



uObserve™ Version 5.0 Release Notes
Release Notes –9/23/2022

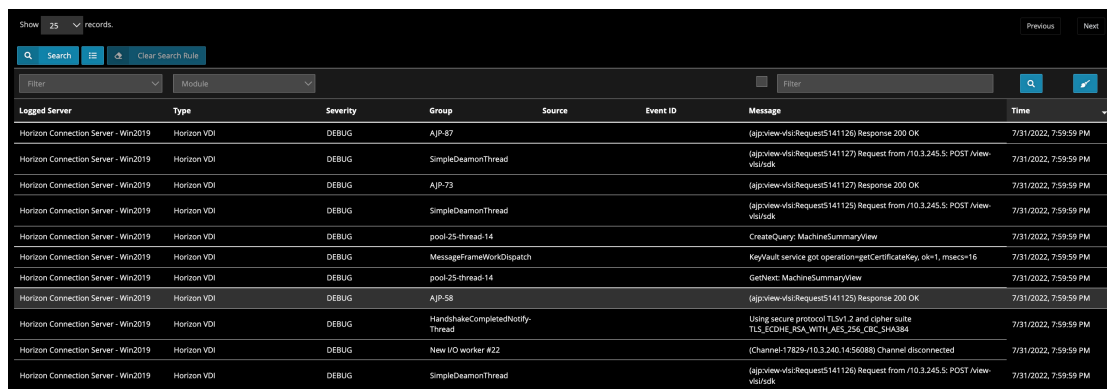
Table of Contents

New Features.....	2
Enhancements	5
Fixed Issues	8
Known Issues	8
Contact Uila Support	9
About Uila	9

New Features

- **Centralized Log Analysis**

With Uila uObserve, you now get instant and automated access to out-of-box correlated and contextualized logs from multiple systems including Windows (Event and Active Directory), IIS servers, Zscaler, Cisco, Barracuda, F5, Checkpoint, Juniper, etc. and applications like Microsoft SQL server, VMware Horizon, IBM MQ, Oracle, Office 365, and much more. Users are now powered with intelligent full-stack observability context in a unified console, that combines metric and log data to improve IT team efficiencies without the need to dig through logs in a separate tool and correlate with metric data.

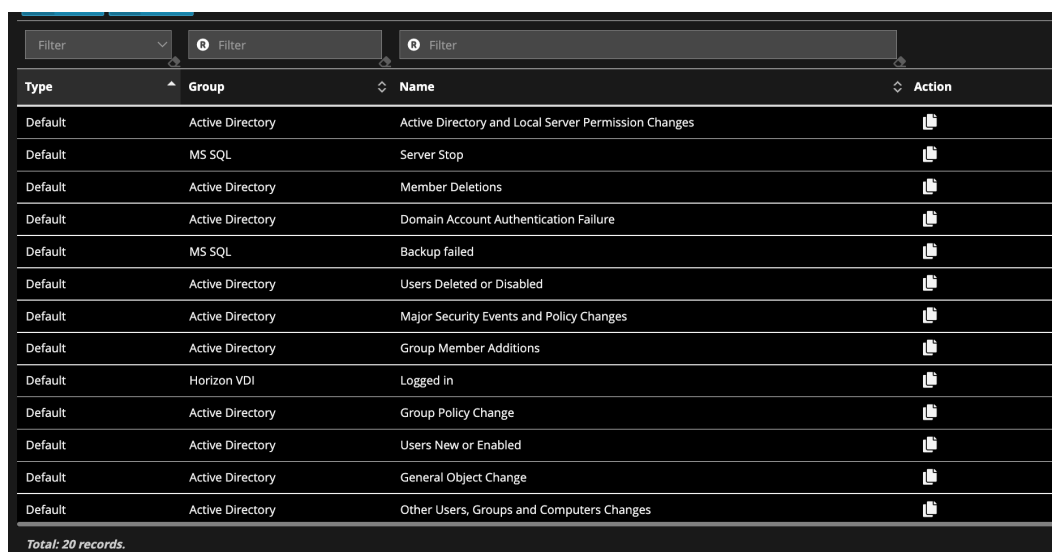















Logged Server	Type	Severity	Group	Source	Event ID	Message	Time
Horizon Connection Server - Win2019	Horizon VDI	DEBUG	AJP-87			(ajpview-vls/RequestS141126) Response 200 OK	7/31/2022, 7:59:59 PM
Horizon Connection Server - Win2019	Horizon VDI	DEBUG	SimpleDaemonThread			(ajpview-vls/RequestS141127) Request from /10.3.245.5: POST /view-vls/sdk	7/31/2022, 7:59:59 PM
Horizon Connection Server - Win2019	Horizon VDI	DEBUG	AJP-73			(ajpview-vls/RequestS141127) Response 200 OK	7/31/2022, 7:59:59 PM
Horizon Connection Server - Win2019	Horizon VDI	DEBUG	SimpleDaemonThread			(ajpview-vls/RequestS141125) Request from /10.3.245.5: POST /view-vls/sdk	7/31/2022, 7:59:59 PM
Horizon Connection Server - Win2019	Horizon VDI	DEBUG	pool-25-thread-14			CreateQuery: MachineSummaryView	7/31/2022, 7:59:59 PM
Horizon Connection Server - Win2019	Horizon VDI	DEBUG	MessageFrameWorkDispatch			KeyVault service got operation=getCertificateKey, ok=1, msec=16	7/31/2022, 7:59:59 PM
Horizon Connection Server - Win2019	Horizon VDI	DEBUG	pool-25-thread-14			GetNext: MachineSummaryView	7/31/2022, 7:59:59 PM
Horizon Connection Server - Win2019	Horizon VDI	DEBUG	AJP-58			(ajpview-vls/RequestS141125) Response 200 OK	7/31/2022, 7:59:59 PM
Horizon Connection Server - Win2019	Horizon VDI	DEBUG	HandshakeCompletedNotifyThread			Using secure protocol TLSv1.2 and cipher suite TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	7/31/2022, 7:59:59 PM
Horizon Connection Server - Win2019	Horizon VDI	DEBUG	New I/O worker #22			(Channel-17829-10.3.240.14:56088) Channel disconnected	7/31/2022, 7:59:59 PM
Horizon Connection Server - Win2019	Horizon VDI	DEBUG	SimpleDaemonThread			(ajpview-vls/RequestS141126) Request from /10.3.245.5: POST /view-vls/sdk	7/31/2022, 7:59:59 PM

Click here to get list of all modules supported by Uila's log analysis:

https://www.uila.com/download/document/508/Log_Modules_supported.pdf

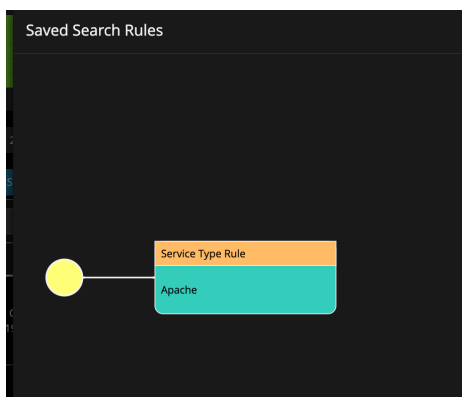
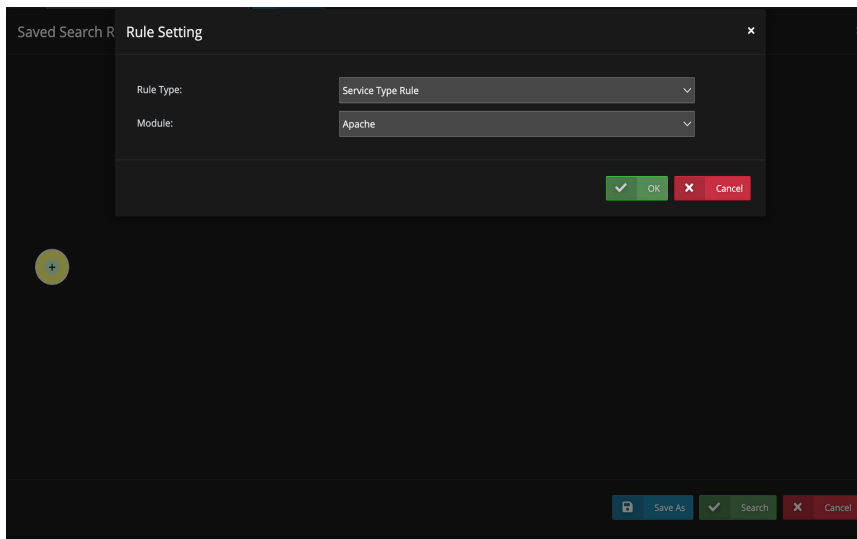
Users can perform contextualized querying and filtering within logs for accelerated troubleshooting and infrastructure management. User can choose from any of the 20 default log filters built inside.



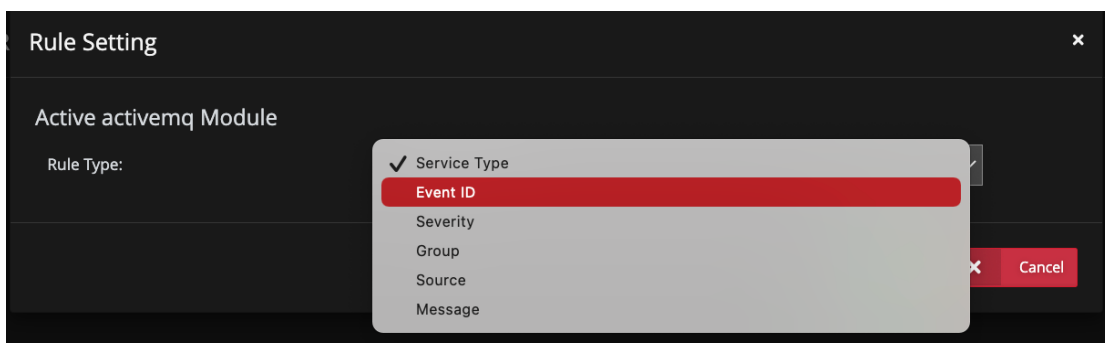
Type	Group	Name	Action
Default	Active Directory	Active Directory and Local Server Permission Changes	
Default	MS SQL	Server Stop	
Default	Active Directory	Member Deletions	
Default	Active Directory	Domain Account Authentication Failure	
Default	MS SQL	Backup failed	
Default	Active Directory	Users Deleted or Disabled	
Default	Active Directory	Major Security Events and Policy Changes	
Default	Active Directory	Group Member Additions	
Default	Horizon VDI	Logged in	
Default	Active Directory	Group Policy Change	
Default	Active Directory	Users New or Enabled	
Default	Active Directory	General Object Change	
Default	Active Directory	Other Users, Groups and Computers Changes	

Total: 20 records.

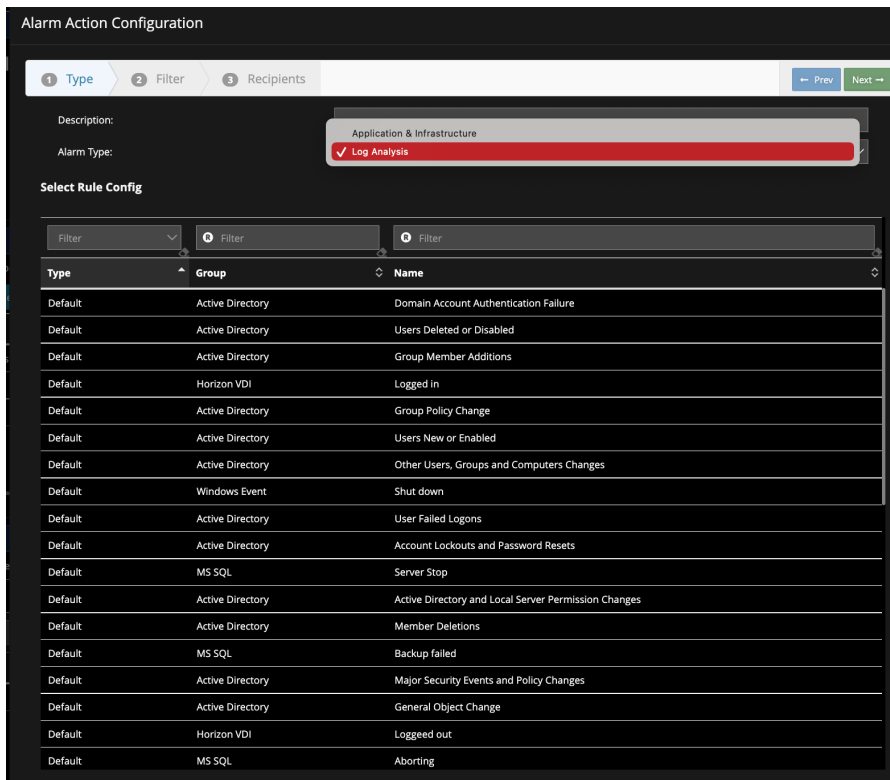
Or they can create their own custom filter using this custom wizard.



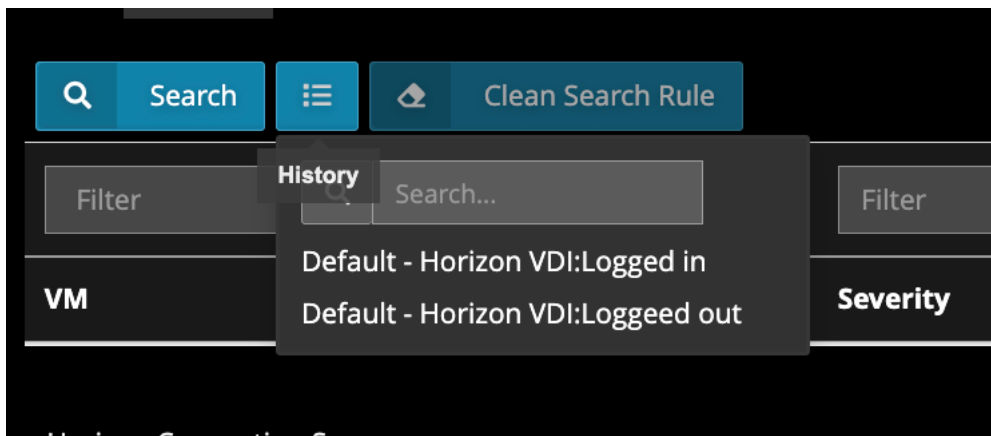
The rules can be customized for service type, event ID, severity, group, source or message rules.



Users can also get alert notification for the default and custom searches for log analysis that they have created.



Users can access the history and rechoose any of the previously used filters.



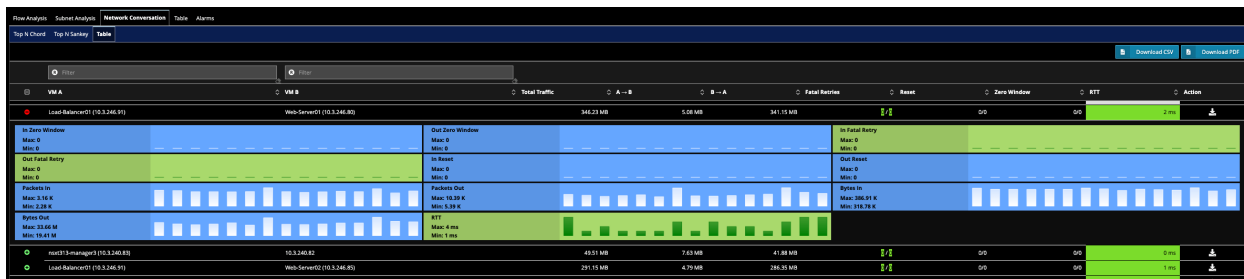
Note:

- Contact Uila sales or partner for regional licensing and pricing information for log analysis
- Refer to the new architecture diagram that includes log analysis, before using this feature: <https://www.uila.com/products/how-it-works>
- Refer to the new system requirements for the log database, before using this feature:

Enhancements

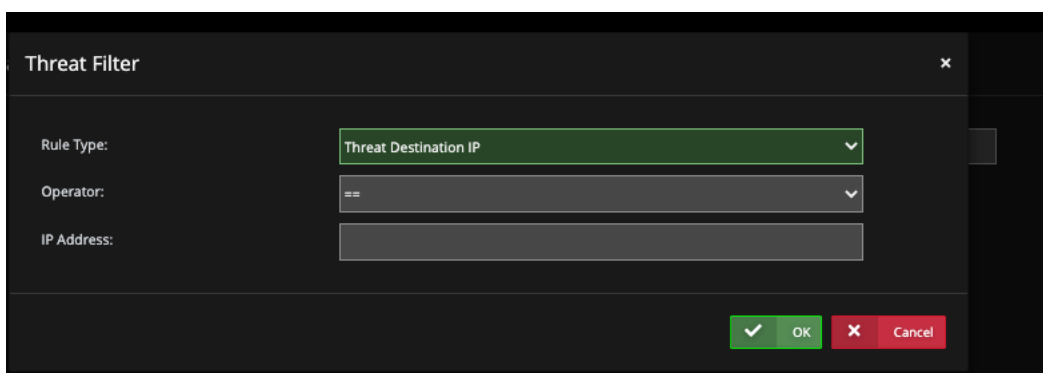
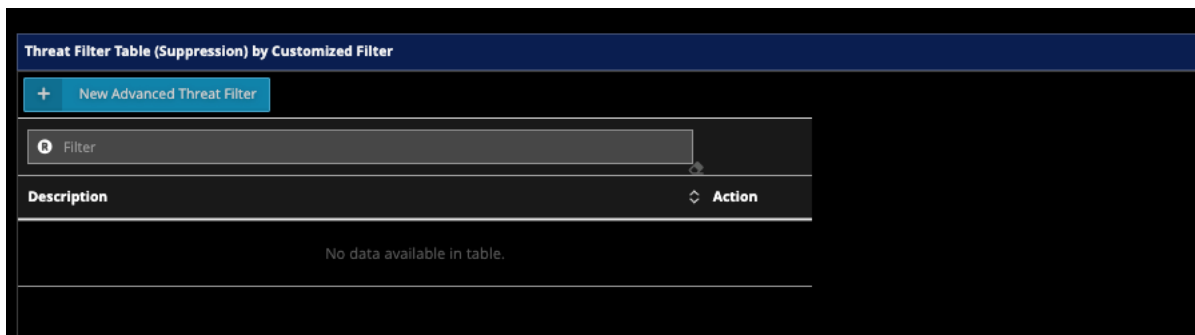
- **Trending charts for Network Conversations**

Users can now visualize trending charts for important network metrics for any Network Conversation. This is accessible from the table tab, and expanding the individual conversation.



- **Whitelist Cyber Threats**

In special cases, and organization may have requirements to whitelist cyber threats. With this new release, users have the option of doing that based on IP address, name, port, threat type, model, etc. This is accessible from the Security Configuration tab in the settings menu.



- **GMT time included in CSV exports**

With this new release, you can visualize the GMT time in the CSV exports from uObserve.

=K3/60/60/24/1000+DATE(1970,1,1)											
A	B	C	D	E	F	G	H	I	J	K	L
App Response Time	Client	Client IP	Client Port	Server	Server IP	Server Port	Service	Request	Reply	Time (in Linux format)	GMT Time
6615	Weblogic_11g-s2	192.168.1.180	43458	Oracle_11g-n4	192.168.1.121	3306	mysql	HERE id BETWEEN 650124-94210477185-06		1.64372E+12	2/1/22 1:23 PM
2520	Weblogic_11g-s2	192.168.1.180	43457	Oracle_11g-n4	192.168.1.121	3306	mysql	HERE id BETWEEN 15670 AND 15670+11099		1.64372E+12	2/1/22 1:19 PM
1151	Weblogic_11g-s2	192.168.1.180	43439	Oracle_11g-n4	192.168.1.121	3306	mysql	HERE id BETWEEN 40175 AND 40175+11099		1.64372E+12	2/1/22 1:06 PM
1123	Weblogic_11g-s2	192.168.1.180	43438	Oracle_11g-n4	192.168.1.121	3306	mysql	HERE id BETWEEN 28638-21036427522-8116		1.64372E+12	2/1/22 1:06 PM

- **Trending tooltips in email alert notifications**

With this new release, you can now visualize the actual values of the trending information in a tooltip. All you need to do is to hover the mouse over the specific bar in the trending chart in your email.

Monday, August 15, 2022 3:45:00 PM GMT-07:00 - Monday, August 15, 2022 4:00:00 PM GMT-07:00					
Severity	Entity Type	Entity	Stat Type	Baseline	Trending
Critical	VM	nsxt313-manager3	CPU Ready	5%	
Critical	VM	nsxt313-manager1	CPU Ready	5%	
Critical	VM	cp-parent-d25116c4-c677-457f-817d-d9f6304af183	Memory Usage	80%	
Critical	VM	cp-parent-75e89e8a-9e1a-448d-9306-291229622e19	Memory Usage	80%	
Critical	Disk	Nutanix2#scsi0_0	Write Latency	83ms	

- **Consolidated configuration for subnet information**

With this new release, users can consolidate configuration for subnet information for remote site end user experience, subnet to routed traffic analysis and physical device tracking. The subnet can be set from the VIC configuration within the settings menu. Once complete, you can import the pre-configured information into subnet configuration and end-user experience settings.


Manual Display External Device by IP/Subnet					
Cloud Type	Cluster/Region	Host/VPC	Prefix	Summary	Actions
Physical Server	ptense	ext4	ptense ip	192.168.1.124/32	
Physical Server	ext client	192.168.1.112	client-1.112	192.168.1.112/32	
Physical Server	San Jose	PhyServers	DB	192.168.1.132	
Physical Server	revtest	revtest	revtest	208.67.222.222/32,10.40.40.2/32	
Physical Server	test	FS-server	FS-server	11.66.11.22/32	
Physical Server	Test 123	Test 123	Test 123	10.3.252.10/32	
Physical Server	hyperv	hyperv03	hyperv	10.10.10.64/28	
Physical Server	hyperv	hyperv	Win2016	192.168.1.183/32	
Physical Server	LongCluster3	LongHost3	LongTest4	192.168.0.151/32	
Generic Cloud	test	uila.com	A ext AB test	38.99.127.1/24	
Physical Server	Long test	Long test	A Long VPN PC	192.168.0.209/32	
AWS	NAS718	host18	hhhh		
AWS	NAS78	host18	hhhh		
AWS	test	test	test	192.168.1.219/32	







Subnet Config		
+ New Subnet Import		
Subnet Name	Summary	Actions
Admin	172.17.0.0/16	Edit Delete
Dot 0 0 - 127	192.169.0.1/32	Edit Delete
Dot 1.x	192.168.1.0/23	Edit Delete

VST ConfigurationAlarm ConfigurationSoftware UpdateVIC ConfigurationSecurity ConfigurationDevice MonitoringServer Monitoring

User Experience Config

+New Site

Import

Site Name	Summary	Actions
11	192.168.2.1/25	 
Dot 0 0 - 127	192.168.0.1/25	 
Dot 0 192 - 195	192.168.0.192/30	 

Import	
Total Selected: 0 selected.	
Select All Deselect All	
<input type="text" value="Filter"/>	
Prefix	Summary
<input type="checkbox"/> est	235.23.2.232/32,185.198.26.172/32,98.137.246.8/32
<input type="checkbox"/> test	1.3.4.2/32,206.55.191.142/32
<input type="checkbox"/> W	10.1.1.1/32
<input type="checkbox"/> SMB Server	192.168.0.8/32
<input type="checkbox"/> cook client	10.128.31.83/32
<input type="checkbox"/> pfsense ip	192.168.1.124/32
<input type="checkbox"/> client-1.112	192.168.1.112/32
<input type="checkbox"/> DB	192.168.1.1/32
<input type="checkbox"/> revtest	208.67.222.222/32,10.40.40.2/32
<input type="checkbox"/> F5-server	11.66.11.22/32

- **Hierarchy Threshold by VM settings**

With this new release, users can set thresholds for the filtered entities. You can access this from Settings→Alarm configuration.

Hierarchy Threshold Settings for VM

Host/VPC

Cluster/Region

Data Center

+ New

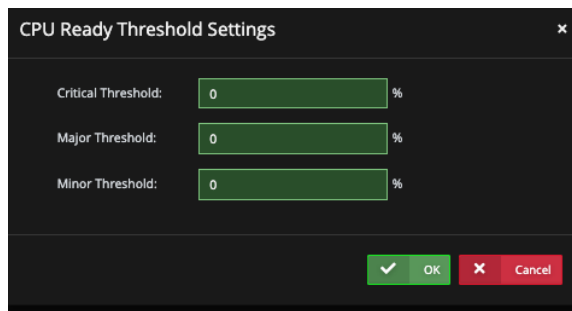
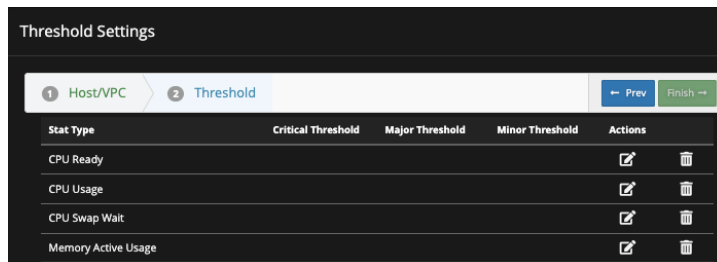
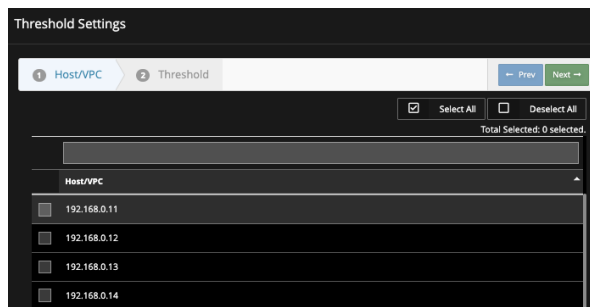
Delete All

Filter

Host/VPC

Action

192.168.0.11



Fixed Issues

1. Migration report would not work.
2. User defined application is showing up as “unknown” in the interface.
3. Email alerts may list a minor alert, but the baseline in report is at a different level
4. Missing values in alert emails.
5. SNMP configuration is missing port related configuration.
6. Wireshark support for Nutanix installations.

Known Issues

- Subnet Analysis: Usage Trending chart and the Conversation table data may not match under certain conditions.
- Process-level Monitoring on Uila iST cannot be controlled by Uila UI. Work around includes using command line interface for controls.
- In Stats Map, the service name maybe hidden behind the icons.
- In End User Experience, the site name maybe cut-off in the drop-down box.
- You may get errors while obtaining the UMAS logs, when switching to another page before all the logs are downloaded. The workaround is to wait until the download is complete.
- Bookmark may not display the image.



- Monthly scheduling of health overview report may fail.
- Exporting of application transactions is limited to only 2000 records.

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:

- 24 X 7 support
- Unlimited support via email or phone call
- Free software minor release update
- Free software major release upgrade

Email: support@uila.com

Phone: +1-(408) 400-3706

About Uila

Uila resolves Complex IT Disruptions for Enterprise Organizations with its Intelligent Full-Stack Observability Platform, that correlates Application and Infrastructure Performance to isolate and remediate issues before business impact. With Uila, IT teams can visualize application workload dependencies across cloud platforms, rightsize infrastructure resources, troubleshoot disruptions for any onsite or remote VDI user due to application/network/infrastructure challenges, plan workload migration strategies for Cloud deployments and use AIOps to streamline troubleshooting and reduce MTTR with remediation actions. And most importantly, this is done WITHOUT any agents. Uila also allows security teams to combat advanced cyber threats, by providing comprehensive application anomaly insights, cyber threats & Data Exfiltration activities. Organizations use Uila to align themselves with their IT teams and cut MTTR from days to minutes to always keep End-User Experience at peak performance & secure, across cloud boundaries.