTIMIZED	0.0	70K	6.5M 13M	48.3	3m 30s	tcp
AppAssure	10.0.2.143	55935	192.168.0.154	8006	OPTIMIZED	18.7	395K	8.2M 12M	32.5	3m 32s	tcp
AppAssure	10.0.2.143	55939	192.168.0.154	8006	OPTIMIZED	26.2	459K	8.0M 12M	33.6	3m 32s	tcp
AppAssure	10.0.2.143	55937	192.168.0.154	8006	OPTIMIZED	22.7	390K	7.8M 12M	33.0	3m 32s	tcp
AppAssure	10.0.2.143	55940	192.168.0.154	8006	OPTIMIZED	18.3	292K	7.7M 12M	33.6	3m 32s	tcp

Links

Silver Peak documentation: http://silver-peak.com/Support/user_docs.asp

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

Microsoft documentation on static routes: http://technet.microsoft.com/en-us/library/cc757323(v=ws.10).aspx

PuTTY download link: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

WinSCP download link: http://winscp.net/eng/index.php

Managing certificates in Windows Server 2008: http://technet.microsoft.com/en-us/library/cc754841.aspx