



Installation Guide for Wireshark VM

Table of Contents

Introduction	2
Scope and Purpose	2
Architecture Overview.....	2
Wireshark VM setup	2
Starting Capture from Uila UI	3
Viewing the packet capture in Wireshark VM.....	5
Contact Uila Support	10
About Uila.....	10

Introduction

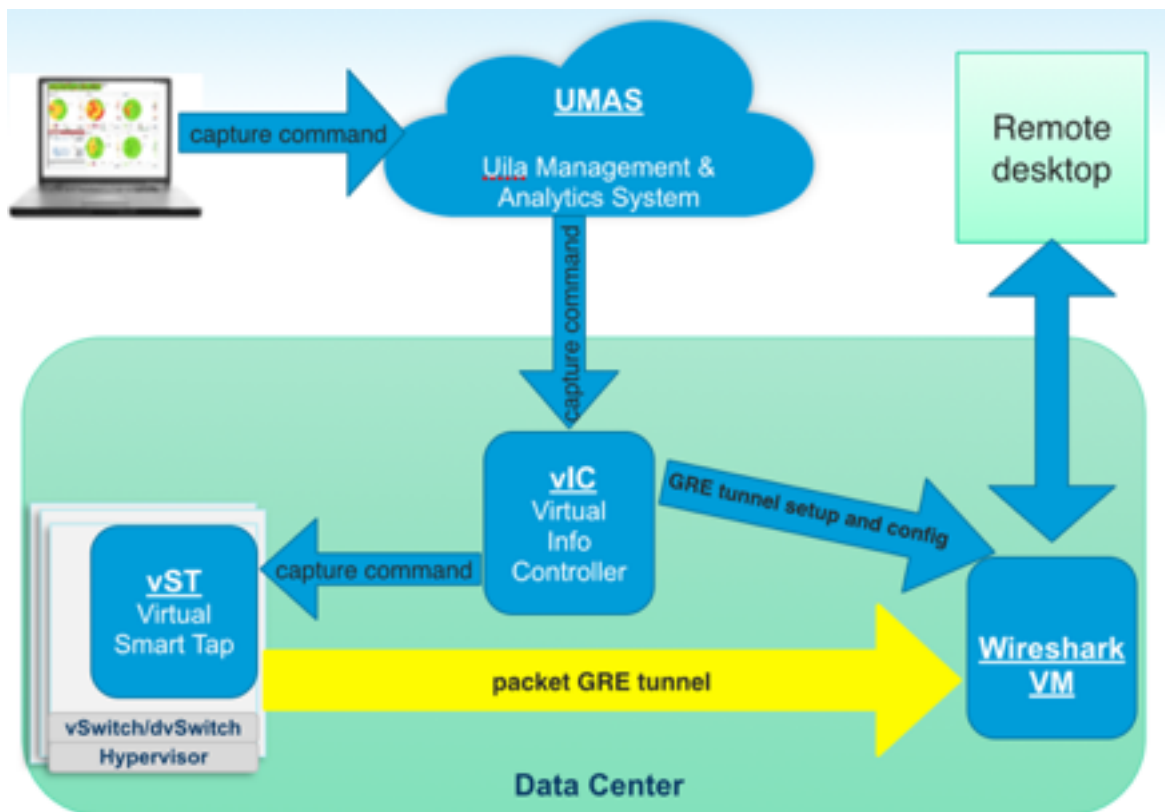
Scope and Purpose

This document describes the installation of the Uila Wireshark VM.

It is assumed that the reader has already installed the Uila software with the UMAS, VIC and vST's

Architecture Overview

The diagram below shows the architectural overview of the Uila Wireshark VM.



Wireshark VM setup

Download the Wireshark VM (OVA file) and deploy it–

<http://site2.uila.com/download/current/Uila-Wireshark-Viewer.ova>

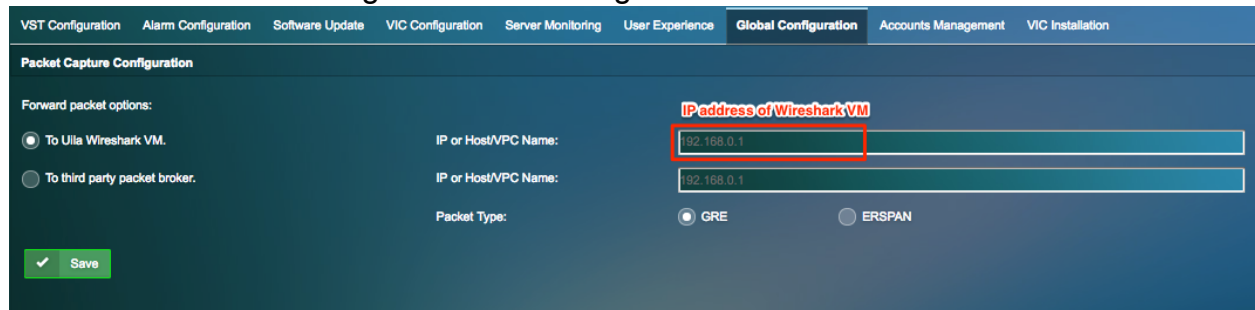
Download username/password: (please contact Uila Support)

Wireshark VM deployment requirements:

- 1 static IP address.
- 1 vCPU
- 2 GB Memory
- 16 GB Storage
- Thin provision
- Sit in the same DC as UMAS and vIC
- Select a port group with IP connectivity with UMAS and vIC

Enter the IP of the Wireshark VM for the destination of the GRE tunnel between Uila VSTs and the Wireshark VM –

- On the Uila UI
 - Go to settings → Global config



- Uila will be using 'GRE' as the default tunnel protocol

Starting Capture from Uila UI

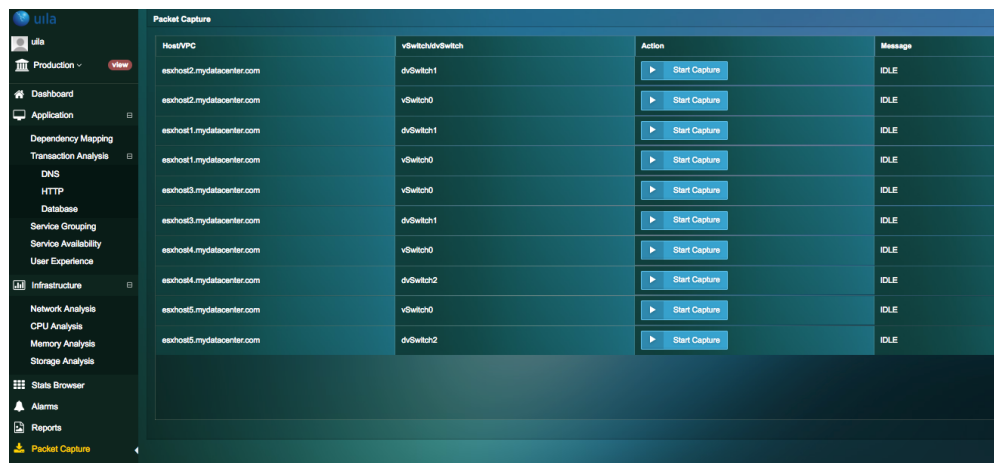
How to capture all traffic on a VM:

Note: the VM has to be monitored by a VST




- click a VM on color wheels or table views to see the tooltip with "Start Capture" as an option.
- click "Start Capture"



- If you want to capture for the entire host by switch
 - On the Uila UI
 - Go to Packet Capture
 - Select the host you would like to capture packet
 - Make sure to Stop Capture when not needed

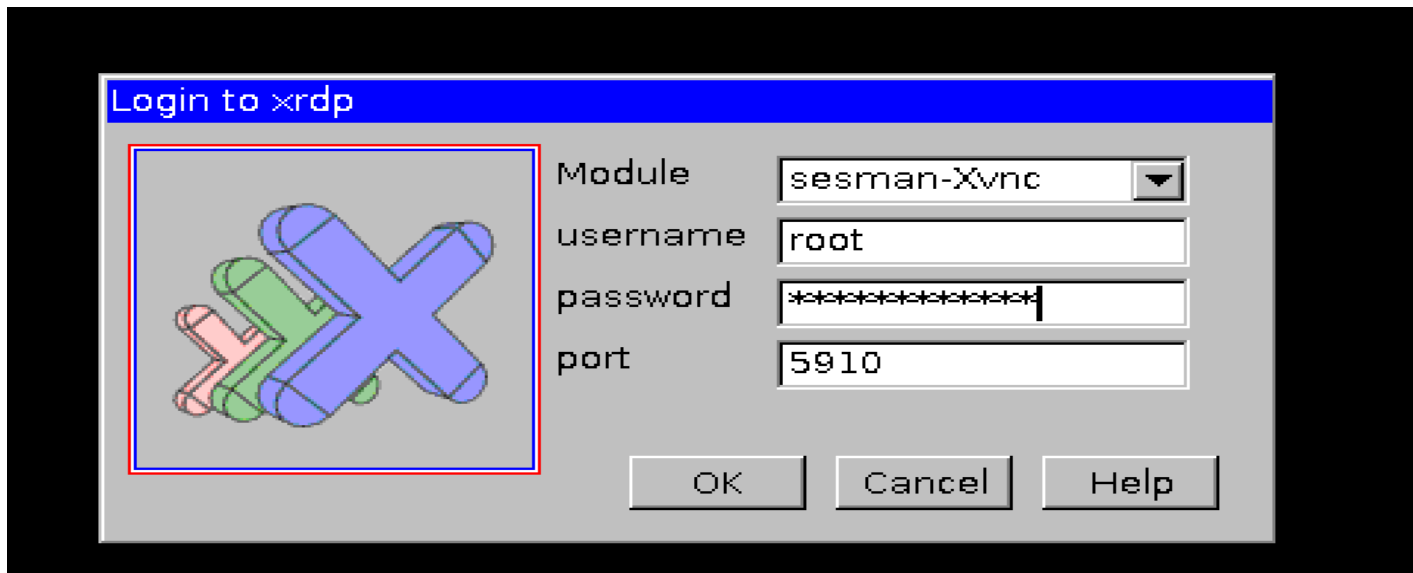


- Wait until the Capture is started and you will see the adapter name that is created, here is it called 'greVST.0.105'.

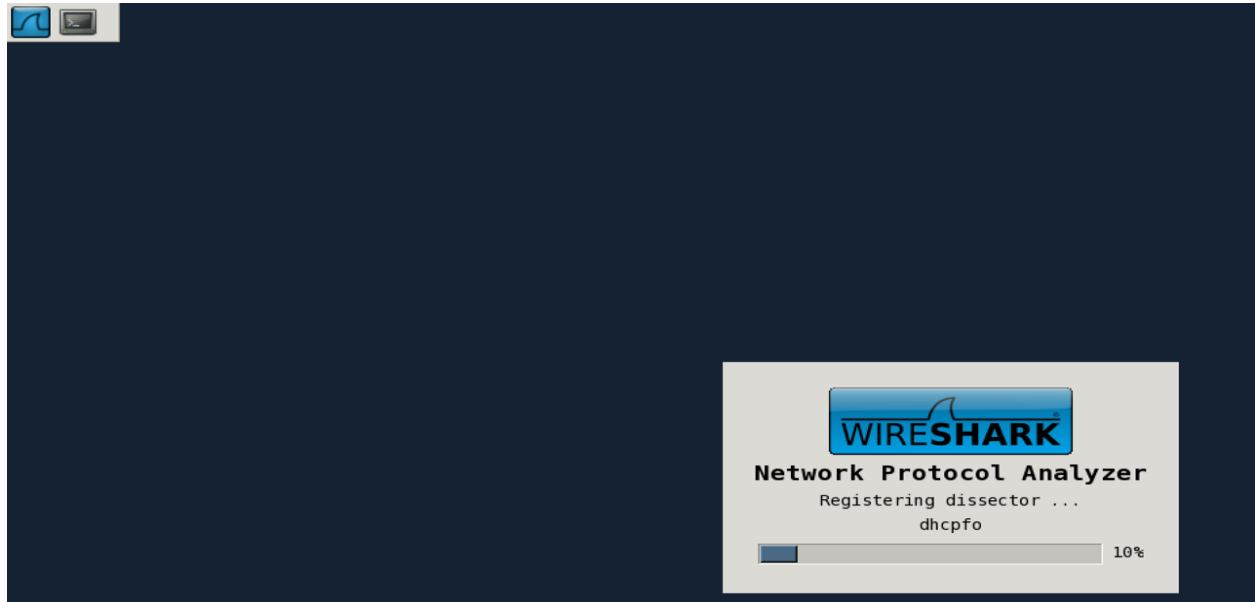
Packet Capture			
Host/VPC	vSwitch/dvSwitch	Action	Message
192.168.0.16	vSwitch0	 Start Capture	IDLE
192.168.0.15	vSwitch0	 Stop Capture	[greVST.0.105] Trans= 722 Trans dropped= 0 Filtered out= 0
192.168.0.14	vSwitch0	 Start Capture	IDLE

Viewing the packet capture in Wireshark VM

- use a RDP application to access the Wireshark VM with root/uilanetworks
- use root/uilanetworks to login to xrdp
 - Note: enter '-1' as port for the first time login, enter '5910' for later login



- click the wireshark icon sitting on the desktop to launch wireshark application



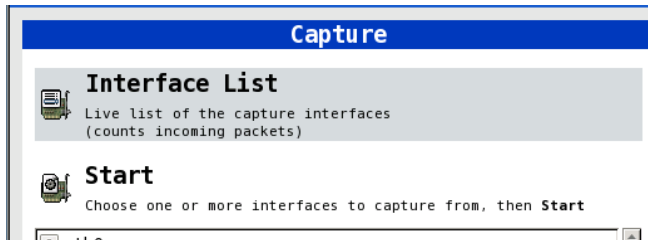
- select the vst interface named like gre.xxx(the last digit of a vst's IP address) to see packets captured by the vst.



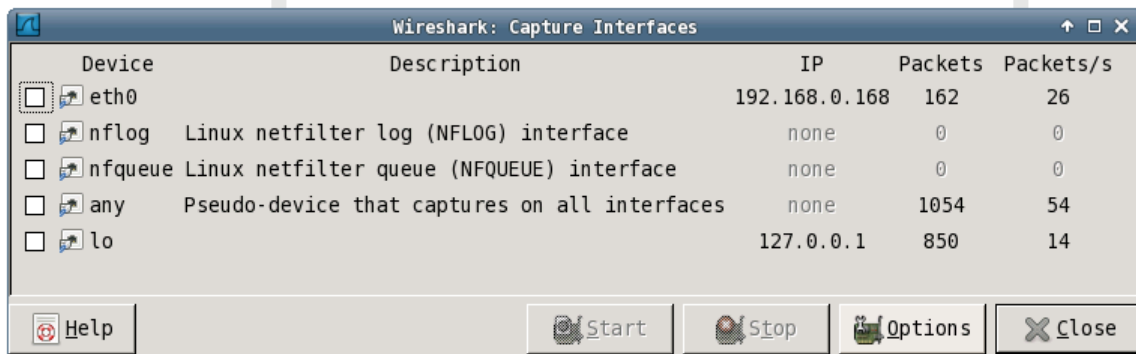
Refreshing Interface list

When Captures Start/Stop from different VSTs, the interface names (e.g. gre will change and will need to be refreshed to see the new list.

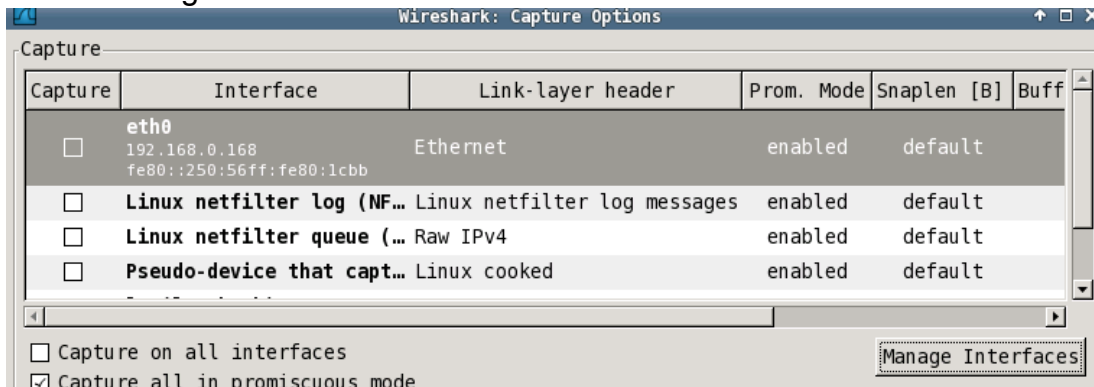
- Select Interface List

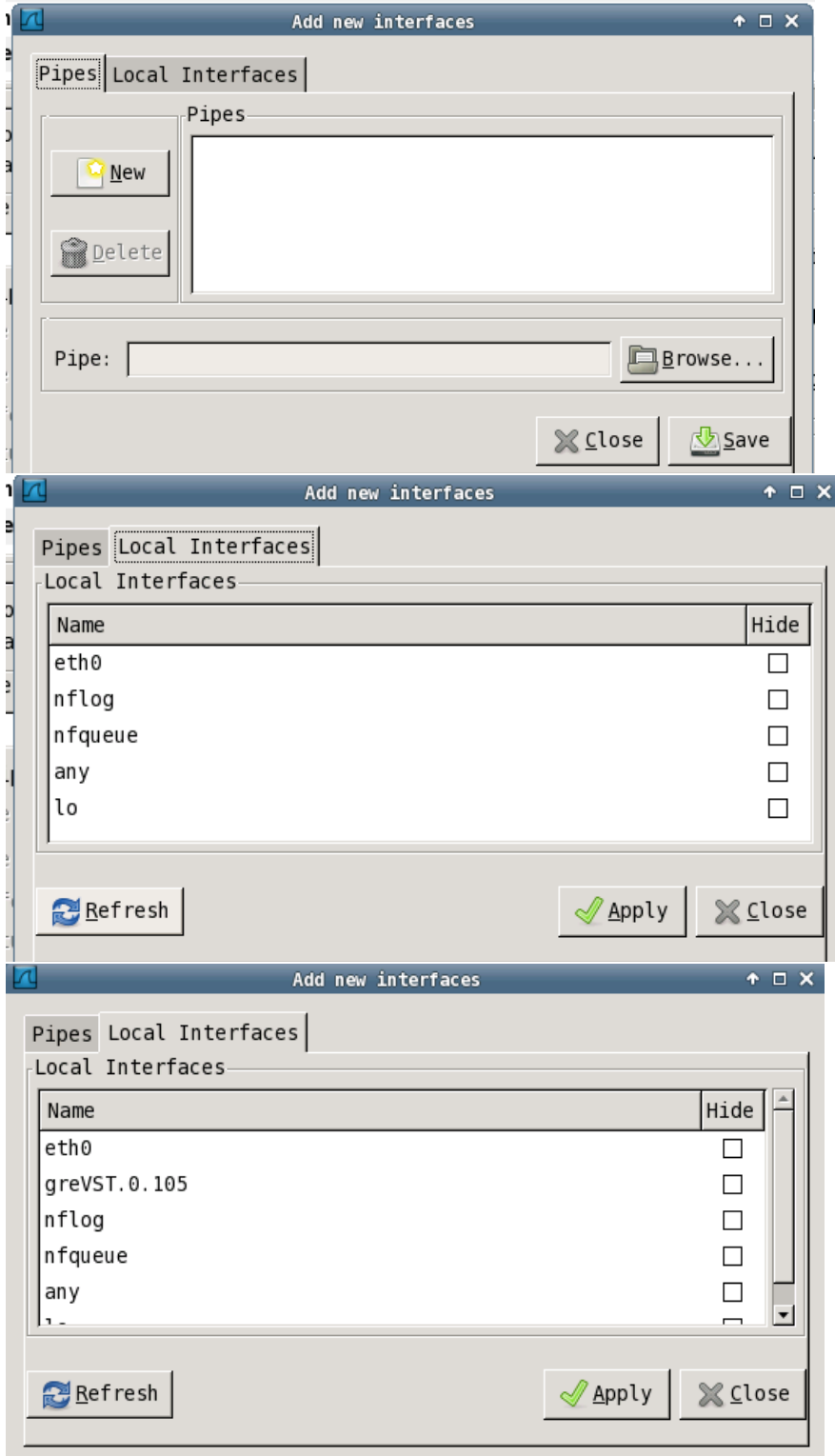


- Select Options

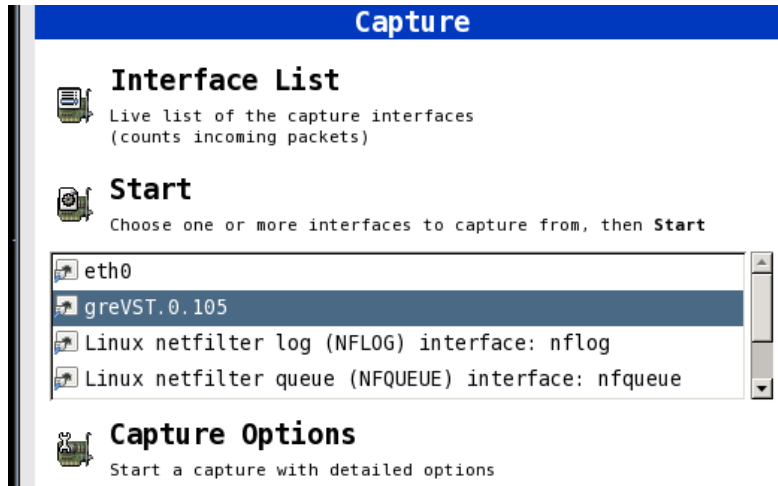


- Select Manage Interfaces >> Local Interfaces >> Refresh





- Now you can select the Interface greVST.x.x to Start capture



Contact Uila Support

Uila software solutions are designed with ease of installation and simplified maintenance in mind. The Uila team is dedicated to exceeding your expectations, and knows that any downtime is too much in today's competitive world. Our goal is to keep your applications running 24 X 7. We offer a simple and effective support program to meet your needs. Customers who purchased Uila products and under support contract will receive the following benefits:

- Unlimited support via email or phone call
- Free software minor release update
- Free software major release upgrade

Email: support@uila.com

Phone: (408) 819-0775

About Uila

Uila gives IT infrastructure teams x-ray vision for their data center operations and end user experience. Designed for Private, Public and Hybrid Cloud environments, Uila's Application-Centric Data Center Infrastructure Monitoring and Analytics provide instant visibility into hotspots and bottlenecks in any data center. Uila provides service dependency mapping, full stack correlation with 1-click root cause analysis and patented deep packet inspection technology that understands over 2,700 application protocols for transactional meta data analysis. Businesses use Uila to align themselves with their IT Operations team and cut time to resolution from days to minutes, keep their application at peak performance at all time and ensure end-user satisfaction to the fullest.