

uObserve™

Intelligent Full-Stack Observability

1. Introduction	5
1.1. Scope and Purpose	5
1.2. Architecture Overview	5 6
1.2.1. Onlyied Central Management Console	
1.3. Feature Highlights	6
1.3.1. Multi-Cloud Architecture – Built for Multi-Cloud Data Center	6
1.3.2. Unified View – Simplify Data Center Operations	7
1.3.3. SaaS Cloud - Automation and Provisioning	7
2. Terminology Used	8
3. Icon Definitions	12
4. Getting Started	13
4.1. System Requirements	13
5. Baseline	21
5.1. Uila Baseline	21
5.2. Health Score and Alarm Definition	22
6. Managing Your Work from the Console Home Page	24
6.1. Tools Pane	24
6.2. Time Matrix Pane	25
6.3. Monitor Pane	27
6.4. Settings	/ 2
6.4.2. Accounts Management with SAMI	28 29
6.4.3. Accounts Roles	
6.4.4. Multi-tenant Roles for Service Grouping	32
6.4.5. Hierarchy Threshold Setting for VM	35
6.4.6. Threshold Setting	37
7. Dashboard	
7.1. Summary of Key Performance Index	40
7.2. Application Performance Metric	
7.3. Network Performance Metric	43
7.4. Storage Performance Metric	45 17
7.6. Memory Performance Metric	
9 Application	E A
8. Application	
8.1.1. Topology Map View	
8.1.2. Dependent Service View	55
8.1.3. Service Filter	56
8.1.4. Multi-Cloud Application Dependency Mapping	56
8.1.5. Kesolve Gateway	57
8.1.7 Display External IP addresses and MAC addresses on the Application	/ 55 59
2 $ i _{a} = (0.2023)$	uide 1/5 2

8.1.8	Application dependency man and server topology man export	61
8.1.9	Automated Application dependency map generation for VDI & Database applications	
8.1.1	10. Automated Application dependency map generation for VDI & Database applications	
8.1.1	1. Conversation Map	
8.2.	Transaction Analysis	64
8.2.2	l. Overview page	64
8.2.2	2. Server page	67
8.3.3	3. Transaction Logaina	68
8.3.	Service Grouping	71
8.3.1	Adding a VM to the service resources page	71
8.3.2	2. Monitoring a Service Group	72
8.3.3	3. Conversation Map	74
8.3.4	Creating New Multi-Tier and Port-Group based Service Groups	74
8.3.5	5. Import/Export Service Groups	76
8.3.6	5. Import CMDB data	77
8.4.	Service availability	78
8.4.	. Add to Service availability view	
8.5.	End User Experience	79
8.5.	Slow end user response time due to application server	80
8.5.2	2. Slow end user response time due to Network	81
8.6.	Horizon VDI Observability & Troubleshooting	82
0		00
9. Ir	irrastructure	
9.1.	Network Analysis	
9.1.2	L. Flow Analysis View	
9.1.2	2. Subnet Analysis View	
9.1.3	3. Network Conversation View	
9.1.4	I. Network Alarm View	
9.2.	Network Device Observability	
9.3.	CPU Analysis	
9.3.	L. Circle Packing View	
9.3.2	2. Iree view	
9.3.3	3. Alarm View	
9.4.	Viemory Analysis	
9.4.		
9.4.2	2. Tree view	
9.4.3	Storage Usage	103
9.5.	Storage Osage	105
10.	Security	
10.1	Application Anomaly	
10.2	Cyber Threat Monitoring	
10.3	Data Exfiltration	110
11	Boot cause view	112
11. 11.1		112
11.1. 11.2	CPU Health	112
11 2	Storage Health	113
тт.J.		
12.	Log Analysis	
13.	Stats Browser	
14.	Alarms View	

<mark>15.</mark> 15.1.	Reports	
16 .	Intelligent Remediations	
16.1.	Custom Scripting for Remediation Actions	
16.3.	Remediation Action Logging	
17. 17.1.	Uila KPI Infrastructure and Application Statistical Counter for Measuring Key Performance Indicators	
18.	Uila Default Threshold Levels	141

1. Introduction

1.1. Scope and Purpose

The first part of this document describes the system requirements, installation, and configuration steps for Uila uObserve[™].

The second part details how to use the console to manage and troubleshoot application and infrastructure related issues in the data center.

1.2. Architecture Overview

uObserve[™] consists of three major components –

 Management and Analytics system (UMAS) – The core of the Uila virtual infrastructure architecture is a big data store and analytics engine that is designed from ground up to scale-out to accommodate large data center deployments with thousands of servers, to scale-in to record data in high resolution, maintain historical data while maintaining real time responsiveness. Built-in redundancy offers high availability, mitigates downtime, and reduces maintenance overhead. UMAS can be installed in the Private, Public or SaaS Cloud.

The analytics engine is the brain that correlates application to infrastructure performance metric by providing the smarts to pinpoint the infrastructure root cause behind application performance degradation. The trending reports generated from the historical data helps identify infrastructure hotspots and maintains optimal application performance.

- Virtual Information Controller(vIC) The vIC can be installed in either the Private or Public Cloud. In the Private Cloud, Virtual Information Controller (vIC) is the integration conduit to the VMware Horizon VDI infrastructure & Virtualization Management System e.g., VMware vCenter, Microsoft Hyper-V, Nutanix Prism Central or OpenStack Controller. The vIC retrieves your infrastructure configuration as a template to build Uila monitoring domain and to streamline deployment. The vIC collects network, storage and compute performance metrics that are maintained by vCenter (or equivalent from Microsoft, Nutanix, OpenStack) and combines it with the application and network metadata from all deployed vSTs. In the Public Cloud, the vIC collects the Instance & VM level networking, application, compute statistics from the vSTs. In both cases, the vIC securely transmits it to the Uila Management and Analytics System, either on-premise or in the cloud.
- Uila Log Database Server- The Uila Log Database Server can be installed in either the Private or Public Cloud. The
 Uila Log Database Server collects and consolidates logs and log statistics from multiple Logging Smart Taps (LST).
 The Uila uObserve web console requests the log data from Uila vIC, which in turn queries the Log Database
 Server and delivers it back to the Uila UMAS server.
- Virtual Smart Tap(vST) Virtual Smart Tap (vST) is deployed in a distributed manner across the Data Center or the Public Cloud. The vST installs in the host (Private Cloud) or VM/instance (Public Cloud) or Kubernetes Node as an efficiently designed guest Virtual Machine or Pod where it promiscuously listens to all traffic from the virtual switch or getting traffic from Uila's Instance Smart Tap (iST) that traverses the virtual networks (North-South and East-West). Using embedded Deep Packet Inspection (DPI) technology, the vST identifies unique applications and their attributes.
- Instance Smart Tap (IST) The Uila Instance Smart Tap (iST) is deployed as a plug-in in a distributed manner across the Public Cloud on the VMs or Instances running the application workload. It collects traffic as well as VM and Instance level Compute statistics and sends it to the vST for Deep Packet Inspection.

 Logging Smart Tap (LST) – The Uila Logging Smart Tap (LST) is deployed as a plug-in in a distributed manner across the Data Center on VMs/Physical Servers and Public Cloud in the VMs or Instances. It collects logs from the server and/or application and sends it to the Uila logging server for further analysis.



Fig 1.1 – Uila Architecture overview

1.2.1. Unified Central Management Console

Modern virtual technology has improved data center's operating efficiency. However, the management tools that IT organizations use may not effectively cope with the increase in complexity to monitor application performance. uObserve[™] management console dashboard offers a simple yet powerful view to visualize the heath of an Applications across a Multi-Cloud environment. It also reveals the underlying physical/virtual infrastructure in the network, compute, and storage segments to pinpoint the application performance degradations and bottlenecks.

1.2.2. Automation and Provisioning

To aid data center operators, uObserve[™] integrates closely with the VMware vCenter and cloud platforms such as Amazon Web Services, Microsoft Azure, Google Cloud, VMware Cloud on AWS, Alibaba Cloud to setup applications and tenants for monitoring. Uila can also configure, deploy, and provision the Uila guest VM's automatically, that eases the additional burden of maintenance and support.

1.3. Feature Highlights

1.3.1. Multi-Cloud Architecture – Built for Multi-Cloud Data Center

Uila uObserve[™]'s architecture is a next-gen platform that utilizes the latest big data technology which offers unprecedented scalability and flexibility to monitor mission critical business applications across the multi-cloud cloud, while maintaining real time responsiveness:

- Scales from small to large data centers with built in redundancy for high availability.
- Maintains historical records of up to one year.
- Small footprint virtual Smart Tap(vST) with minimal overhead is deployed as a guest VM for on-premise datacenter.

- Low resource utilization Instance Smart Tap(iST) with minimal overhead is installed into a VM/Instance for the cloud datacenter.
- Collects application response times with more than fifty critical infrastructure performance metrics in minute intervals.
- Embedded Deep Packet Inspection (DPI) technology to identify over 3,000 unique applications and their attributes.
- The vIC seamlessly integrates with the VMware vCenter leveraging the network, storage and compute performance metrics maintained by it.
- Uila only collects metadata. Packet payload is not examined or stored. Data is transmitted through an encrypted SSL channel, removing the risk of exposing sensitive data.

1.3.2. Unified View – Simplify Data Center Operations

The complexity of Datacenter infrastructure hierarchy that comes with today's multi-Cloud datacenters require an easy but powerful tool set. Uila helps data center operators visualize and pinpoint areas of performance degradation that can identify the root cause immediately:

- Customizable Application and Infrastructure health dashboards that mirror the logical constructs of a data center.
- Uila aggregates data into meaningful Key Performance Indicators for early symptoms of poor performance.
- Powerful analytical tool sets for Application Topology, Flow Analyzer, CPU Usage, Memory Usage, and Storage
 Usage provide unique diagrams that reveal the underlying impact of application performance on the physical
 and virtual infrastructure.
- Innovative web-based UI design which simplifies navigation and speeds up problem resolution.
- New adaptive baseline technique to enable monitoring thresholds that align with actual average performance characteristics for the underlying infrastructure. This baseline technique reduces false positives and provides accurate root cause analysis.
- Integrated alerting and troubleshooting scenario for Help Desk or Network Operation Center.
- Built-in and customizable C level reporting for service level agreement compliance.
- Exportable historical trending data as a template for future planning.

1.3.3. SaaS Cloud - Automation and Provisioning

Wide adoption of virtualization and cloud technologies have made SaaS a widely acceptable consideration for IT. As enterprise and service providers continue to seek better service and lower the cost to service their customers, Uila Cloud helps to reduce IT Operational and Capital Expenditure:

- Single pane of glass view for the performance of the multi-Cloud.
- Integrating closely with VMware vCenter allows data center operators to take advantage of their infrastructure configuration and setup a vApp monitoring profile.
- Automated deployment and provisioning of Uila guest VM to frees up the burden of maintenance and support.
- SaaS deployment model eliminates the requirement to procure, deploy and maintain appliance and/or hardware probes.
- Multi-tenancy offers easy and common access for IT team.

2. Terminology Used

8

This section lists common terminology used throughout the product User Guide. Uila's goal is to use the same terminology as commonly used and defined within the virtualization industry.

Terminology or Legend	Definition
Application Response Time	Time measured on the server from the arrival of a client request to the transmission of a server response.
Application Service	**Refer to Classifier
Classifier	Often used interchangeably with Application service, classifier defines the application name because of Deep Packet Inspection by the vST software agent. i.e MySQL, iMap.
Cluster	Collection of hosts and associated virtual machines. Physical resources from all the hosts in a cluster are jointly owned by the cluster and centrally managed. i.e vCenter Server manages the clusters in a VMware implementation.
DPI	Deep Packet Inspection uses advanced method of pattern matching and session heuristics to identify applications and their associated attributes. This helps IT organizations track mission critical applications and transaction performance issues.
DvSwitch	DvSwitch's or Distributed Virtual Switch's simplify the management of hosts in a cluster by creating a single switch across the cluster to efficiently manage multiple virtual port or dvPorts. i.e. – A single dvSwitch can apply configurations to all applicable ESX or ESXi hosts, while vSwitch can only apply configurations to one host at a time.
DvPortGroup	DvPortGroup represents a group of dvPorts that share the same configuration template. The configuration is inherited from the dvPortgroup to the dvPorts.
Host	A physical server that supports a version of hypervisor. i.e VMware ESXi, Microsoft Virtual Server.
pCPU	A PCPU refers to a physical hardware execution context. This can be a physical CPU core if hyperthreading is unavailable or disabled, or a logical CPU (LCPU or SMT thread) if hyperthreading is enabled. For example, a server equipped with a CPU with 4 cores without hyperthreading will have 4 pCPU. If hyperthreading has been enabled, then a pCPU would constitute a logical CPU. This is because hyperthreading enables a single processor core to act like two processors i.e. logical processors. i.e if an ESX 8-core server has hyperthreading enabled it would have 16 threads that appear as 16 logical processors and that would constitute 16 pCPUs.
Port Group	It is a group of ports on a vSwitch. A 'PortGroup' is created in a Standard switch and Distributed switch. It acts as a logical segmentation of a vSwitch.
RTT	It is the time delay imposed by the networking infrastructure for a client to get a response from the Server. The value is an average of all the TCP connections that is made to the Server.
TCP Fatal Retry	Refers to the count of retry attempts made by either the Client or the Server when it does not receive a response in a TCP conversation. A retry attempt of greater than 3 seconds and over 3 attempts is counted as a single Fatal Retry for a single minute. It is not counted again within that minute. Uila displays the count as a total, not averaged for all flows.

Tenant	Tenants can be used to provide isolation between independent groups in shared cloud environment, where multiple companies, divisions or independent groups are using a common infrastructure fabric. Tenants are useful for isolating the users, resources and services from one tenant from those of other tenants.
ToR Switch	A Top of the Rack or (ToR) switch is a high port count switch, typically 48 1G or 10G ports plus 4 additional up link ports that sits on the top of server rack in Data Centers or Co-location facilities. ToR switches are then connected to the next level aggregation switch or core router to allow communication between servers in different rack or to internet.
vАрр	vApp is a collection of pre-configured virtual machines (VMs) that combine applications with the operating systems that they require. VApp's allow disparate VMs to work together in a stack as an application, and support cloud computing architectures. vApp is a VMware defined term and may be used in other similar products.
vCPU	A vCPU stands for Virtual Central Processing Unit. One or more vCPUs are assigned to every Virtual Machine (VM) within a cloud environment. Each vCPU is seen as a single physical CPU core by the VM's operating system. If the host machine has multiple CPU cores at its disposal, then the vCPU is made up of a number of time slots across all of the available cores, thereby allowing multiple VMs to be hosted on a smaller number of physical cores.
VM/Instance	A virtual machine (VM) or an Instance is a software, emulating a complete system platform (i.e a server) that supports the execution of a complete operating system (OS).
vIC	Virtual Information Manager is a Uila software agent that is implemented as a guest (VM). The vIC (1) interfaces to vCenter to retrieve compute and storage performance data, (2) acts as a proxy for vST to transfer vST meta data to Uila Cloud, (3) receives Uila management commands to install and configure vST. There is only one instance of vIC per vCenter.
vST	Virtual Smart Tap is a Uila software agent implement as a guest (VM) resides in the same Host as other application VM. It captures and analyzes all traffic between VM's within the same host, and other hosts.
vSwitch	vSwitch is short for Virtual Switch and represents networking entities connecting Virtual Machines in a virtual network at layer 2. The Virtual Switch is fully virtualized and connected to a NIC (Network Interface Card) inside a server. The vSwitch merges physical switches into a single logical switch. This helps to increase bandwidth and create an active mesh between server and switches. The VMware Virtual Switch is a switching fabric built into the VMware infrastructure (ESX) that allows you to network your Virtual Machines (VMs).
VPC	A virtual private cloud (VPC) is an on-demand configurable pool of shared computing resources allocated within a public cloud environment, providing a certain level of isolation between the different organizations (denoted as users hereafter) using the resources.

Table 2.1: Uila Terminology Definitions

3. Icon Definitions

This section lists used throughout the product and the documentation.

Icon	Definition	Usage
X	Maximize display viewing area by hiding browser menu and other title bars. Toggle to restore original display view.	
	Logout your Uila session.	
0	Launch help.	
	Select color for the title bar.	
-	Collapse or minimize the individual sub-view within the Dashboard.	
+	Restore the minimized the sub-view within the Dashboard.	
K.	Toggle between full screen and normal mode.	
C	Re-layout the Application Topology view.	
	Select infrastructure component to display in the Flow Analysis view.	
	Select the application and drill down to Root Cause.	
*	Start Packet Capture.	

Table 3.1: Uila Legend

4. Getting Started

This chapter describes the minimum system requirement to install and operate Uila uObserve[™], initial registration steps, and how to install and configure Uila software in vCenter and vSphere environments.

For the following sections, please refer to

- Uila uObserve[™] SaaS Installation Guide
- Uila Management Analytics Systems Installation Guide (for On-Premise deployment ONLY)

for System Requirements, Registration Instructions, and Instructions to install Uila software.

4.1. System Requirements

Always refer to the Uila website for updated system requirements as the first step: <u>https://www.uila.com/products/uila-system-requirements</u>

- Internet Browser for your monitoring console
 - Firefox, Chrome on Windows platform
 - o Safari, Firefox, Chrome on OS X platform
 - Firefox, Chrome on CentOS, Ubuntu Linux platform
- Hypervisor requirements

VMware ESXI

- o vSphere ESXi 5.5 or higher
- o vCenter Server 5.5 or higher
- o NSX 6.2 or higher

Nutanix AHV

- o Prism Central pc.2021.8 or PC.2022.6.0.1
- o AHV 20201105.2096

OpenStack

- Openstack version Q or higher
- Nova Node OS versions: Ubuntu 16 and Centos 7
- Virtual switches: OpenStack Virtual Switch and Linux bridge
- Hypervisor type: KVM
- Uila Virtual Smart Tap (vST) requirements
 - o vST for On-Premise -
 - Installed as a guest VM
 - 1 vCPU (1 Core)
 - 2 Gb memory
 - Uila © 2023

- 3 Gb Storage
- o vST for Public Cloud -
- t2.large for AWS
- D2s v3 for Azure
- VIC for VMware/Nutanix requirements
 - Installed as a guest VM
 - · 4 vCPU
 - Memory:

Small VIC 24 GB RAM allocated (32 GB if using Horizon VDI integration), 12GB RAM reserved, 50GB storage, thin provisioned: <1000 VMs, less than 200 Network Monitoring ports, less than 100 nodes for server monitoring
 Medium VIC 32 GB RAM allocated (40 GB if using Horizon VDI integration), 16GB RAM reserved, 100GB storage, thin provisioned: 1000~2000 VMs, 200~400 Network Monitoring ports, 100~200 nodes for server monitoring
 Large VIC 48 GB RAM allocated (56 GB if using Horizon VDI integration), 24GB RAM reserved, 200GB storage, thin provisioned: 2000~5000VMs, 400~600 Network Monitoring ports, 200-400 nodes for server monitoring

- VIC for AWS
 - t2.medium (less than 500 Instances)
 - t2.large (500-1000 Instances)
 - r4.large (1000+ Instances)
- VIC for Azure
 - B2S (less than 500 VMs)
 - D2s v3 (500-1000 VMs)
 - A2m v2 (1000+ VMs)
- Proper vCenter access right is required for vIC to collect structural information and CPU, memory and storage metrics from vCenter, make configuration changes, deploy and setup vST VM. You must have one of the two options pre-configured before vIC deployment:
 - 1. Full administrative access right (vCenter administrator role), or
 - 2. Partial administrative access right with the following table of privileges enabled (checked).

Privilege Categories	Privilege Items
Datastore	Allocate space
	Browse datastore
	Remove file
Global	Cancel task
14 Uila – © 2023	

Host	Local operations->Create virtual machine
	Local operations->Delete virtual machine
	 Configuration → Network Configuration
Network	Assign network
Resource	Assign virtual machine to resource pool
	Modify resource pool
Scheduled task	Create tasks
	Modify tasks
	Remove tasks
	Run task
Virtual machine	Configuration
	Guest Operations
	Interaction
	Inventory
	Provisioning
	Service configuration
	Snapshot management
	vSphere replication
dvPort group	Create
	• Delete
	• Modify
vApp	Add virtual machine
	Assign resource pool
	Assign vApp
	• Import

Table 4.2: vCenter access rights table

Uila Log Database Server

- 8 core CPU
- 8 GB RAM
- Uila © 2023

- 250 GB SSD

UMAS (Uila Management & Analytics System) for VMware/Nutanix

- For small scale deployment (under 1000 devices including VM and external device): One-box UMAS (1 VM to host UMAS) with 4 vCPU, 48GB RAM allocated and 32GB reserved, 1TB for 1 month data retention

- For medium scale deployment (1000~2000 devices including VM and external device): One-box UMAS (1 VM to host UMAS) with 4 vCPU, 64GB RAM allocated and 48GB reserved, 2TB for 1 month data retention

- For large scale deployment (2000~5000 devices including VM and external device): Two-box UMAS (2 VMs to host UMAS):

Web UMAS: 4 vCPU, 48GB RAM allocated and 32GB reserved, 800GB

DB UMAS: 4 vCPU, 48GB RAM allocated and 32GB reserved, 5TB

- For super-large-scale deployment (greater than 5000 devices including VM and external device): Contact Uila to get customized System Requirements for your deployment

UMAS for Public Cloud

- r4.xlarge for AWS
- E4 v3 for Azure

Visualizing Multiple VMware[®] vCenter[®] in a single view

Users can merge <u>two</u> separate VMware vCenter and enjoy a single pane of glass into the infrastructure, network, and applications. One example of this would be a VDI setup where Virtual desktops are in one vCenter, while the VDI infrastructure servers and backend application servers are hosted in another vCenter. With this new feature, users have the complete end-to-end VDI Application Dependency Mapping visibility across the two vCenters.

Network requirements

- Pre-allocate one IP address for each of the vST's, which can be either static IP address or allocated via DHCP, prior to deployment
- o Pre-allocate one static IP address for vIC prior to deployment
- o Pre-configure your network to open TCP and UDP ports to allow communications between Uila subsystems as illustrated in the chart below.
- o UMAS –
- If Cloud UMAS is being used, add <u>ugw1s.uila.com/38.99.127.15</u> as permitted site on the firewall.
- Pre-allocate one static IP if the on premise UMAS is used.



17





Fig 4.1: Network connection overview for On-Premise Datacenter

User Guide -v5.2



Fig 4.2: Network connection overview for Uila SaaS Cloud (if applicable)



Fig 4.3: Network connection overview for iST Deployments

5. Baseline

A baseline is a process for monitoring the data center infrastructure's network, compute, and storage resources at regular intervals to ensure that the infrastructure which supports business applications are working as intended. It is a process of continually monitoring the key performance indicators to report the health of all applications and its associated data center at a certain point in time. Properly constructing the baseline for your data center, you can obtain the following information:

- Monitor application response time and availability
- Reveal the health state of the infrastructure resources both virtual and physical
- Obtain the current utilization of system resources
- Determine and set alarm thresholds that are unique to your data center operation characteristics
- Alert and identify current system problems that impact Application performance
- Plan for future upgrades and expansions

5.1. Uila Baseline

The baseline methodology is used by Uila extensively. It is the foundation from which *Performance Grades* (*Infrastructure health performance index*) are calculated and *Alarms* are generated in real time.

uObserve[™] maintains a group of *Performance Metrics (See Appendix 15.1)*; for example, Application Response Time, Network Response Time, TCP/IP fatal retry, CPU usage, Memory usage, Disk latency, and many more in its Hadoop data base. Virtual Smart Taps and Virtual Information Manager deployed in user's data center analyze, collect, and transmit these Performance Metrics every minute to Uila Cloud.

Every Metric in per minute interval is compared to a Baseline value for that Metric in real time and a Health Score is calculated based on the formula listed in Table 5.1.

Delta from Baseline	Alarm Severity	Health Score	Color
Less or equal to 5%	Normal	75-100	Green
Between 5% and 10%, including 10%	Minor (1)	50-74	Yellow
Between 10% and 20%, including 20%	Major (2)	25-49	Orange
Above 20%	Critical (3)	0-24	Red

Table 5.1 – Health score calculations

Uila maintains two kinds of Baseline record for each of Performance Metric monitored;

- **Fixed:** it is a constant value; based on VMware best practices, for example, CPU usage for VM is pre-defined as 80%.
- Variable: it is an average of measured metric (per minute) within an hour, i.e. 60 data points. Example of variable metrics are Application Response time, and Network Round Trip time.

During the first day of starting up, current Metrics will be compared to previous hour's value as the default baseline value.

Method of Building Baseline record

Here are the choices you can change how Uila baseline values are defined.

Baseline Metrics	Remarks
Last Hour's value	This is the system default.
Yesterday's value	Select Yesterday's value as the Baseline.
User Configuration option	User selects and locks to a specific week's performance metrics as baseline.

Table 5.2 – Baseline settings

5.2. Health Score and Alarm Definition

<u>Performance Grades</u> are for visual display only and typically color-coded to show the health scores where low score (red) is poor health, and high score (green) is good health. (see Fig 5.1), and are updated every minute.

Here is an example of the Data Center Application Performance summary in color:



Fig 5.1 – Visual display of color-wheel

<u>Alarm</u> is generated based on the performance metric's delta from the baseline. Alarm is generated every 15 minutes by default.

Threshold is defined as the % value that crosses the baseline.

Severity is a user definable indicator to help identify the criticality of the performance metrics monitored to alert user if an entity or entities in his/her data center infrastructure is about to impact the Application's performance.

	Delta from Baseline	Alarm Severity	Health Score	Color
22	Uila – © 2023			User Guide –v5.2

Less or equal to 5%	Normal	75-100	Green
Between 5% and 10%, including 10%	Minor (1)	50-74	Yellow
Between 10% and 20%, including 20%	Major (2)	25-49	Orange
Above 20%	Critical (3)	0-24	Red

Table 5.3 – Alarm color scheme based on severity

Note: These standard color definitions are applied throughout Uila User Interfaces for consistence and ease of recognition. The default threshold levels are listed in Section 18.

6. Managing Your Work from the Console Home Page

Uila uObserve[™] console home page is the default infrastructure monitor where the day-to-day tasks are performed:

- View Application and Infrastructure health dashboard, investigate performance degradation, troubleshooting, and identifying root cause in real time
- Launch additional monitor applications
- Generate reports
- View Syslog
- Change Settings
- Set Preferences
- Go to Full Screen
- See On-line Videos
- Quick Helps



Fig 6.1 – Visual display of dashboard

6.1. Tools Pane

The Tool Pane consists of menu to set up the User profile, and a list of Uila uObserve[™] tools for monitoring, report and configuration.





6.2. Time Matrix Pane

The Time Matrix tool bar allow you to set up a Time Bracket within your timeline horizon where your entire infrastructure performance data are calculated, summarized, compared to prior baseline, and displayed in the Monitor pane. You can customize your time window in minutes, hours, or days depending on how you wish to perform real time monitoring, or root cause analysis.





The Time Matrix pane consists of:

- Calendar box to set up time window which you can select between 'Real Time' and 'Time Travel' mode. Select *Current* for Real Time mode.
- Timeline window with slide brackets; which can be dragged along the time line to widen or narrow the monitoring window (time range between the brackets)
- Up to five (5) user definable key performance index (KPI) to be monitored. The default KPI are *App Performance*, *CPU Health, Memory Health, Storage Health* and *TCP Fatal retry*. The Definition of the first four (4) KPIs are described in the Dashboard chapter in details. Also depending on the screen, there maybe other KPIs available for selection.

Real Time Mode

In real time mode, all the performance counters are calculated and updated every minute. Typically, you use real time mode to identify root causes of critical applications that exhibit performance degradation in short term, typically in past hours or minutes. System defaults to Real Time mode.

Time Travel Mode

In Time Travel mode, performance data and health measurement metrics are aggregated and calculated based on the Time Bracket you selected. Screen update is stopped. However, data collection continues in real time in the background. Time Travel mode is commonly used for

- Setting infrastructure Baseline to monitor for exceptional events that impact Application performance health. We recommend that you set the larger window bracket what is large enough to obtain a Baseline to represent your infrastructure health that is under normal operation. Common best practice is using a full week that average over several weeks to smooth out exceptional conditions.
- Real time troubleshooting where you may need to travel back in time to look for similar alerting event patterns that impacted performance currently.

6.3. Monitor Pane

The Monitor pane is the working space where Uila tools such as, Dashboard, Flow Analysis, Application Topology, reports, and other Uila Tool displays its contents because of your drill down action. By default, a Dashboard that highlights your infrastructure performance health is displayed after you log in to the system.

6.4. Settings

The settings maintain Uila uObserve[™] systems configurations for; (1) vST and vIC software initial installation, and new software updates and upgrades, (2) Interface to physical devices, (3) External systems to receive Alarms.

Here is a list of Configuration Settings Menu:

Menu	Definition						
VST Configuration	View License usage for Uila vST and iST; Use to select which vSwitch(s) in a host to install vST guest VM.						
Alarm Configuration	(1) Select Baseline from						
	- Last Hour						
	- Yesterday						
	- Last Week						
	 Any Week since Uila keeps trending records 						
	(2) Define Alarm Action. Support delivery alarm by e-mail. Syslog, SNMP, Zabbix or Remediation Actions. The frequency of the notifications can be set to the default (15 min), 1 hour, 3 hours, 6 hours, 12 hours, 24 hours						
	3) Hierarchy Threshold settings for VM						
	4) Setup Thresholds for alarms						
Software Update	List your Uila software version installed, and if new update is available.						
vIC Configuration	Contains options to						
	- Monitor external devices						
	- Define custom applications						
	- SNMP configuration for Top of Rack switches						
	- Ignoring certain TCP ports for ART						
	 vIC management (restart, reboot, logging) 						
	- Import External Device Address Book Settings						
	- Setup Multiple vCenter						
	- Setup Subnet Analysis						
	- Setup custom applications						
	- NSX settings						

Device Monitoring	Configure Network Device Monitoring capabilities, license usage, Network device threshold settings,				
Server Configuration	License usage for server monitoring, Automatic Subnet range to scan for Server Discovery & Up/Down monitoring, Manual setup for Server Up/Down monitoring & Process level monitoring				
Security Configuration	Configure threat update intervals and alert filtering				
Log Analysis	License usage for log analysis and configuration				
User Experience	Allows user to configure remote sites for end user response time.				
Horizon VDI	onfigure VMware Horizon Admin Host Name/IP, Alert Threshold ettings & Visualize Connectivity status between VDI Desktop and orizon Connection Server.				
Global Configuration	 Define alert (email, syslog, SNMP, Zabbix) and license configuration Packet capture configuration Custom Script Library 				
Accounts Management	Allows user to create role-based access control for individual users. AD/LDAP integration can also be enabled to give users access into Uila.				
VIC Installation	Step by step instructions to install VIC either the first time, or user wish to deploy VIC in more data centers.				

Table 6.1 – Settings menu

6.4.1. Accounts Management with two-factor authentication

With Uila uObserve, you can take advantage of leveraging your email address for two-factor authentication into the Uila system. This provides an additional layer of authentication beyond a username and password and prevents someone from logging in with only your password.

Authentication		
Authentication Method:	Database	~
Two-Factor:	× off Ena	ble
Configuration		
Registered Admin:	🕑 Edit	Email
Accepted client IP range:	🗹 Acce	oted client IP range

Fig 6.4 – Two-Factor Authentication

Once enabled, users will go through the additional step of entering the authentication code that they receive in their email.

Note:

- 1. Make sure all Uila accounts have an associated email address before enabling 2FA (Two-Factor Authentication).
- 2. Make sure that the "from" email address along with SMTP information is configured in the email configuration section of global configuration settings.
- 3. Make sure the Uila admin has specified an email address before enabling the 2FA (Two-Factor Authentication).

You can now specify the accepted client IP address for valid entries for accessing the Uila portal. You can access this from Settings→Accounts Management

Coles distorts	onec			
Subnet	Begin IP	End IP	Total IP	Actio



6.4.2. Accounts Management with SAML

With Uila uObserve, users can leverage SAML (Security Assertion Markup Language) based authentication for the Uila login. SAML is an open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider.

uObserve users can choose between the Database based 2FA authentication and SAML as shown below in the Accounts Management settings page. The Uila team has verified <u>SAML support for OKTA and Azure AD</u> at this time.

Global Configuration	Accounts Management	VIC Ins	stallation	
Authentication				
Authentication Meth	od:			
Two-Factor:			Database	
			SAML	
Configuration				



Authentication					
Authentication Method:	SAML 👻				
Identity Provider:	Identity Provider				
Metadata Url:	https://dev-10746413.okta.com/app/exkboyyfuuiegGvoc5d7/sso/saml/metadata				
Issuer:	http://www.okta.com/exkboyyfuuiegGvoc5d7				
Service Provider:					
Entity ID:	https://devportal.uila.com/saml/metadata				
Metadata Url:	https://devportal.uila.com/saml/metadata				
Assertion Url:	https://devportal.uila.com/saml/SSO 🕒				



For Uila portal users, the Service provider information will be pre-filled with the information. All you need to do is provide the Identity Provider information. On-premise users have to provide both Service Provider (updating a properties file in UMAS) and Identity Provider.

SAML users do not need to enter the password on the Uila login page. They will need to authenticate with their password at the OKTA/Azure login page as shown below.

OK	α	
Si	gn In	
Unable to sign	in	
Username		
adam@uilanetworks	LCOM	
Password		
	•	>
Keep me signed in		
S	gn in	
Eorgot password?		
Help		

Figure 6.8-SAML OKTA login

Note: It is recommended that users work with the Uila team to configure SAML for your environment. Please send an email to <u>support@uila.com</u> to setup the configuration meeting.

6.4.3. Accounts Roles

Uila offers three user types -

- Uila Administrator
- Data Center administrator
- Standard User

Here is the comparison of the 3 user roles.

User role	Uila admin	Datacenter admin	Standard User			
Number of accounts	Only 1	More than 1	More than 1			
Access to Setting?	Yes, for all datacenters	Yes, (except Software Update, Account Management) for assigned datacenters	Νο			
Uila Operation?	Yes, for all datacenters	Yes, for assigned datacenters	Yes, for assigned datacenters			

Uila administrator can assign pre-built service groups with mission critical servers and applications to a nonadministrator user. This would allow a standard user to focus on their relevant multi-tiered applications without having to look at the datacenter as a whole.

To add a new User:

- 1. Go to Settings -> Accounts Management.
- 2. Click 'New'

New User			×
Account Info	Data Center	+ Prev	Next→
User Type:	Standard User	DC Admin	
"Login ID			L 🕈
*Password	Con	firm Password	
*First Name	Last	Name	-
*Email			
*Phone			<u> </u>



- 1. Select Standard User or DC Admin
- 2. Enter Login ID, Password, First Name, Lost Name, email, and Phone
- 3. Note the Login ID and Password are CASE SENSITIVE.

4. Click 'Next'



Figure 6.10-Data Center Selection

5. Check one or more Data Center. Click 'Finish'.

6.4.4. Multi-tenant Roles for Service Grouping

User can override the default threshold value pre-defined in the system for a group of VM's by Host/VPC, Cluster/Region, or Data Center. Default threshold

With this new release, Managed Service Providers or similar organizations can create tenant accounts within the Uila solution to visualize the multi-tier service groupings for their customers/users. The tenant users will only be able to visualize the VMs/servers that are assigned to them. This folder configuration must be first configured in the VMware system.

Uila – © 2023

32



Figure 6.11-Folder selection in VMware

Here are the steps to configure the tenant in Uila uObserve.

Tenant							
+ New							
Riter	Filter	6 Filter	Filter				
User Name	Organization	Email	Data Center	Folders		Acti	ons
AdamTestTenant	LongTest	adam@eqit.com.tw	Production&Test	test		Ľ	Î
сск	ССК-Согр	chiacheekuan@gmail.com	Production&Test	Service-apache		Ľ	Ē
CTAI	Demo	ctal@uila.com	Production&Test	[Folder: Test2 Tenant-Kimi-test]		Ľ	ŵ
kimi589	LongTest	kimi.wu@uilanetworks.com	DC-test	External_vApp, kevin, Unmanaged-vAp	pp.	Ľ	Î
long-demo	LongTest	long.jlang@ulla.com	Production&Test	VM Network		Ľ	Ī
long.jlang@ullanetworks.com	LongTest	long.jlang@ullanetworks.com	Production&Test	[Folder: Tenant-Kimi-test], [Folder: Test2 Tenant-Kimi-test]		Ľ	È

Figure 6.12-Multi-tenant configuration

Config User							
1 Organization	2 Account Info	3	← Prev	Next →			
Create or select an org	ganization			•			
Main DC							
Main DQ							

Config User	
1 Organization 2	Account Info 3 ← Prev Next →
uila	
Dilip	Advani 🚨
4084003706	ر
dilip.advani@uila.com	





Figure 6.13-Multi-tenant configuration wizard

0	ulla kimi123		Reallime 11/9/202	3 1.59 PM ~ 11/9/2023	2:14 PI	4 Q	e 1	* •		1				Application	Perfo	e 🖻
.	Service Grouping Bookmarks	•	03 PM	06 PM	•	9 PM		Thu 09	03 AM	06 AM	09 AM	12 PN		Memory Heatt Storage He Network He	n ealth saith ealth	
		ø	Service Grouping													÷
			Group Name			Number Of VMs	÷	Application Performance	Network Health	🛊 CPU Health	÷	Memory Health	÷	Storage Health	¢	Actions
			New			6		15	15	15		15		(1)		c' i
			Tesl2 1024			10		15		(15)		15				C' D



6.4.5. Hierarchy Threshold Setting for VM

User can override the default threshold value pre-defined in the system for a group of VM's by Host/VPC, Cluster/Region, or Data Center. Default threshold values are listed in Section 18.

1. Go to Settings -> Alarm Configuration-> Hierarchy Threshold Setting for VM

2.	Select Host/VPC, Cluster/Region or Data Center
ы	erarchy Threshold Settings for VM

Hierarchy Threshold Settings for VM								
Host/VPC	Cluster/Region	Data Center						
+ Nev	+ New							
8 Filter								
Cluster/Region								

Figure 6.11-Hierarchy Threshold selection

3. Click New

Threshold Settings ×								
Cluster/Region O Threshold Frev Next								
Select All Deselect All								
Total Selected: 1 selected.								
Cluster/Region A								
EXT Cluster								
External_Cluster								
Network Device								
Prod								
UnCluster								
hyperv								
windows								
Total: 7 records.								

Figure 6.12-Select Cluster

4. Select one or more Clusters, Click **Next**

Th	Threshold Settings ×									
	Cluster/Region 2 Three	shold			← Prev	Finish →				
	Stat Type	Critical Threshold	Major Threshold	Minor Threshold	Actions					
	CPU Ready				Ľ	Ō				
	CPU Usage				Ľ	Ō				
	CPU Swap Wait				Ľ	Ō				
	Memory Active Usage				ľ	Ō				
	Read Latency				Ľ	Ô				
	Write Latency				Ľ	ā				
	Virtual Packet Drop				Ľ	Ō				
	Network Round-Trip Time				Ľ	Ō				
	Fatal Retries				Ľ	Ō				
	Application Response Time				Ľ	Ē				
	Disk Usage				Ľ	Ē				




Figure 6.14- Threshold selection example

6. Enter new Threshold values, Click **OK**.

Th	reshold Settings						×
	1 Threshold				← Prev	Finish →	
	Stat Type	Critical Threshold	Major Threshold	Minor Threshold	Actions		
	CPU Ready	80%	75%	70%	Ľ	ŵ	
	CPU Usage				Ľ	ŵ	
	CPU Swap Wait				Ľ	Ô	
	Memory Active Usage				Ľ	ŵ	
	Read Latency				Ľ	â	
	Write Latency				Ľ	Ô	
	Virtual Packet Drop				Ľ	ŵ	
	Network Round-Trip Time				Ľ	â	
	Fatal Retries				Ľ	ŵ	
	Application Response Time				Ľ	Ô	
	Disk Usage				Ľ	Ô	

Figure 6.15- Threshold selection summary

- 7. Click **Finish.**
- 6.4.6. Threshold Setting

Users can override the default threshold values pre-defined in the system for a group of VM's or the new threshold value defined through Hierarchy Threshold Setting.

7. Dashboard

Users at the time of login can choose between 2 UI options:

- a. Analysis & troubleshooting Same as Previous versions
- b. Real Time Events and Dashboards Real Time Events and Dashboards like Horizon VDI, Multi-Data Center Dashboard, Custom Dashboard

Sign In	
Login ID	
*Login ID	2
Password	
*Password	
 Analysis and Troubleshooting 	
Real Time Events and Dashboards	
If you have any problem signing in, please cont support at +1-(408) 819-0775 or email to sales(act tech @uila.com.
+)	Sign In
	Fig

Dashboard is the first screen displayed after login in the "Analysis & Troubleshooting" Option. It allows the user to have a unified high-level view of the overall health of the key components in real time and critical alerts that impact the Application performance and Security of the Data Center or Hybrid Cloud deployment.

There are 3 separate Dashboards available: 1) Performance, 2) Security, 3) Network Device

The Performance Dashboard allows the user to decide on the areas of focus to investigate application slowdown and the issues impacting the Applications performance. The center of the screen shows you the overall health scores in five (5) key areas; *Application, Network, Storage, CPU* and *Memory* within the infrastructure components, and organized by hierarchical structure relevant to each component in sun burst (color wheel) format.



Fig 7.2: Performance Dashboard View

The Security Dashboard allows the user to monitor their Cyber Threat status for the entire deployment. This includes getting the overall status for the Cyber Threats that are impacting the Data Center or Cloud deployment, Application Anomalies that have been identified, and finally information on traffic that is exfiltrated (outbound) from the internal VMs.



Fig 7.3: Security Dashboard View

The Security Dashboard allows the user to monitor the down status of the Physical Network Equipment (for example, the Top of the Rack Switch) ports and also visualize the critical network metrics for their favorite ports.

Laast Update Time : 05/26/2020 04 47 PM			•			
Network Device Port Dawn						
Device	Port	Last Oheck	O Duration O			
ProCurve 2524			93d Br 26m 54s			
MO185WD01P	Ethiometrize	05/26/2020 03 49 57 PM	93d 8h 25m 54s			
Cisco (3560	EastEthaneedics	05/25/2020 03 49:57 PM	93d 8h 26m 54s			
MD IBSMD01P	Ethames1/32	05/25/2020 03 49 57 PM	93d 8h 26m 54s			
Tanga	Ethernet)	05/26/2020 03 45 57 PM	93d 8h 26m 54s			
MOTOSWOOTP	Etherneel/E	05/26/2020 07-49 52 FM	93d Bh 75m 5ds			
(Mr6-7)11	ExelCohercer:2/0	45/26/2020 01-N 57 PM	913 Bi 25m 544			
:http-7513	TantDiverget12/1	05/25/200 00 45.52 PM	Stid Bn Zim S4k			
1941-7513	Efframatike:	G525-2018 03-40.57 PM	93d Br Zhm SHe			
1010-7573	Ethamat392	05/25/2010 03 49 57 PM	933 Bir 25m 54a			
Router (ubnt / eth0)	X For ST (class-calb509 / 10/100 utp athe)	🖍 🗴 tgrass 50-WAN	(ubnt / uth 1) /* x			
In Octors Marc 46 M Min 2463 X Gut Details	In Deters N/A N/A Out Deters	in Detains Max; 12.8 M Min: 632,7 K Gut Ostala	ii			
Max: 12.7 M Min: 457.8 K		Max: 8.6 M Min: 273.3 K	an a			
justen port (sankthösikö/ signalitechemet) 💉 🛪 Anti-12800/1% (sankthösikö/ signalitechemet) 🗸 🛪						
In Occess Maxistra 4 M Min 19,7 M	In Detects Mass: 4.7 M Min: 275.2 K					
Out Octate Max: 25.0 M Mity 603.3 K	Gut Octaria Max: 13.9 M Min: 687.9 X					

Fig 7.4: Network Device Dashboard View

For the "Real Time Events and Dashboards" option, users have access to a summary of the alerts identified by Uila, status of the VMware Horizon environment, visualize performance health of their Data Canters or create a custom dashboard as per their needs.



Fig 7.5: Real Time Events and Dashboards Selection

7.1. Summary of Key Performance Index

	КРІ	Metric Monitored	Measurement Method	
40	Uil	a – © 2023		User Guide –v5.2

Application Performance	Application Response Time	Time measured on the server from the arrival of a client request to the transmission of a server response
Network Health	Network Round Trip Time	Packet round trip time spent in the network
	TCP Fatal Retry	TCP re-transmit the same packet for the fourth time or greater
Storage Health	Disk Read Latency	Average amount of time taken process a read command issued from the Guest OS to the virtual machine. The sum of kernelReadLatency and deviceReadLatency in VCDB
	Disk Write Latency	Average amount of time taken processing a Write command issued from the Guest OS to the virtual machine. The sum of kernelWriteLatency and deviceWriteLatency in VCDB
CPU Health	CPU Ready	Percentage of time that the VM was ready, but could not get scheduled to run on the physical CPU due to physical CPU resource congestion
	CPU Usage	Average CPU utilization over all available virtual CPUs in the VM
Memory Health	Swap Wait Time	Time the virtual machine is waiting for memory to be swapped in
	VM Memory Usage	Memory usage as percentage of total configured or available memory

Table 7.1: Infrastructure Health Measurement Metrics and Definitions

41

User Guide –v5.2

7.2. Application Performance Metric

The Application Performance color wheel displays the health of Applications currently running in your data center. The rings present the hierarchical constructs of a virtual Data Center, where you may configure your data center in multiple logical Port Groups. Each Port Group consists of a series of Applications (vApp); such as MySQL, business logics, and web service to perform a specific application function for the end user. These applications depending on the business requirement may run on one or more than VMs.



Fig 7.2: Application performance metrics

Application Performance Health Metric

Measurement Metric	Measurement Method	Definition
Application Response Time (in millisecond)	Monitored at packet transaction level	Time measured on the server from the arrival of a client request to the transmission of a server response

Table 7.2: Application performance health metric

Ring Structure and Size Definition

	Ring Structure	Color	Size
Ring Center	Data Center		
42	Uila – © 2023		

ring)	Cluster/Cloud Region	Color represents the averaged Application Performance for the	Application Transaction
Ring 2	Host/VPC	group over the time range selection	Volume
Ring 3 (outer ring)	VM/Instance		

 Table 7.3: Ring structure and size definition for Application performance

Full Screen View

To gain a detailed view of the Application Performance Health, click the button, to enlarge the color wheel and add a table view of a complete list of VM, host, cluster monitored, and its associated health score, average application response time, transaction/minute, traffic/second, and packet/second. Each of the column can be sorted by clicking the column header.

Worst by Group					
Clueter 27 Standard-Cluster	Host	esxhoat4.mydatac	anter.com	VM	12 Icke_119-01
VM Host Cluster					
•	Health ©	Application Response Time	Transactions/m [©]	Traffic/s	Packata/s
192.168.0.174	100	0 ms	0	162 B	0
192.168.0.218	97	161 ms	25	962 B	2
192.168.0.221	67	139551 ms	2	171 B	1
APP-LB-001	99	1375 ms	0	3.50 KB	3
APP-LB-002	85	6054 ms	2	11.67 KB	18
Apacha_2.4-s2	99	2049 ms	0	2.96 KB	2
D6-L8-002	100	370 ms	92	2.82 KB	8
Gateway [192.168.0.1]	100	18 ms	20	2.50 KB	4
MySQL-N1	99	12 ms	0	6B	0
MySQLMGT	100	t ms	0	78	0
Oracle_11g-n1	12	627 ms	4.4 K	33.78 KB	208
Oracle_11g-n2	34	1558 ms	65	140.48 KB	655
Oracle_11g-n4	44	248 ms	18.1 K	11.93 MB	12.7 K
PostgreSQL_9.2-n2	100	89 ms	556	2.70 KB	30

Fig 7.3: Application performance detailed view

7.3. Network Performance Metric

The Network Health color wheel displays the health of network with respect to the infrastructure currently running in your data center. The rings present the hierarchical constructs of a virtual Data Center, where it typically structures from TOR Switches, Host, to VM's. Each TOR Switch is connected to several Hosts, where one or more VM's resides.



Fig 7.4: Network performance metric

Network Health Metric

Monitored at packet level	Packet Round trip time spent in the network
Monitored at packet level	TCP Fatal retry is the TCP packet retransmission for the same packet for the fourth time, which triggers TCP back off algorithm and significant application delay in response.
	Monitored at packet level Monitored at packet level

Table 7.4: Network Health Metric

Ring Structure and Size Definition

Ring	g Structure	Color	Size
Ring Center	Data Center	Color represents the average	Network
Ring 1 (inner ring)	Cluster/Cloud Region	weighted Network Health score for each respective group over the time range selection in the Time Matrix	Traffic Volume
Ring 2	Host/VPC	bar. See color and baseline	
Ring 3 (outer ring)	VM/Instance	definition in Time Matrix Bar (Fig 6.3)	

7.4. Storage Performance Metric

The Storage Health color wheel displays the health of storage systems currently running in your data center. The rings present the hierarchical constructs of a storage system within your Data Center, where it typically owns multiple Data Stores. Each Data Store groups together several Hosts.



Fig 7.5: Storage Health

Storage Health Metric

Measurement Metric	Measurement Method	Definition
Disk Read Latency (in millisecond)	Sourced from vCenter (VCDB)	Time taken to complete a Read command issued from the Guest OS. This Disk Read Latency includes VM kernel Read Latency and Device Read Latency.
Disk Write Latency (in millisecond)	Sourced from vCenter (VCDB)	Same as the above for Write command.

Table 7.6: Storage Health Metric

Ring Structure and Size Definition

Rin	g Structure	Color	Size
Ring Center	Data Center	Color represents the average	Number of
Ring 1 (inner ring)	Data Store	weighted Storage Health score for each respective group over the time range selection in the Time Matrix	Storage I/O Operations
Ring 2	Host/VPC	bar. See color and baseline	0000000
Ring 3 (outer ring)	Virtual Disk	definition in Time Matrix Bar (Fig 6.3)	

Table 7.7: Ring structure and size definition for Storage Health

Full Screen View

To gain a complete detail view of the Storage Performance Health, click the button, to enlarge the color wheel and add a table view of a complete list of VM, host, data store monitored, and its associated health score, read latency, read IOPS, write latency, write IOPS. Each of the column can be sorted by clicking the column header.

allen 🧑	Host	~	Virtus	I Diek	
\odot		\odot		\odot	
datastorn1 (4)		eschosi4.mydetboanter.com	1	Orace_11g-n2:scs	0_0
Diek Host Datastore					
VDiek	Health C	Read Latency 0	Read IOPS C	With Latency 0	White R
APP-LB-001:scsi0_0	100	0 ms	0	0 ms	
APP-LB-002.scsi0_0	99	0 ms	0	1 ms	
APP-LB-100:scsi0_0	100	0 ms	0	0 ms	
APP-LB-101:scsl0_0	100	0 ms		0 ms	
APP-LB-102:acsi0_0	100	0 ms	0	0 ma	
Apacha_2.4-s1:acal0_0	100	18 ms	0	0 ms	
Apacha_2.4-s2:scsi0_0	100	0 ms	Ō	Q ms	
DB-LB-001:scsi0_0	100	0 ms	0	0 ms	
DB-LB-002:sosi0_0	100	0 ms	0	0 ms	
DB-LB-101:scsi0_0	100	0 ms	0	0 ms	
DB-LB-102:scsi0_0	100	0 ms	0	0 ms	
Exchange_2010-s1:ecsi0_0	100	0 ma		0 ma	
Exchange_2013-s1:sosi0_0	93	0 ms	Ø	7 ms	
FS-100:scal0_0	100	0 ms	0	0 ms	
FS-101:scsi0_0	100	0 ms	Ö	0 ms	
FS-102:scsi0_0	100	0 ms	0	0 ms	
LotusNote_7.5-s1:scsi0_0	100	7 ms	O	0 ms	
MySQL-N1:scsI0_0	18	27 ms	142	1.ms	
MySQL-N2:acsIQ_0	92	12 ms		0 ms	
MySQLMGTaceI0_0	19	38 ms	107	1 ms	
NEX-APP-LB-002:acsi0 0	100	Oms	0	0 ms	

Fig 7.8: Storage performance full screen view

<u>Storage Disk usage charts and alerts</u>: Users now have access to new circle packing views and tables to visualize storage disk usage and capacity.

User Guide –v5.2



Antily Days Table Alams				11 - 1
Usage vilet HostVet Byzate				
2444M	Fire-Girt			
•••		0 Health 0	anala C	capadiy©
	freek.	100	5.00%	476 MB
44.61		1/4	6.67%	12.96.68
	.to_tek	108	5.96%	3.81 CB
	anda	116	4.704	47908
	Analyticula externa	108	9.01%	2.01 GE
Contra les 1 MSR controller 3	A HERO	110	675	2.01 G2 4.75 GA 2.85 GA 1.05 GA 4.75 GA 2.01 GA 2.01 GB 6.01 GA 6.01 GA 5.75 MA 1.05 GA
	5x2	106	11.07%	
	Awing	100	55,22%	
		1/6	40.896	સમાહ્ય
	Jan_bak	106	5.00%	3.81 CB
	Augustation and an endormal	ine in	1.594	KOTIGA
	Anup	106	5.74%	479 GB
Controller 2 MSA controller 11	next	110	11.07%	N 2011 IA N A79 GE N 775 A8 N 1,20 GE
	Aconto	105	11.07% 439.03 11.07% 575.68 6.0% 1.06.03	
	Avertag	100	67.52%	479 68
		1/0	49.16%	3.91 GA
	Assk	106	10.92%	475.115
		ire.	5,10%	25,96.08
	Asat	106	10,92%	476 MB
		110	6,14%	75,98.08
	Asse	106	10.92%	(NEME
		100	5,14%	25.96.68
HIME-GHTOD		1/4	69.76%	\$2.95 GR
HaspServer		106	51.57%	7.74 GS
IN COMMUNIQUE 1	analysis and a second se	ive.	61%	#3,30 GR
Sharing tos 71 at 71 anotaz				

7.5. CPU Performance Metric

The CPU Health color wheel displays the performance of all CPU in your Hosts with respect to the infrastructure currently running in your data center. The rings present the hierarchical constructs of a virtual Data Center, where there clusters, hosts and VMS.

47

User Guide –v5.2



Fig 7.9: CPU metric

CPU Health Metric

Measurement Metric	Measurement Method	Definition
CPU-Ready (%)	Sourced from vCenter (VCDB)	Percentage of time that the VM was ready to run but could not get scheduled to run on the physical CPU due to physical CPU resource congestion.
CPU Usage (%)	Sourced from vCenter (VCDB)	CPU usage is the percentage of active CPU to total configured CPU.

Table 7.8: CPU Health Metric

Host CPU Metric Calculation

Measurement Metric	Normal (Green)	Minor (Yellow)	Major (Orange)	Critical (Red)
CPU-Ready (%) (X = CPU.Ready/ # of pCPU)	X < 6,000 ms (10% per 1 min)	6,000 ms <= X < 9,000ms (10% ~ 15%)	9,000 ms <= X < 15,000ms (15% ~ 25%)	X >= 15,000 ms (>= 25%)
Y=CPU Usage (%)	Y <= 80%	80% < Y <= 85%	85% < Y <= 90%	Y > 90%

Table 7.9: Host CPU Health Metric Calculations

Note:

48

Host CPU Ready Time = Sum of all pCPU's Ready Time.

VM CPU Metric Calculation

Measurement Metric	Normal (Green)	Minor (Yellow)	Major (Orange)	Critical (Red)
CPU-Ready (%) (X = CPU.Ready/ # of vCPU)	X < 3,000 ms (5% per 1 min)	3,000 ms <= X < 6,000ms (5% ~ 10%)	6,000 ms <= X < 12,000ms (10% ~ 20%)	X >= 12,000 ms (>= 20%)
Y=CPU Usage (%)	Y <= 80%	80% < Y <= 85%	85% < Y <= 90%	Y > 90%

Table 7.10: VM CPU Health Metric Calculations

Ring Structure and Size Definition

Ri	ng Structure	Color	Size
Ring Center	Data Center	Color represents the average	
Ring 1 (inner ring)	Cluster/Cloud Region	weighted CPU Health score for each respective group over the time range selection in the Time Matrix bar. See color and	Physical CPU capacity (MHz)
Ring 2	Host/VPC	baseline definition in Time Matrix Bar (Fig 6.3)	Physical CPU capacity (MHz)
Ring 3 (outer ring)	VM/Instance	_	
	Table 7.11:	Ring structure and size definition for C	PU Health

Full Screen View

To gain a complete detail view of the Storage Performance Health, click the button, to enlarge the color wheel and add a table view of a complete list of VM, host, data store monitored, and its associated Health score, Application Response Time, Usage %, Usage MHz, CPU Ready. Each of the column can be sorted by clicking the column header.

User Guide –v5.2

neter	Host		VN		
B4 Standard-Chatler		eschosi5.mydetacenter	.com	Oracle_11) p=64
M Host Cluster					
-	Health	Application Response Time	Unage%	Uosgo Miliz	CPU Reedy
192.168.0.218	100	161 ms	1.25	104	N
APP-LB-001	100	1375 ms	0.27	141	(0.02
APP-LB-002	100	6054 ms	0.32	6	0.02
APP-LB-100	100	N/A	0.15		0.07
APP-LB-101	100	N/A	0.35	.6	0.12
APP-LB-102	100	N/A	0.35	5	0.16
Apache_2.4-a1	100	N/A	0.29		0.03
Apache_2.4-s2	100	2049 ms	0.65	10	0.04
D6-L8-001	100	N/A	0.14	2	0.01
DB-LB-002	100	370 ms	0.4	7	0.08
DB-LB-101	100	N/A	0.28	4	0.15
D6-L8-102	100	N/A	0.28	4	0.16
Exchange_2010-a1	100	N/A	0.06		0.051
Exchange_2013-s1	100	N/A	7.13	270	0.02
FS-100	100	N/A	0.25	9	0.04
F9-101	100	N/A	0.24		0.191
F8-102	100	N/A	0.27		0.141
LotusNote 7.5-s1	100	N/A	7.36	279	0.2

Fig 7.10: CPU performance full screen view

7.6. Memory Performance Metric

The Memory Health color wheel displays the performance of all memory arrays in your Hosts with respect to the infrastructure currently running in your data center. The rings present the hierarchical constructs of a virtual Data Center, where there clusters, hosts and VMS.





Memory Health Metric

50

Measurement Metric	Measurement Method	Definition
Swap Wait time (milliseconds)	Sourced from vCenter (VCDB)	Time the virtual machine is waiting for memory pages to be swapped in.
Memory Usage (%)	Sourced from vCenter (VCDB)	VM Memory usage is the percentage of active memory to total configured memory. Host and Cluster Memory Usage is the percentage of consumed memory (including VMkernel and Guest VMs) to physical memory capacity.
Swap-in Rate (kbps)	Sourced from vCenter (VCDB)	Average amount of memory (kbps) swapped in from disk into memory for VM to run.

Table 7.12: Memory Health metric

Host Memory Metric Calculation

Measurement	Normal	Minor	Major	Critical
Metric	(Green)	(Yellow)	(Orange)	(Red)
Swap-Wait (%) (X = Swap-Wait/ # of pCPU)	X < 6,000 ms (10% per 1 min)	6,000 ms <= X < 9,000ms (10% ~ 15%)	9,000 ms <= X < 15,000ms (15% ~ 25%)	X >= 15,000 ms (>= 25%)

Table 7.13: Host Memory Health calculations

Where:

X=CPU.SwapWait /# pCPU (ref %SWPWT in ESXTOP)

VM CPU Metric Calculation

Measurement Metric	Normal (Green)	Minor (Yellow)	Major (Orange)	Critical (Red)
Swap-Wait (%) (X = Swap-Wait/ # of vCPU)	X < 3,000 ms (5% per 1 min)	3,000 ms <= X < 6,000ms (5% ~ 10%)	6,000 ms <= X < 12,000ms (10% ~ 20%)	X >= 12,000 ms (>= 20%)
Y= Mem Usage (%)	Y <= 70%	70% < Y <= 75%	75% < Y <= 85%	Y > 85%

 Table 7.14: VM Memory Health calculations

Note:

VM CPU Swap Wait Time = Sum of all vCPU's Swap Wait Time.

VM Mem Usage = Active / Virtual machine configured size.

Ring Structure and Size Definition

51 Uila – © 2023

User Guide –v5.2

Rii	ng Structure	Color	Size
Ring Center	Data Center	Color represents the average	
Ring 1 (inner ring)	Cluster/Cloud Region	 weighted MEMORY Health score for each respective group over the time range selection in the Time Matrix bar. See color and baseling definition in Time 	Physical MEMORY capacity (MHz)
Ring 2	Host/VPC	Matrix Bar (Fig 6.3)	Physical MEMORY capacity (MHz)
Ring 3 (outer ring)	VM/Instance	-	

Table 7.15: Ring structure and size definition for Memory Health

The consolidation ratio is a measure of the number of VMs placed on a physical machine. ESX Server's over commitment technology is an enabling technology allowing users to achieve a higher consolidation ratio, thus reducing the total cost of operation. Over commitment is the ability to allocate more virtual resources than available physical resources. ESX Server offers users the ability to overcommit memory and CPU resources on a physical machine.

Full Screen View

To gain a complete detail view of the Storage Performance Health, click the button, to enlarge the color wheel and add a table view of a complete list of VM, host, data store monitored, and its associated Health score, Application Response Time, Usage %, Active, CPU Swap Wait. Each of the column can be sorted by clicking the column header.

ster	Host			VM	
70		6		(2
Sharefurd Charter		\sim			
Charlow Charles				ORDERVIEW	noovvienen
M Host Cluster					
		Application Response 0			
VM	Health	Time	Usego%	Active	CPUSwap Wall
192.168.0.218	67	161 ms	51.87	16.26 GB	-1 ms
APP-LB-001	100	1375 ms	6.77	17.37 MB	20 ms
APP-LB-002	100	6054 ms	7.36	18.86 MB	25 ms
APP-LB-100	100	N/A	0.8	16.49 MB	0 mis
APP-LB-101	100	N/A	6.6	16.93 MB	0 ms
APP-LB-102	100	NA	7.22	18.51 MB	em O
Apache_2.4-s1	100	N/A	8.56	43.91 MB	0 ms
Apache_2.4-s2	100	2049 ma	12.49	64.03 MB	0 ms
D8-L8-001	100	N/A	5.21	3.33 MB	0 ms
DB-LB-002	100	370 ms	2.7	13.90 MB	0 ms
DB-LB-101	100	N/A	6.24	16.01 MB	0 ms
DB-LB-102	100	N/A	5.63	14.95 MB	0 ms
Exchange_2010-s1	100	NA	0	0 KB	0 ms
Exchange 2013-s1	100	N/A	22.66	232.22 MB	0 ma
FS-100	100	N/A	0.91	18.88 MB	0 ms
FS-101	100	N/A	2.65	27.30 MB	Q me
E9.103	100	N/A	2.00	20.10 MD	0.000
13-102	100	NYA	2.10	22.10 MB	0 ms
LotusNote_7.5-s1	100	N/A	24.56	503.35 MB	0 ms

Fig 7.12: Memory performance full screen view

8. Application

8.1. Dependency Mapping

Application Analysis provides you a visual view of all virtual Application (vAPP) service chains within your data center in real time. Applications within a defined Port Group are grouped together to help you quickly identify how each Application and its associated VM is communication with each other. It shows the health of each VM by calculating the average application response time of the VM server.

The application dependency map will also extend beyond

Application Analysis view is directly launched from the Tool Pane menu, and it consists of three tabs (views):

- Topology Map view: See complete view of all application servers inside a vCenter
- Dependent Services view: See application service chaining. Multiple views can be customized
- Table view: Organize in table view to sort by performance grade of the VM. Refer to Chapter 7.2 Application Performance Metrics for details.

8.1.1. Topology Map View

You can use Topology Map view to see all application servers (VM's) organized by Port Group (VLAN) view in a glance, and how they communicate with each other. This view is particularly useful for

- Revealing how and if Port Groups (VLAN) are interconnected
- Showing each application service performance by its response time and transaction load on the associated VM's
- Identifying any orphan VM's (VM's are standalone without communication with any other VM), which are the result of misconfiguration.
- Identifying any application services performance degradation and pinpoint the root cause quickly.



Fig 8.1: Application topology map view

Symbol	Definition	Mouse Over Information	Click Action
	Application VM name with list of protocol identified.	Highlight connections between this Application VM and neighbor VM's Show a list of active Application protocols and associated response time	Select one of the protocols to identify the root cause of slow response time
	Traffic flow between Applications	Displays average transaction response time between two VM's for each of the application service running.	None
	Find Root Cause for Application issue	None	Click to Root Cause view
	Packet Capture Network Traffic for the selected Application	None	Click to start packet capture

Table 8.1: Symbols, definition, information and action

You can visualize the properties of the VM/server, from the properties menu option, when you click on any VM/server.

8.1.2. Dependent Service View

Dependent service view is particularly useful when you have many application servers (VM's) that are crowding your screen, and you are interested in only those critical application service chaining that runs your mission critical business applications. There is no practical limit of how many Dependent Service view you can create and customized.

To create a Dependent Service view, follow these steps:

- 1. Find VM that is the beginning of your critical service chaining, click to show the VM health summary
- 2. Select and click the "Add to Dependent Services View"



Fig 8.2: Application topology to dependent service view

A new Dependent Service is created, see example below, and notes the steps of finding the root cause of application performance degradation.

Special Note: Users can also visualize the dependency map between the real client IP address behind the Load Balancer that is using the X-Forwarded-Proto HTTP Protocol to the server they are connecting.

8.1.3. Service Filter

The function in application dependency mapping filters the Dependency Mapping window to display only the selected service or application. This allows the user to focus on the services or applications that needs to be monitored or troubleshoot for user complaints.





8.1.4. Multi-Cloud Application Dependency Mapping

Uila's Multi-Cloud Application Dependency Maps provides the user with the ability to see the application dependencies across the cloud boundaries. Uila makes it easy to visualize application on the cloud and their dependencies to on-premise servers.

User Guide –v5.2



8.1.5. Resolve Gateway

The "Resolve Gateway" button removes the gateway from showing up on the Application Dependency map. This can be helpful when the user wants to see the direct dependencies of servers within the environment.



Fig 8.5: Gateway resolution in Application Dependency Mapping

8.1.6. Change control Monitoring and Baselining

uObserve[™] 's change control monitoring and baseline feature provides the user with the ability to baseline the application dependency map during the normal course of operation. The application can be baselined and compared to the application dependencies to any given time period. With the change monitoring capability, users can stay on top of all changes in the applications, servers delivering those applications and the interdependencies in the environment, including new entrants and exits.

- 1) Select the "Application Anomaly" menu.
- 2) Select "Config Baseline" for the service group for which you want to track changes. Select the baseline date/date range.

57

0		Config Baseline			
		Start Time:	EndTime:		
	12.9%	← November 2022	← November 2022	.a G	Alg.
		Su Mo Tu We Th Fr Sa	Su Mo Tu We Th Fr Sa		
Applicat	Ion Anomaty				
	Group Name	6 7 8 0 10 11 12	6 7 8 0 10 11 12	IT EVENT.	Exfitratio
jej	Shidage.	13 14 15 16 17 18 19	13 14 15 16 17 18 19	Major	
		20 21 22 23 24 25 25	20 21 22 23 24 25 26		
		27 28 29 30 1 2 3	27 28 29 30 1 2 3	their	
				10 A	
-120		Today	Today	Mann	
			in the second	Magnin .	
			<u> </u>		
		Dynamic Multi Ticr		Mass	
				1.5000	
		Ustranic Multi-Fier		Macr	
	mappile	Dynamic Molti-Lier		and the second se	
				and the	
	DEVO VMware Explore	Multi-Tior			
				(allow)	
		Dynamic Multi-Tier		1000	
				Macr	
9		MultiTicr			
		100000000		Maca	
1		Multi-tier		1	100
				Major	
		Hypanic Motsher		1	

Fig 8.6: Config Baseline

3) Click on the deviations in the Application Map Deviation column.



4) Visualize the changes in the table format as well as on the dependency map itself.

* <u>All</u>	l-in-One Demo		
Applic	cation Map Deviation Cyber Threat Event Exfiltration Map		1 To Overview
III Dev	viation Table		
	Filter VM		
	VM	A Detail	Action
	10.3.240.1	New Server 1. New service https 2. New service TL5_1-2 3. New https request from A4.6-48-ulla-vic	+
	10.3.240.2	New Server 1. New service https 2. New service TL5_1.2 3. New https request from A4.6-48-uila-vic	+
	10.3.240.4	New Server 1. New service https 2. New service TLS_1.2 3. New https request from A4.6-48-ulla-vic	e +
	10.3.240.6	1. New https request from A4.6-48-uila-vic	+
	A4.6-48-uila-vic	1. New service ssh 2. New ssh request from 4.6-48-uila-vic-devportal	+
	Horizon Connection Server - Win2019	1. New TLS_1.2 request from 00505695479D 2. New https request from AK-uila-vic-for-ist 3. New tcp request from AK-uila-vic-for-ist 4. New soap request from AK-uila-vic-for-ist 5. New soap request from 4.6-48-uila-vic devportal	+
		New Server 1. New service space	

Fig 8.8: Application Dependency Mapping deviation table



Fig 8.9: Application Dependency Mapping deviations

Dotted gray line - The dotted gray line seen on the map indicates all the missing inter-connections in comparison to the baseline.

Blue Line – The solid blue line indicates any new dependencies and inter-connections between the individual VM's.

8.1.7. Display External IP addresses and MAC addresses on the Application

External devices may include physical servers, VMs in a separate Data Center, gateways, firewall, load balancer, client devices, VM running in any cloud provider's platform, network switches, etc. Now the user can display those external devices in their Application Dependency Map by entering its IP address. This is enabled from the Settings \rightarrow VIC configuration menu.

• Manually display External Device by IP

- 1) Go to Settings \rightarrow VIC configuration
- 2) In order to add a new External Device by IP, click New

loud Type	Cluster/Region	Host/VPC	Summary	Actions
Seneric Cloud	Internet	internet	98.137.246.8/32	r 0
Generic Cloud	Internet	Internet-US	5.22.149.135/32,8.8.8.8/32	6 9
Google Cloud	G-Cluster	G-Host	192.168.1.175/32	2
Physical Server	CCK-Cluster	CCK-Host	192.168.1.122/32	2 1
Physical Server	ula	ula-umas	38.99.127.23/32	C D
Physical Server	Ulla	sc02	192.168.0.201/29,192.168.0.208/31,192.168.0.210/32	2 1

Fig 8.10: External device setup

3) Add the fields –

Manual Display External	Device Configuration	n by IP/Subnet ×
1 Topology 2 VM IF	P Range	← Prev Next →
Cloud Type:	Google Cloud	*
Cluster/Region / Region:	Google Cloud	
Host/VPC / VPC:	Internet	
vApp / Application Group:	Internet	
Port Group / Subnet:	SMU	

Fig 8.11: Topology selection

4) Select the IP ranges -

M IP Range		← Prev	Completed →
oo-Web			
New Subn	et		
gin IP	End IP	Total IP	Actions
.137.246.8	98.137.246.8	1	e
	New Subn gin IP .137.246.8	New Subnet gin IP End IP .137.246.8 98.137.246.8	New Subnet gin IP End IP Total IP .137.246.8 98.137.246.8 1

Fig 8.12: IP address configuration

5) Now you will see these devices appear on the Application Dependency Map

Manually Display External Device by MAC

- 1) Go to Settings \rightarrow VIC configuration
- 2) In order to add a new External Device by MAC, click New
- 3) Click on "New MAC Address" to add the device -

Device Name:			*Required!	
Subnets	+ New Mac Ad	idress.		
Mac Address		Actions		\$

Fig 8.13: MAC address configuration wizard

4) Add the MAC's

evice Name:	Cisco Switch 1				
Subnets	÷	New Mac Address			
Mac Address			Actions		\$
00:C0:30:56:76:C	1		C	ŵ	

5) Now you will see the device appear on the Application Dependency Map

8.1.8. Application dependency map and server topology map export

Users can export the application dependency map and server topology map into an excel spreadsheet. A common use case for this export is it can be used for datacenter pre-migration assessments to the Hybrid Cloud.

1) To export the application dependency map, go to the Service Grouping menu and click on the gear icon and then click on the "Export Application map".

VDi dema 👻	🔹 Multi-Tier (18 VMs)	1 To Overview
Application Map Conversation Table Alarms User Experience	Log Analysis	n + B
★ VDi dema		× Actions
VDI Thin Client & Connection Server V UDI Thin Client & Connection Server Vir2019 Virvere Client(10.3.255.21)	t desktop ≓ Load Balancer ≓ Web-Server ≓ • VI57/1C2 ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	B) Export Application Map Filter Service Select Service • Node distance



61

- 2) The CSV export provides the user with the excel sheet to help identify the various inter-dependencies and the capacity of individual virtual machines. There are 2 sections in the excel sheet: Dependency and Capacity.
 - a. Dependency This provides us with all the inter-connections between different servers, the source, through the gateway and the destination. It also provides us with the port numbers and the applications.
 - b. Capacity This provides information on each server, the number of CPU cores and the memory allocated to each server.

Hc Past	, X	Insert Cut	Page Layou	nt Form										
Past	. *	Cut		20 (Alexandra)	iulas Di	ata Rev	view	View	11					
Past	1.0		Calibri (Bod	y) • 12	• A-	A= =	=	- 3	9	🗔 Vra	p Text	Genera	il .	
	te es	Copy *	B I 1	<u>ı</u> • 💷	A - A		= 4	=	E +E	Her Mer	ge & Center 🔻	5 -	%)	00. 0. 0. 0.
	~	er men												
C P	Possible [Data Loss	Some feature	is might be l	ost if you sa	ve this work	book in th	he cor	nma-delim	nited (.csv)	format. To prese	erve these	features, a	ave it in an
AI	4	X V	fx Depe	ndency										
d	A	в	c	D	E	F	G		н	T.	1	к	L	м
1 De	pendency	1										17	-	
2 50	urce	Source IP	Through Gat	Destination	Destination I	Port	Applicatio	on						
3 AP	P-LB-002	192.168.0.91	Gateway [19	212.47.239.1	212.47.239.1	123	ntp							
4 AP	P-LB-002	192.168.0.91	1	Weblogic 1	192.168.0.27	80	walmart							
5 AP	P-LB-002	192.168.0.93	1	sc-dc-01.my	192.168.0.20	53	dns							
6 W	eblogic_11	192.168.0.2	7	DB-LB-002	192.168.0.90	3306	mysql							
7 W	eblogic_11	192 168 0.27	7	sc-dc-01.my	192.168.0.20	53	dns							
8 W	eblogic_11	192 168 0 2	7	MySQL-N1	192.168.0.88	22	tcp							
9 Or	acle_11g-	192 168 0 3	1 Gateway [00	10.10.10.13	10.10.10.13	80	http							
10 Or	acle_11g-	192.168.0.3	1	sc-dc-01.my	192.168.0.20	53	dns							
11 Or	acle_11g-	192.168.0.3	5	sc-dc-01.my	192.168.0.20	53	dns							
12 DB	-LB-002	192.168.0.90	0	Oracle_11g-	192.168.0.36	3306	mysql							
13 DB	-LB-002	192.168.0.90	0	sc-dc-01.my	192,168.0.20	53	dns							
14 DB	-LB-002	192.168.0.90	Gateway [19	212.47.239.1	212.47.239.1	123	ntp							
15 sc-	dc-01 my	192.168.0.20	0	FFFFFFFFF	192.168.1.25	137	nbns							
16 sc-	dc-01.myd	192.168.0.20	0	FFFFFFFFFF	192.168.1.25	138	smb							
17 sc-	dc-01 myd	192.168.0.20	0	224.0.0.252	224.0.0.252	5355	dns							
18 sc-	dc-01.myd	192.168.0.20	0	FFFFFFFFFF	255.255.255	67	dhcp							
19														
20														
21														
22 Ca	pacity													
23 Se	rver	Server IP	Number of C	CPU(GHz)	Memory(GB	Application								
24 AP	P-LB-002	192.168.0.9	1 1	1.81	0.25	[walmart]								
25 W	eblogic_11	192 168 0.2	2	1.81	0.5	[ssh][walma	art][icmp][http]						
26 01	acle_11g-	192.168.0.3	4	1.81	- 4	[ssh][icmp][mysql]							
2/ 0/	acle_11g-	192.168.0.3	4	1.81	4	[ssh][icmp][mysql]							
28 08	-LB-002	192.168.0.90	1	1.81	0.5	[icmp][mysc	all deal							
29 50	acla 11-	192.168.0.20		2.7	7.9	[icmp][msrp	stitune)							
30 08	acie_11g-	n.s	-4	1.81	2.96	[icmp][mysc	90							
31														
32														

Fig 8.15: Application Dependency Map export results

8.1.9. Automated Application dependency map generation for VDI & Database applications

For VMware Horizon[®] versions 6 or higher as well as Citrix XenDesktop, Uila uObserve[™] automatically generates the Application Dependency Map which can display the different tiers of the entire VDI environment, including thin clients, VDI desktops, as well as critical infrastructure components such as the Connection server, Domain Controller, etc. With this automatically generated map, Uila users are able to automatically highlight the bottlenecks in their VDI environment.



Fig 8.16: Application Dependency Mapping for VDI

8.1.10. Automated Application dependency map generation for VDI & Database applications

Like VDI, you can get automated end-to-end visibility Dependency Mapping for leading Database applications such as Oracle and MS-SQL.



8.1.11. Conversation Map

Users can visualize the applications or services in use on the VMs. For example, this can be very helpful to visualize applications in use on the VDI desktops.



Fig 8.18: Application Dependency Conversation Mapping

Users can also visualize a brief description on the classified built-in applications/protocols via a tooltip.

Health Score Applicatio Response T		ion Transactions/min 1 Time		Traffic/a	Packets/s	
100	2 00		210.	2.20 KB		
Actions	Actions Services A Provided Res		Transactions/mir	Traffic/s	Packets	
0±	wmi msrpc	2 ms	50	1.49 KB		
Remove VM Add Dependent Add Dependent Move To Previce Move To Previce Move To Next T Add to Depend Co To Stats Ma Setup Server M Start Cepture	I Servers Mic Clients the tas Tor Par ent Services p Ionitioring	rosoft Remote Pr Microsoft impler chanism.	rocedure Call (M nentation of the	SRPC) is DCE RPC		



8.2. Transaction Analysis

Transaction Analysis provides deep insights and analytics into web and database application (HTTP, MySQL, Oracle and PostGreSQL) performance. This is done by collecting application response times through the network and by reading transaction codes and queries from the packet. The goal is to provide deeper insights into client and server errors so that the issues can be narrowed down and mitigated.

Transaction Analysis does not require any additional configurations. The vST can immediately identify the type of application traffic and its status codes and query's by parsing through its header file.

This feature provides the users with an overview and individual server view. The overview provides a quick summary of all status codes and queries seen within the entire datacenter. The server view provides a summary of status codes and queries seen by individual servers.

8.2.1. Overview page

Choose the Database you would like to view statistics on using the tabs -

all						
A						•
📰 հահատոհ	ատակեստելեա	anatal namesa	d ool caabaab	ատասեսեսես	an haa na an had	um and al
06 PM		09 P	М		Nov 13	
DNS HTT	P MYSQL	MSSQL	Oracle	PostgreSQL		
Overview	Servers					
Overview						
Status	Code 🛛					
				Fig 8.20: Ap	plication Tra	insaction selectio

Overview page has 3 components –

• Ribbon View -

This view provides the user with a visual representation of the different queries and statuses of individual servers.



Figure 8.21: Ribbon View

The user can hover over the ribbon to view the server's transaction volume based on queries and the status codes.



Figure 8.22: Hover over to view details

• Status code statistics -

The status code statistics displays the number of status code responses collected. Each vertical bar on the graph represents the number of responses collected per minute.

Status Code Statistics				
Status Code 100s Max: 0 Min: 8	 Status Code 200s Mois: 233 Min: 191		Status Code 310s Max: 36 Min: 0	
Status Code 400s Max: 0 Min: 0	 Blatus Code 500s Max: 10 Min: 0	, de alexan e lidar neraliterali		

Figure 8.23: Status code statistics for HTTP

Status Code Statistics			
SQL Status OKs Max: 4374 Min: 42	ill.J.Illinumu.	SQL Status Errons Max: 0 Min: 0	

Figure 8.24: Status code statistics for MySQL and Oracle

Status Code #	Function
100's	Informational response –continue, switch protocols, processing
200's	Success response – OK, created, Accepted
300's	Redirection response – found, moved permanently, use proxy
400's	Client errors – bad request, forbidden, not found
500's	Server errors – bad gateway, gateway timeout, service unavailable

Table 8.2: Status codes and their function for HTTP

• Query statistics -

Displays the application response times and counts per minute for various HTTP (GET, POST, HEAD) and SQL (INSERT, UPDATE, DELETE) queries.

Query Statistics					
Gaal ART Mas: 127 mm Min: 1 mm	matuatalida micrattik raka atra di	Get Count Max: 256 Min: 178		Get Failed Count Max: 10 Min: 9	er an e thia meralute educates th
Post ART Max: 23 mil Mix: 19 mil		Poet Count Mar: 13 Min: 13		Pout Failed Count Mar:: 0 Mis: 9	
Haad ART Max 0 ma Min: 0 ma	ан на он на на на ко-	Heed Court Max: 9 Min: 0		Head Falled Cours Mac: 0 Mis: 0	
Other ART Max: 171 me Mile: D me	undhuthunut	Other Count Max: 3 Min: 6	mmmmmml	Other Failed Count Man: 0 Min: 0	

Figure 8.25: Query statistics for HTTP

Query	Function
GET	Gets information from the webserver
POST	Sends data to a webserver
HEAD	Checks if a webserver exists

Table 8.3: Query statistics for HTTP

Query Statistics				
SGL Create Art Here: D me Mire: D me	 BQL Onets Court Nex: 8 Mills: 8		BQL Create Fell Court New: 0 Mis: 0	un den die generaliere anderener
SCL. Invent Art Mass: Drive Mire: Drive	BCAL Imaeri Count Macc. 9 Mire 9		8Cal, Insert Fall Court Marc 0 Minr 0	
BQL Update Art. Mas: 27 me Mar: 8 me	 PGL Updele Caura Mac 4 Min: 8	ւււլ է ուտ ուս ուսահստա	BQL Updata Fail Count Mar: 0 May 0	
BQL Databas Art Maxi Binna Minri Binna	BGL Delete Court Marc 8 Mini 8		SQL Delete Pell Court Mexi 0 Mini 0	
SQL Alber Art Mass: Brea Mirr: Brea	SUL Alter Court Marc 8 Mirc 8		BCAL Alber Pall Count Mess: 0 Miss: 0	
BQL Drop Art Mat: 8 mm Min: 9 mil	SGL Drop Court Marc T Min: S		BGAL Drop: Full Count Mas: 0 Mitt D	
DGL Select Art Haz: 473 mm Him: 8 mm	913. Select Count Nac. 2719 Wiv: 34	Internetie	SQL Select Felt Ceant Marc 0 Mint 0	
SQL Other Art Mass Fran Min. 3 ms	SGL Other Count More BE Min: B	Dannta.	BQL Other Fail Count Main 0 Mini 0	

Figure 8.26: Query statistics for MySQL and Oracle

Query	Function					
CREATE	Creates a table					
INSERT	Inserts into table					
UPDATE	Modifies existing records in a table					
DELETE	Deletes existing records within table					
ALTER	Adds, deletes, or modifies columns in existing table					
DROP	Drops an exisiting table from a schema					
SELECT	Select a database where operations are performed					

Table 8.4: Query statistics for MySQL and Oracle

• Network statistics -

Displays network specific information such as transaction volume, network delay time and retry rates for the HTTP or database applications.

User Guide –v5.2

Network Statistics				
ART Max: 122 ms Min: 1 ms	ccdllccdccalloctationallianationatil	Transactions Max: 282 Min: 197	Network Delay Time Max: 1 ms Min: 0 ms	
in Fatal Retry Max: 0 Min: 0		Out Fatal Retry Max: 0 Min: 0	 Packota in Max: 11267 Min: 401	
Peciets Out Max: 29399 Min: 277		Bytes in Max: 820594 Min: 97354	 Byles Out Max: 43112719 Min: 48417	
In Reset Max: 15 Min: 4	k understudierte kanden die hete	Out Rosot Max: 0 Min: 0	 3n Zero Win Max: 0 Min: 0	. <u> </u>
Gut Zero Win Max: 0 Min: 0				

Figure 8.27: Network statistics

Statistic	Function
ART (ms)	Provides the application response times per minute
Transaction	Number of transactions per minute
Network Delay Time	Network delays per minute
In Fatal Retries	Number of fatal retries inbound per minute
Out Fatal Retries	Number of fatal retries outbound per minute
Packets In	Packets inbound per minute
Packets Out	Packets outbound per minute
Bytes In	Bytes inbound per minute
Bytes Out	Bytes outbound per minute

Table 8.5: Network Statistics

8.2.2. Server page

The server page provides an insight into the individual servers providing the service. Each server's queries and statues are displayed individually to help understand the problematic services.

Overview Servers										
Servers										Collapse All
					Query					Status
VM Name	CREATE	INSERT	O UPDATE	O DELETE) ALTER	O DROP	C SELECT	© Other	© OK	C ERROR C
Oracle_11g-n4	0				0	0	9010	50	9060	0
O DB-LB-002	0						28135	98456	28137	96454
Oracie_11g-n3	2	18296	0				28799	100627	47153	100772
() dbserver	0	O			0	0	11446	5721	17167	

Figure 8.28: Server page view

Users can further drill down and get more information on their status, queries, network, usage, dependent services, and process monitoring.

			Query									Status	
VM Name CREATE				CREATE	REATE 💠 INSERT 🗧		O DELETE	C ALTER	O DROP	SELECT	0 Other	OK OK	C ERROR
0	PDOCKER-	-01		36	179	12	24	12	36	60	156	443	72
	Status	Query	Network Usage	Dependent S	iervices Proce	x55							
	<u>OK Count</u> Max: 37 Min: 36	i				ERROR Count Max: 6 Min: 6							

Figure 8.29: Drill down into server

8.3.3. Transaction Logging

To view transaction analysis, the user must redeploy the VST. Once the VST is redeployed -

- 1) On the Uila dashboard settings -> VST configuration
- 2) Click on configuration for the VST you would like to enable transaction logs
- 3) Check "Enable Transaction Analysis" box.

/ST Configuration			*					
VST Name : Uila-vST-123456789-esxhost C Rebool	1 mydelacenier o	om(1.28.0-17)						
Choose a datastore with sufficient disk spa	ice. 1 vST has 20	8 disk:						
detestore1			·					
Choose management portgroup for vST's	1et vNic:							
Ulla-Monitor-eschost1.mydatacenter.com	n-vSwitch0							
Note: Management pg is used to route all y promiscuous mode, mapping to vST's 2nd	vST's network trai vNic.	fic to vIC. " Is create	d and put on					
You can get IP settings assigned automatik you need to ask your network administrato Obtain an IP address automatically C Use the following IP address	cally if your netwo r for the appropria	rk supports this capa ta IP actings.	bility. Otherwise,					
P adms:	192.168	.0.110						
Subnet Mask:	255.255.254.0 Q 192.168.0.1 Q							
Default galeway:								
Cobtain DNS server address automa	dicały 558 – – – –							
Preferred DNS server:	192.168	0.20	•					
Alternate DNS server:	192.168.0.5							
Enable Transaction Analysis								
Used Storage Size:	0 GB							
Set Storage Size:	10	GB						
			-					
		 Apply 	× Cancel					

Figure 8.30: Enable Transaction analysis

Once transaction analysis is enabled, you can view the transaction logs on your Transaction analysis view.

You can click on any of the bold underlined hyperlink to view more information on the individual transactions.

Status Statistics			
CH Count Max 37 Min: 38		ERRSR.Coorr Max: 6 Hin: 8	
Query Type Statistic	*		
CREATE ART		EREATE Count	GREATE Fail Count
Max: 602 ms		Max: 3	Maio: 9
Min: 550 ms		Mirc 3	Maio: 0
INSERT ART	al	MBERU Gount	NBSCHT Feil Count
Max: 10 ms		Max: 15	New: 0
Max: 2 ms		Min: 14	New: 0
UPDATE ART Mas: 19 ms Min: 7 ms	mhumi	LPDATE Count	UPDATE Fail Court Mex: 3 Min: 0
DELETE ART	huuuu	DELETE Count	DELETE Ful Could
Mai: 7 ms		Nex: 2	Mar: 8
Min: 5 ms		Min: 2	Min: 0
ALTER ART	monuli	ALTER Cours	ALTER Fail Count
Mai: 9 ms		Nexi f	Maix: 9
Min: 4 ms		Min: 1	Mm: 0
DROP ART		DRDP Enunt	DRDP hall Court
Mai: 68 ms		Max: 3	Mai: 9
Min: 35 ms		Mir: 3	Min: 0
SELECT ART Max: 35 ms Min: 1 ms	II.	SELECT Courte Nax: 5 Nim: 5	SELECT Fini Gount New: 1 Nin:1
Other ART		Other Count	Other Heil Count
Mar: 10 ms		Mex: 13	Must 3
Min: 8 ms		Min: 13	Min: 6

Figure 8.31: Click on the underlined text to view transaction analysis

Transactions						ويعددون كالأفعاط المعال						/ x	
Table Search Rule													
Showing 10 \$ entite	Stowing 1 to 10 of 7,760 entries ¢ previous > ned												
Client	Server	Service		ART 0	Not o	Request	Response	Traffic 😄	End Time -				
dbserver (192.168.0.20/57468)	so-do- 01.mydalscenier.com (192.168.0.20/53)	dna	0.430	0.430	0.000	QUERY dna[query]:24.0.168.192.in- addr.arpa Domain name pointer 192.168.0.24	RESPONSE No such name dragouery 24.0.168.192.in- addr.arpa Domain name pointer 192.168.0.24 Authoritative Name Sarver	529	0	0	12/16/2017 11:59:59:999:258 PM	12/16/2017 11:59:59:999:688 PM	
dbserver (192.188.0.26/39303)	ac-dc- 01.mydelacenter.com (192.168.0.20/53)	đra	0.407	0.407	0.000	QUERY dns[query]:24.0.168.192.in- addr.arpa Domain name pointer 192.168.0.24	RESPONSE No such name dna[guery]:24.0.168.192.in- addr.args Domain name pointer 192.168.0.24 Authoritative Name Server	284			12/16/2017 11:59:59.993.734 PM	12/16/2017 11:59:59:994.141 PM	
dbsarver (192.188.0.28/59344)	sc-dc- 01. mydatacenter.com (192.168.0.20/53)	dra	0.372	0.372	0.000	QUERY dns[query]:24.0.188.192.in- addr.arpa Domain name pointer 192.168.0.24	RESPONSE No such name dna[guery]:24.0.168.192.in- addr.arps Domain name pointer 192.168.0.24 Authoritative Name Server	264			12/16/2017 11:59:59.990.884 PM	12/16/2017 11:59:59.091.256 PM	
dbsarver (192.168.0.26/36226)	sc-dc- 01. mydalacenter.com (192.168.0.20/63)	dra	0.504	0.504	0.000	QUERY dnsiquery :24.0.168.192.in- addr.arps Domain name pointer 192.168.0.24	RESPONSE No such name draguery 24.0.168.192.in- addr.arps Domain name pointer 192.166.0.24 Authoritative Name Server	264			12/16/2017 11:59:59.881.745 PM	12/16/2017 11:59:59.882.249 PM	
dbeerver (192.168.0.26/38963)	sc-dc- 01.mydatacenter.com (192.188.0.20/53)	dra	0.427	0.427	0.000	QUERY dnsiquery]:24.0.188.192.in- eddr.arpe Domein name pointer 192.188.0.24	RESPONSE No such name dratguery]:24.0.168.192.in- addr.arpa Domain name pointer 192.168.0.24 Authoritative Name Server	284			12/16/2017 11:59:59.863.204 PM	12/16/2017 11:59:59.863.631 PM	
dbeerver (192.168.0.26/58048)	sc-dc- 01. mydatacenter.com (192.168.0.20/53)	dne	0.394	0.394	0.000	QUERY dnajquery 24.0.168.192.in- addrarpa Domein neme pointer 192.168.0.24	RESPONSE No such name dns[quary]:24.0.168.192.in- addr.arga Domain name pointer 192.168.0.24 Authoritative Name Server	264			12/16/2017 11:59:59.849.168 PM	12/16/2017 11:59:59:849:562 PM	
dbaerver (192.168.0.26/51054)	so-do- 01.mydatscentor.com (192.168.0.20/53)	dne	0.395	0.395	0.000	QUERY dnajquery}24.0.188.192.in- eddr.arps Domein name pointer 192.168.0.24	RESPONSE No such name dna[query]:24.0.168.192.in- addr.arge Domain name pointer 192.168.0.24 Authoritative Name Server	264			12/16/2017 11:59:59.837.992 PM	12/16/2017 11:59:59.838.387 PM	
dbaerver (192.168.0.26/41439)	so-do- 01.mydetsoenter.com (192.168.0.20/53)	a ne	0.445	0.445	0.000	QUERY dns[query];24 0, 188, 192, in- addr.arpa Domain name pointer 192, 168,0,24	RESPONSE No such name dratguery :24.0.188.192.in- addr.arps Domain name pointer 192.188.0.24 Authoritative Name Server	264	0		12/16/2017 11:59:59.822.653 PM	12/16/2017 11:59:59.823.098 PM	
dbserver (192.168.0.26/38218)	sc-dc- 01. mydetecenter.com (192.168.0.20/53)	dne	0.367	0.367	0.000	QUERY dns[query]:24.0.168.192.in- addr.arps Domain name pointer 192.168.0.24	RESPONSE No such name draţguary 24.0.168.192.in- addr.arpa Domain name pointer 192.168.0.24 Authoritative Name	528			12/16/2017 11:59:59.810.394 PM	12/16/2017 11:59:59.810.781 PM	

Figure 8.32: Transaction Logs

• **Transaction search analysis** - Users can now search for specific metadata (text) across a multi-tier application chain. For example, you can search for any specific keyword across the datacenter transactions.

The user can search for specific transactions using the search view -

fransaction Det													
Transaction A	nalysis Netw	ork Conversa	tion									G	
Show 10: entries. Showing 1 to 10 of 315 entries.													
Client	Server	Service	EURT 0	ART 0	Net Delay	Requeet	Response	Treffic 0	Retry C	Zero Window	Start Time	C End Time	
VMGWAPPD 5 (10.104.1.5/5 5896)	VMSQL (10.104.1.10 0/1433)	tda	0.428	0.252	0.176	tds[query]:SELECT 1	tds[number_columns]:1 tds[number_rows]:	1078	0	D	09/20/2018 04:11:34.406.234 PM	09/20/2018 04:11:34.406.485 PM	
VMGWAPPD 5 (10.104.1.5/5 6885)	VMSQL (10.104.1.10 0/1433)	tds	0.518	0.294	0.222	tds[query]:SELECT 1	tds[number_columns]:1 tds[number_rows];	1078	0		09/20/2018 04:11:29:264.375 PM	09/20/2019 04:11:29.284.669 PM	
VMGWAPP0 3 (10.104.1.3/6 1881)	VMSQL (10.104.1.10 0/1433)	tds	0.413	0.211	0.202	tds[query]:SELECT 1	lds[number_columns]:1 tds[number_rows]:	1078	0	D	09/20/2018 04:10:58.600.393 PM	09/20/2018 04:10:58.600.604 PM	

Figure 8.33: Search function for transactions

Within the search functionality, the "green +" represents AND and "blue +" represents OR.



Figure 8.34: Search function

The rules can be setup based on 22 criteria's as shown in the picture below.



Figure 8.35: Search Criteria

You can also configure # of transaction records exported in CSV for Transaction Analysis.

orrigition (head)						Export Transaction	Export Transaction Analysis CSV						
Trementine Abalyshe	Hutver Converses						-						1
Show 10 ortran.						Number of entity:	10						1911 Press 199
Chart	Server	Sarvits			- Mee Dalag		100	Apply H. Came	Treffic		0 Sire 1	Stars Time	Ted Time
08438-1081 1100, 1980, 16048046 71	An we birensey 002168.020 (H81168.02050)					D(KAL) (stational) cardinates	1000	Contra de la contra de					BAN MIT YOU MAKE TO
1162,153,2160(3)34 1102,153,2160(3)34 71	Active Directory (V82.108.0.20) (V82.108.0.20/m)						Horsestern	1857-0458 Carver Jahare dra/party/2014- 1001 1929 Million					Carlant Constant
0543-1001 2190-1960-160/0215 81	Active Directory (197)168.02(5) (192.168.0.3555)							1852-DNSE Server Dillow draftparty SIEL & 1001 1949 without					254302-300402300 - M
0418-1081 (192,1880,18899042 5)	Attaction cory (NE218E.0.20 (NO.16E.0.2055)							MithCalor (Server Million) dividipen () (2013 h. 1001 (1976 address)					CTATING TO THE READ AND AND AND AND AND AND AND AND AND A

Figure 8.36: Search count selection

Network Conversation

Network conversation view provides a list of Network conversations between clients and servers along with their End-User Response time, Network Response time and Application Response Time.

ensection Detail									8
Transaction Analysia 🚺	etwork Conversation								
Please select the number (of top transactions to generale	the statistics: [60	0 4)						
Slimt	Server	Bervice	EURT	ART	- Het Delay	~ Tuffic	~ Retry	🛶 Zeco Winstow	Transactions
WAGWAPPO3 (10.104.1.3)	VMSGL (10.104.1.100)	tals	24.060	24.624	0.263	172.65 KB	U	¢	70
(10.104.1.5)	VMBQL (10.104.1.100)	uls	5.180	4.908	0.273	438.34 KB			
WAGWAPP04 (10.104.1.4)	VMSQL (10.104.1.100)	uto .	4.470	4.253	8217	181.58 Kil			60
WWWSUS (10.104.1.57)	VMSGL (10.164.1.100)	104	2,557	2.245	0.312	00.90 KB	0	0	1
MHL7 (10.104.1.25)	VMSGE (10.104.1.100)	1050	1.065	1.095	0.000	7.02 MB	0	0	а
WAGAN/PP02 [10.104.1.2]	VMSGL (10.104.1.100)	uls	0.909	0.661	0.808	94.70 KB			60
MBOLMON 10.104.1.53)	VMBCL (10.104.1.100)	'uto	0.616	0.058	0.150	55.81 MB			
MIGWAPPO1 10.104.1.1	VMSGL (10.104.1.100)	10 8	0.567	0.090	0.173	42.54 KB			40

Figure 8.37: Network Conversation

8.3. Service Grouping

Service Grouping page shows a list of all mission critical VM's servicing applications that are essential for the smooth functioning of the datacenter.

8.3.1. Adding a VM to the service resources page

VM's that are co-dependent must be added to the group. There are multiple ways to add VM's into Service Groups. The easiest way from the dashboard is to click on the virtual machine of interest, and "Add to Service group".



Figure 8.38: Add VM to service group

Add the VM to the correct group in to view it from the service grouping page.

71



Figure 8.39: Select service group

Figure 8.39: Add to service group from dependent service map

8.3.2. Monitoring a Service Group

Service Gro	ouping								<u>A</u> 2	£ +
• •	Group Name	 Group Type 	O Number Of VMs	 Application Performance 	O Network Health	i 🗘 CPU Health	O Memory Health	O Storage Health	0 Acti	ons
:2:	Abbvie	Dynamic Multi-Tier	9	17	14	60	60	1	Ľ	Ô
	ABT	Dynamic Multi-Tier	11	17	14	60	60	(2)	Ľ	Ē
: :	All-in-One Demo	Multi-Tier	5	11	(8)	60	60	2	Ľ	Î
	bank	Dynamic Multi-Tier	11	12	14	60	60	2	ľ	Ŵ
	Brett	Dynamic Multi-Tier	310	17	14	60	60	2	Ľ	Ŵ
	City	Dynamic Multi-Tier	11	17	14	60	60	2	Ľ	Ŵ
	computa	Dynamic Multi-Tier	11	17	14	60	60	2	Ľ	Ô
-	DEMO VMware Explore	Multi-Tier		17	2	60	60	2	Ľ	ŧ
	dicom	Dynamic Multi-Tier	11	17	14	60	60	2	Ľ	面
-	Eric test	Multi-Tier	10	2	60	60	60	60	Ľ	盲
	ERP	Multi-Tier	24	2	14	60	60	60	Ľ	ŧ

On the service group page, click on the group that needs to be monitored.

Figure 8.40: Service groups

Click on the group name to view the map and other details about that service group.
Vobvile					4 Dynamic	Multi-Lier (9.9Ms)					1 To Overvie
pplication Map	Conversation	Table	Alarma	Usar Experiance	Log Anal	ysia.					
Abbvie											
				Tier 1						Tier 2	
				ALCAS	Gia-Janos hi- mes lancedh taga ana la agu la ana la agu la ana la agu la ana la agu la ana la	 .out-Ostance-01 (Cl Health Socro 100 Services Provided 	Application Pargones Time 22 ms Application Response Time	: 6 GD) Transactions/min 2:30 Transactions/min	Traffials 781 KB Traffials	Pathetals 21 Packetals	
				4.5-62-0 Estutes	Ta-umase	wm htp	1 ms 2 ms	188 0	157 KB 18		
Wwate						maapo	Time	52	583 B	t)	
						5080	77.009	81	4.97 KB	5	
				+9/1234 Intel	.42	O Clieit ori hode to an	eble actions,		0.001100	57	
				BSRCH2	[00:00:29: .2,4m/http:/	72:86 CD]					

Figure 8.41: Service groups

You can build-out your Application Dependency Maps on a tier-by-tier basis, to provide you with the ability to visualize dependencies that matter to you. This editing capability allows you to visualize dependent servers as well as clients. This can be added by selecting any VM and then choosing the Add Dependent Server or Client option This feature is only available in the Service Grouping section of the application.

Health Score	Applicati Response	on Time	Transactio	ons/min	Traffic/s		Packets/s
100	34 ms		25		18.34 KB		16
Actions	Services Provided	Appli Respor	cation ise Time	Transactions/min	Tra	ffic/s	Packets/s
0± 0±	top ssh	2	ms ms	6 9	1.3 54	5 KB 41 B	1
Start Capture Remediation Act Properties	lion						
	F 4 4 6 -4	0					
ependent Serv	ers For A4.6-4	8-uila-ui	mas				
ependent Serve	ers For A4.6-4	8-uila-ui	mas				
ependent Servi New Tier + e: Select Service +	ers For A4.6-4	8-uila-ui	mas		Ø	Select All	I De
ependent Serve : New Tier + e: Select Service +	ers For A4.6-4	8-uila-ui	mas v	indows AD-Uila VD	Ø	Select Al	I De Total Selected:
ependent Serve : New Tier + e: Select Service +	ers For A4.6-4	8-uila-ui	mas v	findows-A⊒-Uila-VDi ∕ uila-elastic-5 0-23		Select All	i De Total Selected:
ependent Servi : New Tier + e: Select Service + 48-ania umas	ers For A4.6-4	8-uila-ui	mas v.	Findows AG-Uile VD		Select Al	I De Total Selected:
ependent Servi : New Tier - : Select Service - 48-ailin-umas	ers For A4.6-4	8-uila-ui	mas vu	Findows-AD-Uile VD 1 uille-elestic-5:0-23 1 Dastic 5:0-8 porta		Select Al	I De Total Selected:
ependent Servi : New Tier - e: Select Service - 48-uila-umas	ers For A4.6-4	8-uila-ui	mas w	findows AQ-Uila-VD • Uila elastic 5.0-23 • Dastic 5.0 & porta eteway (00:06:29:72	₩ .t6.coj	Select All	I De Total Selected
ependent Servi : New Tier + e: Select Service + 48-ails-umas Filter VM	ers For A4.6-4	8-uila-ui	mas vu c	findows AD-Uila VD • Uila elastic 5.0-23 • Dastic 5.0 & porta ateway (30:00:29.72	₽.66.CD)	Select All	t De Total Selected
ependent Servi New Tier + e: Select Service + 48-alla-umas Filter VM	ers For A4.6-4	8-uila-ui ter Servic ¢ice ≎	mas vv c G G	Findows AD-Uila-VD Vulla-elastic-5.0-23 Dastic 5.0-8 porta ateway (00.60:29-72 n %		Select All	Image: Description Total Selected:
ependent Servi New Tier + e: Select Service + Readia umas Filter VM VM Elastic 5.0.8 portal	ers For A4.6-4	8-uila-ui ter Servic vice 3	w vv G G Transaction	findows-AS-Uila-VD 2 Uila-eiestic-50-23 7 Dastic 5:9:8-porte ateway-(00:06:29:72 n % 49.0	2:E6:CD)	Select Al	1 De Total Selected:

Figure 8.42: Service group editing

Users can add pre-defined sites from End User Experience to the application dependency maps in Service Grouping. This enables users to identify the problematic areas for performance issues across dependencies for a multi-tier application.

User Guide –v5.2



8.3.3. Conversation Map

Users can visualize the applications or services in use on the VMs. For example, this can be very helpful to visualize applications in use on the VDI desktops.

Appl	cation Map Conversation Table Al	arms User Experience Log Analysis									ß
Clie	nt			Server					,	Applicati	on
Ĩ1	oad-Balancer01 Vindows-AD-Uila-VDI			A4.6-48-uila-u	imas					http	
C	ateway [00:0C:29:72:E6:CD]				r01					icmp https	
	4 6 48 ulla umas 5 62 ulla umas v4.6 .1 1 6 umas 0.3.234 42 Veb-Server01 Veb-Server03			Gateway (00.1	0C 29:72:E6:CD)					icrosoft dns ntp Idap nbns	
								Download CS\	/ 📔 Dow	nload Pi	DF
	8 Filter	O Filter	Filter								
۵	Client	Server	O Service O	Health 🗘	Application Response 🗘 Time(ms)	Transactions/min 🗘	Traffic/s 🗘	RTT 🗘	Fatal Retry 🗘	Actio	n
0	10.3.234.42	Windows-AD-Uila-VDI	ntp	N/A	N/A	N/A	0 B	N/A	0/0	â	£
0	10.3.234.42	Windows-AD-Ulla-VDI	dns	100	67	0	0 B	N/A	0/0	â	Ł
0	A4.6-48-uila-umas	Gateway [00:0C:29:72:E6:CD]	http	100	180	0	2 B	5 ms	0/0	Ô	£
					100 M						

Figure 8.44: Conversation Maps

8.3.4. Creating New Multi-Tier and Port-Group based Service Groups

The creation of new service groups is consolidated into a single menu. Click on "New Group" to start creating the groups.

74



Figure 8.45: Creation of Service groups

You have the choice of creating the "Multi-tier", "Dynamic Multi-tier" or "Port Group" based Service Group.

In the "Multi-tier" group option, you are guided through the addition of VMs/servers within your group. Once the group is created, you can add the VMs. Once the VMs are added at a particular tier, you have the option to add dependent servers/clients or move the existing VMs/servers to different tiers using the Rubber-band selection over the current servers.



Figure 8.46: Multi-Node Actions

It is recommended that you start from the front-end and then move towards the backend and add Dependent Servers/Clients along the way.

In the "Dynamic Multi-tier" group option, you can select VMs/Servers based on the applications. They will have the choice of either automatically including all the servers running the selected application or can manually select the servers. With the first addition, Uila adds the servers as well as 1-tier to the left (client).

Configure AD	M Rule on The Current Tier	*
Application:	dns Automatically include all servers having the selected application. Manually select servers having the selected application.	
		V OK K Cancel

Figure 8.47: Configure rules on current tier

You can continue to add more tiers in the same rule as well. At the end, you do have the option to name your Tier levels. This mode is very beneficial to VDI environments, where there are Non-persistent Desktop options being used, where uObserve[™] can automatically keep track of and add new VMs/Servers as they are introduced at any tier.

Config Service Grou	nb nb			×
Group Type	Group Name	Tier Rules	Tier Names	← Prev Completed →
Tier 1:	Web Servers			
Tier 2:	DataBase Servers			
		Fig	ure 8.48: Naming of Tiers	

Finally, when built out, the Dependency Map would show up with the multiple tiers separated out using vertical separators as shown in the figure below.



Figure 8.49: Viewing Service Groups with Tiered separation

8.3.5. Import/Export Service Groups

Also, "admins" have the option of exporting the service groups to other Uila users. Non-admins can import service groups from their peers (NOT Admins) by using the Import Group button.

User Guide –v5.2

port 1	To Users: Select	User Name +	
	Group Name 🗸	Check All	Overwrite
	1KIII	Uncheck All	× ND
	Adam_Dynamic	lesw-user	8 No
	CCK Test	yssey	* NO
	Demo 🗖 Ada	amSwan	8 No
	import from Depend	Btest Tency Mapping	* No
	Ulla-Monitor-dv5witc	t123	8 ND
Total:	6 records.		

Figure 8.50: Exporting Service groups

8.3.6. Import CMDB data

Users can import the service group and the VMs/servers from your corporate CMDB system. Once imported you will need to map the fields for successfully importing the data.

			×	2	+
\$ CPU Health 💲	Memory Health	Stora ^{Impor} Health	t Gro \$	up Actio	ons
180		180			
180	180	180			Ē

Import Group	×
1 Source 2 Group	← Prev Next →
Import From User	
Import group from CMDB.	
1 Upload CMDB	
Figure 8.51: Importing CMDB data	

8.4. Service availability

Service availability provides an easy to view interface for mission critical services running in the user's environment. It provides the status of the service along the with the uptime. This feature would be used to ensure all systems and ports of a critical VM are up and functional. If any of the services or VM go down, the user will be able to identify the root cause quickly. The view will show both the server (needs server up/down configuration in settings) and service status.

Service Availability						
+ Add				E Download	i CSV 🚺 Daw	mioad PDF
Filter	j filu v	Filter	Fiter	mm/dd/yyyy 🗖		
Service	▲ Service Status ≎	Server Status) IP Address/Port	Last Update Time 💲	Duration	Action
http (unknown)	Down	Web-Server01 (Down)	10.3.246.80/80	11/30/2022, 11:01:26 AM	14d 0h 35m 30s	
msrpc (Microsoft Windows RPC)	Down	Load-Balancer01 (Up)	10.3.246.91/54959	11/30/2022, 11:01:26 AM	7d 20h 35m 6s	Ô
ssifhttps (VMware vCenter Server SOAP API 7.0.1)	Up	10.3.234.42 (Up)	10.3.234.42/443	11/30/2022, 11:01:26 AM	104d 5h 55m 59s	Ē

Figure 8.52: Server availability view

8.4.1. Add to Service availability view

Services can be added to the server availability by clicking the "Add" button and use the discovered or custom options.



Figure 8.53: Add service to critical resources

8.5. End User Experience

Uila uObserve[™] measures end user experience for remote sites as well as servers with mission critical functionalities. The user experience is calculated as the sum of application response time, data delivery time and network delay time.



Figure 8.54: End user response calculation

Utilizing the end user experience, the user can identify where the performance issues lie and pinpoint them to either server or the underlying network based on the color coding as shown in the Table 16.1. On this page, you can visualize the timeline based on health, Application Response Time or Traffic.



Figure 8.55: End user response time broken down into data process, ART and network delay time.

Component	Normal (Green)	Minor (Yellow)	Major (Orange)	Critical (Red)
Server	Less than 5% from baseline	5-10% from baseline	10-20% from baseline	Over 20% from baseline
Network	Less than 5% from baseline	5-10% from baseline	10-20% from baseline	Over 20% from baseline
Block	Less than 5% from baseline	5-10% from baseline	10-20% from baseline	Over 20% from baseline

Table 8.6: Color codes for User experience

8.5.1. Slow end user response time due to application server



Figure 8.56: Slow end user response time due to application server

To get detailed information regarding application server performance, click on "Server". The virtual machines hosted on the server will show up and click on the VM that is of concern based on the CPU, memory, and storage health.

User Guide –v5.2

The end user experience page allows the user to identify the dependent services and get to the root cause of an application slow down & Transaction times.

erver Network Client				
🖯 VM Name	Application Health	CPU Health	Memory Health	Storage Health
10.3.234.100		- O	0	0
Alarms Service Dependent Service	s Conversation Network CPU Memory Storage Process	Log Analysis Worst Transactions		
			_ →⊚ uila5.uila.com (TL5_1.2.https)	
	10.3.234:100 (https)		10.3.240.4 (TLS_1.2.https)	
			→● 10.3.240.6 (TLS_1.2.https)	

Figure 8.57: Dependent services within end user response page

By clicking on the deteriorated service, Uila will show up the root cause analysis page with the correlated root cause with CPU, Memory and Storage.

Root Caues View		2 ×
MYRGE. App Response Time for discervar		1
аланан алана	Caraman Santa Santa Caraman Santa Santa Caraman Santa Santa Caraman Santa S	
👟 diacenser Health		Max account parameter
97. Root Cause means the king is repealed by increased EV antimities and the second se	O., Root Cause Protein Fly 100 No trees found	777 s Root Cause Promoting Distance (Course (Course)) (Course (Course)) (Course (Course)) (Course (Course)) (Course) (Co
CPU Health	Memory Health	Storage Health
Dependent Services		Prev 1 Nest
Application (10)		

Figure 8.58: Root cause view

8.5.2. Slow end user response time due to Network

As seen in the Fig 15.5(below) we can click on "Network" to understand issues between the remote site and the host. Detailed information such as Network delay time and retransmissions are provided to further analyze the issue.

ht	tps	http		Elastic		dns	Icmp	
Site 246					i II.	1		
SENC	Clert	SOLAT NEWLON.	ICOL		Scryer No	Beark Chem	Server Network	Clerk -
Site 245 / 1 <u>ttos</u>	•							
Server Network	(len							
Network IIIT Max: 67 ms Min: 33 ms		i na na dana n	In Retran Maic 2 Min: 0	alex.det.lar.		Dut Retran Max: 146 Min: 111		
In Fatal Retry Max: 0 Min: 0			Out Fatal Retry Max: 0 Min: 0			Packets In Max: 3521 Min: 2874	<u>fotbilition</u>	
Packets Out Max: 7073 Min: 6038			Bytes In Mai: 985745 Min: 843075			Bytes Out Max: 5123271 Min: 4286534		
in Reset Max: 0 Min: 0			Out Reset Max: 0 Min: 0			In Zero Window Max: 0 Min: 0		
Dut Zero Window Miss: 0 Milo: 0								

With remote working becoming the "new normal", being able to isolate and troubleshoot end-user performance challenges becomes very important. In this new release, with the end-user experience capability, you can now track down the challenges all the way to the client. By clicking on the individual application/protocol performance chart, you get a list of all the clients that are using that application/protocol and details on the service, network, and the worst transactions for that end-user client.



Figure 8.60: Client analysis

Below are the screenshots of the different tabs available in the interface.

Service Network Worst 7	atiw08274									
Dair Response Time Mas: 155 me Mar. 15 mi	1	6	11	Application Nexponse Time Nex: 75 ms Nm 28 ms		1	transactions Mass 75 Mar 28			1
Same Network Was	Пыбалаб									
Beswark RTT Max: 71 me Min: 25 ma	1		1	as Belgan Marc O Warc O	 		Chall Hellinan Macc D Marc D			
In Facel Ratry Men: 3 Min: 0				Dut Fatal Ratin Max 0 Min: 0			Perioria In Morc 8 Mirc 1	h.	l.	l.
Packees Gar Nes: 7 With 1	I.	<u> </u>	١.	Synein Mac 2112 Min 108		0	Rytes Cur Macc 4457 Mini Ka]
In Reset Nos: 3 Nin: 0				Duk Resel Skys 0 Win:0			In Zero Window Marc D Mirc D		100	~
Gut Zero Window Merc 1										

scrietor Microsoft Works Tran	on the Treaston									
Application Response Time	- Serve	0 Service	C Request	3 Repty	3 Time					
- 12	6115/324	77055	12888 : (request) 500000; (request) 22888 : (request) 500000; (request) 12888 : (request);	-943: (request_station):1353 (request):	06/13/3022 05:21 FM					
	62,454,752		ereactional reactions to the reaction of the r	and tradical contract radical, radical	(8x1+x212) (HSS1 + M					
	5214515126	1920	52592 voljaniver, na nejseli ngywin dalam kutosti, tan 60820, ki jan verjeana (sedingaver,	52.149.151.26/443	08/15/2525 05/40 FM					

Figure 8.61: Client analysis tab options

8.6. Horizon VDI Observability & Troubleshooting

With the integration with VMware Horizon, Uila uObserve[™] users have deep insights into the entire VDI deployment, VDI sessions & Host level GPU metrics for faster troubleshooting at the end-user level.

With the new VDI Dashboard, users have deep insights into critical metrics for their VMware Horizon deployment. Users have access to Application traffic over VDI, VDI Desktop Session status, Blast Protocol metrics, PCoIP metrics, etc.

Horizon Integration Configuration 1) Go to settings --> Global Config 2) Click New -

User Guide –v5.2

/ST Configuration Alarm Configur	tion Software Update	VIC Configuration	Security Configuration	Device Monitoring	Server Monitoring	User Experience	Global Confi
acket Capture Configuration							
Forward packet options:							
💽 To Uila Wireshark VM.		IP or Host/VPC Nar	ne:	192.168.0.1			
To third party packet broker.		IP or Host/VPC Nar	ne:	192.168.0.1			
		Packet Type:		GRE			C ERSPAN
✓ Save							
Save ortzon VDI settings New Hortzon Admin Host Name/P		* Use	name		\$	Domain	
Save ortzon VDI settings New Hortzon Admin Host NameIP		- User	name	No data available	≎ e in table.	Domain	
Save ortzon VDI settings New Hortzon Admin Host NameIP		▲ Usea	name	No data availabid	≎ e in table.	Domáin	
Save Save VDI settings Horizon Admin Host Name/IP		* Use	name	No data available	≎ e in table.	Domain	



3) Add the necessary information to integrate with VDI -

acket Capture Configuration	Horizon VDI settings	÷	
Forward packet options; To Uila Wireshark VM. To thind party packet broker.	Horizon Admin Host Name/IP: Username:	Es Es	
✓ Save	Password: Domain: Collect Process Level CPU and Memory Resou	rce Metrics	ERSPAN
+ Naw	I Test 🌣 Advanced	V OK K Cancel	
	Herneme	A Bunda	
Horizon Admin Host Name/IP	Userhanie	🗸 Demain	

Figure 8.63: Horizon Integration configuration

Here is a list of the charts that are available for VDI in this new release:

Application Traffic Distribution	% Packet Loss for Transmitted PCoIP Packets (VDI Desktop to End-User)
Application Traffic Distribution by Time	% Packet Loss for Transmitted PCoIP Packets
	(VDI Desktop to Client) by Time
VDI Desktop Sessions Status	Transmitted PCoIP: Average & Peak Packet Loss
	(VDI Desktop to Client)
VDI Desktop Sessions by Display Protocol	% Packet Loss for Received PCoIP Packets
	(Client to VDI Desktop)

VDI Desktop Session Logon Time	% Packet Loss for Received PCoIP Packets (Client to VDI Desktop) by Time
Blast Protocol Packet Loss %	Received PCoIP: Average & Peak Packet Loss (Client to VDI Desktop)
Blast Protocol Packet Loss % by Time	PCoIP Protocol Round Trip Latency
Blast Protocol: Average & Peak Packet Loss	Blast Protocol Round Trip Latency



Figure 8.64: Overall VDI Metrics

You also have the option of viewing the information in a consolidated manner for your entire Site, Pods or Pools by accessing that information by using the "View" button and then the "Horizon VDI" Tab.



These views are also customizable for any time-period you select.

05/17/2021 09:47 AM - 05/18/2021 09:46 AM	1H	6H	12H	24H	Customize	C
Figure 8.66: Time S	electio	n for th	e VDI Da	shboard		

You can also use the "Custom Dashboard" option from the "View" tab to customize your various VDI views and compare them in real-time. For example, you can compare Blast performance between 2 different Pods in this custom view.

	×		Summary	Config Dashboard
+ Prov Finish ++	•	Pool	Group Type	C Layout O Window
	~ -	VDI-Win10-IC-Timing-NEW	Group Name	
0		Application Traffic Distribution	Stats Type	Horizon VOL Summary 👻 🖬
	Cancel	🗸 ок		•
	0	c		•

Figure 8.67: Customizable Dashboard

In the sessions tab on this page, for each user session, you can visualize the username, associated virtual desktop VM, session start time, protocol, logon duration, pool or farm information, status, etc.

View	DC-UilaTech-01																38
Sum	mary Blast PColP	Session															
	O Film	0 Filer	C Filer	Filer Y	file Y									O Filter.	O Film		
8	User +	Desklop 💠	Pool or Farm	State 0	Protocol 💠	Logon Duration(ms) \$	Network	Health C	CPU Heal	n:	C Memory	Health O	Storage Health 🗘	Client	IP Address 🗘	Start Time O	Action
0	ula.com/Administrator	win10-FC-1	vdi8-win10- full-clone	Disconnected		NA	100	o me 97 B/s	100	I	(100	1	100	DESKTOP- ONADVKH	10.3.252.89	5/14/2021, 12:32:14 AM	Ø
0	ula.comVaini1	VDI-IC- TimNew2	VDI-Win10- IC-Timing- NEW	Connected	BLAST	21850	(100 ² K	me 26 B/s	100		(10)		100	DESKTOP- ONADVKH	10.3.252.89	5/13/2021, 10:48:01 PM	\$
0	ula.comVsimi1	VDI-IC- TimNea3	VDI-Win10- IC-Timing- NEW	Connected	BLAST	35019	100	0 B/s	100		(10)		99	DESKTOP- ONADVKH	10.3.252.89	5/14/2021, 12:21:24 AM	۲
0	ula.comV/mi1	vdiS-IC-5	vdi-desidop- IC	Disconnected		N/A.	100	M B/s	100		(10)		100	DESKTOP- ONADVKH	10.3.252.89	5/14/2021, 12:22:06 AM	۲

For every session, you can measure the time for every step in the logon process like broker duration, agent duration, app launch duration, etc. and isolate issues leading to failed or slow logins for your VDI end-users.

😑 ulla con/kimi1	i i	VDI-IC- TimNew2	VDI-Win10- IC-Timing- NEW	Connected	BLAST		21850	100	0 ms 2.26 KB/s	(100	1	100	r	100	DESKTOP- ONADVKH	10.3.252.89	5/13/2021, 10:48:01 PM
Logon Duration	Session	Alams	Dependent Services	Conversation	Network	CPU	Memory	Storage	Process								
Logon Tim	e				05/13/202	1 10:47 1	PM										
Logon Du	ation				21850 ms				_								
Broker	Duration				1339 ms				-								
Age	nt prepare D	Juration			1125 ms				_	-							
Pio	ocol Slartup	Duration			1125 ms												
Aut	nentication S	Startup Du	ration		N/A												
Agent	Duration				20511 ms												
Clie	nt Connect V	Wait Dural	lion		1457 ms												
Clie	nt Logon Du	ration			19053 ms												
	icarrispin				1600 mc												

Figure 8.69: Logon Duration for user sessions

The Sessions tab will show detailed network statistics.

Logon Duration Session	Alarms Dependent Services Conversation Ne	twork CPU Memory Storage Process	
Bandwidth Uplink Max: 153.6 K Min: 4.4 K		Bytes Transmitted Max: 77.8 M Min: 254.1 K	Packet Loss Uplink Max: 0 Min: 0
Round-Trip Time Max: 3 Min: 1	<u>"</u>		

Figure 8.70: Session Statistics

The Dependent Services tab for VMware Horizon[®] versions 6 or higher, automatically displays the Application Dependency Map which can provide the different tiers of the entire VDI environment, including thin clients, VDI desktops, as well as critical infrastructure components such as the Connection server, Domain Controller, etc. With this automatically generated map, Uila users are able to automatically highlight the bottlenecks in their VDI environment.



Figure 8.71: Application Dependency Mapping for VMware Horizon

Also, for the associated virtual Desktop VM, users have full visibility into the associated alarms, conversation, infrastructure resources, applications in use and process information.

User Guide –v5.2

Section M	lep Post									
mé	File Cesting	Later 9M/agene	t tterPlai o Fam							
User -	Client	O Desktop	© Pool or Farm	O Protocol	🗧 Start Time	Network Health	0 CPU Health	O Nemory Health	C Storage Health	C Action
Cita.co muser1	MacDook Pro (3)(1/2,1) 01)	6.1 vdi8-win10-1			02/19/2021 11:46 AM	000 000 00 Bits		0		۲
Name	Uependent Services	Conversation Network								
Miware				vd8 win10.1						
<u>External 1</u>							••11 3 240 (top,SVB	10 n2,dns, krb5)		

Figure 8.72: Additional details for Virtual Desktop

You can also visualize the last 7 days history of any VDI user's session login data. You can access that information by clicking the icon in the Logon Duration column for the user sessions as shown below.



ser Na me : 2	ame : uilla.com\kimi1 2021/9/21 下午11:59 ~	2021/9/28 下午11:59						
	8 Filter	S Filter	Fitter	×		6 Filter	8 Filter	
8	Desktop	Pool or Farm	≎ Protocol	Cogon Duration (ms)	Logon Time	Client	≎ Client IP	≎ Start Time
•	farm-desktop1	farm-desktop	BLAST	27324	2021/9/23 下午 3:49:15	MSI	172.16.200.3	2021/9/23 下午 3:49:30
e	farm-desktop1	farm-desktop	BLAST	4904	2021/9/27 上午 11:23:16	MSI	172 16 200 3	2021/9/23 下午 3:49:30
•	VDI8-win10-FC1	VDI8-win10-FC	PCOIP	20592	2021/9/28 上午 10:49:42	MSI	172.16.200.3	2021/9/28 上午 10:49:53
0	farm-desktop1	farm-desktop	BLAST	13388	2021/9/28 上午 11:16:00	MSI	172 16 200 3	2021/9/28 上午 11:16:11

Figure 8.73: Historical user login tracking

You can get alerted to VDI issues that are impacting your environment including user logon time, Desktop protocol round trip time and packet losses.

Threshold Settings				
Default				Š.
Stat Type	Critical Threshold	Major Threshold	Minor Threshold	Actions
Logon Time	18	0.5 s	0,1 9	ß
PColP Protocol Round-Trip Latency	3 ms	2 ms	1 ms	ß
PCeIP Rx Packet Loss	3 %	2 %	1 %	ß
PCoIP Tx Pecket Loss	3%	2 %	1.5	Ľ
Blast Round-Trip Time	3 ms	2 ms	1 ms	ß
Blast Packet Loss Uplink	3%	2%	1.%	ß

Figure 8.74: Configure threshold for VDI alerts

Severity 🤟		Alarm Type -	Entity -
Crisca	Eritical — Horizon VIII	Herton VDI	VD/8-wint0 FC
	19 (100%)		VUIS-edista C
Files V Files	riter 2	• Eller	
Severity 🗸 Entity Type 😂 Entity	🗘 Type	≎ Count 🔅 Message	🗢 Time
Hanizon VDI		1 Average Logon Duration was 13s over baseline 0s	2021/9/28 上午11.15.00
Horizon VDI		7 Average Blast Round Trip Time was 5ms over baseline 1ms	2021/9/28 下午12.45.00
Hodzon VDI VDI8-win 10-KC	Horizon VIN	1 Average Logon Duration was 14s over baseline 0s	2021/9/28 1 + 2:15:00

You can also visualize the connectivity status between your critical VDI Desktop VM and the VMware Horizon Connection Server.

• Filter	• Filter	R Filter
DNS Name	♀ Power State	
vdi8-win10-ic4.uila.com		CONNECTED
vdi8-win10-0.uila.com		AVAILABLE
vdi8-win10-ic1.uila.com		ALREADY_USED
vdi8-win10-0.uila.com		CONNECTED
vdi8-win10-ic3.uila.com		AGENT_UNREACHABLE
vdi8-win10-0 uila com Total: 7 records.		AVAII ARI F

Figure 8.76: Visualization of Connectivity status

Horizon VDI session data can be exported in the CSV and PDF format.

Vie	N :	Produ	tior	n																	-
Sum	nmary	Bla	st	PColP	Sessio	'n															
																	a D	ownload CSV	A	Downlo	oad PDF
	0	Filte		R Filte) Filt	. [F V	Filt 🗸	2								6 Filte	B	Filt	
۲	Use	,	ì	Desktop	≎ Po Fa	ool or arm	¢	State 🗘	Protocol≎	Logon Duration \$ (ms)	Peak Packet Loss (%)	Peak Round- Trip ۞ Time (ms)	Peak GPU Usage (%)	Network Health	сри 🗘	Memory 🗘	Storage 🗘	Client 🗘	Clien	t IF A	nediation Action

Figure 8.77: Export VDI user session data

Nvidia GPU Analysis

uObserve also provides intelligent NVIDIA GPU metrics using the NVIDIA System Management Interface (NVSMI) to allow desktops teams to provide the maximized performance for GPU-enabled virtual desktops. With this update, desktop teams can now enable their hybrid virtual desktop enabled workforce with optimized performance, similar to GPU-enabled desktops.

Use the slider bar on top to see trending information on GPU usage, memory usage and peak VM count.

Figure 8.75: VDI alert visualization

Uila's new GPU monitoring capability allows users to tap into critical GPU insights like VM-level Peak GPU usage, frame buffer, GPU decoder/encoder usage, memory usage, etc. for the individual user sessions. It also provides host level trending metrics like GPU ID, driver version, number of user sessions using GPU, frame buffer, GPU decoder/encoder, peak/average GPU & memory usage.

	<u>.</u>		and the set of a set of the second	ner andre syn i staat	a da andre da ana an	al sheadle	onna di
Health	E 44	D. 84	(CPPR)	26.2			6.4
0.14		D	0	2.0			
E Newson:		ç ayun	😄 tatvis Version	(iii) (iii)	k ve saaa g	Pactors stage ()	Average SP10
O 110		B B B B (1)	1541 1940			.D'h	
0 prx		at the state of the	150 100		a	32%	
O #*0		1.0.10A	120 9.0			315	
0 mo-		x xx xx x x	450.102		4	e5	
0 no-		domoto.	-50.102			25	
0 0.0-		R MOROA	480,102			40%	
0 mai		a) (0.0203	10411917		- Z	170	
0		11 (0 (2×11)	100/100			675	
• <i>us</i>		XXXIII	197-100		. E.	345	
0 m/		3030000.3	450.056		5	205	
0 too-		30.30.30.0	-490, 102		1.2 T	275	
0 max		# 10 (B) /A				(173)	
0 1/2		# # # # #	1041.1817			80	
d 100.		1.0.0.m	1501910		. ú. (80	
Teeding Servor							
SPUCing Ber 30 % Ber 19			Gentley Gents Gents			Twenty Uriger Mex 54 % Main 175	
Ver. # N							

Figure 8.78: GPU hosts and metrics



Figure 8.79: GPU metrics

9. Infrastructure

9.1. Network Analysis

Network Analysis view has a collection of visualization tools; Flow Analysis, Network Conversion, and Table views. Each view is specifically designed to enhance your ability to quickly:

- Identify which infrastructure entities are impacting the Network Health in the Time Frame that is being monitored (one with the Red or Orange color)
- Review network round trip time, application response time and traffic volume of each application service (Classifier) of the respective entity.
- Facilitate further drill down to correlate Application performance impacts.

Network Analysis view is directly launched from the Tool Pane menu, and it consists four tabs (views):

- Flow Analysis view: Visualize how your vAPP network traffic traverses through physical devices (ToR switches, hosts), virtual entities (vSwitch, Port Group, vAPP, VM), and finally, to Application Services (or Classifier) in the data center.
- Subnet Analysis: Visualize usage trending and conversations for subnet to subnet communication.
- Network Conversation view: See top-N (100) network traffic volume pairs between VM's and applications served by the VM, and its associated network performance and application performance metrics.
- Network Table view: Organize by all VM's in table view. See Chapter 7.3 Network Performance Metrics
- Alarm View: List of Network alerts generated; Round Trip Time (RTT), Virtual Packet Drops, TCP Fatal Retry, or Reset that exceeds thresholds.

9.1.1. Flow Analysis View

Flow Analysis diagram (also called Sankey diagram) is a powerful visualization tool to show you how your vAPP network traffic are traversing across physical devices (ToR switches, hosts, etc.), virtual entities (vSwitch, Port Group, vAPP, VM), and finally, to Application Services (Classifier) inside your entire data center. You can quickly identify where the network traffic hot spots are, and if they are impacting your application performance. See the sample graphic view below:

90

User Guide –v5.2



Figure 9.1: Flow Analysis View

Additional Drop-Down list and Buttons in Fig 10.1:

1. Click to display a drop-down list to select a specific view of:



Figure 9.2: Flow Analysis View

2. Click **III** to display a selection box to select which infrastructure components to display



Figure 9.3: Flow Analysis View

• Select the entities that you wish to display in the Flow Analysis diagram.

Graphic	Definition	Mouse Over Information	Click Action
	Name of physical or virtual entity. Color reflects the	Review network round trip	Enable Analyze
_	network round trip time grading at this entity.	time and traffic volume of each application service	Performance. Launch Application
		(Classifier) of the respective entity.	lopology with filtered view.

Table 9.1: Flow Analysis Graphic

Users can also filter the number of nodes that can be viewed on the Network Analysis screen. The options include 100 nodes, 200 nodes and All nodes based on the traffic volume.

9.1.2. Subnet Analysis View

Users can visualize subnet to subnet traffic to identify network bottlenecks and identify top talkers for those conversations. You also have deep insights into the usage trending and conversations taking place within a subnet.

You have access to all the communication-to-subnet traffic analysis.



Figure 9.4: Overall Subnet analysis

You can dig in deeper to visualize the overall RTT for the subnet-to-subnet communication, and retries, fatal retries, packets, resets, bytes and zero window for the bi-directional communication between the subnets.

Usage Trending	Conversation					ويور الالار وحديدة			t	Overview
Network										
Network RTT Max: 4711 ms Min: 578 ms			Ι.							
Internal Test 192 -	- 255 -> Dot 0 0 - 12	27								
Retry Max: 8 Min: 0		. 1.	h	Fatal Retry Max: 0 Min: 0			Packets Max: 21.7 K Min: 1.9 K	1.1	_1	
Bytes Max: 33.9 M Min: 1.1 M				Reset Max: 6 Min: 0	1.1		Zero Window Max: 0 Min: 0			
Dot 0 0 - 127 → In	ternal Test 192 - 2	55								
Retry Max: 24 Min: 1	11	11		Fatal Retry Max: 0 Min: 0			Packets Max: 23.6 K Min: 2.0 K			
Bytes Max: 37.7 M Min: 894.1 K	_		1	Reset Max: 2 Min: 0			Zero Window Max: 1 Min: 0			

Figure 9.5: Usage Trending for selected subnet

Visualize conversation details and metrics within the subnets.

Flow Analysis Subnet analysia Network Conveniation	Tablo Alarma						_		
Usage Trending Conversation									vew
Source		Destination						upplica	hon
Internal Test 192 - 255									
		eschoal 3 mydataceriter.com						40	
		- hypers 62 mydalacanter com						doarp	
		- SMI Server (192,185,0.8)						WI	
		162 165 0 23						perma	
Centiset-DevPortel-VIC		WebBerver02	-					10	
		DBServer 2						JDA-ss	
		- Hortzon Connection Server						-	9
		VMwara vCnoter Server Applaces – new1							
Source	Destination	O Sentos O	Health ()	Application Response () Time (ms)	Transactions Jonin C	Treffic is ()	RTT (ms) 🗘	Ar	son
	hyperv-02 mydatacenter.com	dowpe	160	61	0	0	3	۰	*
	hyperv-02.mydatasenter.com	merpe	100			23 B		a	±
	hyperv-02.mydetscenter.com		NA	NA	NGA		NIA -	٠	٠
	humany 02 mediatacenter com		100			40 B		•	٠
	ngper Facing adapted in the set	2019.6							
	Horizon Connection Server	https	100	204		78 8		٥	*
	Harizon Connection Server SMB Server (182.168.0.8)	intpa disergic	100 100	204 12		78 B 4 B		0 0	*
	Harizon Connection Server SMB Server (192:168.0.8) SMB Server (192:168.0.8)	titps diserpc marpc	100 100 100	204 12 1		78 B 4 B 22 B		0 0	*
	Hardian Correction Server SMB Server (192, 166.6.8) SMB Server (192, 166.6.8) SMB Server (192, 166.6.8)	titps deepc marge: top	100 100 100 NA	204 12 1 NW	0 0 1 NiA	78 8 4 8 22 8 0		0 0 0	*

Figure 9.6: Conversation details for selected subnet

9.1.3. Network Conversation View

Network Conversation provides three types of diagrams to view network traffic volume pairs between VM's and applications served by the VM, and the associated network performance and application performance metrics

• Top-N Chord View -

Top-N Chord view displays the top 100 highest network traffic volume VM pairs.



Figure 9.7: Top-N Chord View

• Top-N Sankey View -

Top-N Sankey view displays the top 100 highest network traffic volume VM pairs from left to right.



Figure 9.8: Top-N Sankey View

• Table View -

The Table view lists all the conversations in a tabular format, and also provides critical network metric trending information.

Row Analysis Submit Analysis Network Conversa	ition Table Alams							_	
lop N Chend Top N Sankay Table									
							Downlose 750	🔺 nav	un kasi SPCP
0 Rim	© (10)								
E VNA	© VM B	O Total Traffic C	A8 0		atal Netrics 🗢 Nesot	ê Zere	window O RTT		Action
Packets In Maxe: 4 Min: 1	Pockets Out	- 1			Bytes III Mac: 612 Mite: 60				
Bytes Cut Mas: 677 Min: 60	NUA NUA								
0 ulevic-i Dove (192 163.0 196)	MySQL-N2 (sbC2 as shifts a com/152.106.0.89)	600 h	500 R	700 D	878	nm	0.93	ым	±
Welvare sfertter Server Appliance - new1 Overteer myderarenter.com/192.168.0.21)	esahostā mydata serturi som (192-168-0-15)	7.15 MB	3.03 MB	4.10 MB	8/8	0.0	00	0 ms	±
o en webserver (10.10.10.12)	001550001703	2.71 MB	775.34 KB	1.35 MB	8/8	0.0	0.92	0 ms	*
O ulevic-10-ove (192.163.0.199)	Dis-Lis-102 (dis-lis-102 m/maximu/102/168.0367)	500 S	302.0	300 8	8/8	wu	uvi	N/A	*
ullevic-6 D-ske (192.163.0.194)	hyperv-10. mydatakamer.com (152, 168, 0.23)	220 5	301.0	3 0 01E	8/8	0.41	141	N/A	±
 Centosi DevPonal VIC (devponali vitud acom/192 168 1,195; 	095erver-2 (web/o2.dtybank.com/092.168.0.32)	8.5° KB	451 KA	4.03 KB	8/8	DV10	an	0.evr	*
In Zem Window Mar: 0 Min: 1	Dur Zein Win Nias: 0 Nin: 0	dow			In Faral Reny Max: 0 Mirc 0				
Out Fastal Raviny Max: 0 Min: 0	Nin: 0	4	-	-	Dut Reset Max: 2 Mirc 2				
Packets in Mase: 15 Min: 14	Packets Our Max: 11 Min: 11				Bytes In Max: 976 Min: 916	I			
Bytex Dut Nax: 519 Nor: 519	RTT Nas. 1 ms Nim 0 ma								

Figure 9.9: Table View

9.1.4. Network Alarm View

Network Alarm view displays network alerts when network performance metrics are above the baseline thresholds. See Chapter 7.3 Network Performance Metric and Chapter 5.2 Health Score and Alarm Definitions.

Network Alarm view provides a detail list of what performances metrics that cause each network alert in the time matrix window you selected. Expand the time matrix window will show more alerts (if any) that were generated in the expanded time slot. If any application service shows performance issue, the name the application service will be displayed in the 'Services'. However, both the network alert and the application performance issues exhibit at the same time do not imply that the cause of application slow is related to networking issue. You need to select and click the root cause view to find the actual root cause.

Severity	Mossage	Mouse over	alert to view	details and	Stat-Type	C Baseline	Start Time	End Time
	Average Virtual Packet Drop Oracle_11g-n3 was 1 time	app services		actans and	Virtual Packet Drop	0 time	09/01/2017 12:45 PM	09/01/2017 01:00 PM
	Average Round-Trip Time for SQL_2012-n1 was 3006 ms	🗩 Oracla_11g-n3 (0	Oracle, 11g-n3 (CPU: 4 x 1.81 GHz Memory: 2.96 GB)			2836 ma	09/01/2017 12:30 PM	09/01/2017 12:45 PM
	Average Round-Trip Time for	Health Score	Network Resp. Time	Fatal Retry	Virtual Packet Drop	Traffic/s	09/01/2017 12:45 PM	09/01/2017 01:00 PM
	SQL_2012-n1 was 2735 ms	84	1 ms	0/0	8/16	25.27 KB		
		Services Provided	Application Resp. Time	Transactions per minute	Trafficies	Packets/s		
		apdy	0 ms	2.9 K	24.95 KB	145		



9.2. Network Device Observability

Uila uObserve[™] users can pinpoint the performance bottleneck down to the network for any dependency chain for a multi-tier application. Users are armed with operational insights on network devices, such as switches, routers, load balancers, firewalls, etc. with detailed info into the availability status, utilization, congestion, errors, discards. In addition, users get full visibility into connected VMs for every single network switch port and its respective Application, CPU, Memory and Storage Health to pinpoint performance challenges due to the network device bottleneck. For remote location monitoring, in addition to its existing end-user experience monitoring capability to measure the performance from the end-user's perspective & proactively identify issues, users can visualize the status of the WAN link and the interconnection status with the rest of the switch fabric.

The Network Device view will display all the network devices (switches, routers, firewalls, load balancers) along with their port information in the main windowpane. For each network device, you can obtain detailed status and configuration settings for network devices including vendor, model, OS versions, uptime, serial number, VTP domain, detailed description, IP/MAC address, etc.

ystem Name	Cisco Catalyst WS-C4006
Location	gambit
Contact	support@gambitcomm.com
/endor/Model	cisco / wsc4006
05/Version	catalyst / 6.3(4).Copyright
Serial Number	0
Description	Cisco Systems, Inc. WS-C4006, Cisco Catalyst Operating System Software, Version 6.3(4), Copyright (c) 1995-2002 by Cisco Systems, Inc.,
Uptime	50 days, 14:51:06
Layers	0100000
MAC Address	
P Address	10.1.120.19
TP Domain	

Figure 9.11: Network device properties

Open (no Ethernet cable plugged in) and down/disabled ports are indicated by a "Hollow" port icon. If it is "green", the port is open, while "red" indicates that the port is down or disabled.

cat-5505 (10.1.120.13) cat-5505 (10.1.120.15) ProCurve 2524 (10.1.120.2)	Port Name: 18 Port Name: 18 Status: down Bandwidth: 10 Mbps
cat-5505 (10.1.120.13)	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
cat-5505 (10.1.120.15)	Status: open Bandwidth: 10 Mbps
ProCurve 2524 (10.1.120.2)	

Figure 9.12: Network port status

For each port, you can visualize the following statistics in a chart format (1st tab).

- In/Out Utilization
- In/Out Discards
- In/Out Errors
- In/Out Unicast Packets

Uila – © 2023

- In/Out Non-Unicast Packets
- In/Out Octets
- Queue Length
- Unknown Protocol packets

The following charts define the solid colors seen for the ports in the User Interface.

- In/Out Utilization
- In/Out Discards
- In/Out Errors

You can set the thresholds for the parameters from the "Threshold Settings" tab for individual ports.



Figure 9.13: Network alarms threshold setup

The Default baselines are as follows:

- Utilization: 80%
- Discards: 10,000 pkts/min
- Errors: 100 pkts/min

Alarm is generated based on the performance metric's delta from the baseline. Alarm is generated every 15 minutes by default.

Threshold is defined as the % value that crosses the baseline.

Severity is a user definable indicator to help identify the criticality of the performance metrics monitored to alert user if an entity or entities is (are) about to impact the Application's performance.

Delta from Baseline	Alarm Severity	Color
Less or equal to 5%	Normal	Green
Between 5% and 10%, including 10%	Minor (1)	Yellow
Between 10% and 20%, including 20%	Major (2)	Orange
Above 20%	Critical (3)	Red

Note: These standard color definitions are applied throughout Uila User Interfaces for consistence and ease of recognition.

NoCurve 2924 10.1 120 29				0
Statistics Connected VMs/Da	A1420			K Si w. 10Muja
In UKE Pet Mar: 0-4 Min: 0-5		In Discards Max: 0 Min: 9	In Ernuns Maxi 61 Min 39	
Out Lk8 Fet Max: 0% Min: 0%		Out Discands Mas: 0 Nim: 0	Out Friday Mate: D Min: 0	I
In Occess Mas: 140913 Min: 146623		In Licast Pitts Nat: 2539 Min: 2460	In Nilkast Pitts Mar: 11 Nim: 11	
In Unk Protos Marc D Min: S		Out Octebs Nove: 114512 Min: 112351	Dut Utant Pith Mixe: 3499 Min: 3382	
Out N-Ucart Plans Max: 0 Min: 2		Out Q Lan Max: 0 Nin; 8		

Figure 9.14: Network port statistics

Cross arrow inside the square icon for a port indicates a connection from that port to other switches/routers. The same logic applies for colors, as the solid colors mentioned in question #8. Note: This feature is supported for switches and routers only, and not for other network devices.

This can be used to show the status of the WAN link and the interconnection status with the rest of your switch fabric.

Fx10540356		consenas						
Balikis Kanstal Seide tat								
In Uld Pet More D % Mine D %	In Obscards Miss 1 Mins 0	Man 0 Mar 0						
Curt UEB Per Nanc D % Nin: 5 %	Our Discards Max 8 Min: 0	Qui Sirran Mac Q Min Q						

Figure 9.15: Network port statistics

Also, for each port, you can visualize the Connected VMs/Devices in the next tab. For every VM, you can visualize the Application, Network, CPU, Memory and Storage Health. Further VM statistics (Usage, Alarms, Process, Dependent Services, etc.) can be obtained by clicking on the VM name.



Figure 9.16: Connected VM statistics

You can also visualize alarms in the alarm tab within Network Device if a particular port is congested (high utilization) or has errors (errors, discards).

Raukimu (N OD								
CO AN	DI PU	26.70	10 194		Weatta	ET AN	ESAN	Network Health
Station of the second	Alerent	* *		A. 444	A 100 000		A (1917-194)	
-	Restore	U BAREA	- Net		o the type	10	000000000000000000000000000000000000000	to data contra del
	Average in Discards for cal-3505(10.1.125.1.19485.55.	- cat-dotto(10, 140-11)	sc0	~	in Decime	10	03/19/31/9/02/11/66	Lon Walls George
	Average In Errors for cat 3909(10.1.120.14) was 1920.	Gir 5505(10,1 125,14)	starbit etherinet		In Errors		03/13/2019 02:15 AM	05/13/2019 (01:80 AM
	Average In Errors for cot-SSIS(18.1.120,14) was 1970.	ar-5505(10,1 122,16)	long haul fiber gigs bit othermet	1902	in firmes		05/15/2019 02:15 444	MA DECIDI E DECEDI E DECEDI E DECEDI E DECEDI
	Average in Discards for cm-5505(10,1,120,15) was 55.	une-0500(10.1.120.15)			In Discards		00V13/2019 02:15 AM	00/13/2019 02:30 AM
	Average in Discards for sites(192.168,0.1) see 128.	ubrid(192,198,0.1)	ettő	120	In Distants	10	03/10/2019 02:15 AM	06/13/2019 (D:30 AM
	Average in Errors to : ProCurve 2524(10.1.120.38) was 35.	PreGarve-2524(10.1.120.30)			In Fromes		03/13/2019 02:15 AM	05/13/2019 (21:30 AM
1001	Average in Errors for ProCurve 2524(10.1.120.23) was 65.	PreCurve 2524(10.1.1.20.31)			In Errors		05/15/2019 (02,15 AM	05/13/2019 02:30 AM
	Average in Discards for cal-5805(10.1.120.13) vasi 55.	uk 6909(10, * 120,15)			In Obserds		05/15/2010 02:15 AM	05/13/2019 (02:90 AM
	Average in Errors for ProCarve 2524(10.1.120.30) was 23.	ProGarve 2524(10.1.120.32)			in Errora		05/15/2010 02:15 AM	15/13/2019 (0:30 AM
	Average in Errors for ProCurve 2534(10,1,123,2) was 23.	Prefurve 2534(10.1.120.2)			in Errora		00/15/0319 02:15 AM	00/13/2019 02:30 AM
	Average in Errors for ProCurve 2534(10,1.120.7) see 65.	ProCurve 2534(10.1.120.7)		60	in From	10	03/13/2019 02:15 AM	09/13/2019 02:30 AM
	Swerage in Error for ErroCurve 2524(10,1.120,2) was 30,	FreQueve 2524(10.1.1.20.2)			In Firtors		03/13/2019 02:15 AM	08/13/2019 02:30 AM
	Average in Errors for sal-3505(12.1.120.15) was 1950.	cat-0505(10,1,125,12)	long hast fiber gigstik etherner	1920	In Errora		03/15/2219 02-15 AM	CO/13/2019 02:30 AM
	Average in Discards for VCD427C344500FP(10.1.123.42) was 19521	VC2A27C344500F7(10.1.123.42)	HPVC Rev 10/100 Norker 4.40 X11	1963.0	In Obsands		03/13/2017 2 02:15 AM	CONTRAVEROND ORDERING AMM
	Average in Discards for VED527C344500F7(10.1.123.42) was 13393.	VC2A27C344500F7(10.1.120.42)	HPVC Res-10/100 Norkel 4.40 X10	19580	In Discards		03/15/2319 02:15 AM	ES/13/2019 (02:30 AM
	Average in Discards for VC2827C344500FP(10.1.123.42) was 31.	VC2A27C344920F10(10.1.120.42)	HP VC Res-15/105 Norke 4.40 39		In Discarda		03/13/2017 2 62:15 AM	05/13/2019 02:30 AM
	Average in Errors for cat-0905(10.1.120.12) was 1920.	cel-0505(10.1.120.12)	long haul fiber	1920	in Drora		05/15/2319 02-15 AM	10/13/2019 02:30 AM

Figure 9.17: Network alarms

9.3. CPU Analysis

CPU Analysis view has a collection of visualization tools; Circle Packing, Tree, Table and Alarm views, each is specifically designed to enhance your ability to quickly:

- Identify the infrastructure entities impacting the CPU Health in the Time Frame that is being monitored (one with the red or orange color)
- Review application response time and traffic volume of each application service (Classifier) related to CPU usage %, CPU MHz, and CPU ready % with respect to each element.
- Facilitate further drill down to correlate Application performance impacts by CPU performance.

CPU Analysis view is directly launched from the Tool Pane menu, and it consists of four tabs (views):

- Circle Packing view: Visualize CPU Capacity, and CPU Usage of each VM, host and cluster within the data center infrastructure. The size of the circle is determined by CPU capacity, while the width of the ring is related to the CPU usage of each element.
- Tree view: Alternative view to visualize CPU Capacity, and CPU Usage of each VM, host and cluster within the data center infrastructure. The size of the circle is determined by CPU capacity, while the width of the ribbon is related to the CPU usage of each element.
- Table view: Organize in table view to sort by performance grade of the VM. Refer to Chapter 7.5 CPU Performance Metrics for details.
- Alarm View: List of CPU alerts generated; CPU Usage %, or CPU Ready time (in %) that exceeds thresholds.

9.3.1. Circle Packing View

Circle Packing view allows you to visualize CPU capacity, and CPU usage, and Health of each VM, host and cluster within the data center infrastructure. The size of the circle is determined by CPU capacity, while the width of the ring is related

99

to the CPU usage of each element. When CPU usage percentage reaches certain thresholds, the circle turns yellow, orange, or red, indicating which entity is busy. By comparing the size of all VM circles under a host, you can quickly know how evenly CPU capacities (vCPU cores) are allocated across all VMs. Sometimes, a big VM in term of CPU core numbers may impact its peer VM's performance. Mouse over the element that exhibits health performance issue, you can further drill down to reveal how application response time is impacted.



Figure 9.18: CPU Circle packing view

9.3.2. Tree View

Tree view is an alternative view to allow you to visualize CPU capacity, and CPU usage, and Health of each VM, host and cluster within the data center infrastructure. The size of the circle is determined by CPU capacity, while the width of the ribbon (same as the size of the pie slice) is related to the CPU usage of each element. When CPU usage percentage reaches certain thresholds, a circle turns yellow, orange, or red, indicating which entity is busy. By comparing the size of all VM circles under a host, you can quickly know how evenly a CPU capacity (vCPU cores) are allocated across all VMs. Sometimes, a big VM in term of CPU core numbers may impact its peer VM's performance. Mouse over the element that exhibits health performance issue, you can further drill down to reveal how the application response time is impacted.



9.3.3. Alarm View

CPU Alarm view displays CPU performance alerts when CPU usage or CPU ready metric is above the baseline thresholds. See Chapter 7.5 CPU Performance Metric and Chapter 5.2 Health Score and Alarm Definitions.

CPU Alarm view provides a detail list of what performances metrics that cause each CPU performance alert in the time matrix window you selected. Expand the time matrix window will show more alerts (if any) that were generated in the expanded time slot. If any application service shows performance issue, the name the application service will be displayed in the 'Services' column. However, if both the CPU alert and the application performance issues exhibit at the same time, it does not imply that the cause of application slowness is related to CPU issue. You need to select and click the root cause view to find the actual root cause(s).

Severity -	Message 🗘	Entity	0	Services	Stat	Stat-Type	C Baseline	C Start Time	© End Time
	Average CPU Usage Percentage for Exchange_2013-s1 was 100.00%	VM: Exchange_2	013-61		100.00%	CPU Usage Percentage	80.00%	09/01/2017 01:30 PM	09/01/2017 01:45 PM
	Average CPU Usage Percentage for Exchange_2013-s1 was 100.00%	VM: Exchange_2	013-s1		100.00%	CPU Usage Percentage	80.00%	09/01/2017 12:30 PM	09/01/2017 12:45 PM
	Average CPU Usage Percentage for	VM:	🗭 Exchang	e_2013-s1 (C	PU: 2 x 1.81 GH	z Memory: 2 GB)		09/01/2017 12:45 PM	09/01/2017 01:00 PM
-	Exchange_2013-s1 was 100.00%	Exchange_	013-51	Critica	ıl	100% Minor	0%	CPU	
	Average CPU Usage Percentage for Exchange_2013-s1 was 100.00%	VM: Exchange_2	013	Major	100.00%	CPU Usege Percentage 0% Normal	80.00% %0	09/01/2017 01:15 PM 100%	09/01/2017 01:30 PM
	Average CPU Usage Percer tage for	VM:	Health		TANK AGE	124th 21 Jacobil Story and the		000000000000000000000000000000000000000	00/01/2017 01-15 PM
	Exchange_2013-s1 was 100.00%	Exchange_	Healt	h	Application	Usage	Usage	CPU	080 02017 01.101 m
-	Average CPU Ready for observer	100 change	Scon	9	Resp. Time	Percentage	MHz	Ready	0001/2017 01:45 PM
	was 6.53%	YIM. GUACIN	0		N/A	100%	4378	0.01%	030 1/2017 01.40 PM

Figure 9.20: CPU alarm view

9.4. Memory Analysis

Memory Analysis view has a collection of visualization tools; Circle Packing, Tree, Table and Alarm views, each is specifically designed to enhance your ability to quickly:

- Identify which infrastructure entities are impacting the Memory Health in the Time Frame that is being monitored (one with the red or orange color)
- Review application response time and traffic volume of each application service (Classifier) related to Memory usage %, and CPU Swap Wait time with respect to each element.
- Facilitate further drill down to correlate Application performance impacted by Memory performance.

Memory Analysis view is directly launched from the Tool Pane menu, and it consists of four tabs (views):

- Circle Packing view: Visualize Memory Capacity, and Memory Usage of each VM, host and cluster within the data center infrastructure. The size of the circle is determined by Memory capacity allocated, while the width of the ring is related to the Memory usage of each element.
- Tree view: Alternative view to visualize Memory Capacity, and Memory Usage of each VM, host and cluster
 within the data center infrastructure. The size of the circle is determined by Memory capacity, while the width
 of the ribbon is related to the Memory usage of each element.

- Table view: Organize in table view to sort by performance grade of the VM. Refer to Chapter 7.6 Memory Performance Metrics for details.
- Alarm View: List of Memory alerts generated; Memory Usage %, or CPU Swap Wait time that exceeds thresholds.

9.4.1. Circle Packing View

Circle Packing view allows you to visualize Memory capacity, Memory usage, and Health of each VM, host and cluster within the data center infrastructure. The size of the circle is determined by Memory capacity, while the width of the ring is related to the Memory usage of each element. When Memory usage percentage reaches certain thresholds, a circle turns yellow, orange, or red, indicating which entity is busy. By comparing the size of all VM circles under a host, you can quickly know how evenly a Memory capacity are allocated across all VMs. Sometimes, a high Memory usage VM may require allocation of more memory compared to VM's that are less frequently run. Mouse over the element that exhibits health performance issue, you can further drill down to reveal how application response time is impacted.



Figure 9.21: Memory circle packing view

9.4.2. Tree View

Tree view is an alternative view to allow you to visualize Memory capacity, and Memory usage, and Health of each VM, host and cluster within the data center infrastructure. The size of the circle is determined by Memory capacity, while the width of the ribbon (same as the size of the pie slice) is related to the Memory usage of each element. When Memory usage % reaches certain thresholds, a circle turns yellow, orange, or red, indicating which entity is busy. By comparing the size of all VM circles under a host, you can quickly know how evenly a Memory capacity are allocated across all VMs. Mouse over the element that exhibits health performance issue, you can further drill down to reveal how application response time is impacted.



Figure 9.22: Memory tree view

9.4.3. Alarm View

Memory Alarm view displays Memory performance alerts when Memory usage or CPU Swap Wait time metric is above the baseline thresholds. See Chapter 7.6 Memory Performance Metric and Chapter 5.2 Health Score and Alarm Definitions.

Memory Alarm view provides a detail list of performances metrics that cause Memory performance alert in the time matrix window that has been selected. Expand the time matrix window will show more alerts (if any) that were generated in the expanded time slot. If any application service shows performance issue, the name the application service will be displayed in the 'Services' column. However, if both the Memory alert and the application performance issues exhibit at the same time, it does not imply that the cause of application slowness is related to Memory issue. You need to select and click the root cause view to further pinpoint the actual root cause(s).

	17 1000 - 1000	_								
leverly -	Mensage	0 Em	4	÷	Services	561 C	Start-Type:	C Reading	Alari Time	
	test-N2In6 was 85.48%	VN	Welmart-test-%2	(nő)		85.48%	Active Usage	50.00%	08/01/2017 03:15 AM	09/01/2017 03:30 AM
	Average Active Usage for MySQI N1 was 78.46%	- vn	: My90L-N1			78.46N	Active Usage	50.00%	09/01/2017 03:15 AM	09/01/2017 03:30 AM
	Average Active Usage for Weima tosi-%2h6 was 74.24%	nt- VN	Welmart-test-%2	in5		74.24%	Active Usage	50,00%	09/01/2017 03:45 AM	08/01/2017 04:00 AM
	Average Active Usage for MySQ N1 was 50.97%	vN	MyBQL-N1	Mo deta	ouse ove ails and a	r to view opplication	Act re Usage	50.00%	09/01/2017 03:45 AM	09/01/2017 04:00 AM
	Average Active Usage for Zimbra 8.0-s1 ([test+name]) was 64.12%	-VM Qre	amora_8.0-e (st+name))		servi	Ces Milian	Autive Usage	50.00%	09/01/2017 03:00 AM	09/01/2017 03:15 AM
	Average Active Usage for MySCI N2 was 68.72%	Zimbro	8.0-s1 (best+nam	i) (CPU:	4 x 1.81 GHz P	Aemory: 4 GB)	Autor Unepe		09/01/2017 03:00 AM	09/01/2017 03:15 AM
	Average CPU Bwep Wall for eschoold mydatecenter.com 7429 ms	79	Critical	ili com	15%	Minor Normal	10% - 0711 Swop Mart 70%	Memory Usage 43.07%	09/01/2017 03:15 AM	09/01/2017 03:30 AM
Ö	Average Active Usage for LotusNote_7.5-s1 was 37.99	Health	100.000 7.50		a ())	37.50%	Antra Usarda	50.00%	09/01/2017 03:45 AM	09/01/2017 04:00 AM
	Average CPU Bwep Wall for Exchange_2013-s1 was 133	5001 79	R	sp. Time 442 ma		Jsoge 3.07%	Active	Swap Walt	08/01/2017 03:30 AM	09/01/2017 03:45 AM
	Average CPU Swap Wait for eschost4.mydatacenter.com	Actions	Servic Provid	*	Application Reep. Time	Transaction per minute	Trafficis	Packets/s	06/01/2017 03:30 AM	08/01/2017 03:45 AM
	1917 ms			_						Care in 2011 Care of Aut

Figure 9.23: Memory alarms view

9.5. Storage Usage

Storage Usage diagram is a visualization tool to show you Storage usage and Health Score within your data center physical or virtual entities. Storage Usage view can be launched from Dashboard's Storage Health color wheel, or directly from the Tool Pane menu.



Figure 9.24: Storage IOPS Usage View

Refer to Section 7.4, Storage Performance Metric for Storage metric definition, and how metrics are calculated to determine health score and the associated base line values.

To help investigate performance issues, you can place the mouse over the vertical bar of each storage infrastructure component to reveal the health and performance summary of its upstream and downstream neighbors in a Tool Tip.

You can visualize the Health, Read/Write IOPS and Read/Write Latency for vDisk, Host and Datastores as well.



Users can also filter the number of nodes that can be viewed on the Storage Analysis screen. The options include 100 nodes, 200 nodes and All nodes based on IOPS.

From the Capacity/Usage tab, you can visualize the capacity as well as usage for the storage disks. The size of the circle is determined by storage capacity, while the width of the ring is related to the usage of each element. When Storage usage percentage reaches certain thresholds, a circle turns yellow, orange or red, indicating which entity is busy.



Figure 9.26 Disk Capacity Usage View

10. Security

Uila uObserve[™] 's Cyber Threat Monitoring module leverages its Deep Packet Inspection (DPI) capability to make use of network packet data as the root of truth and identifies advanced threats that are moving laterally (insider threats). Users can detect and manage cyber alerts and anomalous deviations in dependencies for applications that are business critical to the enterprise organization to bring an unique Application-centric view to cyber threat monitoring. Uila provides the necessary Intelligence & Diligence to reduce the attack surface and becomes a force multiplier for security operations teams. Security and Network teams are automatically alerted to the latest malicious threats and attacks, including malware, exploit kits, outbound traffic issues, C & C threats, etc. In addition to the latest threats, IT teams can confidently track the chain-of-evidence for critical Network and Application workload characteristics in real time to identify anomalous outliers such as dependency changes between the critical application and infrastructure resources, deletion or addition of new VMs, etc.

The time slider for security will indicate the levels of threats that have been identified in the deployment.

Beat: me R Correl Producting Davids Ald -	06/06/2019/05/45/48 + 🧶 🔸						💼 Production -
• Networkshipstone			Time (B(CB(20)9)9 Chickli D				
DS PM	Mar 09	03 AM	Najori 5 Nince 0	ANT			166 P.W.
			Figure 1	0.1: Sec	urity Time sl	ider	

10.1 Application Anomaly

You can now visualize Application deviations for your multi-tier applications (created based on Service Groups) indicating anomalous behavior in a single view. In addition to insights into detailed cyber threat event information and outbound traffic behavior to the Internet for the group, you can visualize deviations after the creation of your desired baseline for the application or service. Deviations include unauthorized dependency changes, new applications/services/protocols running on the VMs, additions of unauthorized VMs or tearing down of your mission critical VMs, etc. You can visualize those deviations in the Application Dependency Map and add deviations to the baseline or security policy.

All Service Groups that have been created will appear automatically on this screen. For every service group, uObserve[™] will list if there is any deviation from the configured baseline, Cyber threats that have been identified as well as Data Exfiltration transactions.

🛞 uila		Rankers Richts Contractor Monte And - Contra	121122040 АМ- 🥂 🔶						III Frenchin-
🛄 una 🏛 Production v 🛛 🧐		 vojnijubiliterativa 				NAUL INC.	Announa		
# Desilboard		LO PM.	Non 09						
Application	w.	Application Anomaly							
C Security	е	Group Kerne	Application	Map Devlation		Cyber Threat Roost		Refferation Map	A CONTRACTOR OF A CONTRACTOR A
Application Anistraty	4	ART Group		Dectrion 60			Najor 7		
Threat Detection Delitration Map		DEGRUP		0 Contractional me			ů	Colory B	
🖬 Infrastructure	te.	Countred		0 Conty Research			0	to,my 0	Entrina Sciver B
Stats Browser Alerms		Domain Controller Services		Config Sase in:			D	ioranicy S	trians strive 21
🔛 Reports		Envergence Danabase Senakee		O configuration	91		0	Charry C	t denna Server 15
 Packet Capture Settings & Logs 	e	Pag-Test		O Contry Generation			Kajor S		Torney Server 15
X FullStreen		104		0 Conty Research			Kajor B	Co.my a	terma trair 11
🗩 Logad		74410		 Confgisatel or 			Napr 2		driema bersit 19
		Uta M. H. Child Worksdag		• Configuration			Najor 7		inema levar 25
		Ula New Dame Aselication		O Corrighteed or	<u>1</u>		Kajor B	- n. my -	Science Server 13
		Antoine		• Controllandor			Kapr B	0.172 1	Branna Scher 18
				• Configuration			Kaur 2	tar.m.y Sil	trana saya 6

Figure 10.2: Application Anomaly Overview

106

The first step is to configure the baseline for the known good time for the Application dependencies.

art	Time	s:					End	lime:	5					
÷	S	epte	mber	201	9		÷	🗲 September 2019						
Su	Мо	ти	We	Th	Fr	Sa	Su	Мо	ти	We	Th	Fr	Sa	
	2	3	4	5	6				3					
8	9						8	9						
		1	loday	1					1	loday	1			

Once the baseline is configured, users can visualize the application anomalies or deviations in the tabular format, as well as visually as an Application Dependency Map.

Uila will list all the individual deviations taking place for every asset as part of the Service Group. Few examples include addition or removal of VMs, addition of services, new dependencies, new requests and responses, etc.

* AB	C Group		
Applic	stion Map Deviation Cyber Trzest Event Exfibration Map		
I Devi	iation Table		1
The Distance of the	File VM		
-		- Drail	Action
	Ganeway (020): 29 94 79 (11)	1. New cmp request from 064 0-1601	
	Generaty (Biol School School)	1. New service htp 2. New top request from Grade_11g-r2	
	Garaney (PCEC DA42/9455)	 View Sanet 1. Nov samins dirup: 2. Nov samins dirup: 3. Nov samins dirup: 4. Nov samins dirup: 4. Nov samins dirup: 4. Nov samins dirup: 6. Nov samins dirup: 7. Nov dirup:	
	NysqL#MGT	1. New service inaccorp.hdfs 2. New scrifte kg:	*
	Pertai-NDM-MC	1. New websecket request from cloud-vst-portal!	¥
	se-de-01 mydata enter a am	3. New service isoto	+
-	31/24.05	1. Now were it is in regional to the second se	

Figure 10.4: Application Anomaly Table



Figure 10.4: Application Anomaly Dependency Map

Users can also visualize the deviations for each individual asset, by checking the individual boxes. Also, if the deviation is expected or valid, it can be directly added to the baseline by clicking the "+" button.

10.2 Cyber Threat Monitoring

uObserve[™] users can now get alerted to thousands of cyber threats based on support from the largest group dedicated to advances in the network security industry. These alert categories include malware, exploit kits, port scans, Command and Control threats, OS fingerprinting, Buffer overflows, SMB probes, Obfuscation, etc. Uila supports latest signature support and updates from the largest group dedicated to advances in the network security industry (Snort, Cisco[®] Talos Security Intelligence and Research Group, ClamAV). This can be viewed for the entire Data Center or for a Service Group.

Uila provides graphical summary of the following information:

- Threat Severity (Critical, Major or Minor)
- Threat Models or Categories
- Threat Types
- Threat Source and Destination



Figure 10.5: Cyber Threat Summary

Each cyber threat is also listed with information on its severity level, threat model, type, source and destination, related country and the event count (tracked on a minute-by-minute basis). You can also get transaction analysis details for HTTP, DNS and DB related to the alarm.
	//1+	The Track Societ	сын тыны тура	٥	Him-T-real-Source	0	Riber Thread Gerlination	0		*
Threa	t Severity	Threat Model	ç Threat Type		Threat Source		Threat Destination		Event Count	¢.
•		Potentially Bad Traffic	ET SCAN Susaidaus Inbrune to 17450, port 3326 /1 20 (1937)		Partal-NEM-WC (192, 68.0.194/45463)		DB-LE-1001 (192.168.0.160:3306)			
۲	i.	Potentially Red Traffic	ET FOLKY HTTP million part 443 (OPTIONS) (13013929)		Partal-NEN-V/C (1922-1888-194427155)		esclos 3 mycatatenter com (192.1888-13344);			
۲		Amempted Information Leak	TT STAM Non-Allowed Host Tried to Connect to MySOL Security1-2010/939		Mysqi D6 1051 (192. 161 n 1619306)		Portal NDM VIC (192,168.0.194657458)			
۲		Attempted Information Leak	ET SCAN Potential SSH Scan (1 2001215)		152,168.0.198 (192,168.0.198;52187)		WE 24.96 (192.1080.0215:22)			
۲		Attempted Information Leaf	ET SCAN Providal SEH Scan OUTBOUND // 20050691		1.02.166.0.198 (192.) 68.0.198:51890(VK-24-96 (192.168.0.219:22)			
۲		Peterfally Bed Italfic	a 1 SIGM Seavedous information (nd 01, ppr. 3836 (1-301-0037)		Partal-NCM-VC (192, 168.0.194:47505)		MyxgH08-1021 (192.168.0.164/3505)			
۲		Potentially Bad Traffic	ET FOLICY HTTP staffic se part 443 (SPTICING) (* -2013929)		PartsHNEN-NC (192.158.8.194.95561)		eschosti mycatacenter.com (1911-168.0.11.446)			

Figure 10.6: Cyber Threat Summary Table

For each of the threats, you are powered with information on the Application Dependencies. uObserve[™] highlights the source and destination of the threat (which indicate the attacking or the attacked/compromised entity). As you have visibility into all the dependencies, you have insights into entities or assets that could get compromised in the future. For example, a webserver that is currently facing an attack, may not be the goal for the attacker. The goal could be to reach and compromise the database server that is connected to that webserver. Knowing all the dependencies gives you the proactive knowledge into future attacks or vulnerabilities. Also, with Uila you can get access to all transactions at the application level that can be maintained as forensic evidence.

Al +	- Ffier Thingas Middal 🛛 😆	Hear The Loc Type	0	Riter Threat Source	Plan Threat Destination	0	*
Threat Severity -	Threat Model 0	Threat Type	c	Threat Source	O Threat Destination	¢	Event Count
Conversation	Source Leage Source Process	Destination Librage Destination Process	liejptullisks				
		use of grad					
	•	which the eloca	And all the second as	participation 2.4 co preference de las DSLD-1021			
			4-46	Prina rarat			
	-	ana) Farra a trans					
	4	raged 2004.39/30/36/FC/10:40/F7] 2015.67.98					
	•				010		
						Seamers.	

Figure 10.8: Cyber Threat Conversation Maps

You can also apply a variety of display filters to the table to help you focus on cyber threats that matter to you. In the example below, we chose to visualize alerts based on threat models with the term "leak" in it.

AI =	laak. O	The Presid Lyse	۰	Titles throws Scarce 🔹 📀	The These Devination	÷
Threat Severity	Threat Model 0	Threat Type		Threat Source	Threat Descination	C Event Count
۰	Attempted Information Leak	ET SCAN Not-Allowed Host Tried on Constant on MySQL Server (1-2015/43)		Mysql DB 1001 (192 106.0 1045000)	Portal NDM MC (1971-108,0 1945-1958)	
۰ ا	Attempted information cask	kt. Sceb. Ibram. al Sain Scance. 4107-4731		192, '68,0,198 (192,166,0,'98,52187)	V C-2.4-16 (192.158.3.219.22)	
© 📕	Attempted Information Leak	ET SCAN, THURN, al SSH SLAPI COTRICUND IT-2000080		192. ° 68. (5. 198) (192. 166, 5. ° 98, 51 890)	V 0-2.4-58 (192.168.3.219.22)	

Figure 10.8: Cyber Threat Display Filters

For every threat, you can visualize the impact that the threat has on the entity's infrastructure (CPU, memory, storage, network stats).

	AU -	Tibe (InsetMedia) 🔍 🔍		0		O Ob		۰	8
Thre	at Severity -	Threat Model 0	Threat Type		Threat Source	C Three	at Destinacion	© Event Count	0
•		Potentially Bad Traffic	ET SCAN Suspidaus inbound to mySQL port 3336/1 20:0937		Portal NDM V/C (1927-08-0-194/d5463)	08. 092	8 1001 168 0 160:3308(80 E
	Corversation	Source Livege Source Process	Desindion Large Destine on Process Perpful Links						
	CPU Cores	CPU Ready Max: 0.12 % Mix: 0.06 %		CPU Usage Max: 55.04 % Min: 1.91%	երբերություն	h.h.h.h.h.h.h.h.h.h.h.h.	Mamory Active Usage Max: 17.92 % Min: 8.32 %		torratial .
	CPU Capacit	CPU Swap Wait Max: 9 ms Mirc 9 ms		Road Latency Max: D ms Mir: 0 ma			Write Latency Max: 7 ms Min: 9 ms		. 1
	1.81 GHz	Neswork RTT Max: 29 ms Mirr 8 ma	d. d.	In Facal Retry Max: 0 Min: 0			Out Fatal Recry Max: 0		
	8 GB	In Virtual Pit, Drop Max: 8 patkets Mic: 8 packets		Out Virtual Pkt Drop Mex: 0 packets Min: 0 packets	_				

Figure 10.9: Source & Destination Infrastructure usage

You can also visualize the processes running on the source and destination entities

	411 -	Table Linear Man		Line firmat type	0	- kan tinaa Seama 🛛 🔍 🔍	Titler1) and Distribution	0	e
Thr	eat Severity –	Threat Model		Threat Type		Threat Source	Threat Destination		Event Count
۲		Potentially Bac Tra	atte	ET ICAN Suspectous interand to mySQL part 330E (1-2010337)		Fortal-NDM-NE (192-165.0.194-48463)	D6-L2-1001 (192.1 68.0 160:3306)		10000000000000000000000000000000000000
	Conversition	Scurte Jsage	Source Process	Destination Usage Destination Process Helpful Units					
	i Infol ^s ioss	o config outs for mor	iboring process						@Canig
	Process		CPU Usage %	(Mas: %, Min: %)		- Memory Usage % (Max: %, Min: %)			
					No da	ata aval able in table.			

Figure 10.10: Source & Destination Process Information

You can also visualize helpful links on each of the cyber threats. You get expert guidance on those threats, their symptoms, the impact, and corrective actions to solve and avoid future reoccurrences.

AI -	Trias Crisial Modul 🛛 🔍	traar thosan type	0	The Pastagere 0	rstær fillest Descristion 🛛 🔍 🔍		e
Threat Severity	Threat Nodel	Threat Type		Threat Source	Threat Declarition	Event Count	¢
0 -	Potentially Gast Traffic	17 5044 Supprove recount to mySQL cort 1100 (1-2010617)		PortsHNDNHVIC (1922-19818-1949-49402)	06-4 8-1001 (1922-156 0-16023106)		50
Conversation Alternative Kit	Source Jeage Source Process wordes to from cont 3306 Jaco som wordes Document for FT 9045 Jaco	Destination Jaage Distination Process Helpful Links Lessid Briddling Lessid Briddling					
			Eic	une 10 11: Cuber Th	reat Heleful Links		

You can also export the list of threats that have been identified in their deployment to a CSV file with a single click.



Figure 10.12: Exporting Cyber Threat List

10.3 Data Exfiltration

uObserve[™] users can now map Outbound Traffic from the Data Center to the Internet on a world map to identify and reduce risk associated with general Internet connectivity. You can visualize Outbound traffic details including Internal VM details, Destination IP, Destination Server location, Application/Service for the outbound traffic, etc. This can be viewed for the entire Data Center or for a Service Group.

You also have the option to filter on information that matters to you on this screen as well as the option for visualizing the transactions at the application level and add to dependent services and external devices.



Figure 10.13: Data Exfiltration on world map

11. Root cause view

The root cause view provides quick root cause analysis of persisting application-level issues within the datacenter. The application response time is correlated with the infrastructure (compute, storage and network) as well as the services the problematic VM relies on.

Worst Transaction details are also provided in to help the systems administrator investigate the transaction history and troubleshoot the application in case there are no issues on the infrastructure side.

All and all and all all all all all all all all all al	Rool Cause View										
 A obset type transmit A obset type transmit					ļi. dinnid u		ha qata da na da La della finali a nga na m		11.20		An Petrometer (166)
0 Root Cause 1 Water 1 0 Root Cause 1 Water 2 0 Root Cause 0 Root Cause <th>· Crocko_11g-e1H</th> <th>weath //</th> <th></th> <th></th> <th></th> <th>T</th> <th></th> <th></th> <th></th> <th></th> <th>Mer Hort Marine</th>	· Crocko_11g-e1H	weath //				T					Mer Hort Marine
CPC Health Refmony H	O No muse found)R	toot Cause			O., nying application wappin teal assistant Anglossen teal assistant of Anglossen Mark mysel application in	Root Cause Protectly within a children by within a children by a processing the software recommendation of the software of the software recommendation of the software of the software processing the software of the software of the software of the software of the software of the software of the software of the software of the software of the software of the	to and using to menary uses in at minest. Corrup seaso worked yelatecenter.com 6 prevent	100.	Root Cause Presently In Market Angeleric Carrier and Angeleric In Market Angeleric Carrier Carrier Angeleric Caused The ICAN Or	og atoga med henry at chier in atoga circle (circ) and takey her descript at in at type circle (circ) med hand y her.
Provided Barbar Application Notwork Notwork <td>CPU Health</td> <td></td> <td>_</td> <td>_</td> <td></td> <td>Memory Health</td> <td></td> <td></td> <td>Storage Health</td> <td></td> <td>in the second second</td>	CPU Health		_	_		Memory Health			Storage Health		in the second second
Application 000	Dependent Service	-			14						Prev 1 Next
And Provided By ac-dc-01.mydatacenter.com The Wordt Transaction The Wordt Transaction Th	Root Cause	2.	ation	•	Network						Veget fry Gana Conser Bankarto Ran antros f.red
In Neutrine International Int	dns Provid	ied By sc-dc-l	01.mydatace	nter.com							¹¹¹
APT Closel Invance Restance Restance Restance Restance 5555 Wedge, 1spect Owder, 1spect ready B1050-range@exclushinklebiorprograms/space/	m Worst Transa	ction									P. Swisting
Statistic Mediagi: Stylet Owek, Stylet Statistic	ART	Chief	0 Burner	0.000	Report			() ()			
1525 Mediagle (tyret) Owek, Ugret mpul Mitrographical (tyret) (tyret) State Mitrographical (tyret) State Mitrographical (tyret) State Mitrographical (tyret) State Mitrographical (tyret) Mitrographical (83539	Weblagia 11g-e1	Orada 11g-c1	o rend	Stillerandisciple?withis:	175 rowaling well reportioner	y kij 21 mynaj bind matakinj mynajkanistan kij 1 j mynajk				DAV10/2017 05 18 AM
4271 Medigit, 1941 Orack, 1941 Orack, 1941 Medigit, 1941 Medig	51205	Weblagic_Highert	Oracle_tigent	- TOTAL	SHG2:rssg[and;0x7b2b88a	ne (mysolinovial) months and	v, 10) 12 (myorafizinal, veninitie) myorafizerietie. 34) 1 (myoraf	Gerieki. 3300 svynajisciele	An and Alif(1933		DIV10/2017 02:18 AM
4400 Mediagi_16y1 Orack_16y1 Test (1) (mediation (1)	48371	Weblagic_11p=1	Oncie_Hig-til	animal .	31145-manger@cb/76/264ed	no (nyaatimaani) maalaani)	y_d)2 mondliket_verselensel[versel=1] mondli				04/16/2017 05:38 AM
4473 Weblgt_1[g+1 Dank_1]g+1 npst 917/50npst_60(5/x/k393363) (nyk3pt_sol)(nyk3	45420	Wablogic_11g-s1	Oracle_11g-r1	Type	51100cmyagend;0x76220032	72 myseline and myseligany	LS:12 mysqCdrd_ex.bddq:mysqCatalda_15;1 mysqC	No.			04/16/2017 05:44 AM
	44375	Wablagic_11g-s1	Oracle_11g-r1	resd	51175cmpages()0576258886	20) nyaginganginyagigan	y 10,2 (mysofficial, variable) mysofficializati, 10,1 (mysofficial, mysofficial, 10,1 (mysofficial)	and the		States of the local division of the local di	04/16/2017 05: 17 AM

Figure 11.1: Storage Usage View

The user would be able to further drill down by further clicking on the health panes or dependent service pane to get indepth information.

11.1. CPU Health

Under the CPU health analysis view, Uila can provide detailed information on CPU usage, CPU ready as well as the CPU MHz. This information can help the user analyze the factors responsible for the high ART.

Process level information can also be gathered from the OS through WMI(Windows) or SSH(Linux) integration.



Figure 11.2: CPU Health Root Cause View

11.2. **Memory Health**

Under the Memory health analysis view, uObserveTM can provide detailed information on Memory usage and CPU Swap wait time. This information can help the user analyze the factors responsible for the high ART.

Process level information can also be gathered from the OS through WMI(Windows) or SSH(Linux) integration.



Figure 11.3: Memory Health Root Cause View

11.3. **Storage Health**

Under the Storage health analysis view, Uila can provide detailed information on read/write latency and IOPS. This information can help the user analyze the factors responsible for the high ART.

By clicking on the bars, the user can understand the neighboring VM's that share the same resources.

Uila – © 2023 113

User Guide –v5.2



Figure 11.4: Storage Health Root Cause View

12. 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.

With uObserve's Log Analysis you have information on the logged server, type, severity, group, source, event ID, Message, time, etc.

Show 25 😽 records							*ewas Not
Q Search 🗄 🗗 Chier	sainte mila						
	Many					- 14 (۹.
Logged Server	Туре	Security	Group	Source	Event ID	Massage	Time v
Horizon Connection Server - Min2019	Horizon VDI	DEBUG	AJP.87			(appixiew vial Programs)5141126(Response 200 OK	7/51/2022, 7/59:55 PM
Florbon Connection Server - Win3015	Hortmon VICI	nenus	SimpleDeamonThread			je polove zbedla spanski 141127 (Bespere from 7103-245-5: PSS) Znezo obačnik	7/31/2033, 7:59:59 FM
Horizon Connection Server - Win2015	Horizon VDI	DEBUG	AJP-73			Jajp všew visi Request51411271 Response 200 OK	7/31/2022, 7:59:59 PM
Horizon Connection Server Min2019	Horizon VDI	DEBUG	SimpleDearnonThread	4		popolewide Proposition (10.5.245.5: POST Mexico international population (10.5.245.5: POST Mexico) wished in	7/31/2022, 7:59:59 PM
Herban Connection Server - Win2010	Horizon VEI	00000	prok21-itmac-14			CristicQuery, Nachristöur mary/daw	2/31/2012, 050:50 PW
Harbon Connection Server - VAn2015	Hertron VEI	crous	NewsgeFrame/NorkS	Aquaira		KeyVault service got operation specificatificateKey, sk=1, msect=16	7/31/2022, 7/58/19 FM
Horizon Connection Server - Win2019	Horizon VDI	DEBUG	pool 25 throad 14			GetHatt: MachineSummaryMew	7/31/2012, 7:50:50 PW
Horuan Connection Server - Win2010	Herian VDI	рениц	AJIYAS			(a provisivo faid la spasia (5141125) Hasponisa 200 DK	//31/2012, A58:50/W
Horizon Contection Server - Mic2015	Hotton VDI	ornus	HanrishakeCompleter Thread	Not fy		Using sective protocol IT Sx1.2 and opher suize TLS_TODATURESCATTURESCATTURESCATTURESCATTURESCATTURESCATTURESCATTURESCATTURESCATTURESCATTURESCATTURESCATTURESCAT	7/81/2022; 7:58:59 PM
Horizon Connection Server - Win2019	Herizon VDI	DEBUG	New IrO worker #22			(Channel 17829 /10.5.240, '455088) Channel elscennected	7/31/2022, 7:50:50 PM
Horizon Connection Server - Win2018	Herizon VD1	DEBUG	SimpleDeamonThrea	4		(approximately approximately a	7/51/2022, 7:59:59 PM

Figure 12.1: Log Analysis view

Click here to get list of all modules supported by Uila's log analysis: <u>https://www.uila.com/download/document/508/Log Modules supported.pdf</u>

With Uila uObserve, you can now visualize trends for the logs collected by uObserve for your applications, servers, networking equipment, etc. using the time slider on the top of screen. The time slider shows the number of logs collected during the selected time period for the filtering/search rule options selected in the table below.

Users also have access to donut charts to visualize logged servers, windows event count vs agent-based log count, module log counts, windows event log counts, etc.

User Guide –v5.2



Figure 12.2: Log event charts

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.

	e Filter	e Fiter	_
Туре	* Group	Name	Action
Default	Active Directory	Active Directory and Local Server Permission Changes	Ľ.
Default	MS SQL	Server Stop	
Default	Active Directory	Member Deletions	Ľ.
Default	Active Directory	Domain Account Authentication Failure	Ľ
Default	MS SQL	Backup failed	Ľ
Default	Active Directory	Users Deleted or Disabled	<u>ئل</u>
Default	Active Directory	Major Security Events and Policy Changes	
Default	Active Directory	Graup Member Additions	
Default	Horizon VDI	Logged in	<u>ل</u>
Default	Active Directory	Group Policy Change	
Default	Active Directory	Users New or Enabled	13
Default	Active Directory	General Object Change	Ľ
Default	Active Directory	Other Users, Groups and Computers Changes	

Figure 12.3: Default search options

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



	Saved Search Rules	
	Service Type Rule	
	Apache	
ç		
	Figure 12.4: Custom Log Search	

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

Rule Setting		×
Active activemq Module Rule Type:	✓ Service Type Event ID Severity Group Source Message	× Cancel
	Message	

Figure 12.5: Custom Log Search configuration

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

Type Ø Riter	Recipients		+ Free Hour
Description Alarm Type elect Rule Config		zp.ikadiji is trifozzori,kue - √ i spišatkoda	
na 👻	@ riter	• the	
Type *	Group	© Name	
Default	Active Directory	Domain Account Authentication Failure	
Cefest	Active Directory	Users Detetted or Disabled	
Default	Active Directory	Group Memoer Additions	
Default	Horizon VD	Lagged in	
Default	Active Directory	Group Policy Drange	
Default	Addres Directory	User's New or Enabled	
Default	Aroke Directory	Other Users: Groups and Computers Changes	
Cefault	Windows Event	Shut down	
Cofee)	Active Directory	Unier Forfeed Logers.	
Default	Active Directory	Account Lockouts and Password Resets	
Cefacit	MS SQL	Server Ship	
Cefault	Active Directory	Active Directory and Local Server Permission Dranges	
Default	Active Directory	Member Deletions	
Default	MS SQL	Backup falled	
Cefault	Active Directory	Major Security overds and Policy Changes	
Default	Active Directory	General Object Change	
Default	Horizon VD	Unggeed out	
Definat	MS SQL	Abserving	

Figure 12.6: Log Alerting configuration

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



Figure 12.7: Historical Log Search

Users can also visualize raw logs in the log analysis table.



Figure 12.8: Raw Log messages

Users can also download a CSV with all the logs that are captured by uObserve by clicking on the Download CSV button.

Show 25 🗸 records.	First	Previous 1	2 3	4 5	85	Next
Q Search ∷≣ I Clear Search Rule						Download CSV
Filt V Filt V	lter					۹ 🖌
Event Service Severity Group Source Event Message ID						Time 🗸
A4 5-48-						11/14/2022.

Figure 12.9: Log message CSV download

Users can visualize minute-by-minute granular log events, by using the slider bar as shown below.

		06 РМ	09 PM	Tue 28	O3 AM	06 AM	09 AM	12 PM	03 PM
I	Q	Search							
÷	⇒	12:54 PM						3:25 PM	3:54 PM
T _+									

13. Stats Browser

Stats Browser is another powerful visualization tool that places all the metrics collected for any of the infrastructure components; Cluster, Host, and VM in one single unified screen view. It is a particularly useful when the root cause of an application performance issue has been identified and the user wishes to further validate it across all the infrastructure metrics.

You also have the option to visualize detailed information that is specific to a server or VM or external IP address. Users are powered with a map that displays all related network, infrastructure, and application (service) associated with the VM/Server/IP address. By clicking on any entity in the map, you can then get further details on related metrics and statistics.



Figure 13.1: Stats Map view

The figure below shows the navigation method and tool tips in the Stats Browser view:

Stats Browser	
Type Name	
DebStore • debatoric (4)	
Select the infrastructure type and name	Î.
Mas 10/2 Mas 10/2 Mas 10/2	
	Webs Laterey
1997 - 1997 1997 - 1997 1-11 - 111 - 1111 - 1111 - 111	Net 192
Mare 3 ma Mine 1 mai	

Figure 13.2: Stats browser

Use the Drop-down box below to select Type and name of the specific infrastructure units to view the summary of metrics over time bracket selected:

Туре		
Select a type		
DataCenter		
Cluster Host Storage		
PortGroup		
VM datastore2 (4)		
TorSwitch DataStore IOPS		

Figure 13.3: Types drop-down

Name	
datastore2 (4)	
	م
Datastore	
datastore1	
datastore1 (1)	
datastore1 (2)	
datastore1 (3)	Write IOPS
datastore1 (4)	
datastore2 (4)	
External_DS	

Figure 13.4: Names drop-down

Here is the Example of the Metric summary selected for VM 'Oracle_11g-n1' between 5:05am to 5:52am, when applications *postgres* and *mysql* performance are degraded, and where the root cause is pinpointed.

Stats Browser	
Type Name	
- Onade_11g-r1	
O Alerm O Application Response Time O Network O CPU O Memory O Storage	
e) Onde_tignt	
mp	kmp
	n
ARCI-Max 1 Transition	194 APT-Max: NA Two-Max: NA
ARTAIN: 1 TraiseMit	193 ARTANIC NA Trans-Atts NA
postgres	selt
andronomanananananananananananananananananan	π fammunanninanninanninninninninninninninninnin
and to the sector of the sector is the secto	1. 1.11.11.11.1.11.111.11111.1.11111.11111.1.
ART Max, 7 Tarre Ma	122 ARTANJA; 3 Trans-Max 22
ART-Mn 2 Trans-Mn	IB ARTMIN 1 Trans Min 4
top	
ART-AUX: NA Tars-Ma	NOK CONTRACTOR OF
ARTAIN: NA TransAir	

Figure 13.5: Application Response metrics for selected VM

Type Name	
VM - Orecie_11g-r1	
Alarm O Application Response Time O Network O CPU O Memory O Storage	
Onde_tipnt	
Road IOPS	
Nax Ofmas Min Dimas	Acar 6 tree Mil: 1 trea
Meri I ma	Me. Ons
Tote Laborsy	

Figure 13.6: Application Response metrics for selected VM

Users can also access logs for the selected logged server by using the "Log Analysis" tab.



Figure 13.7: Log Analysis

Users can now visualize and export the list of all the VMs/servers from the VM Table tab that are part of their deployment and download it in the PDF or CSV format.

Stats Map Stats Browser	VM Ta	able								
								100	2	Å
Filter		B Filter	8 Filter	B Filter	8 Filter	8 Filter	R Filter	Filter		
VM Name		IP Address	DNS Name	MAC Address	vSwitch	Port Group	Host/VPC	Cluster/Regio	n	
00155D0017BE				00155D00178E	External_vSwitch	External_PG	External_Host	External_Clust	er	
00155D00179E				00155D00179E	External_vSwitch	External_PG	External_Host	External_Clust	er	



14. Alarms View

Alarms Overview tab gives a quick summary of all the alerts that uObserve[™] has identified in your environment. Alarms overview is available in 2 different view options: Donut view or Flow analysis view.

By clicking on any of the 3 columns (Severity, Alarm Type or Entity), or on any of the bands, you can filter the desired information in the table below. You can choose to also filter data in the table by selecting from the "type" drop down option.



Alarms								0 =	•
	sution floopores T B	e cr • sau	ered ur	an Thread 31			Natarak.	Server Decor	
	Service Draws 2	• 9	sta						
Tile ×	O Fte	File ~	0 TH	Elu 🗠			Q Fix		
Severity ‡	Data Center 🔹	Entity Type 📫	Linhy	‡ Туро *	Count		Wessage	œ ≇ Time s	
	DC-UlaTech-01	VN.	0052569A1CD4			1	Average top response time was 1010 ma over baseline 200 ma	2021/10/6 F/#12.00.00	
	DC/UllaTech 01	VM	10.3.234.101			1	Average https:response time was 305 ms over baseline 315 ms	2021/10/6 F/#12:00:00	
	DC-U laTech 01	VM:	10.3.234.42			્ય	Average sol response time was 59699 ms over baseline 49333 ms	202:/*0/6 F/† 12:00:00	
	DC UlaTech 01	'VM	-indusia:	Application Response			Average http response time was 978 ms over baseline 200 ms	2021/10/6 (F-†+12:00:00	
	DC UlaTech 01	W	(4.4.284) (l πe			Average top response time was 396 ms over laseline 13 ms	2021/10/6 (F 112:00:00	
	No. LANSING.	100	Sarahan dari					total in any respective day.	

Figure 14.1: Alarms overview in Flow & Donut Charts

15. Reports

To view reports, click on the "reports" button the menu bar.



Figure 15.1: Reports selection

Uila allows you to either generate On-Demand reports or Schedule reports. You also have the option to generate reports in the CSV format.



Figure 15.2: Report creation

15.1. Report types

You can generate multiple types of reports:



Figure 15.3: Report types

Migration Guide (CSV only) – Provides a pre-migration assessment of the entire environment before
migrating to the Cloud or consolidating Data Centers. It shows all the details of the assets, and their
dependencies.

Dependency						
Source	Source IP Through Ge	iteway Destinction	Destination IP	Port	Application	Traffic(bytes)
uila-vic-4.0-ova	192.168.0.194	Controller-2-NSX-controller-11	192.168.0.181	1234	liop	2451298
ulla-vic-4.0-ova	192.168.0.194	Controller-2-NSX-controller-11	192.168.0.181	1234	пср	2315900
Centos8-DevPortal-VIC	192.168.1,193	Controller-2-NSX-controller-11	192.166.0.181	1234	ncp	2384021
Centos8-DevPortal-VIC	192,168.1.193	Controller-2-NSX-controller-11	192.168.0.181	1234	tna	2687962
Centos8-DevPortal-VIC	192.168.1.193	Controller-2-NSX-controller-11	192.168.0.181	1234	http	9442200
Centos8-DevPortal-VIC	192.168.1.193	Controller-2-NSX-controller-11	192.168.0.181	1234	sal	5454308
uila-vic-4.0-ova	192.168.0.194	Controller-2-NSX-controller-11	192.168.0.181	1234	sip	3201330
uila-vic-4.0-ova	192.168.0.194	Controller-2-N5X-controller-11	192.168.0.181	1234	java_rmi	1221543
esxhost1.mydatacenter.com	192.168.0.11	Controller-2-NSX-controller-11	192.168.0.181	1234	ssi	1477796228
uila-vic-4.0-ova	192.168.0.194	Controller-2-NSX-controller-11	192.168.0.181	1234	k/b5	2722801
uila-vic-4.0-ova	192.168.0.194	Controller-2-NSX-controller-11	192.168.0.181	1234	dns	2327560
ulla-vic-4.0-ova	192.168.0.194	Controller-2-NSX-controller-11	192.168.0.181	1234	idap	4710360
Centos8-DevPortal-VIC	192.168.1.193	Controller-2-NSX-controller-11	192.168.0.181	1234	java_rmi	2364760
Centos8-DevPortal-VIC	192.168.1.193	Controller-2-N5X-controller-11	192.168.0.181	1234	tds	2516532
uila-vic-4.0-ova	192.168.0.194	Controller-2-NSX-controller-11	192.168.0.181	1234	tcp	12468414
uila-vic-4.0-ova	192.168.0.194	Controller-2-NSX-controller-11	192.168.0.181	1234	x11	2255698
uila-vio-4.0-ova	192.168.0.194	Controller-2-NSX-controller-11	192.166.0.181	1234	portmap	4773280
Centos8-DevPortal-VIC	192.168.1.193	Controller-2-NSX-controller-11	192.168.0.181	1234	portmap	4991500

Minration Guide for Multi-DC from 2021-08-01 000000 to 2021-08-10 235959

Figure 15.4: Migration Report

• Application Performance – Provides trend chats of the overall application performance of the entity selected (Datacenter, Cluster, Hosts or VM's) along with the CPU, Memory, Storage and Network.



Figure 15.5: Application Performance Report

 VM Resource Usage report – With VM Resource usage report you can optimize cloud costs and coordinate between cloud governance teams and resource owners (IT teams) based on actual usage and uncover inefficiencies to reduce waste. You can visualize under-provisioned hosts or instances leading to application performance issue.

Capacity (MHz) 3622	core(s) 2	Avg Usage(%) 9.3	PU Peak Usage(%)	Top 10% Peaks Avg(%)	O/U Provision Rec	Capacity (MB)	Avg Usage(%)	Peak	O/U Provision
Capacity (MHz) 8622	core(s) 2	Avg Usage(%) 9.3	Peak Usage(%)	Top 10% Peaks Avg(%)	O/U Provision Rec.	Capacity (MB)	Avg Usage(%)	Peak	O/U Provision
8622	2	9.3				- 18. S	000000(10)	Usage(%)	Rec.
			49.5	25.6	-1 core	2048	26.8	48.5	
716	1	0.4	0.6	0.4		1024	5.9	8	-512MB
716	1	0.5	5.6	2.2		512	8.7	78.3	
3432	2	0.1	0.1	0.1	-1 core	512	3.1	4.8	-256MB
6864	4	0.1	0.1	0.1	-3 cores	4096	0	0	
716	1	0.7	1.1	0.8		1024	4.1	6.2	-512MB
58	116 132 164 116	116 1 132 2 164 4 116 1	1 0.5 132 2 0.1 164 4 0.1 116 1 0.7	1 0.5 5.6 132 2 0.1 0.1 164 4 0.1 0.1 16 1 0.7 1.1	16 1 0.5 5.6 2.2 132 2 0.1 0.1 0.1 164 4 0.1 0.1 0.1 116 1 0.7 1.1 0.8	11 0.5 5.6 2.2 132 2 0.1 0.1 0.1 164 4 0.1 0.1 0.1 161 1 0.7 1.1 0.8	11 0.5 5.6 2.2 512 132 2 0.1 0.1 0.1 512 164 4 0.1 0.1 0.1 -1 core 512 1664 4 0.1 0.1 0.1 -3 cores 4096 116 1 0.7 1.1 0.8 1024	16 1 0.5 5.6 2.2 512 8.7 32 2 0.1 0.1 0.1 512 3.1 364 4 0.1 0.1 0.1 -3 cores 4096 0 164 1 0.7 1.1 0.8 1024 4.1	16 1 0.5 5.6 2.2 512 8.7 78.3 132 2 0.1 0.1 0.1 512 3.1 4.8 164 4 0.1 0.1 0.1 $-3 \operatorname{cores}$ 4096 0 0 116 1 0.7 1.1 0.8 1024 4.1 6.2

Resources Provisioning Summary

Figure 15.6: VM Resource Usage Report

Please refer to the table below to understand the different colors in the Resources Provisioning Summary:

Resource (Color)	Provisioning	Peak Usage(%)	Top 10% Peak Ave(%)	Average Usage(%)
CPU (Orange)	OVER		< 50%	< 20%
CPU (Green)				20% ~ 60%
CPU (Yellow)				60% ~ 70%
CPU (Red)	UNDER			> 70%
Memory (Orange)	OVER	< 40%		< 30%
Memory (Green)		>= 40%		< 30%, or
				30% ~ 80%
Memory (Yellow)		80% ~ 90%		
Memory (Red)	UNDER	> 90%		

Figure 15.7: VM Resource Usage Report

 Host Resource Usage report – The host resource usage report provides the health summary of each host on its CPU, Memory, Storage and Network.



Figure 15.8: Host Resource Usage Report

• Service Performance Report – The service performance reports provides the health of individual services running within the virtual machines.





 Health Overview Report – 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.

Overview Application Performan	ce			2020/10/	08-2020/10/12
VM Name	Health	ART(ms)	Transactions/m	Traffic/s	Packets/s
Horizon-Wew-ConnectionServer-Windows2016	73	151	267	10.05 KB	29
VMware vCenter Server Appliance	66	201	510	68.67 KB	85
Gateway [192.168.0.1]	91	15	287	9.46 KD	26
exchosit5.mydatacenter.com	98	29	52	13.01 KB	28
192.168.1.183	98	141	4	1.42.10	3
exchosi4.mydatacenter.com	99	24	47	12.20 KB	28
client-1.112 (192.168.1.112)	99	163	1	1.84 KD	5
SMB Server (192.168.0.8)	100	2	30	334.0	2
umas (38.99.127.23)	100	9	5	2.21 KB	1
LongText3 (192.168.1.152)	100	10	6	473.8	2
InstantClone-1	100	7	2	308.0	0



Threat Detection (CSV only) – Provides details on cyber threats and vulnerabilities that have been
identified in the environment. It includes information on the severity of the treat, threat model, threat
type, source and destination, and the number of times the event has occurred.

Threat Severity	Threat Model	Threat Type	Threat Source
Major	Attempted Information Leak	ET POLICY Python-unlits/ Suspicious User Agent (1-2013031)	VMware vCenter Server Appliance - nev
Major	Attempted Information Leak	FT POLICY Python-urlio/ Suspicious User Agent (1-2013031)	VMware vCenter Server Appliance - ner
Critical	Web Application Attack	ET SCAN Possible Nmap User Agent Observed (1-2024364)	APP-LB-1
Major	Attempted Information Leak	ET POLICY Python-unito/ Suspicious User Agent (1-2012081)	VMware vCenter Server Appliance - no
Critical	Web Application Attack	ET SCAN Possible Nmap User-Agent Observed (1-2024384)	APP-LB-1
Major	Attempted Information Leak	ET POLICY Python-unito/ Suspicious User Agent (1-2019081)	VMware vCenter Server Appliance - nei
Major	Attempted Information Leak	ET SCAN Non-Allowed Hast Tried to Cannect to MySGL Server (1-2010493)	DBServer-2
Critical	Web Application Attack	ET SCAN Possible Ninap User-Agent Observed (1-2024384)	Centos8-DevPortal-VIC
Critical	Web Application Attack	ET SCAN Possible Ninap User-Agent Observed (1-2024384)	Centos8-DevPortal-VIC
Major	Attempted Information Leak	ET POLICY Python-unite/ Suspicious User Agent (1-2013081)	voenter.mydatacenter.com
Major	Attempted Information Leak	ET SCAN Non-Allowed Host Tried to Connect to MySQL Server (1-2010493)	DBServer-2
Major	Attempted information Leak	ET POLICY Python-unito/ Suspicious User Agent (1-2013081)	VMware vCenter Server Appliance - ner
Major	Attempted Information Leak	ET POLICY Python-urillo/ Suspicious User Agent (1-2018081)	VMware vCenter Server Appliance - ne-
Major	Attempted Information Leak	ET POLICY Python-unlib/ Suspicious User Agent (1-2013031)	VMware vCenter Server Appliance - nei
Critical	Web Application Attack	ET SCAN Possible Nmap User-Agent Observed (1-2024384)	Centos8-DevPortal-VIC
Major	Altempted Information Leak	ET POLICY Python-unlib/ Suspicious User Agent (1-2013081)	VMware vCenter Server Appliance - ner
Major	Attempted Information Leak	ET POLICY Python-urillo/ Suspicious User Agent (1-2013031)	VMware vCenter Server Appliance - nev
Major	Attempted Information Leak	ET POLICY Python-unlib/ Suspicious User Agent (1-2013001)	VMware vCenter Server Applance - nev
Malar	Allowasked Information Lask	ET BOLICY Bulker (#Bb/ Quesials of Lice Asset H. 30(\$008)	UNIVERSIONAL CONTRACT ADDRESS OF

Figure 15.11: Threat Detection Report

 VDI User – Uila users can now generate a detailed VDI user report, including information on Top 20 users by active session time, session idle time, round trip latency, packet loss, logon delay, CPU/memory usage, process info, and many more.



• Server/Device Uptime – Uila users can generate a server uptime report with details on status, start/end time and duration.

Ser Dat	rver/Device UpTime(I	2023/10/20 00:00 ~ 2023/10/20 15:		
Dat		Up %	Down Time	Deurs Pariode
Uila-vST-98	37654321-192 168 0 11	09-10	15.78hr	10/20 00:00 - 10/20 15:47
uila-vst-4.6	5.0-60-2	0%	15.78hr	10/20 00:00 - 10/20 15:47
Uila-vST-12	23456789-192.168.0.12	0%	15.78hr	10/20 00:00 - 10/20 15:47
umas-dhn-	-240	0%	15.78hr	10/20 00:00 - 10/20 15:47
Uila-vST-12	23456789-192.168.0.14	0%	15.78hr	10/20 00:00 - 10/20 15:47
Uila-vST-12	23456789-192.168.0.15	0%	15.78hr	10/20 00:00 - 10/20 15:47
Uila-vST-12	23456789-192.168.0.16	0%	15.78hr	10/20 00:00 - 10/20 15:47
Uila-test-hy	yperv	0%	15.78hr	10/20 00:00 - 10/20 15:47
Uila-vST-12	23456789-192.168.0.11	0%	15.78hr	10/20 00:00 - 10/20 15:47
nsxt-vcente	er	0%	15.78hr	10/20 00:00 - 10/20 15:47
Uila-vST-98	37654321-192.168.0.15	0%	15.78hr	10/20 00:00 - 10/20 15:47
Uila-vST-99	99991103-192.168.0.11	0%	15.78hr	10/20 00:00 - 10/20 15:47
Uila-vST-12	23456790-192.168.0.16	0%	15.78hr	10/20 00:00 - 10/20 15:47
Uila-vST-12	23456790-192.168.0.15	0%	15.78hr	10/20 00:00 - 10/20 15:47
Uila-vST-98	37654321-192.168.0.12	0%	15.78hr	10/20 00:00 - 10/20 15:47

- Figure 15.12: Server uptime Report
- ESXi Host GPU This report contains host level trending metrics like GPU ID, driver version, number of user sessions using GPU, frame buffer, VM Count, GPU decoder/encoder, peak/average GPU & memory usage.



Figure 15.13: ESXi host GPU Report

• **Storage Usage** – Provides details on the storage and disk capacity and usage.

VM Name	Disk Name	Time	Usage (MB)	Capacity (MB)	Usage (%)
APP-LB-1	1	Mar 21, 2023 12:00 AM	946	13,892	6.8
APP-LB-1	1	Mar 21, 2023 12:15 AM	946	13,892	6.8
APP-LB-1	1	Mar 21, 2023 12:30 AM	946	13,892	6.8
APP-LB-1	1	Mar 21, 2023 12:45 AM	946	13,892	6.8
APP-LB-1	1	Mar 21, 2023 1:00 AM	946	13,892	6.8
APP-LB-1	1	Mar 21, 2023 1:15 AM	946	13,892	6.8
APP-LB-1	1	Mar 21, 2023 1:30 AM	946	13,892	6.8
APP-LB-1	1	Mar 21, 2023 1:45 AM	946	13,892	6.8
APP-LB-1	1	Mar 21, 2023 2:00 AM	946	13,892	6.8
APP-LB-1	1	Mar 21, 2023 2:15 AM	946	13,892	6.8
APP-LB-1	1	Mar 21, 2023 2:30 AM	946	13,892	6.8
APP-LB-1	1	Mar 21, 2023 2:45 AM	946	13,892	6.8

Storage Usage for Data Center [Production] 2023-03-21 000000 _ 2023-03
--

16. Intelligent Remediations

16.1. Remediation Actions

Uila supports Intelligent Alert-based triggers and Manual triggers to provide complete control in proactively preventing issues as well as streamlining problem resolution. Actions include Power off VMs, Suspend VMs, Reset VMs, Power on VMs, logging off VDI users, Updating VMware tools, Restart Guest OS, Kill a process running on a VDI desktop, etc.

For VDI session, the actions are accessible by using the



icon in the individual user session.

Remediation Action		×
Log Off (uila.com\kimi1)		
Power On (farm-desktop1)		
Power Off (farm-desktop1)		
Suspend (farm-desktop1)		
Reset (farm-desktop1)		
Restart Guest OS (farm-desktop1)		
Update VMware Tools (farm-desktop1)		
	✔ ОК	X Cancel

Figure 16.1: Remediation Action options for VDI users

User Guide –v5.2



icon in the Processes tab for the

You can also kill processes running for a VDI user, using the individual user session.

Process CPU Usage % (Max: 37%, Min: 0%) Memory Usage % (Max: 1.7%, Min: 0%) A clion (Tasking axe(5240) 1	Logon Duration	CONSOLE	Alarms	Dependent Services	Conversation	Network	CPU	Memory	Storage	Process			
Tasking exe(524) f* kase exe(688) f*	Process							CPU Us	age % (M	ax: 37%, Mir	n: 0%) .	, Memory Usage % (Max: 1.74%, Min: 0%)	
haos.exe(683)	Taskmgr.exe(524	0)							.				ŕ
	Isass.exe(688)												î

Figure 16.2: Remediation Action to kill processes

You can also access the remediation action for any VM from different screens by clicking on the node to open actions.

Health Score	Applicat Response	Application Transactions/min Response Time		Traffic/s	Packets/s
97	4 ms		245	232.30 KB	195
Actions	Services Provided	Application Response Time	Transactions/min	Traffic/s	Packets/s
6 🛓	tcp	20 ms	2	342 B	0
i 🕹 🕹	ssh	0 ms	232	144.00 KB	126
@ ± ≓	http	203 ms	0	79.25 KB	61
6 🕹	https	68 ms	8	8.73 KB	7
Remove VM					
Add Dependent	Servers				
Add Dependent (Clients				
Move To Previou	s Tier				
Move To Next Tie	er				
Add to Depender	nt Services				
Go To Stats Map					
	nitoring				
Setup Server Mo	nitonita				

Figure 16.3: Remediation Action for VMs

To configure the Remediation action as an automatic response to any violations, you can assign it from "Settings \rightarrow Alarm Configuration".

O Type O S	Severity	• Filter	Remediation Activ	n	+ Prev Finish -
Please select an o	ption				
Power On					
Power Off					
Suspend					
Reset					
Restart Guest OS					
					

Figure 16.4: Configuring alert-based remediation actions

16.2. Custom Scripting for Remediation Actions

Uila provides extensive agility and flexibility to IT teams to automate remediation actions as well as configurations using its customizable scripting capability. With this, Uila users can empower their organization with continuous optimization across the full stack to maximize application performance and security. Uila's scripting provides the ability for the custom Power-Shell based scripts to be executed on VMware vCenter[®] as well as VMware Horizon[®] Connection Server. Once created the script would show up in the remediation action for the VM or the VDI user session for you to execute. These scripts can be executed either as part of a manual remediation/configuration or automate it based on alerts for a zero-touch experience.

You can create the custom scripts from Settings \rightarrow Global Configuration.



Custom Script Library			
O Initiator O Varial	oles 3 Script		← Prev Next →
Choose Known Variable	'S	Define Custom Va	riables
SessionId (VDI Session ID)		Variable Name	
vmName (Virtual Machine N	lame)	Keep Value Hidden	For example, check it
processName (A Process Na	ime)		when a password is passed in .e.g., a
processid (A Process ID)			password.
createTime (A VDI Process C	reation Time)	+ Add Variable	

Figure 16.6: Choose from pre-built/define custom variables

1		
Initiator O Variables	Script	+ Prev
Script Name	power-off-vm	
Build Script Content		
Add Variable	Select Variables +	
Power off a particular VM. .DESCRIPTION Uses the VIServer1 to send	command to power off a VM.	
PARAMETER vmName		
.PARAMETER vmName Name of the VM		
.PARAMETER vmName Name of the VM .OUTPUTS Uila_OK if success, otherw	ise PS error	
.PARAMETER vmName Name of the VM .OUTPUTS Uila_OK if success, otherw .EXAMPLE PS>.\poweroff_VM.ps1 -vmName w	ise PS error :bserver	

Figure 16.7: Script Editor

Note: Custom Scripting is part of the AIOPS add-on module.

Once created you can either execute the scripts manually by clicking on the Remediation Action icon or menu for the VM or the VDI user OR by assigning the custom script to an alarm.

mediation Action	
Power On VM - Kimi-uila-umas-4.0-71	
Power Off VM - Kimi-uila-umas-4.0-71	
Suspend VM - Kimi-uila-umas-4.0-71	
Reset VM - Kimi-uila-umas-4.0-71	
Restart VM Guest OS - Kimi-uila-umas-4.0-71	
Indets (04) 04 miles Trades (2001) allo meres 4 0 74	

Figure 16.8: Execute script manually

16.3. Remediation Action Logging

All remediation actions (manual or automated) are logged in the system log files section within settings.

VIC System Log UMAS System Log	Script System Log						
System Logs							
💼 Delete Ali	Deleter Al						
	Q Filme		Fall ~				
Time	. Deer	≎ infe	Status	Молици	Action		
2021/10/5 上午5:35:45	admin	Kill Process (Taskingr.exe - 5240)	Faled	Query Session failed – output= (91mkilf_Process.ps1: (91mCannot validate argument on parameter 'oreate 'lime'. The argument 'U' cannot be validated because its value is not greater then zero (0m			
2021/10/1 上午12:36:36	admin	Update VMware Tools (VIIN10-Kevin)	(Faled)	Query Session failed - output: WARNING Automatic update of VMware tools is not fully supported for non-Windows OSs. Manual intervention might be required.			
2021/9/30 上午11:02:12	kimi	Restart Guest OS (A-ulla-vic-4 1-16)	CK.	Successful	E		
2021/9/30 上午10:45:06	kimi	Update VMware Tools (A ulla vic 4.1.16)	Falled	Query Session failed - output+ WARNING: Automatic update of VMware tools is not fully supported for non-Windows OSs. Manual Intervention might be required			
2021/5/30 上午10:44:41	kimi	Power On (A-uite-umas-1 1-16)	OK	Successful			
2021/9/30 上午10:43:40	kimi	Power Off (A ulla unitas 4.1-16)	OK	Successful	i.		
2021/9/30 上午10:43:22	kimi	Restart Guest OS (WIN10-Kevin)	C OK -	Successful			
2021/9/30 上午9:46:14	admin	Restart Guest OS (A-ulla-umas-4.1-16)	OK)	Successful	ĩ		
2021/9/29 下午11:36:05	admin	Power On (farm-desktop1)	OK S	Successful	ī		
2021/9/29 下午4:47:53	admin	Restart Guest OS (A ulla umas 4.1-16)	OK	Successful	ĩ		

Figure 16.9: Logging of remediation actions

135

17. Uila KPI

17.1. Infrastructure and Application Statistical Counter for Measuring Key Performance Indicators

This Table summarizes all the statistical counters that Uila measured and collected from VMware vCenter or Hyper management server, and network packets, and stored in UMAS Big Data database:

Category	Counter	Туре	Measurement Method	*Uila Built-in Best Practice Threshold (that overrides baseline value)
Application Performance	Applicatio n Response Time (ART)	KPI used for categorizing health score	Time (mSec) measured from the arrival of a client application request to the transmission of a server response.	Minimum ART baseline is 200 mSec. This means applications with less than 200 mSec response time will have Normal (green) ART health score.
	Network Round Trip Time (NRT)	KPI used for categorizing health score	Network round trip time (mSec) spent in the network	Minimum NRT baseline is 50 mSec. This means device with less than 50 mSec NRT will have Normal (green) NRT health score.
	TCP Fatal Retry	KPI used for categorizing health score	TCP re-transmit the same packet more than 3 times	No auto-learned baseline directly on TCP Fatal Retry packets. Health score is defined by the percent of TCP Fatal Retry count to total TCP packet count. If (x == 0) Normal If (0< x < 0.01%) Minor If (0.01% < x < 0.05%) Major If (x >0.05%) Critical
Network Infrastructure	Virtual Packet Drop (VPD)	KPI used for categorizing health score	# Of Packet lost between vSwitch and virtual network driver	No auto-learned baseline directly on Virtual Packet Drops. Health score is defined by the percent of Virtual Packt Drops to total packet count. If (x < 0.01%) Normal If (0.01%< x < 0.05%) Minor If (0.05% < x < 0.1%) Major If (x >0.1%) Critical
	Zero Window	Statistics used for troubleshoot ing & investigation	TCP receive window closed. TCP receiver refused to receive more TCP data from the sender.	

	Reset	Statistics used for troubleshoot ing & investigation	TCP connection reset	
	Rx Bytes Average	Statistics used for troubleshoot ing & investigation	Number of bytes received	
	Tx Bytes Average	Statistics used for troubleshoot ing & investigation	Number of bytes transmitted	
	Usage Average	Statistics used for troubleshoot ing & investigation	Number of bytes transmitted and received	
	Packets	Statistics used for troubleshoot ing & investigation	Number of network packets transmitted or received	
	Disk Read Latency	KPI used for categorizing health score	Average amount of time (mSec) taken to process a disk read command	No auto-learned baseline for VM and Host Read Latency. Health score is determined by comparing to a fixed baseline value of 22 or 20 mSec for VM and host respectively.
Storage	Disk Write Latency	KPI used for categorizing health score	Average amount of time (mSec) taken to process a disk write command	No auto-learned baseline for VM and Host Read Latency. Health score is determined by comparing to a fixed baseline value of 22 or 20 mSec for VM and host respectively.
Infrastructure	Kernel Latency	Statistics used for troubleshoot ing & investigation	Kernel average latency (KAVG) time an I/O request spent waiting inside the vSphere storage stack	
	Device Latency	Statistics used for troubleshoot ing &	Device average latency (DAVG) coming from the physical hardware,	

		investigation	HBA and storage device	
	Read I/O Ops	Statistics used for troubleshoot ing & investigation	# Of Read operations per second	
	Write I/O Ops	Statistics used for troubleshoot ing & investigation	# Of Write operations per second	
	CPU Ready	KPI used for categorizing health score	Percentage (%) of time that the VM was ready, but could not get scheduled to run on the physical CPU due to physical CPU resource congestion	No auto-learned baseline for CPU Ready. Health score is determined by comparing CPU Ready value against fixed threshold below – For VM If (x < 5%) Normal If (5%< x < 10%) Minor If (10% < x < 20%) Major If (x >20%) Critical For host If (x < 10%) Normal If (10%< x < 15%) Minor If (15% < x < 25%) Major If (x >25%) Critical
CPU Infrastructure	CPU Usage	KPI used for categorizing health score	Average CPU utilization (%) over all available virtual CPUs in the VM	No auto-learned baseline for CPU Usage. Health score is determined by comparing CPU Usage value against fixed threshold below – For VM If (x < 80%) Normal If (80%< x < 85%) Minor If (85% < x < 90%) Major If (x >90%) Critical For Host If (x < 85%) Normal If (85%< x < 90%) Minor If (85%< x < 95%) Major If (x >95%) Critical
	CPU MHz	Statistics used for troubleshoot	Average CPU MHz usage	

		ing & investigation		
	CPU Swap Wait Time	KPI used for categorizing health score	Average time (mSec) spent per minute a virtual machine is waiting for memory pages to be swapped in	No auto-learned baseline for CPU Swap Wait Time. Health score is determined by comparing CPU Swap Wait time percentage against fixed threshold below – For VM If (x < 300ms) Normal If (300ms< x < 1200ms) Minor If (1200ms< x < 3600ms) Major If (x >3600ms) Critical For Host If (x < 600ms) Normal If (600ms< x < 3000ms) Minor If (3000ms < x < 6000ms) Major If (x >6000ms) Critical
	Memory Active Usage GB/MB	Statistics used for troubleshoot ing & investigation	Amount of memory that is actively used, as estimated by VMkernel based on recently touched memory pages.	
Memory Infrastructure	Memory Active Usage %	KPI used for categorizing health score	Amount of memory percentage that is actively used, as estimated by VMkernel based on recently touched memory pages.	No auto-learned baseline for Active Memory directly. Health score is determined by comparing Active Memory percentage (to total memory) against fixed threshold below – For VM If (x < 50%) Normal If (50%< x < 55%) Minor If (55% < x < 65%) Major If (x >65%) Critical For Host If (x < 40%) Normal If (40%< x < 45%) Minor If (45% < x < 55%) Major If (x >55%) Critical

|--|

Uila Default Threshold Levels 18.

This Table summarizes all the default values of the threshold setting pre-defined in the system.

Threshold Settings	Default Value				
Threshold Type	Critical	Major	Minor		
Under Setting/Alarm Config					
CPU Ready	>20%	10~20%	5~10%		
CPU Usage	>20%	10~20%	5~10%		
CPU Swap Wait	>3600ms	1200~3600ms	300~1200ms		
Memory Active					
Usage	>85%	75~85%	70~75%		
Read Latency	>85%	75~85%	70~75%		
Write Latency	>85%	75~85%	70~75%		
Virtual Packet Drop	>1	N/A	N/A		
Network Round-Trip Time	>(20ms*1.2)	(20ms*1.1)~(22ms*1.2)	(20ms*1.05)~(22ms*1.1)		
Fatal Retries	>1	N/A	N/A		
Application Response Time	>(200ms*1.2)	(200ms*1.1)~(200ms*1.2)	(200ms*1.05)~(200ms*1.1)		
Under Setting/Alarm Config/Data Store					
Read Latency	>85%	75~85%	70~75%		
Write Latency	>85%	75~85%	70~75%		
Under Storage Analysis					
Usage	95%	90%	85%		
Under Setting/Device Monitoring					
In Utilization	90%	85%	80%		
In Discards	999000000 packets	998000000 packets	997000000 packets		
	999000000				
In Errors	packets	998000000 packets	997000000 packets		
Out Utilization	90%	85%	80%		
	999000000				
Out Discards	packets	998000000 packets	997000000 packets		
141 Uila – ©	2023		User		

Uila – © 2023

User Guide –v5.2

	999000000		
Out Errors	packets	998000000 packets	997000000 packets
Under Setting/Server Monitoring			
Service Down	N/A		
Server Down	N/A		
Under Setting/Horizon VDI			
Logon Time	60 s	45 s	30 s
PCoIP Protocol	350 ms	300 ms	250 ms
PCoIP By Packet Loss	550 ms	2 50%	1%
PCoIP Tx Packet Loss	5%	2.50%	1%
Blast Round-Trip			
Time	350 ms	300 ms	250 ms
Blast Packet Loss Uplink	5%	2.50%	1%