



**Version 3.7**  
**Release Notes –10/30/2020**

---

**Table of Contents**

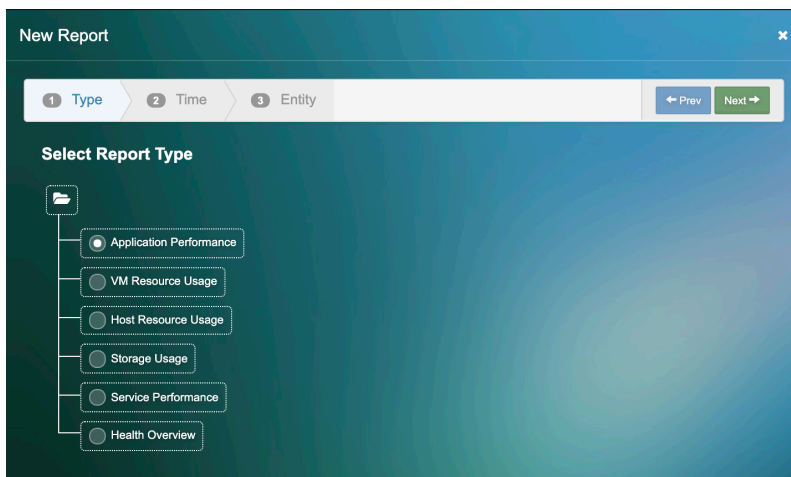
<b>New Features</b> .....	<b>2</b>
<b>Enhancements</b> .....	<b>2</b>
<b>Bug Fixes</b> .....	<b>5</b>
<b>Known Issues</b> .....	<b>5</b>
<b>Contact Uila Support</b> .....	<b>5</b>
<b>About Uila</b> .....	<b>6</b>

## New Features

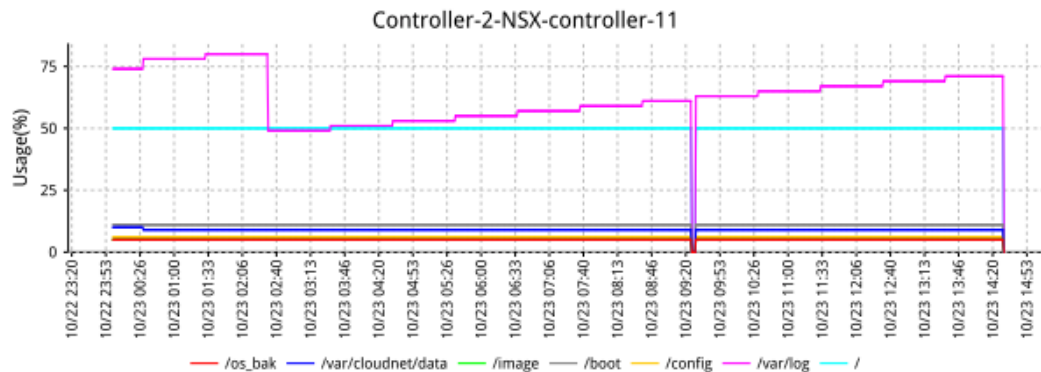
### Enhancements

- New Health Overview & Storage Usage Reports**  
 The Health Overview reports provide the overall health of your deployment as described in the Uila Dashboard. This includes Application Performance, Infrastructure Performance (Compute & Storage), Network Performance and Performance for your mission-critical Service Groups.

While the Storage Usage report, provides details on disk usage trends.



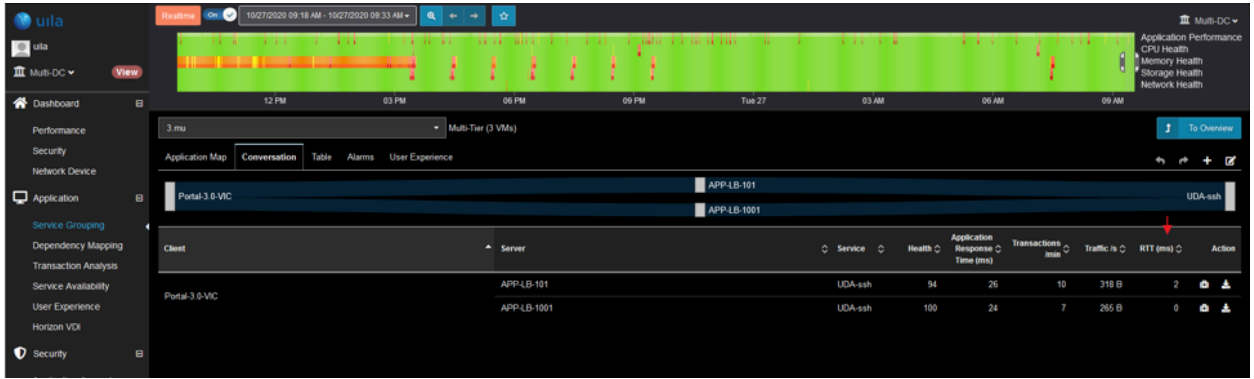
Health Overview Report		2020/09/03--2020/10/19				
Application Performance						
VM Name	Health	ART(ms)	Transactions/m	Traffic/s	Packets/s	
VCSA-7.0	94	1324	7	1001 B	1	
InstantClone-2	98	328	3	557 B	0	
Horizon-View-ConnectionServer-Windows2016	98	136	43	1.86 KB	4	
VMware vCenter Server Appliance	99	202	117	15.06 KB	18	
Gateway [192.168.0.1]	99	30	40	3.18 KB	5	
SMB Server (192.168.0.8)	100	1	2	20 B	0	
umas (38.99.127.23)	100	9	1	300 B	0	
LongTest3 (192.168.1.152)	100	16	1	33.62 KB	32	
InstantClone-1	100	32	0	524 B	0	



- Country information and Detailed Transaction Analysis for Cyber Threat Alerts**  
 Users can now visualize country name for source/destination for any cyber threat. You can also get transaction analysis details for HTTP, DNS and DB related to the alarm.

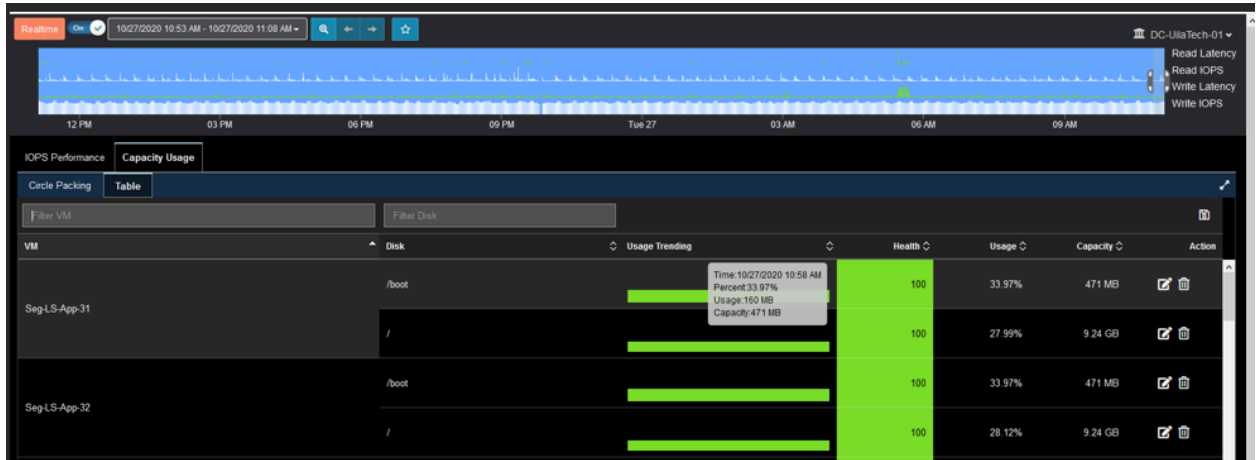
Threat Severity	Threat Model	Threat Type	Threat Source	Country	Threat Destination	Country	Event Count	Action
High	Web Application Attack	ET_SCAN Possible Nmap User-Agent Observed (1-2024364)	Portal-3 0-VIC (192.168.0.194-59564)	United States	WebServer01 (192.168.0.37-80)	United States	34	[Action]
High	A Network Trojan was Detected	ET_TROJAN ELF/muBoT_IRC Activity 4 (1-2021915)	Centos8-VIC (192.168.1.193-9001)	United States	192.168.0.104 (192.168.0.104-38046)	United States	169	[Action]
High	Potentially Bad Traffic	BAD-TRAFFIC same SRC/DST (1-527)	0.0.0.0 (0.0.0.0-68)	United States	255.255.255.255 (255.255.255.255-67)	United States	584	[Action]

- New Applications and Protocols Supported**  
 This release includes support for over 16 new application and protocol classification including Microsoft Dynamics 365, Siemens Apogee, Toyo PLC protocol, Schneider Integrated Object Network (SCADA), Yokogawa's control communication network, Acronis Cloud, Multicast DNS, Siemens Apogee for Building Automation, Fanuc equipment, Keyence Barcode scanners and many more. Access the supported list from: <https://www.uila.com/resources/documentation>
- Visualize RTT in conversation analysis chart in Service Grouping.**  
 Users can now visualize RTT in the conversation analysis charts for their multi-tier application groups.



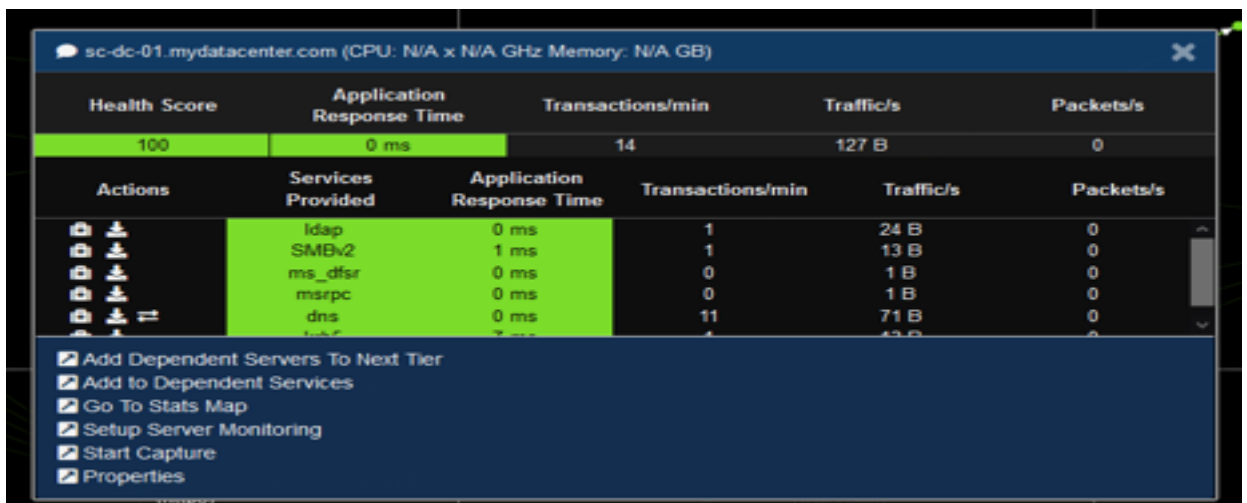
- **Disk usage trends**

With this release, Uila users can visualize disk usage trends in the Capacity Usage tab in Storage monitoring.



- **Display SMB version in protocol name**

Starting with this release, you can now visualize the version for the SMB protocol.



- **Visualize Nutanix storage statistics when used in Microsoft Hyper-v environments.**

## Bug Fixes

- In certain situations, network device monitoring may show incorrect utilization values and you may see duplicate ports on the stats map.
- Under certain circumstances, you may not be able to generate any reports.
- Incomplete topology queries and information.
- Wrong mapping between VM names and MAC address.
- In certain situations, Uila may fail to catch up with multiple vMotion events.
- Upper limit of 1000 when querying AD/LDAP users
- Cyber Threat Monitoring license warning messages even though module is not activated.
- Failed to pick up performance counters for Horizon virtual desktops when they are continuously removed and spawned.
- Filter by location does not work for Data exfiltration traffic.
- Network Device Monitoring in Uila shows Cisco UCS virtual ports.

## Known Issues

- In certain situations, Network Device monitoring may not list connected devices on certain ports.
- Certain Internet services may generate too many alerts.
- Cannot hold threshold adjustments for non-persistent Horizon Virtual Desktop VMs.
- ART threshold on a group of VMs may not work correctly.

## 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](mailto:support@uila.com)

Phone: (408) 819-0775



## About Uila

Uila provides Performance and Cyber Threat Analytics in a single pane of glass for the Hybrid Enterprise. With Uila, IT Operations teams can visualize application workload dependencies across cloud platforms, right-size resources and investments for their workloads and plan workload migration strategies for Hybrid and Multi-Cloud deployments. Uila allows security teams to combat advanced cyber threats by providing immediate and comprehensive application-centric insight into lateral movement-based threats for the Hybrid Enterprise. Businesses use Uila to align themselves with their IT teams and cut time to resolution from days to minutes, keep their application at peak performance and secure at all times and ensure end-user satisfaction to the fullest across cloud boundaries.