Technical Overview:

Omnissa Horizon

Goliath Performance Monitor

> *"Goliath is a great alternative to vRealize Operations. It's easy to setup and deploy, has the ability to create simple overview of the metrics required for troubleshooting. Also, the ability to monitor application availability is a great feature to troubleshoot one part of the user experience that is often quite neglected."*

- Johan Van Amersfoort

VMware EUC Champion, VCDX-DTM, and author of VDI Design Guide

Contents

Goliath Technologies: Transforming IT from Reactive to Proactive 3

Benchmark Your User Experience 4

AI-Powered Troubleshooting 4

An Early Warning System 5

  End User Screenshot Analytics 7

Proactive Monitoring and Troubleshooting 7

  Real-Time Omnissa and VMware Performance Metrics 7

  Omnissa & VMware Delivery Infrastructure Performance 8

  Integrated RDSH Hosts Display 8

  Real-Time Session Display 8

  In Session Real-Time Analytics Overview 8

  Real-Time PCoIP/BLAST Drill Down from Session Display 10

  Real-Time Horizon Logon Duration Drilldown 11

  Embedded Intelligence for Common Failure Points 12

Advanced Remediation Capabilities to Improve 13

  Troubleshooting 13

  Threshold-Based Alerting 13

  Alert Resolution Feature 14

  Automated Remediation Actions 15

Reporting 16

  Sample Reports 16

Goliath Technologies: Transforming IT from Reactive to Proactive

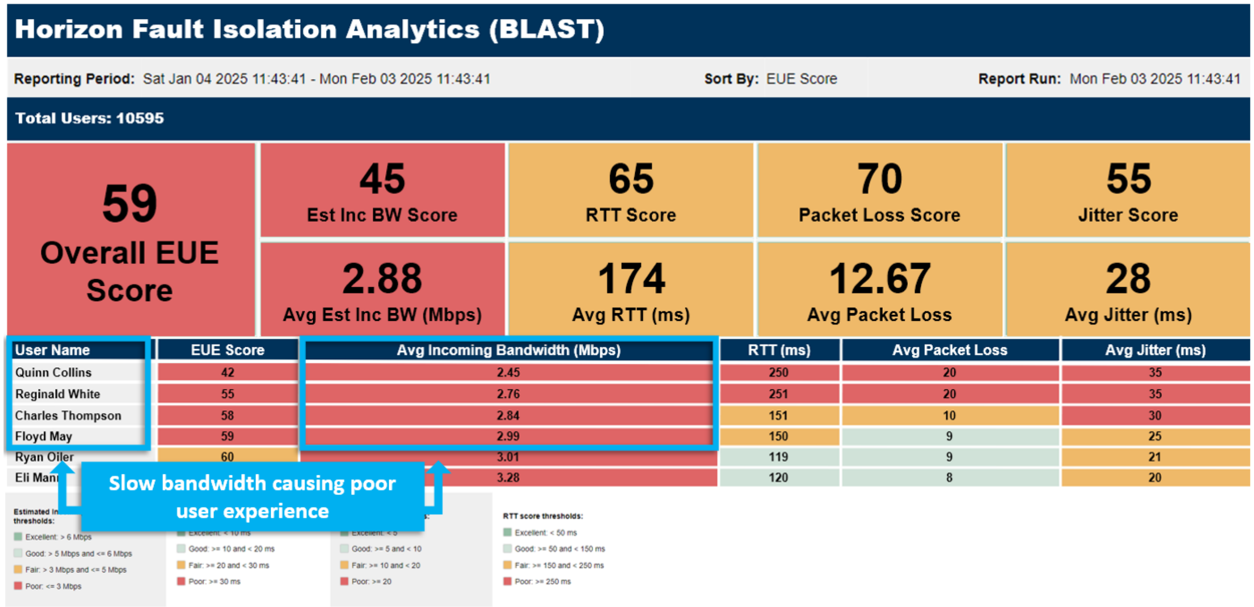
This product overview document highlights some of the differentiating features Goliath Technologies offers that are currently unavailable with any other solutions in the marketplace today. These capabilities enable organizations to proactively monitor and troubleshoot not only their VMware Horizon environments but associated end-user experiences. As a member of the Omnissa and VMware TAP programs, Goliath works alongside Omnissa and VMware product managers to bring to market solutions which allow Omnissa and VMware customers to improve the experience for their end users.

Goliath provides software with AI, embedded intelligence, and automation that enables IT professionals to anticipate issues before they happen, provide the data to troubleshoot quickly when they do & documentation that proves root cause so permanent fix actions can be implemented and IT can objectively report on the quality of the user experience they are delivering - regardless of where IT workloads or users are located. By doing so, Goliath helps IT break out of reactive mode, into proactive mode.

Benchmark Your User Experience

Establish an objective baseline of the health of your IT delivery and quantifiably measure improvement over time.

The Horizon End User Experience report utilizes embedded intelligence to provide a distilled objective view of user experience. Goliath automatically analyzes complex connectivity and performance metrics from the user's perspective and calculates a top-line user experience score. The report then enables easy filtering to analyze subsets of the environment for focused analysis, even down to individual users. Not only is IT able to easily see what the objective user experience is, but also explains why by breaking out the primary elements responsible for the user experience score (RTT, Jitter, Bandwidth, and Packet Loss). This capability expedites cross-departmental analysis and streamlines both IT operations and IT management's ability to act confidently on objective data.



Horizon Fault Isolation Analytics (BLAST)

Reporting Period: Sat Jan 04 2025 11:43:41 - Mon Feb 03 2025 11:43:41 **Sort By:** EUE Score **Report Run:** Mon Feb 03 2025 11:43:41

Total Users: 10595

59 Overall EUE Score

45 Est Inc BW Score

65 RTT Score

70 Packet Loss Score

55 Jitter Score

2.88 Avg Est Inc BW (Mbps)

174 Avg RTT (ms)

12.67 Avg Packet Loss

28 Avg Jitter (ms)

User Name	EUE Score	Avg Incoming Bandwidth (Mbps)	RTT (ms)	Avg Packet Loss	Avg Jitter (ms)
Quinn Collins	42	2.45	250	20	35
Reginald White	55	2.76	251	20	35
Charles Thompson	58	2.84	151	10	30
Floyd May	59	2.99	150	9	25
Ryan Oiler	60	3.01	119	9	21
Eli Man	[illegible]	3.28	120	8	20

Slow bandwidth causing poor user experience

Estimated In
thresholds:
🟩 Excellent: > 6 Mbps
🟩 Good: > 5 Mbps and <= 6 Mbps
🟧 Fair: > 3 Mbps and <= 5 Mbps
🟥 Poor: <= 3 Mbps

🟩 Excellent: < 10 ms
🟩 Good: >= 10 and < 20 ms
🟧 Fair: >= 20 and < 30 ms
🟥 Poor: >= 30 ms

🟩 Excellent: < 5
🟩 Good: >= 5 and < 10
🟧 Fair: >= 10 and < 20
🟥 Poor: >= 20

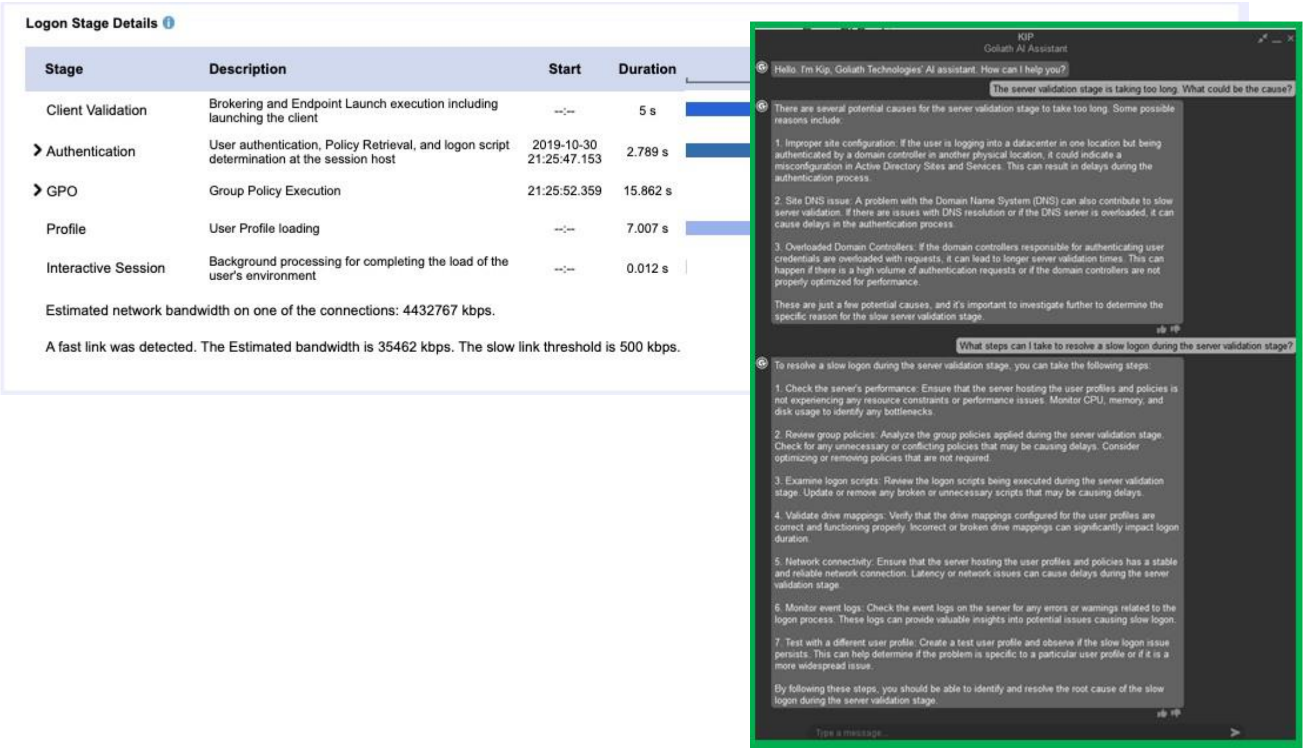
RTT score thresholds:
🟩 Excellent: < 50 ms
🟩 Good: >= 50 and < 150 ms
🟧 Fair: >= 150 and < 250 ms
🟥 Poor: >= 250 ms

Use this report to provide a benchmark for new pilots or deployments, provide management with objective reporting that is easy to consume, proactively identify trouble spots and focus resources on areas of need, and much more.

AI-Powered Troubleshooting

Goliath introduced the first AI Horizon troubleshooting assistant. By leveraging AI in the troubleshooting workflow, IT teams can:

- Quickly troubleshoot Horizon issues without Horizon-specific expertise
- Make up for limited resources such as IT budget and headcount
- Empower all levels of the IT Support team to troubleshoot ultimately reducing escalations
- Reduce remediation times



Logon Stage Details

Stage	Description	Start	Duration
Client Validation	Brokering and Endpoint Launch execution including launching the client	--:--	5 s
Authentication	User authentication, Policy Retrieval, and logon script determination at the session host	2019-10-30 21:25:47.153	2.789 s
GPO	Group Policy Execution	21:25:52.359	15.862 s
Profile	User Profile loading	--:--	7.007 s
Interactive Session	Background processing for completing the load of the user's environment	--:--	0.012 s

Estimated network bandwidth on one of the connections: 4432767 kbps.

A fast link was detected. The Estimated bandwidth is 35462 kbps. The slow link threshold is 500 kbps.

Hello. I'm Kip, Goliath Technologies' AI assistant. How can I help you?

The server validation stage is taking too long. What could be the cause?

There are several potential causes for the server validation stage to take too long. Some possible reasons include:

1. Improper site configuration: If the user is logging into a datacenter in one location but being authenticated by a domain controller in another physical location, it could indicate a misconfiguration in Active Directory Sites and Services. This can result in delays during the authentication process.

2. Site DNS issue: A problem with the Domain Name System (DNS) can also contribute to slow server validation. If there are issues with DNS resolution or if the DNS server is overloaded, it can cause delays in the authentication process.

3. Overloaded Domain Controllers: If the domain controllers responsible for authenticating user credentials are overloaded with requests, it can lead to longer server validation times. This can happen if there is a high volume of authentication requests or if the domain controllers are not properly optimized for performance.

These are just a few potential causes, and it's important to investigate further to determine the specific reason for the slow server validation stage.

What steps can I take to resolve a slow logon during the server validation stage?

To resolve a slow logon during the server validation stage, you can take the following steps:

1. Check the server's performance: Ensure that the server hosting the user profiles and policies is not experiencing any resource constraints or performance issues. Monitor CPU, memory, and disk usage to identify any bottlenecks.

2. Review group policies: Analyze the group policies applied during the server validation stage. Check for any unnecessary or conflicting policies that may be causing delays. Consider optimizing or removing policies that are not required.

3. Examine logon scripts: Review the logon scripts being executed during the server validation stage. Update or remove any broken or unnecessary scripts that may be causing delays.

4. Validate drive mappings: Verify that the drive mappings configured for the user profiles are correct and functioning properly. Incorrect or broken drive mappings can significantly impact logon duration.

5. Network connectivity: Ensure that the server hosting the user profiles and policies has a stable and reliable network connection. Latency or network issues can cause delays during the server validation stage.

6. Monitor event logs: Check the event logs on the server for any errors or warnings related to the logon process. These logs can provide valuable insights into potential issues causing slow logon.

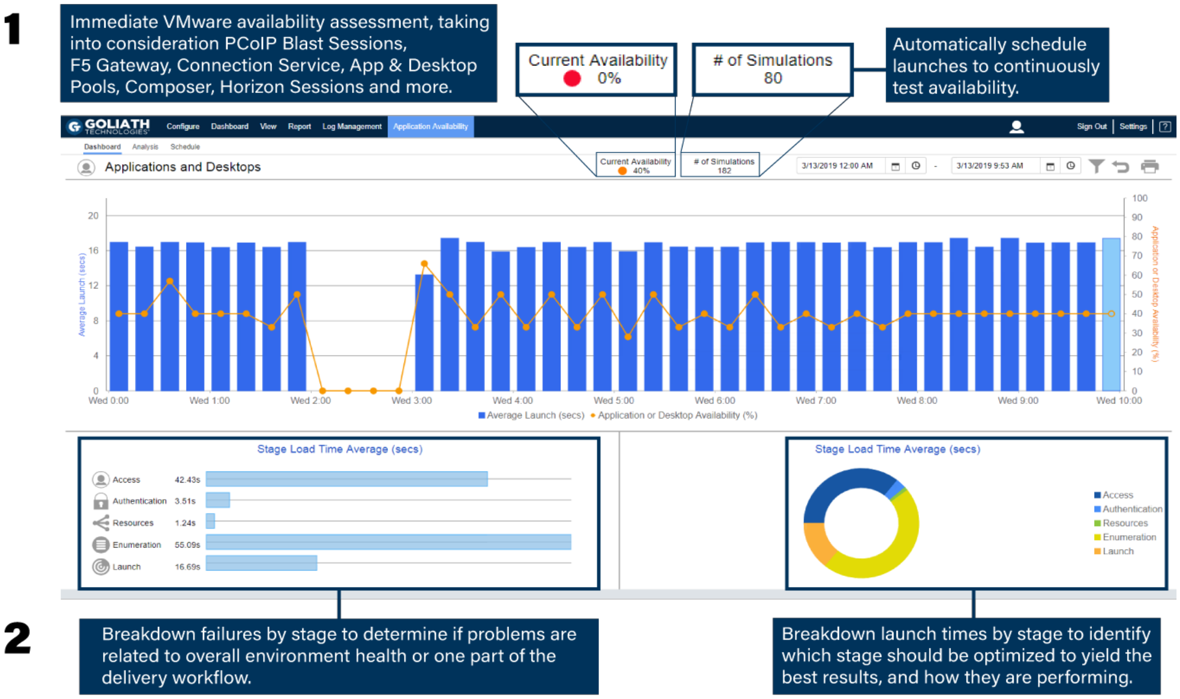
7. Test with a different user profile: Create a test user profile and observe if the slow logon issue persists. This can help determine if the problem is specific to a particular user profile or if it is a more widespread issue.

By following these steps, you should be able to identify and resolve the root cause of the slow logon during the server validation stage.

An Early Warning System

Goliath is the industry's only proactive, production-ready end-user experience software that validates the availability of the entire Omnissa and VMware Horizon delivery infrastructure. It intelligently ensures availability by executing real Horizon sessions that exercise the exact same steps a user takes during the Horizon logon process leveraging virtual users. Regardless of whether a user is remote or local, Goliath gives administrators an "early warning system" that allows them to know exactly what the Hroizon end-user experience will be like for their users - in advance of them logging in.

Illustrated Below: (1) The Application Availability Monitor Dashboard displaying a real-time assessment of Horizon availability and then (2) breaking down launch times by stage.



1

Immediate VMware availability assessment, taking into consideration PCoIP Blast Sessions, F5 Gateway, Connection Service, App & Desktop Pools, Composer, Horizon Sessions and more.

Current Availability ● 0%

# of Simulations 80

Automatically schedule launches to continuously test availability.

2

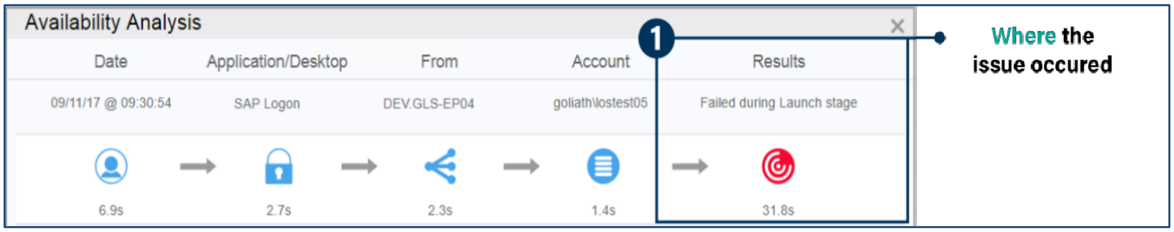
Breakdown failures by stage to determine if problems are related to overall environment health or one part of the delivery workflow.

Breakdown launch times by stage to identify which stage should be optimized to yield the best results, and how they are performing.

End User Screenshot Analytics

The Goliath Virtual User proactively accesses Horizon and other mission-critical applications just like a real user. This provides hard data on what will happen when an actual user logs on from their location and begins launching applications. IT professionals are alerted immediately if an issue occurs, and the system provides specific data on where the failure happened. This allows IT to identify root cause and troubleshoot quickly before actual users are impacted.

When there is a logon failure, an administrator will be alerted immediately. Using the virtual user logon details, an administrator can quickly pinpoint where the failure occurred and the root cause. What the administrator will see is if an issue occurred is an exact snapshot of where the issue occurred as shown below.



Availability Analysis

Date	Application/Desktop	From	Account	Results
09/11/17 @ 09:30:54	SAP Logon	DEV.GLS-EP04	goliath\lostest05	Failed during Launch stage

Below that the administrator will see screenshot evidence of exactly what the virtual logon screened looked like and what applications were launched at each step of the logon process.

Finally, with details spelled out for each stage at each second, administrators can quickly see that the launch failed at a specific point in time (like launching Google Chrome).

Proactive Monitoring and Troubleshooting

Real-Time Omnissa and VMware Performance Metrics

Goliath for VMware Horizon consolidates all the pertinent data about your infrastructure into a single view for broad and deep visibility into Omnissa, VMware, and the end-user experience. You get metrics for 5 layers (Hardware, Host, VMs, OS, Apps) of the Horizon infrastructure in the form of detailed screens and customizable performance graphs.

- **RDSH Host Display**: Number of users, sessions, and resource utilization
- **Real-time Session Display:** user, farm/site, machine, session ID, session start, duration, logon time, CPU usage, memory, RTT and more
- **PCoIP Blast Protocol Metrics:** RTT, bandwidth, channels, FPS, session latency, packet loss
- **Server Info:** CPU, memory, disk drives, host latency, datastore usage, queue length, IOPs, storage latency
- **Logon Duration**: All stages of the logon process for precise troubleshooting
- **End-User Experience**: Pertinent metrics to quickly determine a user's experience

Omnissa & VMware Delivery Infrastructure Performance

Goliath provides visibility into the underlying delivery infrastructure supporting Horizon including:

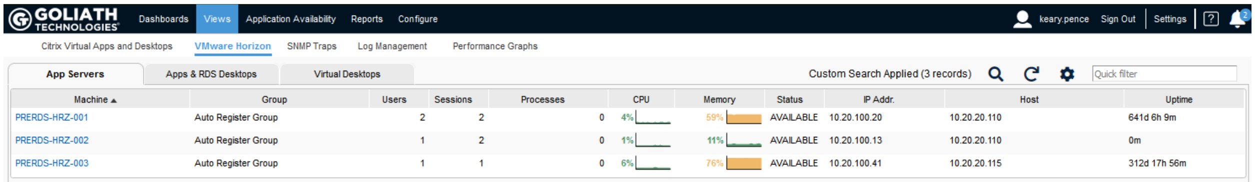
- vSphere hosts
- Connection servers
- Secure gateway’
- RDSH servers
- Supporting infrastructure such as:
  - Active Directory,
  - Back-end applications
- And more

This enables administrators to quickly identify the root cause whether it be due to specific user behavior, impacting a focused group of users, or impacting everyone due to a core infrastructure challenge.

Integrated RDSH Hosts Display

Goliath for Horizon provides a single place to view all the RDSH servers, the number of users, sessions, and resource utilization of each. With a single glance, administrators can immediately determine if:

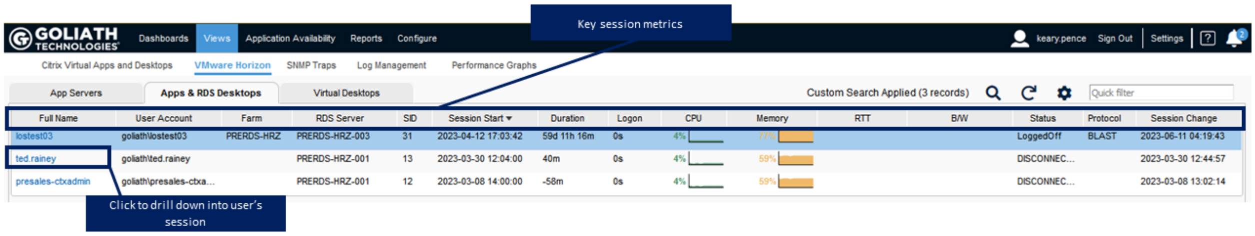
1. An RDSH server is overloaded with users which may indicate a load balancing issue.
2. The environment is properly balanced or if certain servers have more users than others.
3. User activity may be generating high CPU or Memory conditions



Machine ▲	Group	Users	Sessions	Processes	CPU	Memory	Status	IP Addr.	Host	Uptime
PRERDS-HRZ-001	Auto Register Group	2	2	0	4%	59%	AVAILABLE	10.20.100.20	10.20.20.110	641d 6h 9m
PRERDS-HRZ-002	Auto Register Group	1	2	0	1%	11%	AVAILABLE	10.20.100.13	10.20.20.110	0m
PRERDS-HRZ-003	Auto Register Group	1	1	0	6%	76%	AVAILABLE	10.20.100.41	10.20.20.115	312d 17h 56m

Real-Time Session Display

Goliath provides granular real-time and historic data for all Horizon sessions. When there are end-user experience issues, drill into a user session to gain deeper visibility and identify the root cause.



Key session metrics

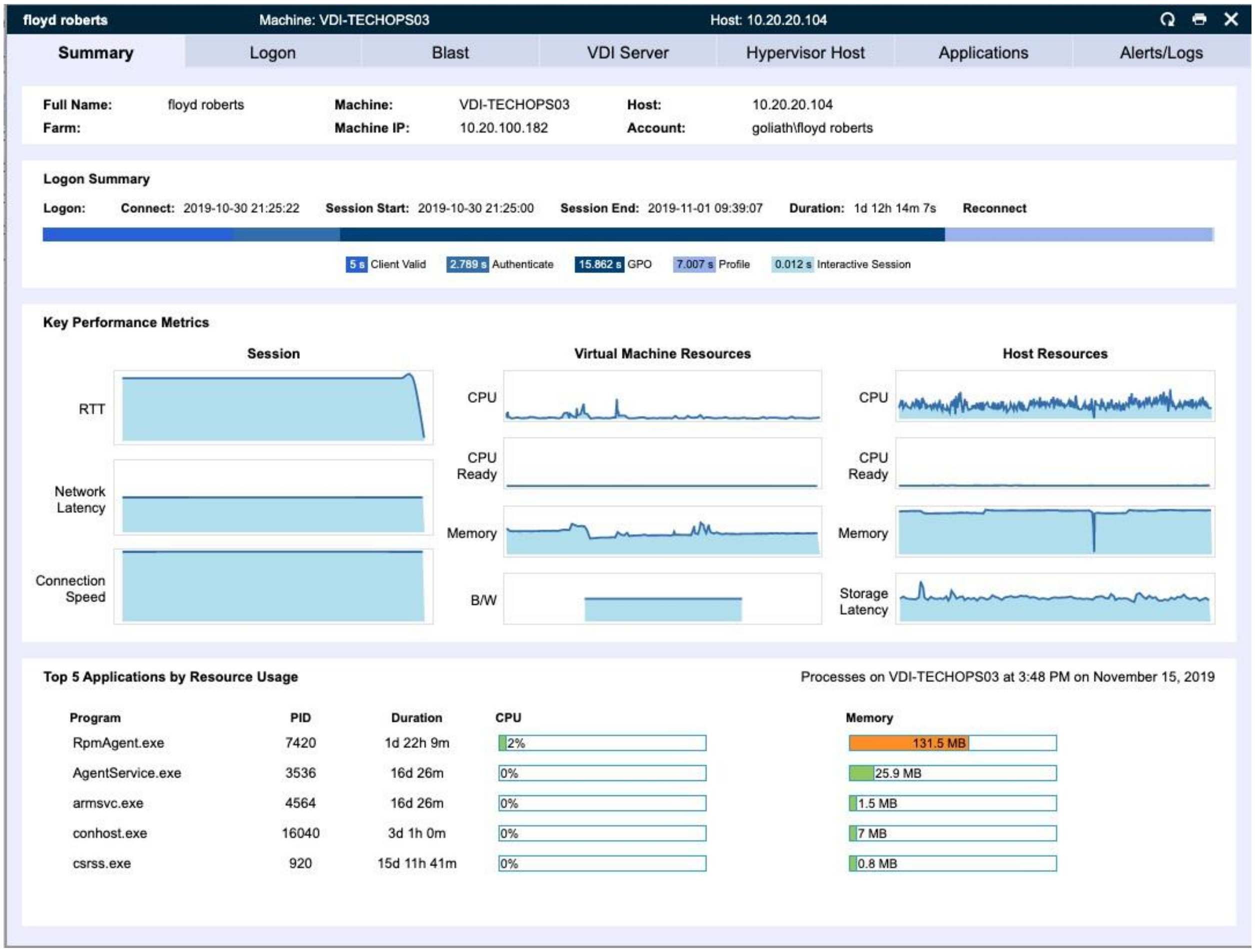
Full Name	User Account	Farm	RDS Server	SID	Session Start ▾	Duration	Logon	CPU	Memory	RTT	B/W	Status	Protocol	Session Change
lostest03	goliath\lostest03	PRERDS-HRZ	PRERDS-HRZ-003	31	2023-04-12 17:03:42	59d 11h 16m	0s	4%	77%			LoggedOff	BLAST	2023-06-11 04:19:43
ted.rainey	goliath\ted.rainey		PRERDS-HRZ-001	13	2023-03-30 12:04:00	40m	0s	4%	59%			DISCONNEC...		2023-03-30 12:44:57
presales-ctxadmin	goliath\presales-ctxa...		PRERDS-HRZ-001	12	2023-03-08 14:00:00	-58m	0s	4%	59%			DISCONNEC...		2023-03-08 13:02:14

Click to drill down into user’s session

In Session Real-Time Analytics Overview

Goliath provides the ability to drill down into a single end user's session and, at a glance, review key analytics around that session performance: logon duration summary, key performance metrics from PCoIP/BLAST, VM resources, host resources along with application resource usage data.

This quick summary enables an administrator to quickly view correlated performance metrics and rule out what isn't causing the performance bottleneck and focus on the metrics that appear to indicate root cause.



Full Name: floyd roberts **Machine:** VDI-TECHOPS03 **Host:** 10.20.20.104
Farm: **Machine IP:** 10.20.100.182 **Account:** goliath\floyd roberts

Logon Summary

Logon: **Connect:** 2019-10-30 21:25:22 **Session Start:** 2019-10-30 21:25:00 **Session End:** 2019-11-01 09:39:07 **Duration:** 1d 12h 14m 7s **Reconnect**

5 s Client Valid 2.789 s Authenticate 15.862 s GPO 7.007 s Profile 0.012 s Interactive Session

Top 5 Applications by Resource Usage

Processes on VDI-TECHOPS03 at 3:48 PM on November 15, 2019

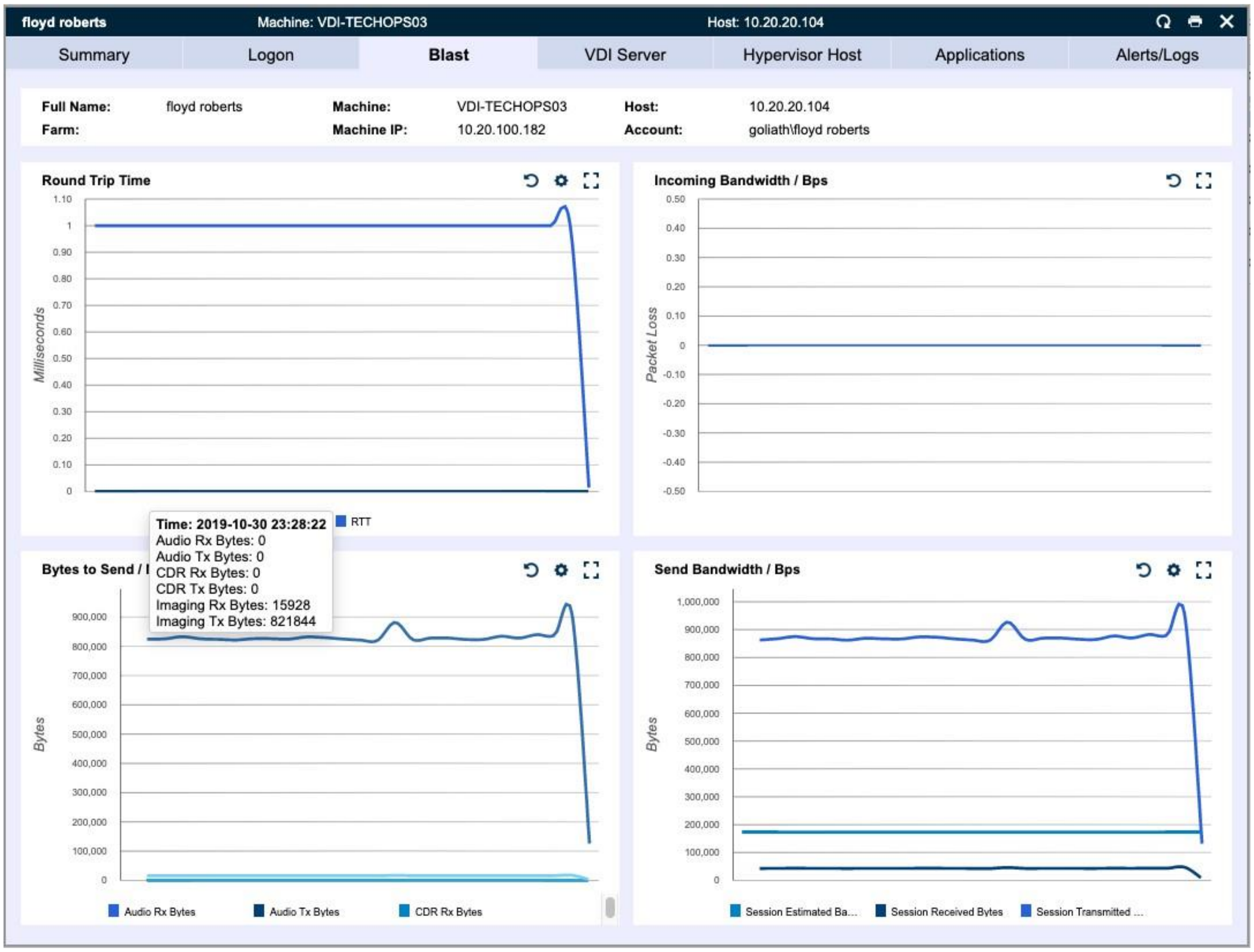
Program	PID	Duration	CPU	Memory
RpmAgent.exe	7420	1d 22h 9m	2%	131.5 MB
AgentService.exe	3536	16d 26m	0%	25.9 MB
armsvc.exe	4564	16d 26m	0%	1.5 MB
conhost.exe	16040	3d 1h 0m	0%	7 MB
csrss.exe	920	15d 11h 41m	0%	0.8 MB

Real-Time PCoIP/BLAST Drill Down from Session Display

Goliath provides industry-leading visibility into Horizon session performance by breaking down the PCoIP/BLAST protocol into its key parts. Viewing these metrics in a single dashboard gives administrators the ability to quickly identify relationships between user behavior and connection performance.

Details metrics include:

- **Round Trip Time:** Round Trip Time is the primary indicator of user experience. Values over 400ms are indicative of poor performance. RTT includes network latency, server TCP load, and presentation layer response time in the calculation.
- **Bandwidth:** These charts include the bandwidth usage and break it down into various factors analyzing bandwidth at different channels. For example, on the bottom left chart you can see audio bandwidth.


floyd roberts

Machine: VDI-TECHOPS03

Host: 10.20.20.104

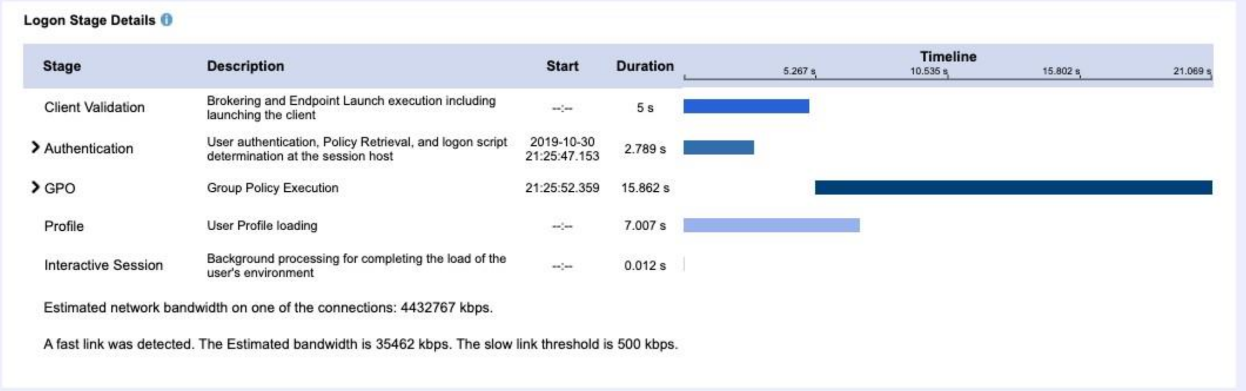
Full Name:	floyd roberts	**Machine:**	VDI-TECHOPS03	**Host:**	10.20.20.104
Farm:		**Machine IP:**	10.20.100.182	**Account:**	goliath\floyd roberts

Time: 2019-10-30 23:28:22
Audio Rx Bytes: 0
Audio Tx Bytes: 0
CDR Rx Bytes: 0
CDR Tx Bytes: 0
Imaging Rx Bytes: 15928
Imaging Tx Bytes: 821844

Real-Time Horizon Logon Duration Drilldown

If you can't drill down into all of the detailed stages of the Horizon logon process, then you can't isolate and fix root cause of logon slowness. With the Horizon Logon Duration monitoring and troubleshooting functionality, you can capture real-time Logon Duration times and get alerted to end user logon slowness on all of the detailed Logon Duration Stages.

The real-time Horizon Logon Duration Drilldown breaks down a user's logon process into each of the stages to help understand what needs to be optimized to improve logon times. This report can also be used to identify and troubleshoot session load problems by identifying what may be getting stuck or taking too long to process. Threshold-based alerting on user logon times is also possible.



Logon Stage Details

Stage	Description	Start	Duration	Timeline 5.267 s 10.535 s 15.802 s 21.069 s
Client Validation	Brokering and Endpoint Launch execution including launching the client	--:--	5 s	
› Authentication	User authentication, Policy Retrieval, and logon script determination at the session host	2019-10-30 21:25:47.153	2.789 s	
› GPO	Group Policy Execution	21:25:52.359	15.862 s	
Profile	User Profile loading	--:--	7.007 s	
Interactive Session	Background processing for completing the load of the user's environment	--:--	0.012 s	

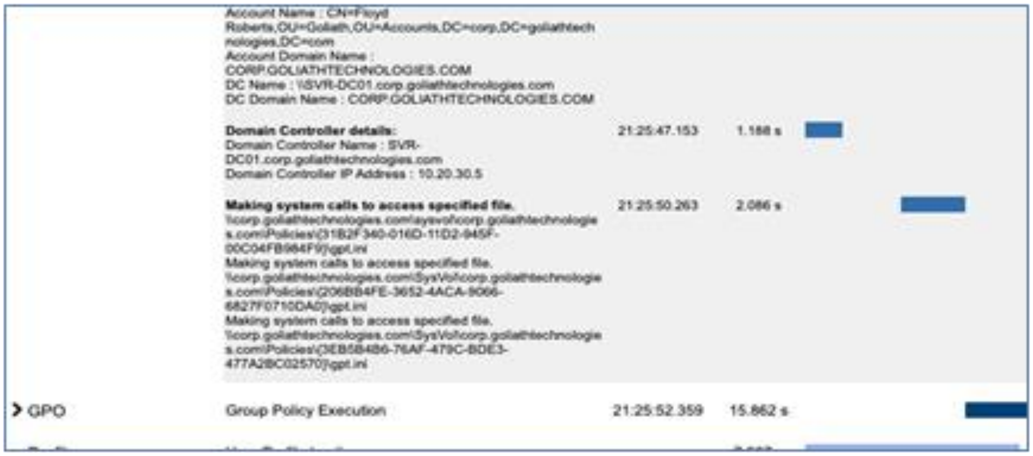
Estimated network bandwidth on one of the connections: 4432767 kbps.

A fast link was detected. The Estimated bandwidth is 35462 kbps. The slow link threshold is 500 kbps.

The logon duration drill down allows an administrator to parse logon times into each stage, policy, application and machine. This includes the details from the time that the connection server determines where the user is connecting to (RDSH Server or VDI) to the point where the session is fully established. The same capability is present for both VDI and RDSH published applications and desktops.

These stages include:

- Client Validation
- Authentication
- Group Policy Processing
- Profile Loading
- Interactive Session



Account Name : CN=Floyd Roberts,OU=Goliath,OU=Accounts,DC=corp,DC=goliathtechnologies,DC=com
Account Domain Name : CORP.GOLIATHTECHNOLOGIES.COM
DC Name : \\SVR-DC01.corp.goliathtechnologies.com
DC Domain Name : CORP.GOLIATHTECHNOLOGIES.COM

Domain Controller details: 21:25:47.153 1.188 s
Domain Controller Name : SVR-DC01.corp.goliathtechnologies.com
Domain Controller IP Address : 10.20.30.5

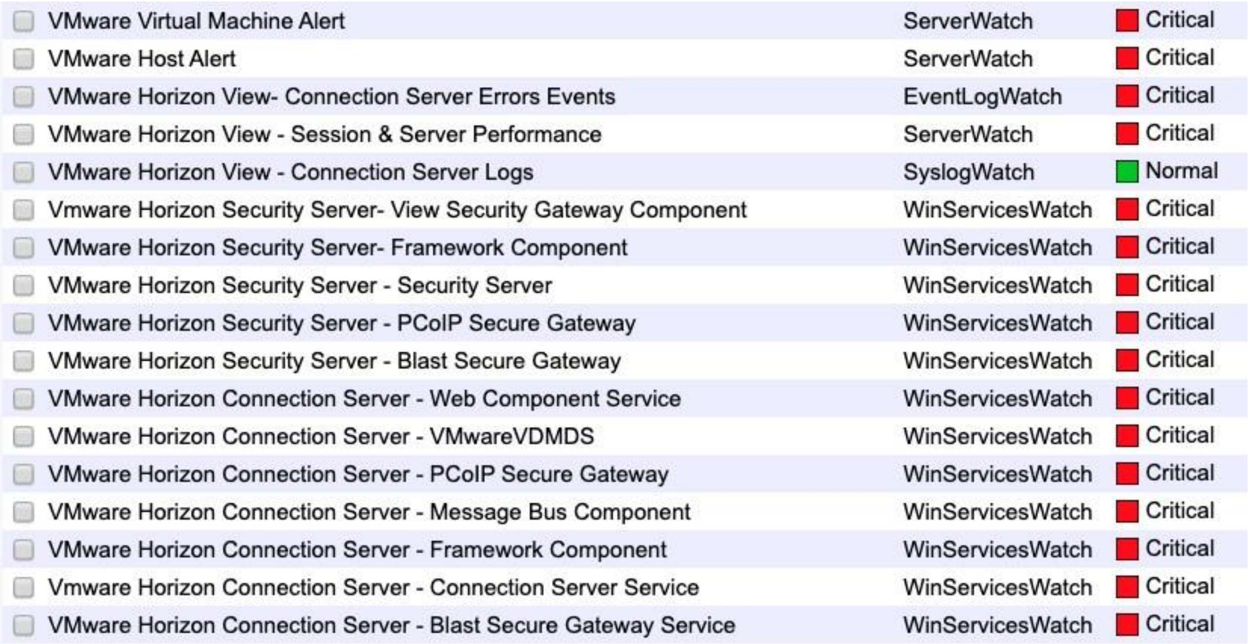
Making system calls to access specified file. 21:25:50.263 2.086 s
\\corp.goliathtechnologies.com\sysvol\corp.goliathtechnologies.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini
Making system calls to access specified file.
\\corp.goliathtechnologies.com\SysVol\corp.goliathtechnologies.com\Policies\{206BB4FE-3652-4ACA-9066-6827F0710DA0}\gpt.ini
Making system calls to access specified file.
\\corp.goliathtechnologies.com\SysVol\corp.goliathtechnologies.com\Policies\{3EB5B4B6-76AF-479C-BDE3-477A2BC02570}\gpt.ini

› GPO Group Policy Execution 21:25:52.359 15.862 s

Embedded Intelligence for Common Failure Points

Goliath Performance Monitor comes with "embedded intelligence" consisting of hundreds of pre-configured monitoring rules and alerts based upon best practices from Omnissa & VMware and our own Goliath consulting experience. This means that immediately upon deployment, the product begins using this embedded intelligence to automatically search out these known failure points and conditions. This out-of-the-box functionality simplifies deployment and allows for administrators to immediately begin focusing on improving environmental bottlenecks or failure points. These alerts scan for common problems end users may encounter:

- Applications: crashes, hangs, leaking CPU and memory
- Profile: profile corruption, temporary profiles, profile load failures, insufficient rights
- Printing: printing service failures, printer driver issues, printer mapping, and driver compatibility
- Registry: registry corruption, profile load failures, registry loading failures



☐	VMware Virtual Machine Alert	ServerWatch	🟥 Critical
☐	VMware Host Alert	ServerWatch	🟥 Critical
☐	VMware Horizon View- Connection Server Errors Events	EventLogWatch	🟥 Critical
☐	VMware Horizon View - Session & Server Performance	ServerWatch	🟥 Critical
☐	VMware Horizon View - Connection Server Logs	SyslogWatch	🟩 Normal
☐	Vmware Horizon Security Server- View Security Gateway Component	WinServicesWatch	🟥 Critical
☐	VMware Horizon Security Server- Framework Component	WinServicesWatch	🟥 Critical
☐	VMware Horizon Security Server - Security Server	WinServicesWatch	🟥 Critical
☐	VMware Horizon Security Server - PCoIP Secure Gateway	WinServicesWatch	🟥 Critical
☐	VMware Horizon Security Server - Blast Secure Gateway	WinServicesWatch	🟥 Critical
☐	VMware Horizon Connection Server - Web Component Service	WinServicesWatch	🟥 Critical
☐	VMware Horizon Connection Server - VMwareVDMDS	WinServicesWatch	🟥 Critical
☐	VMware Horizon Connection Server - PCoIP Secure Gateway	WinServicesWatch	🟥 Critical
☐	VMware Horizon Connection Server - Message Bus Component	WinServicesWatch	🟥 Critical
☐	VMware Horizon Connection Server - Framework Component	WinServicesWatch	🟥 Critical
☐	Vmware Horizon Connection Server - Connection Server Service	WinServicesWatch	🟥 Critical
☐	VMware Horizon Connection Server - Blast Secure Gateway Service	WinServicesWatch	🟥 Critical

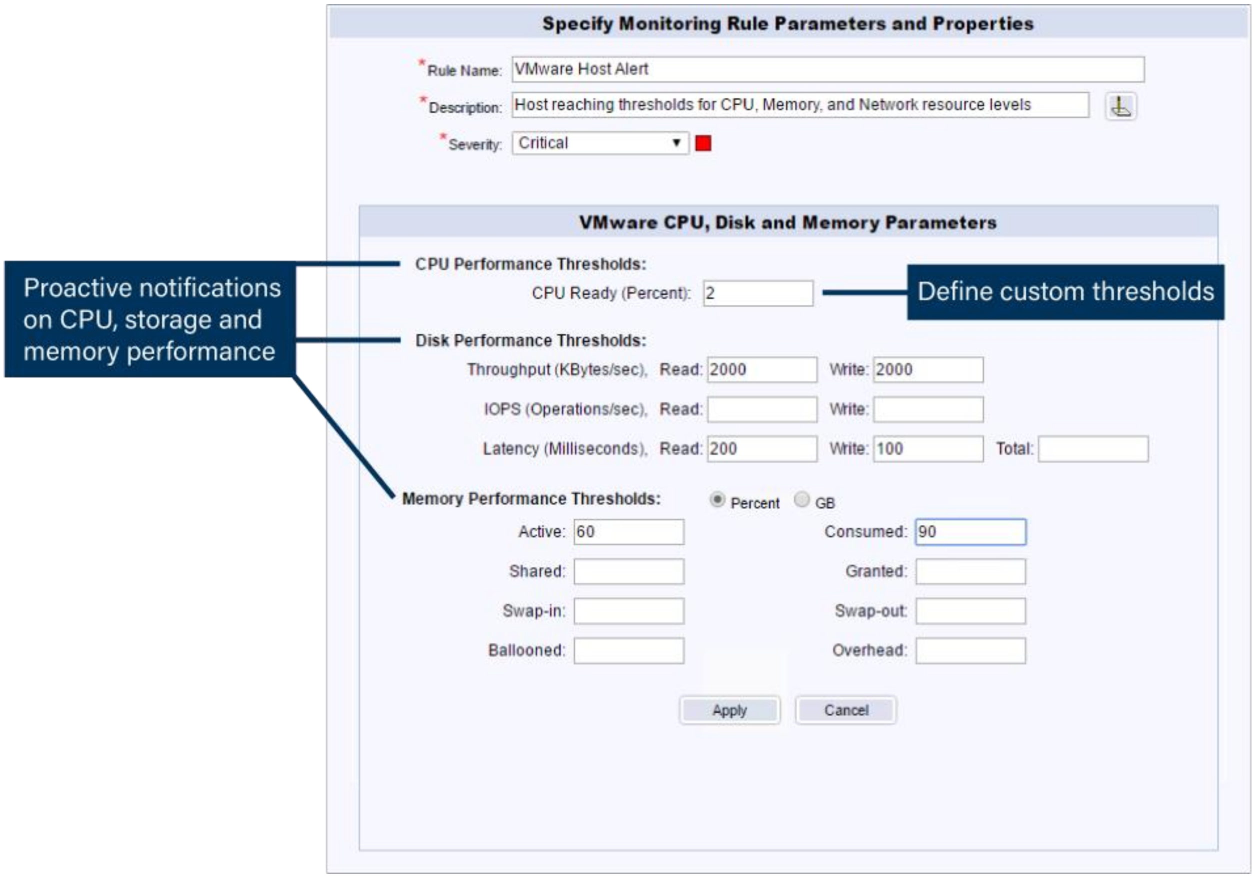
Advanced Remediation Capabilities to Improve

Troubleshooting

Goliath goes beyond providing differentiating Horizon visibility and granular metrics by also delivering unique operational features that allow organizations to take the next step in improving operational IT troubleshooting and Help Desk workflows.

Threshold-Based Alerting

Define custom thresholds and receive proactive notifications based on faults, errors, and conditions so administrators can resolve issues before end users complain. Configuring alerts and tuning them to the specifications of each department requires no scripting or customizations because there are prebuilt templates for each type of alert.



Specify Monitoring Rule Parameters and Properties

*Rule Name: VMware Host Alert
*Description: Host reaching thresholds for CPU, Memory, and Network resource levels
*Severity: Critical 🟥

VMware CPU, Disk and Memory Parameters

CPU Performance Thresholds:
CPU Ready (Percent): 2

Disk Performance Thresholds:
Throughput (KBytes/sec), Read: 2000 Write: 2000
IOPS (Operations/sec), Read: Write:
Latency (Milliseconds), Read: 200 Write: 100 Total:

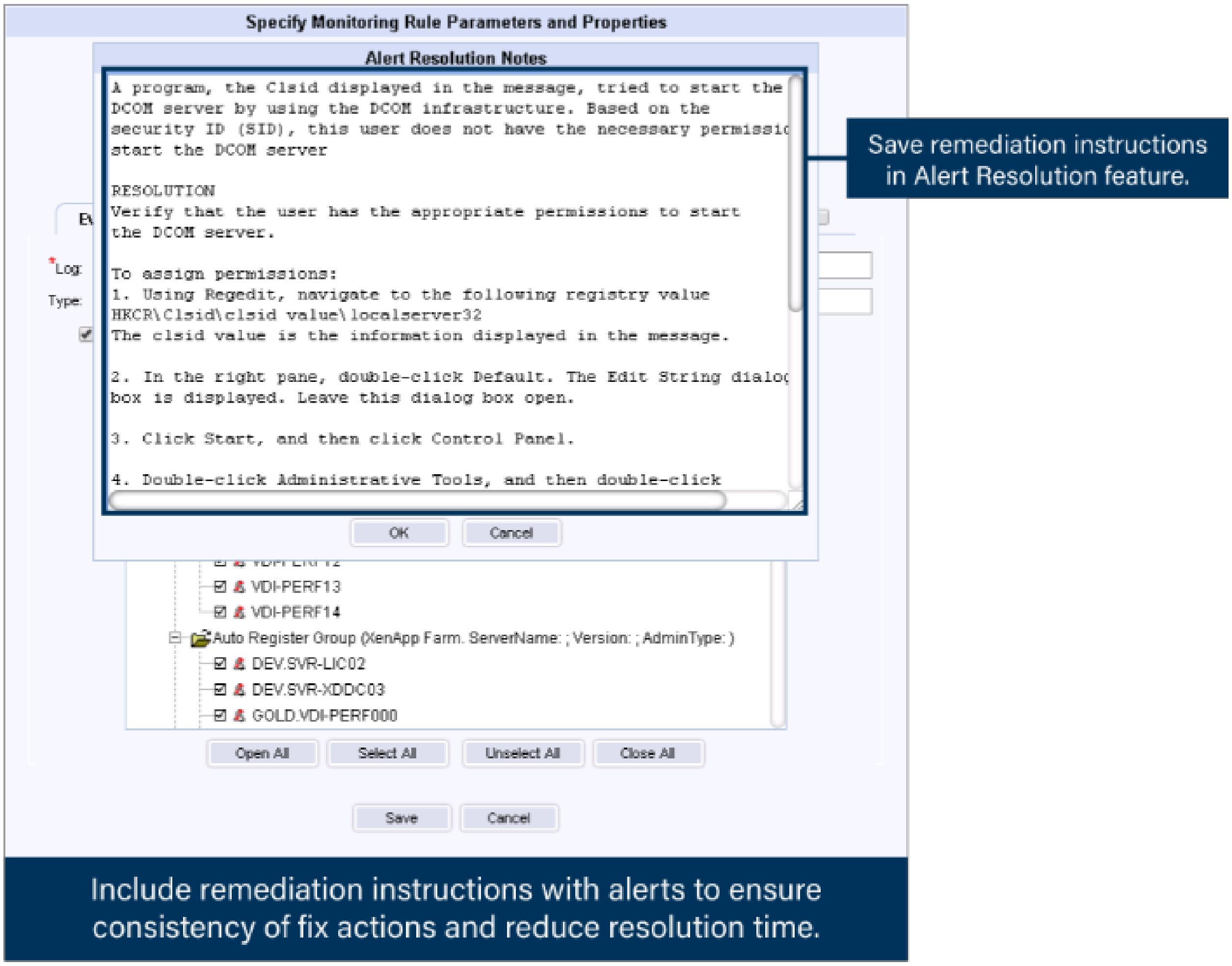
Memory Performance Thresholds: ● Percent ○ GB
Active: 60 Consumed: 90
Shared: Granted:
Swap-in: Swap-out:
Ballooned: Overhead:

Proactive notifications on CPU, storage and memory performance

Define custom thresholds

Alert Resolution Feature

For workflows that cannot be automated, Goliath allows administrators to automatically pass on troubleshooting instructions to the appropriate administrators when certain alerts are triggered. This enables consistent response quality regardless of the help desk responder and frees up senior resources for other projects rather than responding to recurring issues.



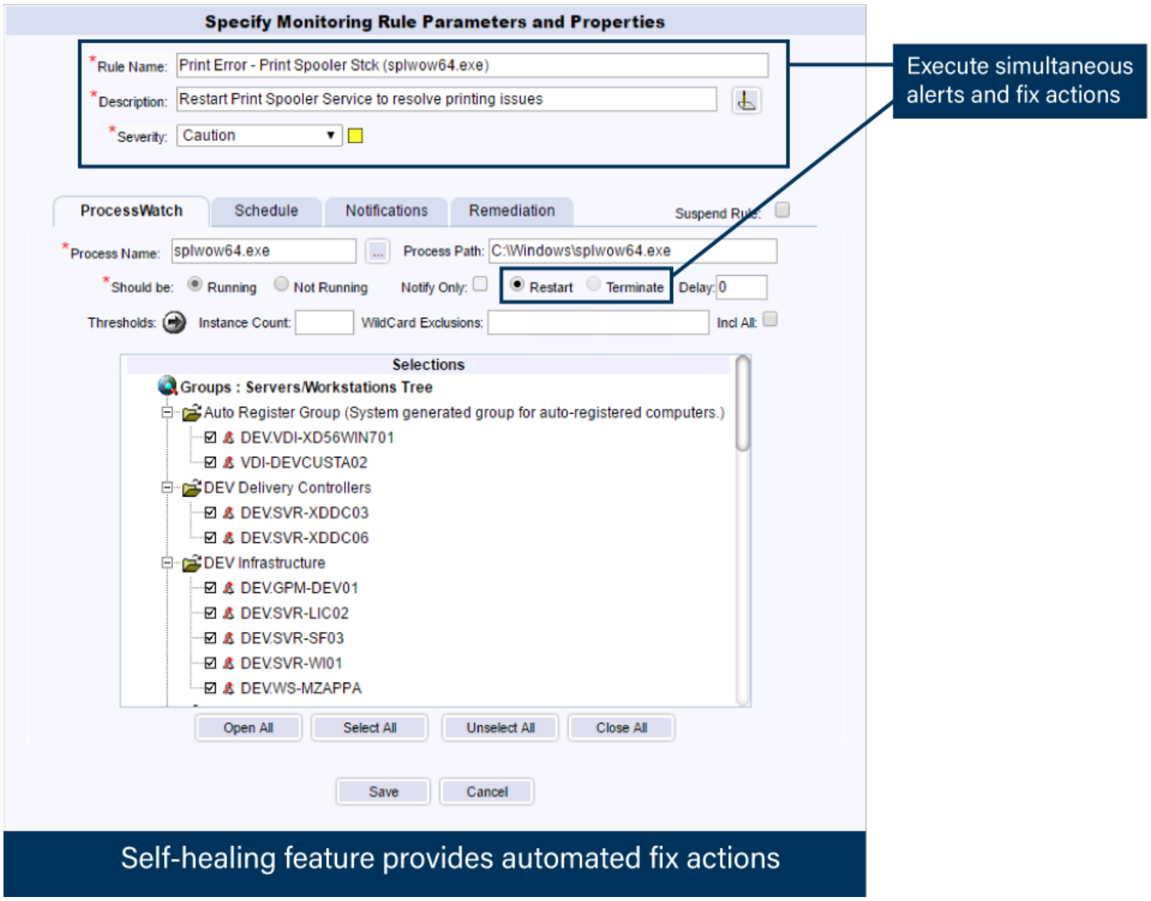
```
A program, the Clsid displayed in the message, tried to start the
DCOM server by using the DCOM infrastructure. Based on the
security ID (SID), this user does not have the necessary permissi
start the DCOM server

RESOLUTION
Verify that the user has the appropriate permissions to start
the DCOM server.

To assign permissions:
1. Using Regedit, navigate to the following registry value
HKCR\Clsid\clsid value\localserver32
The clsid value is the information displayed in the message.

2. In the right pane, double-click Default. The Edit String dialo
box is displayed. Leave this dialog box open.

3. Click Start, and then click Control Panel.

4. Double-click Administrative Tools, and then double-click
```

Save remediation instructions in Alert Resolution feature.

Include remediation instructions with alerts to ensure consistency of fix actions and reduce resolution time.

Automated Remediation Actions

You can configure automatic remediation fixes to take place when certain alerts are triggered based on faults, events or conditions. Whether it be restarting a service or running a PowerShell script, Goliath supports a number of "self- healing" workflows to allow IT organizations to dramatically increase Help Desk response times and implement truly proactive IT processes.



Specify Monitoring Rule Parameters and Properties

*Rule Name: Print Error - Print Spooler Stck (splwow64.exe)
*Description: Restart Print Spooler Service to resolve printing issues
*Severity: Caution 🟨

*Process Name: splwow64.exe
Process Path: C:\Windows\splwow64.exe
*Should be: ● Running ○ Not Running
Notify Only: ☐
● Restart ○ Terminate
Delay: 0
Thresholds:
Instance Count:
WildCard Exclusions:
Incl All: ☐

Selections
Groups : Servers/Workstations Tree
- Auto Register Group (System generated group for auto-registered computers.)
  - ☑ DEV.VDI-XD56WIN701
  - ☑ VDI-DEVCUSTA02
- DEV Delivery Controllers
  - ☑ DEV.SVR-XDDC03
  - ☑ DEV.SVR-XDDC06
- DEV Infrastructure
  - ☑ DEV.GPM-DEV01
  - ☑ DEV.SVR-LIC02
  - ☑ DEV.SVR-SF03
  - ☑ DEV.SVR-WI01
  - ☑ DEV.WS-MZAPPA

Execute simultaneous alerts and fix actions

Self-healing feature provides automated fix actions

Automated infrastructure fix actions:

- Restart SQL service
- Unlock user account
- Rebalance VDI sessions across host
- Restart ANY application
- Terminate applications processes
- Restart backup job
- Reboot servers

Reporting

Out-of-the-box reports allow administrators to report on session activity, trending faults and errors, and trend performance. Whether for troubleshooting or capacity planning, reports in Goliath enable administrators to have a historical reference to environment performance and events.

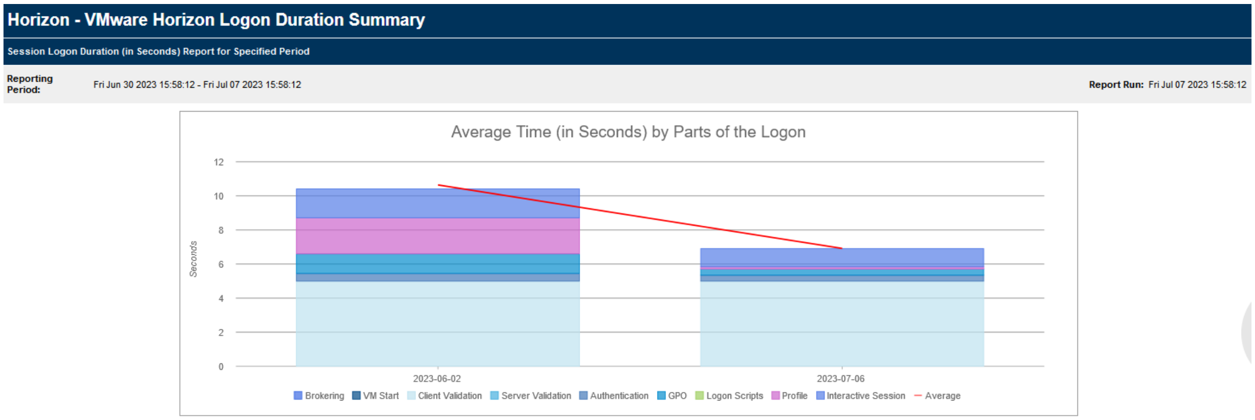
- Horizon End User Experience Reports
- Horizon Logon Duration Summary
- VMware Performance Reports
- VMware ESX/ESXi - Host Performance
- VMware ESX/ESXi - Virtual Machine Performance
- VMware ESX/ESXi - Storage Usage

In order to assist you in proactively managing your entire virtual and physical IT infrastructure, along with your operation systems and network, Goliath offers a variety of IT Infrastructure Performance Reports that can help you get ahead of infrastructure performance issues that may cause end users to experience problems such as printing and profile failures. Here is a sample of reports available:

- Alert analysis
- Group policy & registry health
- Logical drive utilization status
- Memory utilization status
- Printing health
- Profile errors
- Registry monitor status
- Sever configuration details
- User security
- Server monitoring rules assignments
- SSL & communication errors
- Syslog message analysis
- Uptime & availability
- Windows event log analysis
- Windows server & configuration errors
- Operating system inventory
- Group inventory

Sample Reports

Horizon Logon Duration Summary: Summary breakdown of logon duration by stage over a set period of time.



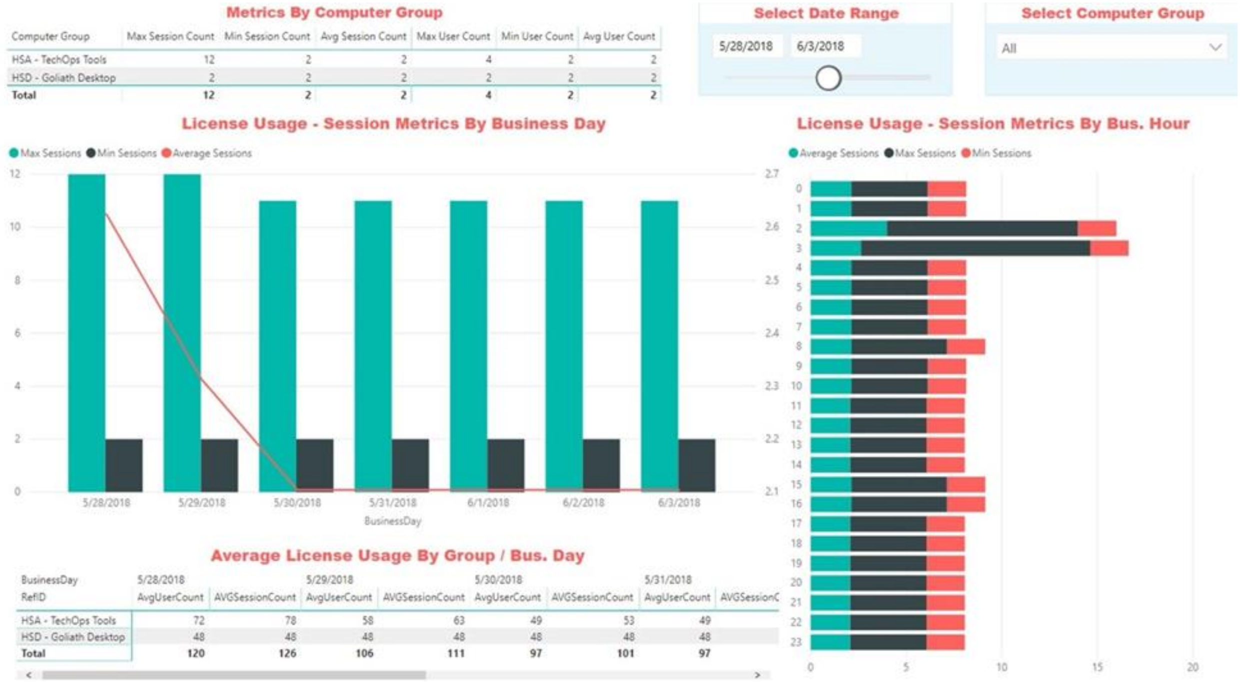
Horizon - VMware Horizon Logon Duration Summary

Session Logon Duration (in Seconds) Report for Specified Period

Reporting Period: Fri Jun 30 2023 15:58:12 - Fri Jul 07 2023 15:58:12

Report Run: Fri Jul 07 2023 15:58:12

License Usage Report: This interactive template shows license usage by group or time period, with adjustable filters for date ranges and specific groups.



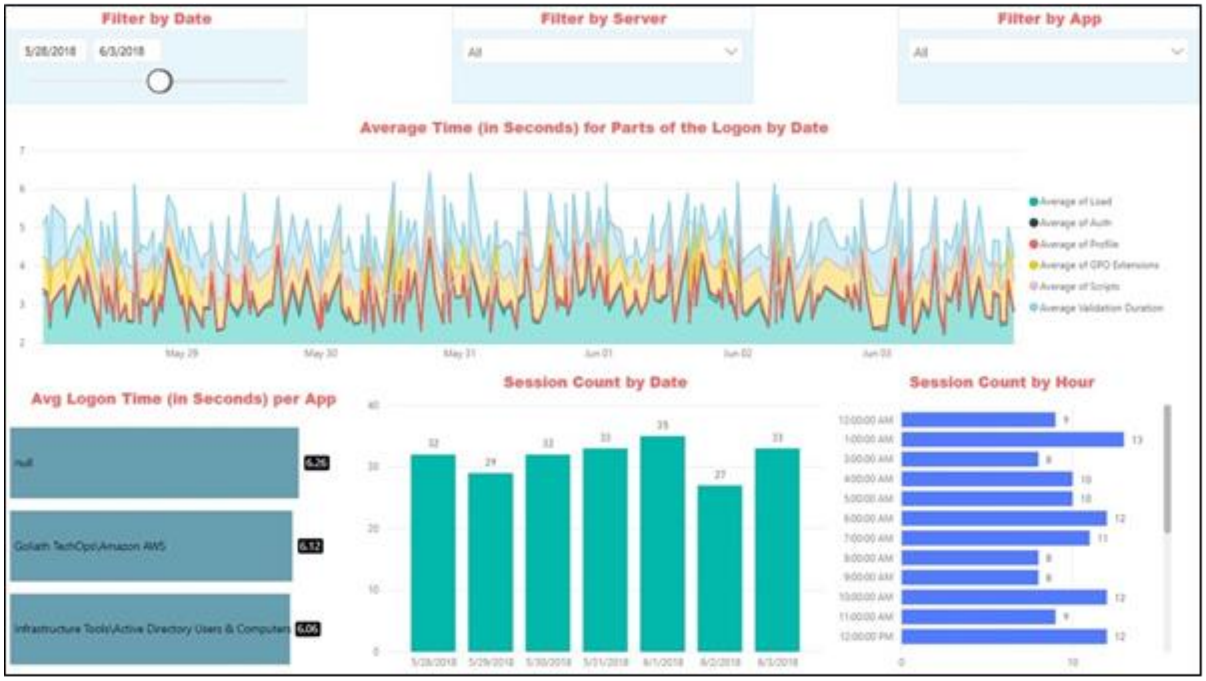
Metrics By Computer Group

Computer Group	Max Session Count	Min Session Count	Avg Session Count	Max User Count	Min User Count	Avg User Count
HSA - TechOps Tools	12	2	2	4	2	2
HSD - Goliath Desktop	2	2	2	2	2	2
Total	**12**	**2**	**2**	**4**	**2**	**2**

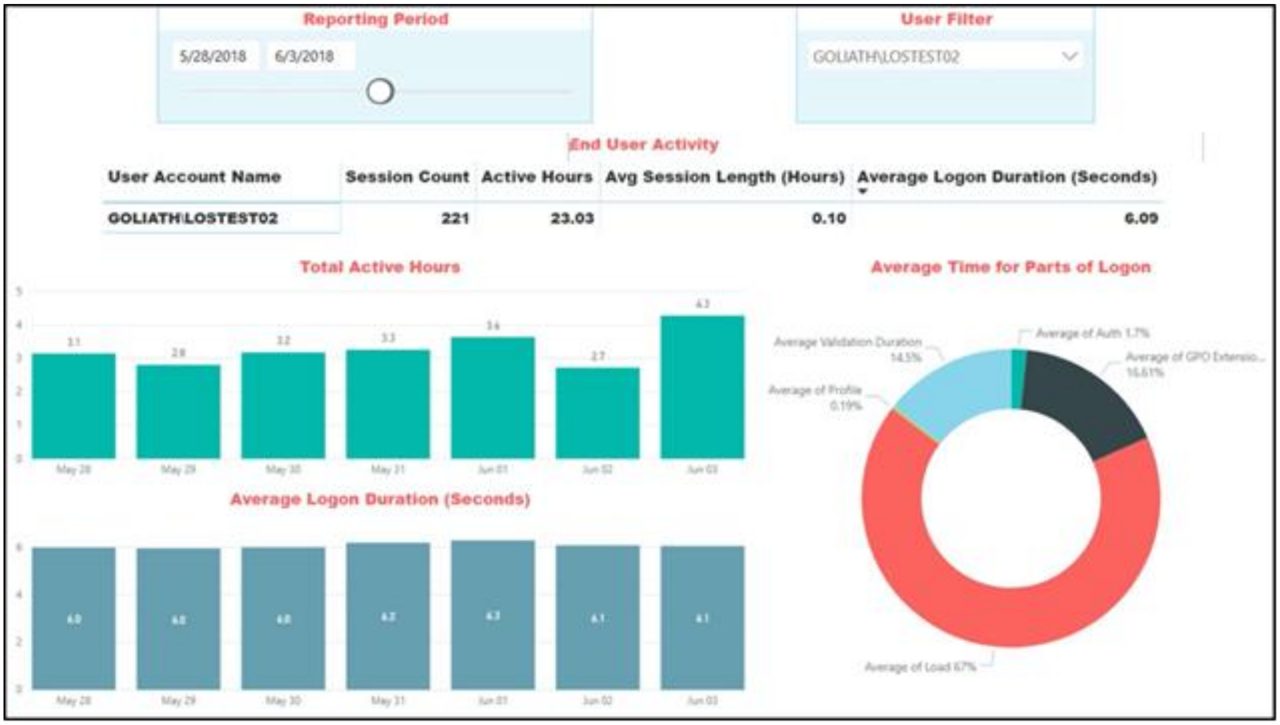
Average License Usage By Group / Bus. Day

BusinessDay	5/28/2018		5/29/2018		5/30/2018		5/31/2018	
RefID	AvgUserCount	AVGSessionCount	AvgUserCount	AVGSessionCount	AvgUserCount	AVGSessionCount	AvgUserCount	AVGSessionC
HSA - TechOps Tools	72	78	58	63	49	53	49	
HSD - Goliath Desktop	48	48	48	48	48	48	48	
Total	**120**	**126**	**106**	**111**	**97**	**101**	**97**	

Session Logon Duration Pivots: This template shows another way to visualize and interact with Logon Duration data in pivot tables and charts.



End User Activity: This template shows end-user activity by time period and account name. It displays number of sessions, active hours, and session length.



Reporting Period

5/28/2018 6/3/2018

User Filter

GOLIATH\LOSTEST02

End User Activity

User Account Name	Session Count	Active Hours	Avg Session Length (Hours)	Average Logon Duration (Seconds)
GOLIATH\LOSTEST02	221	23.03	0.10	6.09

Get started today with a free demo or a trial of Goliath Performance Monitor for Omnissa Horizon

GOLIATH
TECHNOLOGIES®
BE PROACTIVE