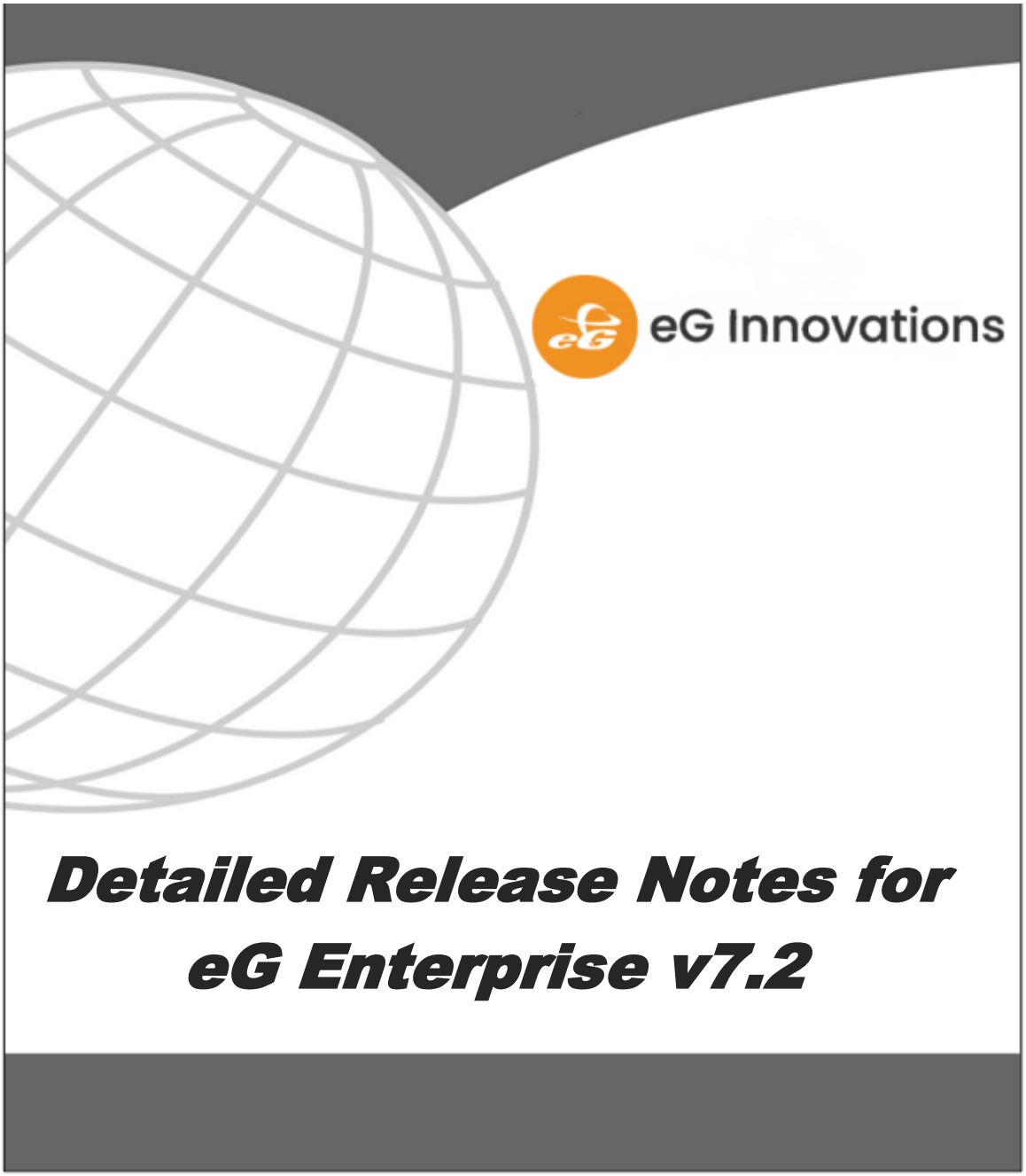


Detailed Release Notes for eG Enterprise v7.2

Table of Contents

1. RELEASE NOTES FOR EG ENTERPRISE V7.2 1
2. DIGITAL WORKSPACES MONITORING 1
2.1 Citrix Monitoring Enhancements 1
2.1.1 Citrix Logon Simulator 1
2.1.2 Citrix Cloud Monitoring Enhancements 3
2.1.3 Enhancements to Citrix Virtual Apps / Virtual Desktops Monitoring 5
2.1.4 Enhancements to Citrix ADC VPX/MPX Monitoring 8
2.1.5 Automatic Problem Resolution 10
2.1.6 Other Citrix Monitoring Enhancements 14
2.1.7 Citrix Reporting Enhancements 14
2.2 VMware Horizon Monitoring Enhancements 18
2.2.1 VMware Horizon Reporting Enhancements 20
2.3 Microsoft Azure Virtual Desktops Monitoring 23
2.3.1 Reports for Microsoft Azure Virtual Desktops 28
2.4 AWS DaaS Monitoring 29
2.4.1 Reporter Enhancements for Amazon Cloud Desktops 30
2.5 Endpoints Monitoring 33
2.5.1 IGEL Monitoring 33
2.5.2 Other EndPoints Monitoring Enhancements 37
2.6 GPU Monitoring Enhancements 38
3. USER EXPERIENCE MONITORING 38
3.1 Real User Monitoring Enhancements 38
3.2 Web App Simulation Enhancements 41
4. APPLICATION PERFORMANCE MONITORING 46
4.1 Microsoft .Net/Node.js BTM Enhancements 46
4.2 Enhancements to Java Business Transaction Monitoring 50
4.2.1 New Reports for eG Business Transaction Monitor 52
4.3 Java Application Servers Monitoring Enhancements 55
5. ENTERPRISE APPLICATION MONITORING 57
5.1 Enhancements for SAP Monitoring 57
5.2 Other Enterprise Application Monitoring Enhancements 59
6. CLOUD MONITORING 59
6.1 AWS Monitoring Enhancements 59
6.2 Microsoft Azure Monitoring Enhancements 61
6.3 Other Monitoring Enhancements for Cloud / SaaS Applications 63
7. VIRTUALIZATION AND CONTAINER MONITORING 64
7.1 Monitoring Container Environments 64

7.2 Nutanix Monitoring Enhancements 64
7.3 Other Monitoring Enhancements 65
8. UNIFIED COMMUNICATIONS MONITORING 66
8.1 Enhancements to Office365 Monitoring 66
8.1.1 Reporter Enhancements for Microsoft Office365 75
8.1.2 Reporter Enhancements for Microsoft Teams 77
8.1.3 Reporter Enhancements for Microsoft Yammer 81
8.1.4 Reporter Enhancements for Microsoft OneDrive 83
8.2 Other Unified Communications Monitoring Enhancements 85
9. OPERATING SYSTEMS MONITORING ENHANCEMENTS 87
10. DATABASE MONITORING ENHANCEMENTS 88
10.1 Reporter Enhancements for Microsoft SQL Database Servers 92
11. MOBILITY MONITORING ENHANCEMENTS 97
12. ENHANCEMENTS TO MONITORING MESSAGING SERVERS 97
13. APPLICATION MIDDLEWARE MONITORING ENHANCEMENTS 99
14. STORAGE AND BACKUP MONITORING ENHANCEMENTS 102
14.1 Storage Enhancements 102
14.2 Monitoring Backup Technologies 103
15. HARDWARE AND NETWORKING TECHNOLOGIES MONITORING ENHANCEMENTS 103
16. SELF-MONITORING ENHANCEMENTS 109
17. ENHANCEMENTS FOR INCREASED AUTOMATION, SIMPLICITY, SCALABILITY AND SECURITY 109
17.1 Architecture Enhancements 109
17.2 Auto-Discovery Improvements 112
17.3 Usability Enhancements 113
17.3.1 Admin Interface 114
17.3.2 Monitor Interface 123
17.3.3 Reporter Interface 128
17.4 Installation Enhancements 131
17.5 eG Mobile Application Enhancements 133
17.6 Enhancements to eG CLI 141
17.7 Enhancements to eG REST API 142
17.8 Integration Enhancements 142
17.9 Security Enhancements 143
17.10 Scalability Improvements 144
18. CONCLUSION 144

1. Release Notes for eG Enterprise v7.2

Version 7.2 is a major release of eG Enterprise. While this release predominantly has bug fixes and scalability improvements, a few new capabilities have also been added. This document provides a comprehensive list of enhancements and bug fixes that are part of this release.

2. Digital Workspaces Monitoring

2.1 Citrix Monitoring Enhancements

2.1.1 Citrix Logon Simulator

The Citrix Logon Simulator provides a simple way for organizations to monitor the ability of users to logon to the Citrix farm, from an external perspective. eG Enterprise v7.2 includes several new enhancements to the Citrix Logon Simulator:

- **Capturing ICA File Availability and Download Duration:** When a published application / desktop is enumerated in Citrix StoreFront, the ICA file will be downloaded immediately. If this file takes too long to be downloaded, the user's logon experience will be adversely impacted. To accurately isolate the root-cause of slow/failed logons, administrators should track the availability of the ICA file and its download duration. In v7.2, the eG Citrix Logon Simulator, provides additional insights into the logon process by reporting the availability of the ICA file and the time duration taken to download the file. The administrator is alerted if the ICA file is unavailable during the simulation or takes too long to be downloaded. These metrics help administrators easily identify whether/not Citrix StoreFront is the root cause of application / desktop launch failure. The ICA file download

duration is also represented in the graphical view of the simulation.

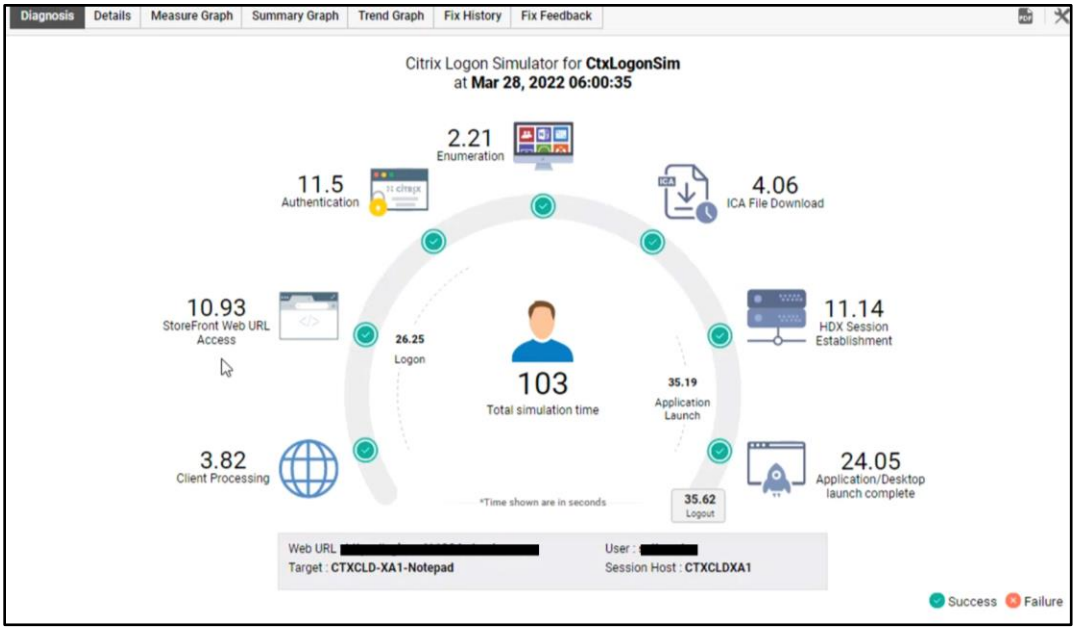


Figure 1: Tracking the ICA File download duration

- **Support for Dynamic 2FA (MFA) using TOTP Authentication Mechanism:** Two-factor authentication (2FA), often referred to as two-step verification, is a security process in which the user provides two authentication factors to verify who they say they are. In previous versions, only static 2FA was supported for Citrix Logon simulations. In v7.2 however, the simulator uses the Time-based-One-Time-Password (TOTP) authentication mechanism to lend support to two-factor authentication enabled users who log into the Citrix environment via any of the following as well:
  - Citrix Gateway
  - Citrix Workspace
  - Citrix integrated with Microsoft Azure Active Directory using OATH Soft token

  When the Citrix logon simulation endpoint is registered as a TOTP device on any of the above, a secret key will be generated. This secret key should be provided as an input in the **TOTP Code** text box that appears when the **Is 2FA enabled?** flag is set to **Yes** in the test configuration page. Once the simulation endpoint is registered as a TOTP device, during every simulation, the logon simulator will automatically generate the TOTP code based on the specified secret key for the user whose logon is simulated.

- **Capturing Additional HDX Channel Details in Citrix Logon Simulator:** Where simulations were performed through HDX virtual channels, in previous versions, the eG agent used Citrix APIs to collect and report metrics revealing the HDX experience. Starting with this version, this capability has been improved to report additional metrics that report the count of error-prone frames that were sent from/received by the Citrix logon simulator while launching the application/desktop. The client latency for the last request from the user is also reported.

- **Maintaining User Sessions in Active state on Simulation Endpoints:** By default, the simulator requires a user account with local administrator rights on the simulation endpoint - i.e., on the system hosting the Logon Simulator Agent / Citrix Workspace. This user should be logged in at all times for the simulator to run continuously. Sometimes, if the logon simulation endpoint is idle for a prolonged period, the screen of the endpoint may be locked, or a screensaver may appear. In this case, the logon simulation will not work and will eventually fail due to the user session being in an inactive

state. To avoid such failures, it is essential to ensure that the user session on the logon simulation endpoint remains 'Active' at all times. To this effect, starting with v7.2, an **Enable Session Active** flag is introduced in the test configuration page of the Citrix Logon Simulator test. By default, this flag is set to **Yes** indicating that the user session will always be 'Active' on the logon simulation endpoint.

- **Support for Citrix Cloud Integrated with On-Premises ADC:** Starting with this version Citrix logon simulator supports Citrix Cloud Configurations where on-premises Citrix ADC is used as an Identity Provider.
- **Capability to Set Additional Session Idle Time During Simulation:** By default, you can configure a launch timeout i.e., the maximum time the simulation should wait at any step for the application / desktop launch using the **LAUNCH TIMEOUT** parameter in the test configuration page. By default, this parameter is set to 90 seconds. Changing this launch timeout value will change the timeouts at all stages of the simulation. Therefore, administrators may not wish to change this default time; but they may still want to set some idle time as a buffer after the Citrix session is established. To aid the request of such administrators, starting from this version, you can add an additional idle time by editing the *SessionIdleTimeInSecs* key in the **ICALogonSimulator.exe.config** file available in the **<eG_Agent_Install_Dir>\egurkha\lib** folder. You can specify the idle time of your choice in seconds against this parameter and save the file.

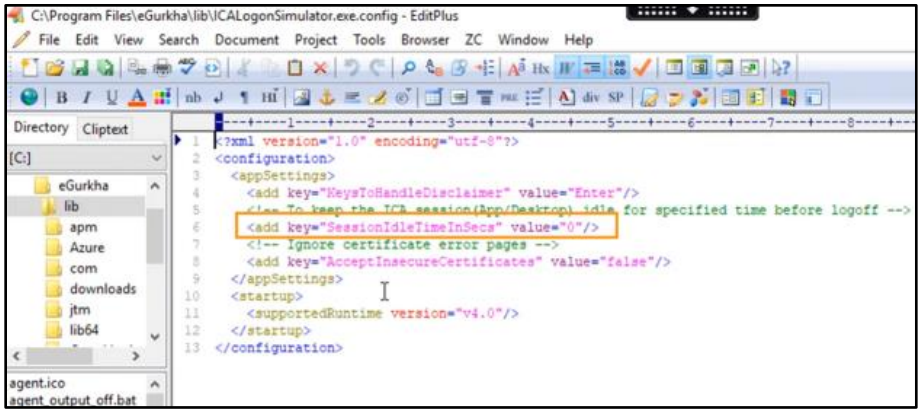


Figure 2: Setting Additional Session Idle Time

2.1.2 Citrix Cloud Monitoring Enhancements

- **Ability to Use New ODATA Cloud APIs for Monitoring Citrix Cloud Control Plane:** Starting with this version, the eG agent supports the latest version of OData Cloud APIs for Citrix Cloud Control Plane monitoring. These APIs use region-specific endpoints namely US, EU and AP-S. If the users and resources are in a region close to for e.g., EU, then, eG Enterprise allows the administrators to pick the region-specific endpoint as EU while configuring the test for the Citrix Cloud Control Plane component. To this effect, a **Region Endpoint** drop-down list has been introduced as a parameter in the **TEST CONFIGURATION** page for all the tests associated with the Citrix Cloud Control Plane component. This way, metrics are collected at a faster pace by the eG agents without time delays.
- **Changes to Agentless Monitoring of Citrix Cloud Control Plane:** In previous versions, in order to monitor the Citrix Cloud, administrators were required to deploy the eG remote agent on the Citrix Cloud Connector host. In environments where Citrix Cloud Connector was not deployed/monitored, administrators could not monitor the Citrix Cloud. To help administrators monitor the Citrix Cloud effortlessly, starting with this version, administrators are no longer required to deploy the remote agent on the Citrix Cloud Connector host and are allowed to deploy any VM/system with outbound internet connection as an eG remote agent. While doing so, administrators are also required to

download and install the Citrix DaaS SDK and install it on the eG remote agent host. The eG remote agent uses this SDK to pull metrics on virtual desktop sessions and logins from the Citrix Cloud. This approach to monitoring Citrix Cloud has the following advantages:

- There is no additional load on the Citrix Cloud Connectors;
- This monitoring approach works irrespective of the operating system of the Cloud Connectors. In previous versions, the Cloud Connector used for Citrix Cloud monitoring had to be installed on a Windows operating system whereas, starting with this version, the Cloud Connectors can be installed on a Linux operating system too for Citrix Cloud monitoring;
- This monitoring approach also works on Citrix Cloud deployments where Cloud Connectors are not used;
- The remote agent can be installed on a Windows cluster providing HA capabilities which were not available in the previous mode of deployment.

- **Ability to Gauge the Performance of Citrix Cloud Connector while the Monitoring Citrix Cloud Control Plane:** The Citrix Cloud Connector serves as a channel for communication between Citrix Cloud and the resource locations, enabling cloud management without requiring any complex networking or infrastructure configuration. If a Citrix Cloud Connector is slow, user experience will be affected. eG Enterprise v7.2 provides deep-dive insights into the performance of the Citrix Cloud Connector from the Cloud control panel itself i.e., without needing to install an eG agent on each Citrix Cloud Connector. The metrics are directly collected while the Citrix Cloud Control Plane is monitored. eG Enterprise v7.2 tracks and reports the overall status of each Citrix Cloud Connector, notifies if maintenance mode is enabled and helps administrators determine if connector upgrade is disabled by the admin. The CPU, memory and disk resources of each Citrix Cloud Connector is monitored and the Citrix Cloud Connector that is running short of resources are identified from the control plane itself. The data transfer rate through the network interfaces of each Citrix Cloud Connector helps administrators identify the Citrix Cloud Connector that is handling maximum data traffic.
- **Monitoring the Citrix Cloud Gateway Connector:** Citrix Gateway Connector serves as a channel of communication between Cloud services (Secure Workspace Access service, ADM, and so on) and on-premises components such as Web servers. The Citrix Gateway Connector facilitates remote access to enterprise web applications. To maintain data integrity and secure communication between Cloud services and on-premises components, it is imperative to ensure the uninterrupted functioning of the Citrix Cloud Gateway Connector. eG Enterprise v7.2 offers a specialized monitoring model that continuously monitors operations performed by the Citrix Cloud Gateway Connector and helps administrators ensure the high availability and peak performance of the Citrix Gateway Connector. Using this model, administrators can instantly find out whether/not the Gateway Connector is registered with Citrix Cloud services. Network traffic flowing through the Application Firewall is continuously tracked and the count of requests that were aborted/redirected by the Application Firewall is duly reported. Administrators can also accurately assess the effectiveness of the compression feature and keep a close watch on all factors influencing compression. The CPU, memory, and disk utilization on the Gateway Connector is tracked, and abnormal usage patterns are highlighted. The current status of the Gateway Connector in the high-availability setup is reported, and alerts are sent out if that state changes. HTTP connections handled by the Gateway Connector and the amount of data transacted over the connections is revealed. The integrated cache utilization of the connector is closely monitored, and abnormal cache utilization patterns are captured. SSL session load is continuously tracked, so that a potential overload condition is proactively detected. The throughput and uptime of the Gateway Connector is periodically monitored and abnormalities if any, are brought to light.
- Starting with this version, Citrix Cloud Connector hosted on a Linux appliance can also be monitored

using an exclusive **Citrix Cloud Connector – Linux** monitoring model.

2.1.3 Enhancements to Citrix Virtual Apps / Virtual Desktops Monitoring

- **Monitoring Microsoft Teams Status on Citrix Virtual Apps and Desktops:** In recent times, Microsoft Teams has become one of the most sought-after client applications to be accessed via Citrix. For Citrix users to seamlessly participate in audio-video or audio-only calls to and from other Microsoft Teams users, the Citrix HDX Optimization pack is recommended. This pack when installed offers a rich user experience and a clear media communication that goes point to point between clients and the Teams conferencing service. This pack when installed consumes less HDX bandwidth too. To improve the user experience of the Citrix users who are using Microsoft Teams, it is necessary to ensure that the Citrix HDX Optimization pack is enabled for those users. eG Enterprise v7.2 reports whether/not the Citrix HDX Optimization pack has been installed on the Citrix Virtual Apps or desktops. Administrators are also provided insights into the version of Microsoft Teams installed on the Citrix Virtual Apps server. This way, Citrix administrators can get proactive indicators and can take action to enable the optimization pack, thereby improving the user experience.

- **Monitoring Connection Latencies between Citrix Tiers:** In a Citrix environment, communication bottlenecks are one of the common reasons for poor connectivity, processing slowness, and data loss. Latencies between Citrix tiers can delay delivery of applications to users, thus adversely impacting user experience. To improve the quality of the Citrix service and the user experience with it, administrators should keep a constant vigil on the latencies between the key Citrix components – e.g., VDA, Active Directory, Citrix License server etc. that are engaged in service delivery. eG Enterprise v7.2 helps administrators in this regard. By integrating with Windows Resource Monitor, eG Enterprise tracks the latency between different Citrix tiers such as VDA and Active Directory, VDA and Citrix Control Plane, Citrix Delivery Controller and Citrix License server etc.

- **Monitoring White-listed Applications:** In some highly secure virtual environments, administrators whitelist an index of business-critical and most commonly used applications that are permitted to be present and active on the target server. The goal of whitelisting is to protect the target server from potentially harmful applications and prevent any unauthorized files from executing. Application whitelisting places control over which applications are permitted to run on the target server and is controlled by the administrators, rather than the end-user. In such environments, administrators may wish to monitor only the applications that are whitelisted on the target server. To this effect, a **SHOW ONLY WHITELIST APPS** flag has been introduced in the test configuration page of the **Citrix Applications** test. By default, eG Enterprise offers a comma-separated list of whitelisted applications (in terms of monitoring) specified against the **WhiteListProcesses** option in the **[EXCLUDE_APPLICATIONS]** section of the **eg_tests.ini** file available in the **<eG_INSTALL_DIR>/manager/config** folder. Administrators are also allowed to append this list with the applications of their choice for monitoring. This capability is also supported for applications launched in Citrix VDI, Microsoft RDS, VMware Horizon RDS and Microsoft AVD environments.

- **Identifying Users Consuming Excessive Bandwidth for Clipboard Operations:** The clipboard is a set of functions and messages that enable applications to transfer data. Because all applications have access to the clipboard, data can be easily transferred between applications or within an application. The clipboard is user-driven. A window should transfer data to or from the clipboard only in response to a command from the user. In a Citrix Virtual Apps session / Citrix VDI environment, if the bandwidth is excessively used for clipboard operations (such as cut and paste) initiated by a user, then, he/she may not be able to perform other operations on the target server/virtual desktop. As a result, user experience may suffer. To avoid this, eG Enterprise v7.2 periodically measures the bandwidth used when performing clipboard operations from and to a user's

endpoint. By closely observing the metrics reported for each user, administrators can figure out the user who has been performing bandwidth-intensive clipboard operations.

- **Improvements to User Experience Dashboard:** The 'look and feel' of the **USER EXPERIENCE OVERVIEW** dashboard has been enhanced in eG Enterprise v7.2. Additional tiles have been introduced in this dashboard, using which, administrators can instantly determine the count of users logged in, and the number and severity of alerts associated with the users. The tiles also reveal:
  - Is any user accessing VMs/desktops over a poor-quality connection?
  - Are users seeing any slowness when launching applications?
  - Is the overall HDX user experience above-par?
  - Are users experiencing slowness when communicating over the network?

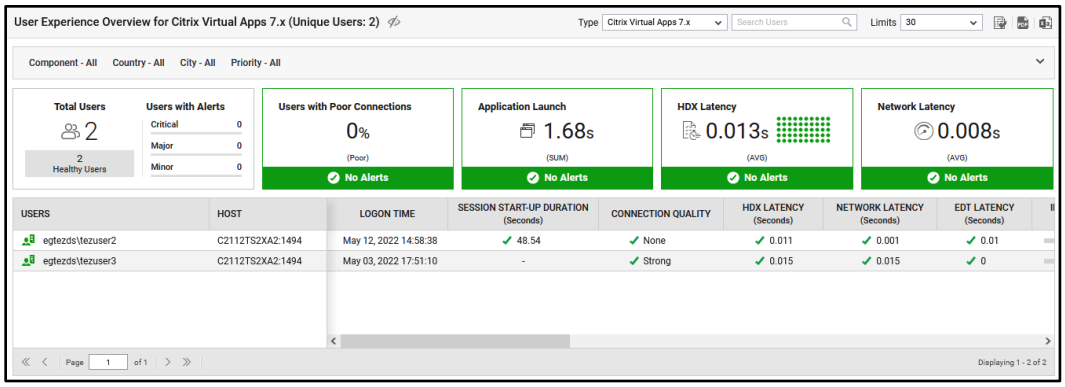


Figure 3: The User Experience Overview dashboard

Earlier, from the Session Topology of a user in the User Experience Dashboard, administrators were unable to glean why the connection quality between that user's terminal and the target VMs/virtual desktops was poor – is it owing to the bandwidth? or is it due to network latency? or is it due to the ICA RTT? To help administrators identify the accurate cause of poor connection quality, starting with this version, a detailed connection quality report is included in the dashboard. This report appears as a **CONNECTION QUALITY DETAILS** window, which pops up when drilling down the Connection strength in the Session Topology.

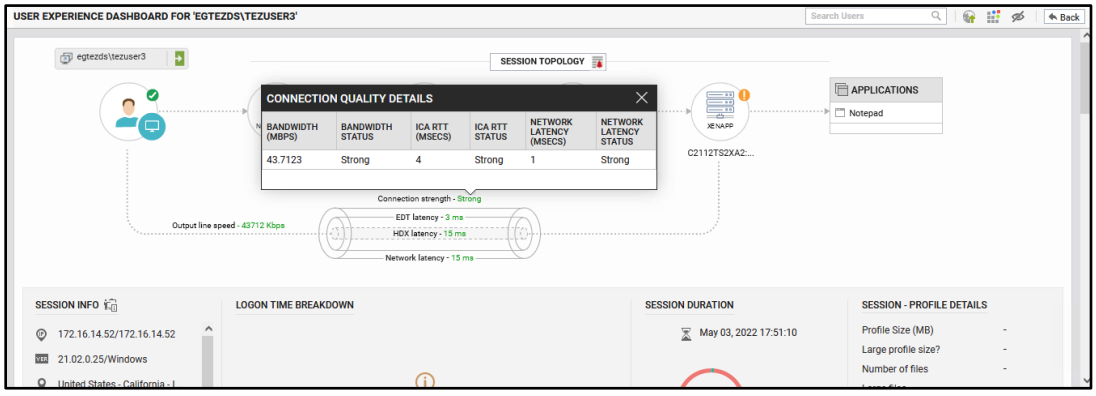


Figure 4: The Connection Quality Details pop up window

Also, starting with this version, administrators can drill down to the alerts associated with a user from the Session Topology. Clicking the icon next to the **SESSION TOPOLOGY** will lead you to the **CURRENT ALARMS** page that displays all the alerts raised for the components associated with the

chosen user. By default, this icon will blink with the priority of the highest state of alert raised for the component.

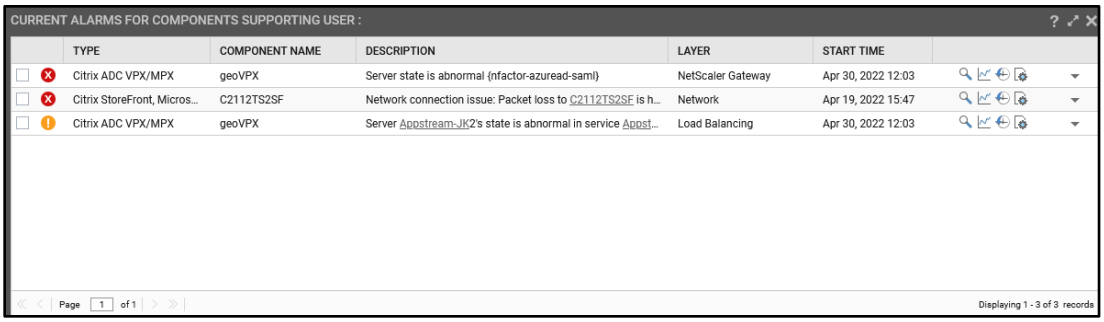


Figure 5: The CURRENT ALARMS page

- **Track Applications used in the Citrix Environment from a Single User Interface:** To receive quick insights into the performance of applications running in a Citrix Virtual Apps/Desktops farm, administrators can use the **Applications** dashboard offered by eG Enterprise v7.2. The unique applications executing in the Citrix environment are reported in a single pane of glass. The hosts on which the applications are executing and the users using those applications too can be tracked with ease. The resource utilization of each application too can be promptly tracked and reported. This way, resource-intensive applications can be identified at a single glance. This dashboard can also be used to track the unique applications that are executing in Terminal server environments, Microsoft Azure Virtual Desktops, VMWare Horizon RDS environments etc.

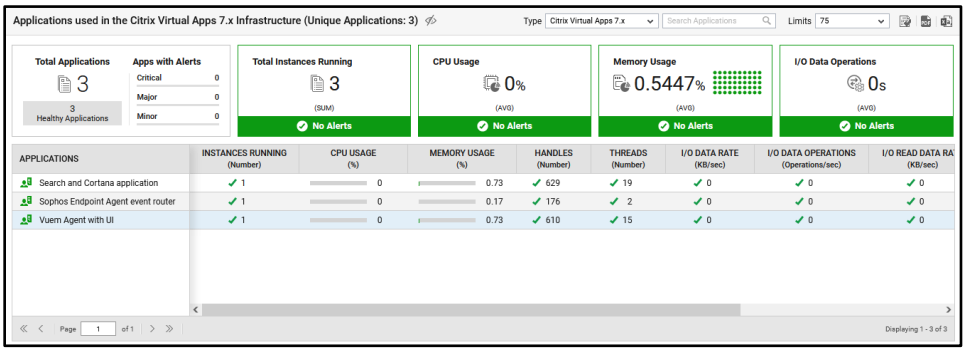


Figure 6: The Citrix Applications Dashboard

- **Improvements to Virtual Apps Dashboard:** In previous versions, administrators could not obtain an end-to-end visibility of their environment from the Virtual Apps Dashboard since they were unable to view the performance of the Citrix brokers and the statistics relevant to individual delivery groups. To fill this void, starting with this version, the Virtual Apps Dashboard includes additional **Brokering** and **Delivery Groups** pages. The **Brokering** page reveals the total number of sessions brokered to the Citrix Virtual Apps server, the number of logons to the desktops/VMs, the count of delivery groups, and the delivery group that is over-utilized. This page helps administrators identify if users used the desktops or servers to initiate the sessions, login to the Citrix infrastructure. The **Delivery Groups** page helps administrators identify those delivery groups that are utilized to the maximum, the delivery groups that are experiencing frequent connection failures/machine failures, delivery

groups through which maximum session were established etc.

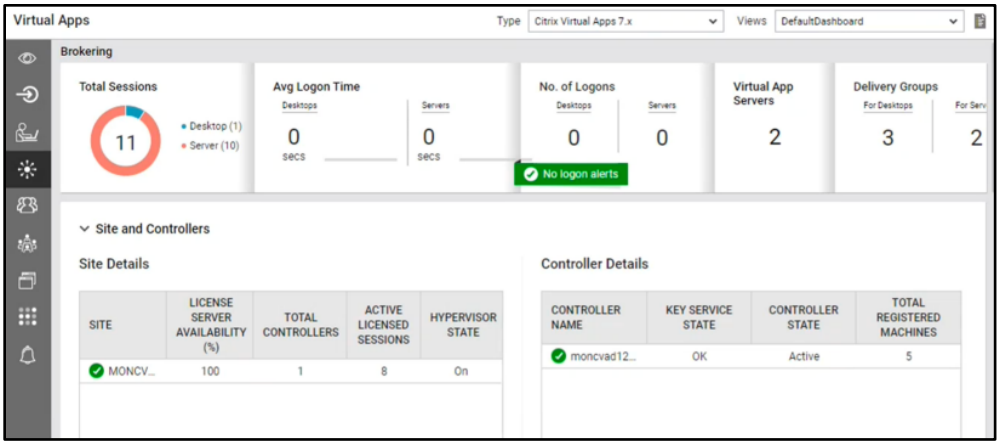


Figure 7: The Brokering page of the Virtual Apps Dashboard

2.1.4 Enhancements to Citrix ADC VPX/MPX Monitoring

- **External Check of Citrix ADC VPX/MPX:** In Citrix environments, if the Citrix ADC is unavailable or takes too long to respond, then, users may not be able to swiftly access their virtual applications/desktops. To assure users of on-demand access to their virtual resources at all times, administrators should track the availability and responsiveness of the Citrix ADC, promptly capture the non-availability or poor responsiveness of the appliance, and resolve the issues before users notice. Using eG Enterprise v7.2, administrators can externally run an API check on the Citrix ADC at regular intervals, and be instantly alerted if the ADC is unavailable or is responding slowly to requests.
- **Monitoring Citrix ADC Events:** When a problem event occurs on the Citrix ADC VPX/MPX appliance, administrators should determine what triggered that event, so that such anomalies can be prevented from re-occurring. By tracking events on Citrix ADCs, administrators can be proactively alerted to potential abnormalities. eG Enterprise v7.2 performs agentless monitoring of Citrix ADCs using ADC NITRO APIs and reports the events recorded in the system log of the Citrix ADCs. The detailed diagnostics further reveals the reason behind the triggered events using which administrators can proactively avert potential issues.
- **LDAP Server Configuration for Citrix ADC VPX/MPX Appliance can now be Indicated:** By default, to authenticate users, Citrix ADC VPX/MPX appliance can be configured with one/more LDAP servers. eG Enterprise v7.2 offers a brand-new LDAP Authentication test that indicates which LDAP servers are configured for authentication and if authentication is enabled or not through Citrix ADC VPX/MPX. This way, the LDAP servers that are disabled for authentication can be identified.
- **Identifying System Sessions/Connections established by Users on Citrix ADC VPX/MPX Appliance:** In Citrix environments, there may be multiple users authorized to access the console of the Citrix ADC VPX/MPX appliance. These users may initiate sessions using Putty/API/browser (GUI) at the same time to access the console for various purposes such as to monitor the appliance or troubleshoot/manage the appliance. If multiple sessions/connections are established by the users to access the console, sometimes, the connection limit may be reached, and system users will not be allowed to access the console. This may lead to a connection overhead on the appliance. Connection leaks may also be noticed which may degrade the performance of the target appliance. eG Enterprise v7.2 offers to track such abnormalities by reporting the connections/sessions established by the users accessing the console of the target appliance. Further, the detailed diagnostics reveals the Session ID, the login time of the system users and the client type through which they established the

sessions. This way, the users who have been established connections/sessions to access the console for a longer duration can be identified.

- **Monitoring Synchronization between NTP Servers and Citrix ADC appliances:** Sometimes, users belonging to an Active Directory group could not log into the Citrix ADC appliance using Native OTP functionality. This issue was mainly noticed when there was a time difference between the user's endpoint and the Citrix ADC appliance. This can happen if the Citrix ADC appliance is unable to synchronize its time with the NTP servers associated with it. To enable users to login to ADC without a glitch, it is important that administrators determine whether the target appliance's clock synchronizes with that of the NTP servers associated with it, and if not, sync them up. eG Enterprise v7.2 periodically monitors the time synchronization between the Citrix ADC and the NTP servers associated with it. Alerts are sent out if the Citrix ADC server is not synchronized with the NTP servers. Also, administrators can identify the NTP server on which maximum time delay and jitter was noticed.

- **Enhancements to NetScaler Request Flow Dashboard:** In previous versions, the NetScaler Request Flow Dashboard provided an aggregated view of the health of all the traffic flows within the NetScaler ecosystem. However, administrators of some environments may prefer to zoom into specific flow records instead. To address this requirement, the NetScaler Request Flow Dashboard in v7.2 displays a **NetScaler Load Balancing Flow** list. To view the flow path of a specific NetScaler Load Balancing flow, administrators can select that path alone from this list. This enables administrators to analyze a single flow at a time, and rapidly isolate where and why the flow was bottlenecked.

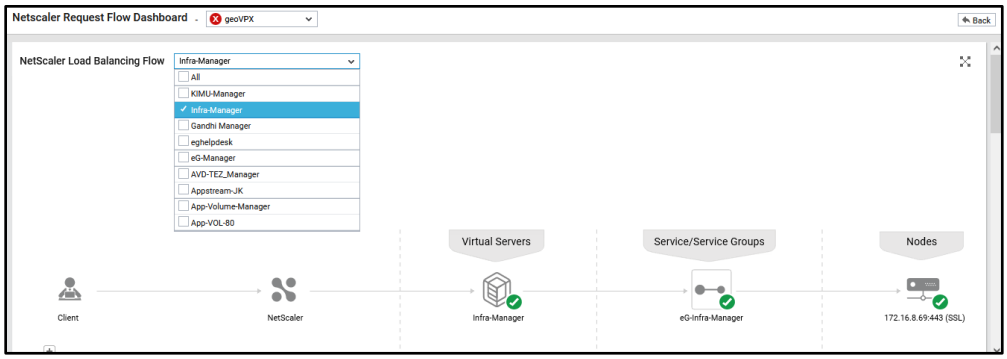


Figure 8: Viewing a single Load balancing traffic flow

Also, you can now quickly spot AAA authentication-related issues on Citrix ADC using the dashboard. The new AAA Statistics section of the dashboard draws administrator attention to authentication failures, authorization failures, and frequent AAA session timeouts, thereby urging them to take

immediate action.

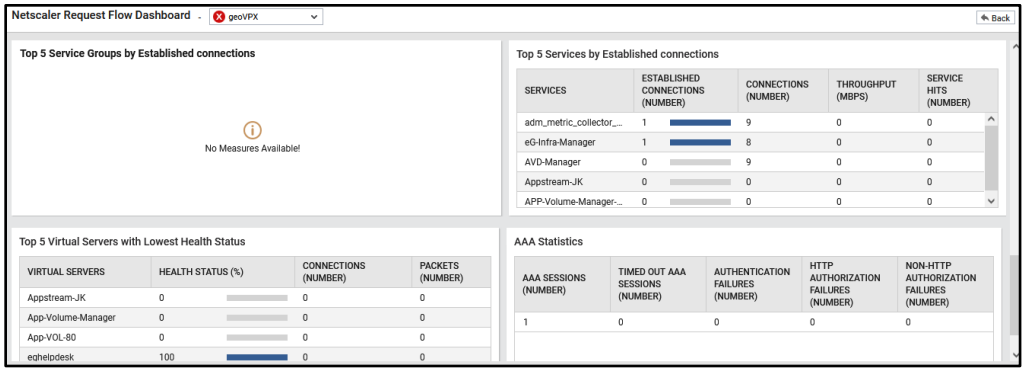


Figure 9: Viewing the AAA statistics

Starting with this version, the NetScaler Request Flow Dashboard can be accessed from the layer model page of the Citrix ADC VPX /MPX components by clicking the icon. You can even set the NetScaler Request Flow Dashboard as the eG Monitor Home page, if you so want.

Furthermore, using the flow dashboard of v7.2, you can now quickly and easily determine whether/not the Citrix ADC being monitored is the primary node in a High Availability setup. If it is, then you will find the icon displayed in the title bar of the dashboard.

2.1.5 Automatic Problem Resolution

Version 7.2 of eG Enterprise embeds rich automatic problem correction capabilities. Without the need for writing complex rules or scripts, the eG agent can now automatically resolve common problems it detects, well before users even notice the issue. This saves troubleshooting time, reduces support costs, improves user productivity, and ensures the high uptime of business-critical servers/services.

Administrators are allowed the flexibility to choose which issues they want to auto-correct, and which ones they do not. Also, administrators can control how and when the automatic resolution is to be triggered.

Currently, this capability can automatically resolve the following issues:

- High disk space usage
- Abnormal memory usage issues
- Excessive resource utilization due to Sessions in Idle/Disconnected state on a Citrix server/desktop

The below sections describe on how this capability helps automatically resolve the above-mentioned issues:

- **Automatically Resolving High Disk Space Usage Issues:** If a server does not have enough free disk space, the performance of that server and the applications executing on it will degrade significantly. Abnormal disk space usage can often be attributed to the accumulation of a large number of temporary files. While system created temporary files will be automatically deleted/purged, a few other files – say, the temp files created when a Windows OS update fails – may not be so deleted. To ensure that such files do not hog the disk space and choke critical applications running on the server, administrators can configure eG Enterprise v7.2 to automatically remove these files from disk. This way, the eG agent ensures that your business-critical applications never run out of disk space.

  To enable remedy automation, you need to set the **Automated Action Enabled** flag in the test configuration page of the Disk Space test to **Yes.** Then, using the **CONFIGURATION OF AUTOMATIC CLEANUP RULES** pop up window, you need to configure when the auto-cleanup action is to be triggered by the test.

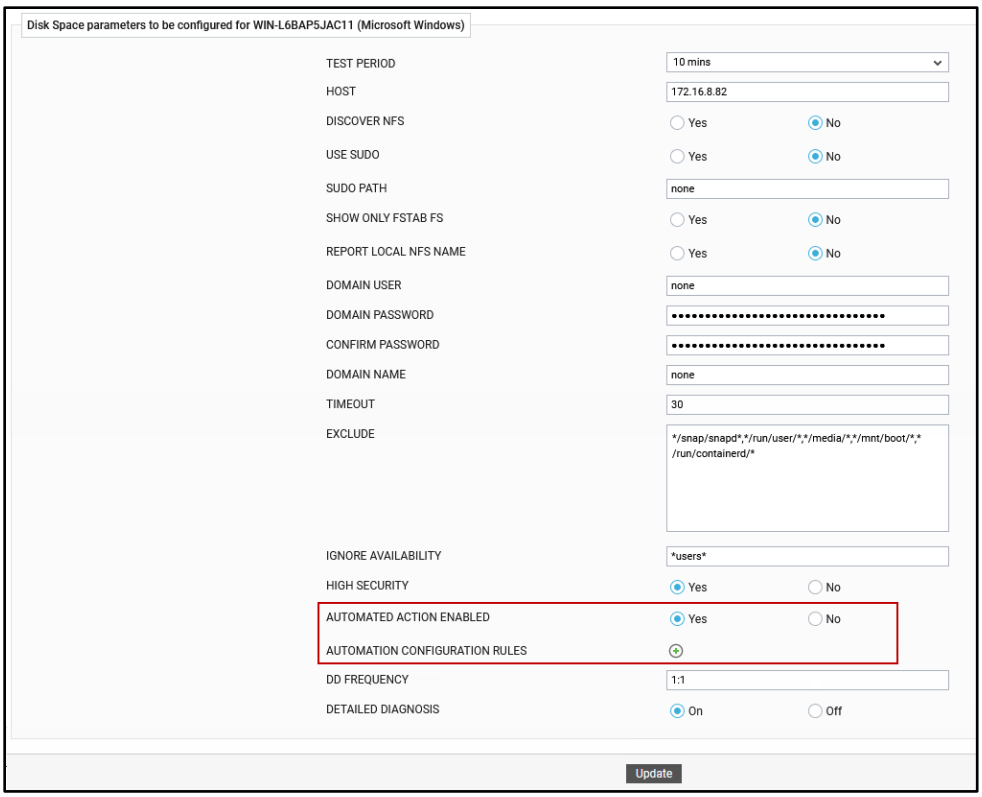


Figure 10: Enabling Automatic Actions on Disk Space

The Disk Space test now reports an additional *Cleanup automation status* measure, which indicates whether the cleanup action succeeded/failed. In the event of a cleanup failure, you can use the detailed diagnostics of the measure to quickly identify the files that could not be automatically removed during the current and last cleanup. If the automatic purging is failing on the same set of files repeatedly, you may want to dig deep and figure out why.

This automated action can be configured on both Windows and Unix systems, VMs and Azure Virtual Desktops.

- **Automatically Resolving Abnormal Memory Usage Issues:** Modified memory is the memory that was allocated by some application and then removed from the application's working set, usually because it hasn't been used for a long time. Standby memory contains pages that have been removed from process working sets but are still linked to their respective working sets. The Standby list is essentially a cache. In some environments, the Windows operating system may frequently become unresponsive. One of the most common reasons for the operating system to become unresponsive is that the standby memory is not released by the operating system when memory is required. Also, the free memory is depleting rapidly. To optimize memory resources on a system/VM automatically, you can have the eG agent automatically cleanup standby memory and/or modified memory. For this, first enable **Automated Action** for the **Memory Usage** test of the target system / VM. Then, specify the memory usage limit beyond which the cleanup is to be triggered.

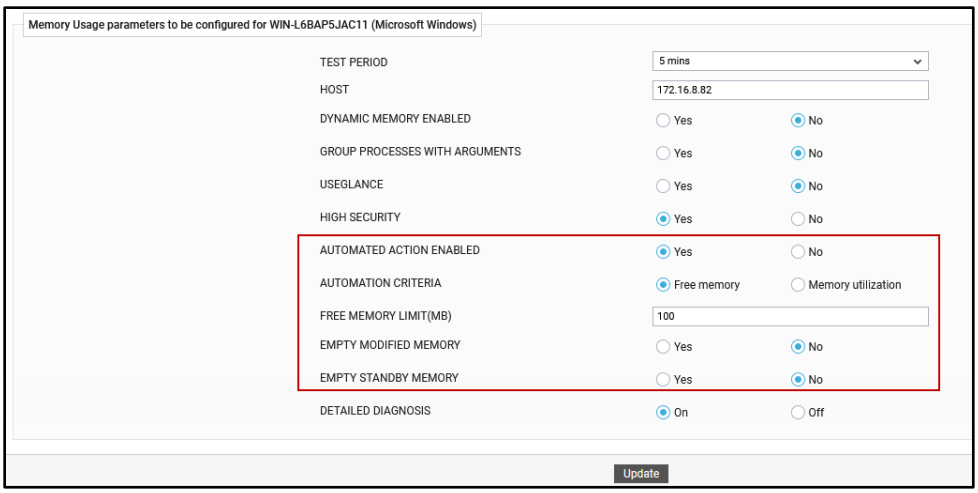


Figure 11: Enabling Automatic Actions to optimize Memory Usage

Where the automatic resolution is enabled, eG Enterprise also tracks and reports the success/failure of the automation. In the event of a failure, use detailed diagnostics to analyze the action taken for automatic cleanup. **Note that eG Enterprise performs automatic memory resource cleanup only on Windows systems/VMs.**

- **Automatic Actions on Citrix User Sessions:** In multi-user environments like Citrix Virtual Apps/Desktops, server resources are shared by all user sessions on that server. In such environments therefore, it is important to ensure that users engaged in business-critical operations have the resources they need. A resource shortage can not only impair user productivity but can also bring crucial business processes to a halt and can severely degrade overall user experience with the application delivery service. To avoid such an outcome, administrators need to rapidly identify and intelligently manage those types of user sessions that consume resources unnecessarily - i.e., user sessions that are 'unproductive resource consumers'. This way, administrators can make sure that adequate resources are always available for carrying out important business tasks.

  Idle sessions and disconnected sessions on a server are often considered to be a waste of valuable resources. If administrators are empowered to quickly identify these sessions and automatically eliminate them or limit their resource usage, they can:

  - Ensure that server resources are put to good business use;
  - Avoid resource contentions, and the resultant delay in delivery of business services;
  - Improve user productivity;
  - Assure users of an above-par experience with Citrix Virtual Apps

  To enable administrators to achieve all the above, eG Enterprise v7.2 offers Automatic Actions on Citrix user sessions. These actions are governed by the **AUTOMATED ACTION ENABLED** flag in the test configuration page of the Citrix User Sessions test. Once this flag is enabled, the eG agent automatically initiates user-configured actions on idle and disconnected sessions, so that they do not consume more resources than they should. Such an action can restrict the amount of resources used by these sessions, change the priority level of processes running in these sessions, and completely log off the sessions.

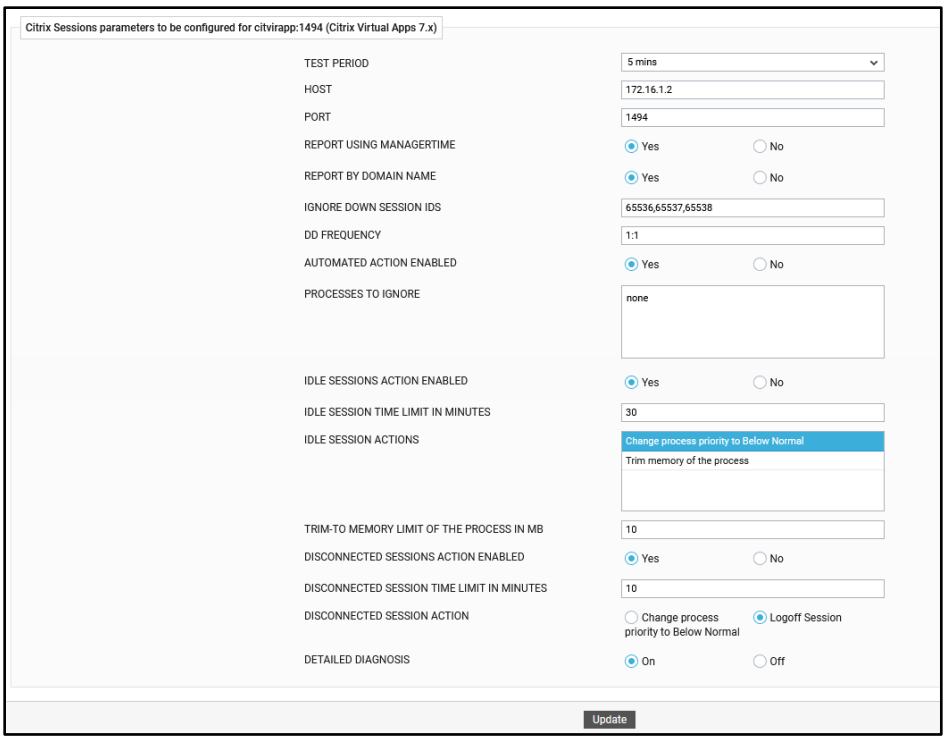


Figure 12: Enabling Automatic Actions on Citrix User Sessions

- **Enabling Automatic Actions on Citrix VDAs:** In a Citrix application delivery infrastructure, VDA enables the target machine to register with the Delivery Controller and establishes and manages the connection between the machine and the user device. The VDA communicates session information to the Broker Service in the Delivery Controller through the broker agent in the VDA. If the VDA is not registered with a valid Delivery Controller or is in the "Unregistered" state, then, communication between the target machine and user device will not be established. As a result, users will be unable to login to the target machine and access their business-critical applications. This in turn can seriously impact user's productivity and degrade the overall user experience with the application delivery service. To prevent such an outcome, administrators need to intelligently find out the registration status of VDAs on the target machine and take the remedial actions if the VDAs are in "Unregistered" state. To help administrators in this regard, eG Enterprise offers 'Automation Actions'. These actions are governed by the 'Automated Action Enabled' flag of the **Citrix Server Information** test. If this flag is enabled, then, the eG agent automatically initiates user-configured actions when the VDA is in the "Unregistered" state, so that the status of VDA is restored before it impairs application delivery to users. Such an action can restart the Citrix services running on the target machine, or completely restart the machine. The automatic corrective actions are governed by the **AUTOMATED ACTION ENABLED**, **AUTOMATED ACTION DURATION MINS**, **RESTART CITRIX SERVICES WHEN**

UNREGISTERED and **RESTART MACHINE WHEN UNREGISTERED** parameters.

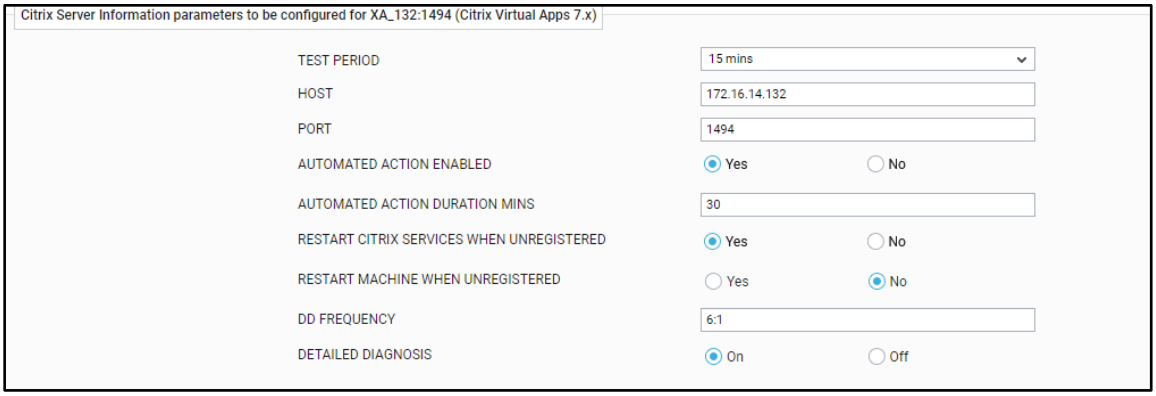


Figure 13: Enabling Automatic Actions on Citrix VDAs

2.1.6 Other Citrix Monitoring Enhancements

- **Monitoring Citrix App Layering Manager:** Citrix App Layering is a flexible solution that provides a complex set of Windows applications to a diverse set of users on any non-persistent supported platform. The primary goal of Citrix App Layering is to simplify Windows application management using a single interface. Citrix App Layering allows administrators to create and manage enterprise applications regardless of the underlying hypervisors or cloud infrastructure. eG Enterprise v7.2 offers complete monitoring support to Citrix App Layering Manager. Using the metrics collected, administrators can find out the responsiveness of the Citrix App Layering Manager and the current status of each App/OS/Platform Layer created by the App Layering Manager. The size of each App/OS/Platform Layer is duly reported along with the count of images/collections/desktops that are currently using each App Layer. Administrators can also determine the exact layered image that is not ready to be published and the size of each image on the virtual disk. The hit ratio of Packaging cache enabled on each connector and the number of times that the target appliance has not found disk in the Packaging cache of each connector are also duly reported.
- **Monitoring Machine Creation Services in VDI environments:** The Citrix Machine Creation Service, an alternative to Citrix Provisioning services, creates new virtual desktop images, and provisions virtual machines/desktops based on the desktop image. The Machine Creation Services (MCS) Storage Optimization (MCSIO) is a new feature within MCS provisioning. The MCSIO reduces the I/O load through a two-tier caching system. An in-memory cache, known as the "temporary memory cache", is used as the first storage tier. If the in-memory cache fills up, subsequent writes will be cached using an additional disk attached to the provisioned machine as the second tier - this is known as the "temporary disk cache". To achieve this, MCSIO provisioned machines have an additional MCSIO driver to intercept and manage I/O operations. eG Enterprise v7.2 monitors the I/O load on the MCSIO driver available on virtual machines / virtual desktops and helps administrators figure out how well the driver uses the in-memory and disk cache for managing the I/O operations in those VMs / virtual desktops. In the process, administrators can rapidly determine whether/not the caches are adequately sized to support the I/O operations. This way, administrators can be alerted to potential resource crunch in the caches and also identify the VM/virtual desktop that is impacted by this.

2.1.7 Citrix Reporting Enhancements

Following are the reports that are introduced in eG Enterprise v7.2 with respect to Citrix:

- **User Experience by Geo Report:** One of the key factors that influence user experience with a

Citrix/VDI environment is the geographic location of users. For instance, a highly latent network link from a specific geography can adversely impact the connectivity of all users who access VMs/desktops from that geography. To isolate such issues and diagnose their root-cause, administrators should historically analyze user experience based on geography. The **User Experience by Geo** report offered by the eG Enterprise v7.2 helps with this. A quick look at this report reveals whether/not the Citrix experience of users from the chosen geography was good during the designated time period. If not, the report also instantly leads you to the probable cause of the poor experience – is it because of abnormal line speed? High screen refresh latency? or high client network latency? The report also pinpoints the precise day, during the given period, on which latency was highest in the selected geography. If the report is generated for all geographies, then the top-10 graphs displayed in the report will lead you to the exact regions where line speed and latency were consistently deviant during the said time period.

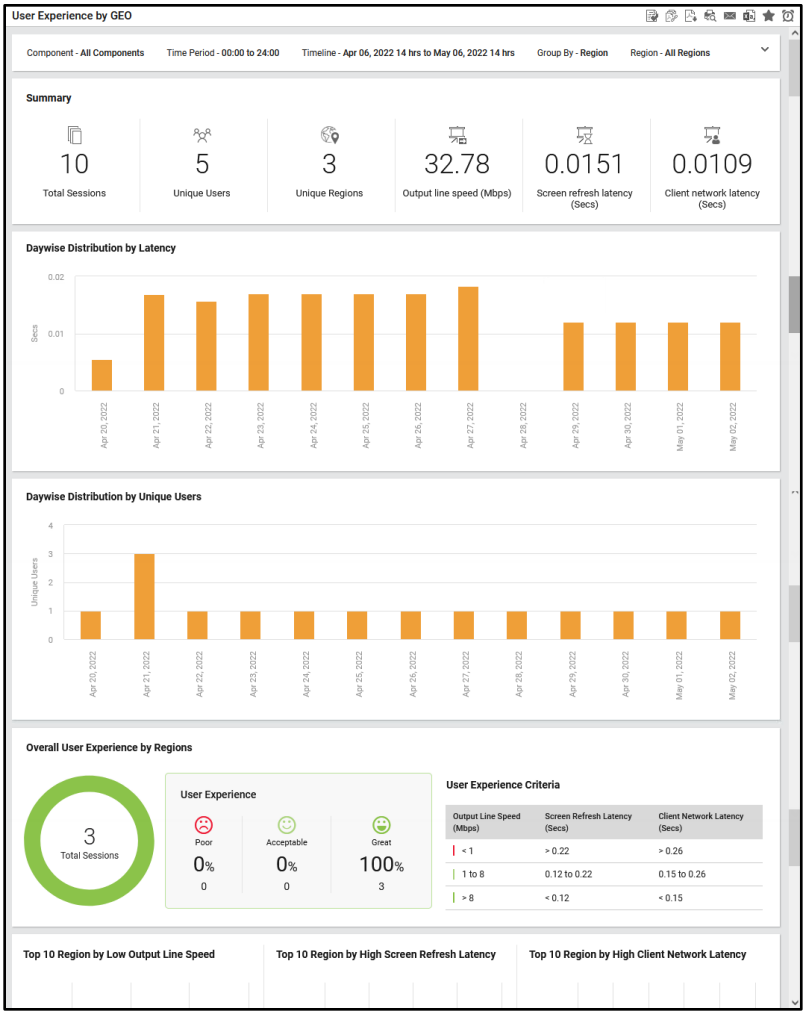


Figure 14: The User Experience by Geo Report

- **GPO Performance Report:** In Citrix environments, a delay in / failure of group policy processing can affect the logon experience of Citrix users. Under such circumstances, it is imperative that administrators identify the exact client-side extension that is running slowly or has failed, thus stalling / suspending group policy implementation. Sometimes, updates to group policies / client-side extensions may not be applied to all relevant servers/users. Besides exposing the Citrix environment to malicious attacks, this oversight can also significantly degrade user logon performance. To avoid this, administrators must track group policy processing over time, rapidly isolate processing delays /

failures, and identify the client side extensions that are causing them. The GPO Performance Report of v7.2 helps with this. Using this report, administrators can historically analyze GPO processing during user logons. With the help of this report you can quickly determine the following:

- Is any GPO failing frequently? If so, why? Is any CSE implementing that GPO, erroneous? Which CSE is this, what errors were impacting its performance, and when did these errors occur?
- Which GPO took too long to be processed?
- Which CSE has been consistently taking too long to execute?
- Is there any GPO / CSE that has not been applied to some servers/users? Which GPO/CSE is this?

This way, the report helps administrators identify GPOs and CSEs that need to be optimized, so that the logon experience of users can be enhanced.

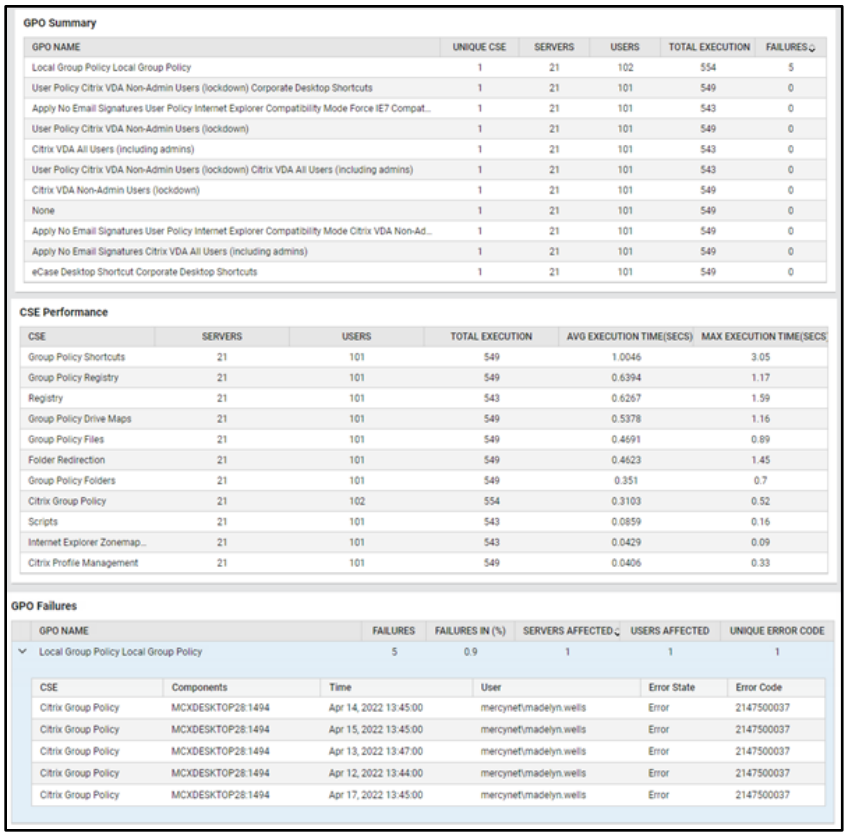


Figure 15: The GPO Performance Report

- **Browser Activity Report:** Active desktop users may not always be 'productive' users. In recent times, web browsing habits have emerged as a key-criteria for determining how productive an enterprise user is. For example, a user may appear to be active on his/her virtual desktop all through the day, but in reality, he/she may be busy accessing frivolous web sites, outside their line of work. If this abuse and its perpetrators are not rapidly detected and controlled, then user productivity will be affected. This is where, the Browser Activity Report offered by eG Enterprise v7.2 helps! By historically analyzing browser activity in a Citrix/VDI environment, this report quickly leads administrators to frequently visited web sites, the users accessing them, and the virtual desktops on which they were accessed. This way administrators can accurately identify the users who often access web sites that they are not supposed to, and the desktops on which such accesses frequently

occur. Administrators can then take appropriate action on the users with 'bad browsing habits'.

Figure 16: The Browser Activity Report

- **Reporting Session Activity by Delivery Groups:** In large VDI environments, it is common practice to group virtual desktops into multiple delivery groups – one for every department, geography, support group etc. – for easy management. In such environments, administrators may want to analyze session activity and logon experience by delivery group, so that they can figure out if any particular department / geography is consistently experiencing logon slowness or abnormal session loads. This is where, a **Delivery Groups** list box has been introduced (for Citrix Director 7.x and Citrix Virtual Apps / Desktop Site 7.x component types) in version 7.2 in the **Sessions by Users** report. By choosing a delivery group, administrators can easily obtain in-depth insights into the user sessions, unique users, and logon time duration for that delivery group.

- **Improvements to NetScaler – User Sessions Report:** Often, administrators generated the NetScaler – User Sessions Report to obtain a historical analysis of the users who have initiated Citrix sessions through Citrix ADC VPX/MPX. Though this report was useful in tracking the session load of the target environment, administrators of MSP environments wanted more granularity in terms of generating a report based on completed sessions/active sessions. This session-wise report generation would be of greater help to those administrators who wanted to bill the users based on the duration for which they were active on the Citrix environment. To offer the flexibility to generate this report based on completed sessions/active sessions, starting with this version, a **Show By** list has been introduced in the **More Option**s window. Choosing the **Completed Sessions** option from this list will ensure that all the sessions that were completed by the users in the Citrix environment will be considered for generating this report. Also, the Summary section of the generated report will now list the Active sessions in the target environment. The day-wise distribution of unique users based on the connection type used for connecting to the Citrix environment through Citrix ADC VPX/MPX helps administrators to explicitly figure out the day on which maximum number of users had initiated sessions. A **Summary** report when generated helps administrators identify the duration for which unique users have initiated sessions on the target Citrix environment through Citrix ADC VPX/MPX.

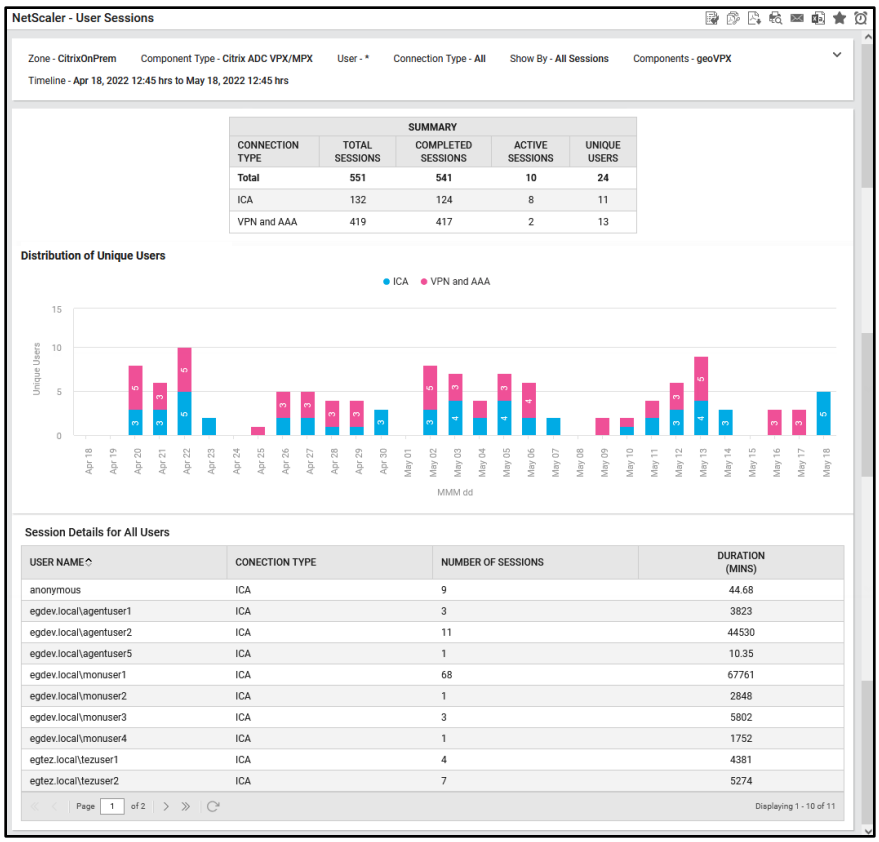


Figure 17: The NetScaler – User Sessions Summary Report

2.2 VMware Horizon Monitoring Enhancements

eG Enterprise v7.2 adds several enhancements for VMware Horizon monitoring:

- **Monitoring VMware Horizon Components Using VMware Restful APIs, instead of VMware PowerCLI:** In older versions, eG agents collected metrics from VMware Horizon Connection Servers and VMware Horizon Clusters/Pods using the VMware PowerCLI, an executable installed on the eG agent host. However, from VMware Horizon 7.10 onwards, VMware Horizon has deprecated the use of VMware PowerCLI and Horizon View API and has transitioned to use VMware Restful API. This was mainly introduced to facilitate the creation of complex applications that support multiple languages, which is difficult with VMware PowerCLI. To keep pace with this development, starting with this version, the eG agent is now capable of collecting metrics from the VMware Horizon Connection Servers and VMware Horizon Cluster/Pods using VMware Restful APIs. This way, metrics collection is simplified as there is no need to explicitly install VMware PowerCLI for data collection and monitoring.

- **Enhancements to VMware Horizon Cluster/Pod Monitoring:** eG Enterprise's VMware Horizon Cluster/Pod monitoring capabilities have been enhanced in v7.2 to provide in-depth insights into the usage of application/desktop pools managed by the pods. The users connecting through internal and remote gateway sessions are monitored for each application pool/desktop pool and the application pool/desktop pool that is currently experiencing a sudden influx of sessions is identified. The break-up of session count by client type is also available for each application pool/desktop pool, so that the popular client types can be identified. The metrics also lead you to the application pool/desktop pool where many sessions are idle; you may want to investigate the reasons for this inactivity, as idle sessions are resource drainers. The protocol that is frequently used to initiate sessions on the application/desktop pools is also pinpointed. Administrators are alerted if the desktop provisioning

status of any desktop pool is abnormal. Pod health KPIs such as connection server status, SSL certificate expiry, and LDAP backup status are continuously tracked and reported, so that anomalies can be promptly detected. The endpoint status of the remote pods is also monitored, and offline pods are isolated. The availability and usage of datastores is tracked, and in the process, inaccessible / over-utilized datastores are highlighted. The license utilization of the entire VMware Horizon Infrastructure can also be tracked from a single, central interface. This helps administrators proactively plan and implement license purchases and prevent infrastructure downtime due to a license shortage.

- **Virtual Apps dashboard can now be plotted for VMware Horizon RDS Servers:** In previous versions, the Virtual Apps Dashboard helped administrators receive an overview of the performance of the Citrix Virtual Apps Servers alone. In version 7.2 however, this dashboard support has been extended to VMware Horizon RDS servers as well.

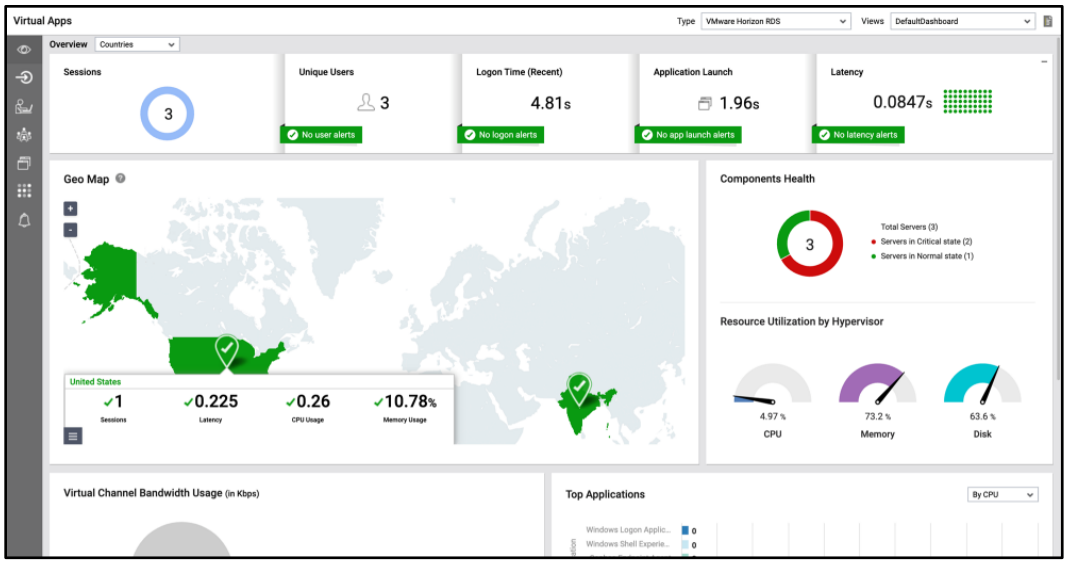


Figure 18: The Virtual Apps Dashboard for VMware Horizon RDS Servers

For further insights into the logon experience, user sessions, applications, resource usage and alerts, administrators can use the dashboards that appear upon clicking the icons available in the left pane of the Virtual Apps dashboard.

- **User Specific Session Topology for VMware Horizon RDS users:** To enable administrators to easily troubleshoot user experience issues of VMware Horizon RDS users, the **User Experience Dashboard** of v7.2 provides an end-to-end topology view of a single user's session. This topology representation reveals every component in the user's access path and the health of each component. A quick look at this topology will help administrators instantly figure out which Horizon Unified Access Gateway front-ended the user session, which connection server brokered the connection, on which VMware Horizon RDS server the user logged into, and the desktop from which desktop pool was eventually accessed. Using conventional color-codes, the dashboard also quickly and accurately pinpoints which component of the session topology is adversely impacting user experience with VMware Horizon RDS. Additionally, the dashboard also provides a breakdown of the logon time of the chosen user, so that administrators can easily figure out if the user's logon experience is sub-

par, and if so, what is contributing to it.

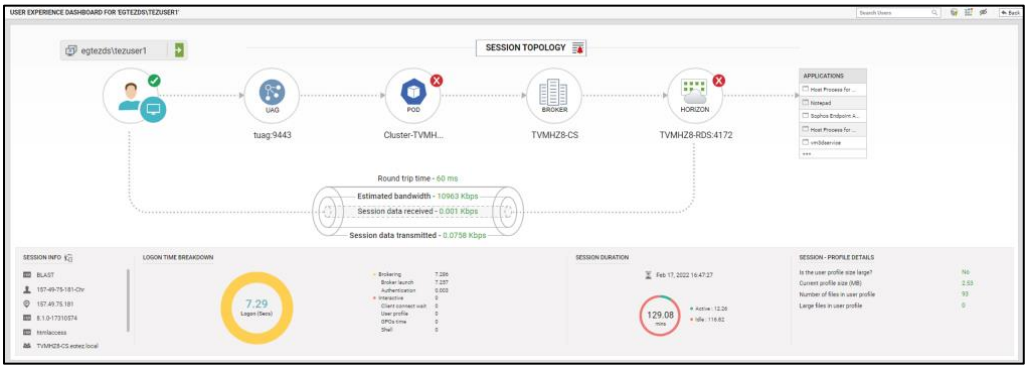


Figure 19: Viewing the Session Topology for users logged into VMware Horizon infrastructure

- **Tracking Configuration Changes on VMware Horizon Servers:** eG Enterprise v7.2 is capable of tracking configuration changes on VMware Horizon Clusters/Pods, VMware Horizon Connection servers, VMware Horizon RDS servers and VMware Horizon Unified Access Gateway component.

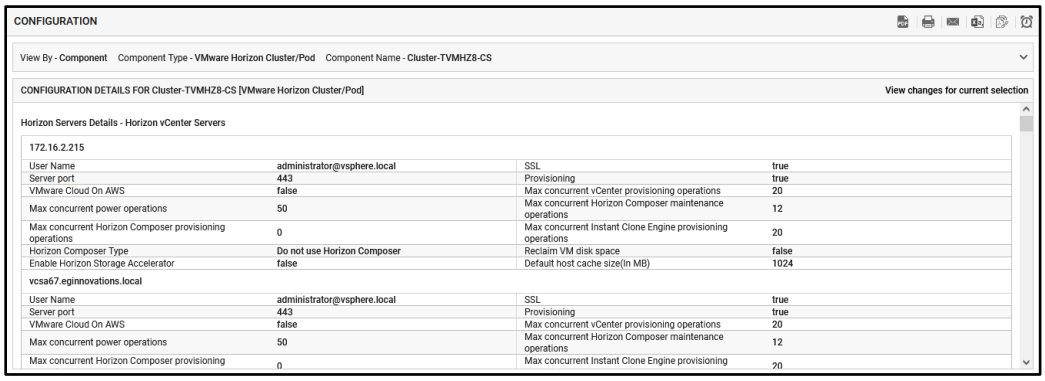


Figure 20: Viewing the Configuration of a VMware Horizon Cluster/Pod

2.2.1 VMware Horizon Reporting Enhancements

Reports offered by eG Enterprise v7.2 are more predictive as opposed to prescriptive. Foresight analysis is the key motivation that helped in building these new reports. Following are the reports that have been included for in-depth analysis in VMware Horizon environments:

- **VMware Horizon Overview Report:** eG Enterprise v7.2 now includes a VMware Horizon Overview report that provides an at-a-glance preview of the key performance indicators for the target infrastructure. From a single report, you can see a consolidated view of user experience trends, session-level metrics, application usage data, events, server resource utilization, and license usage levels. All the charts shown in this report link to other reports available in eG Enterprise, so that you

can drill down into individual reports for more granular data.

Figure 21: The VMware Horizon Overview Report

- **Horizon Events Report:** Use this report to historically analyze the problem events captured on VMware Horizon nodes, so that you can rapidly identify the type of events that frequently occur. The report also provides granular details about the events captured during the given period, thereby enabling you to uncover the exact problem, when it occurred, on which component, and which users were impacted besides shedding light on problem events that administrators may have missed. The report also reveals how problem-prone the VMware Horizon environment is, and the precise problems that are affecting its health.

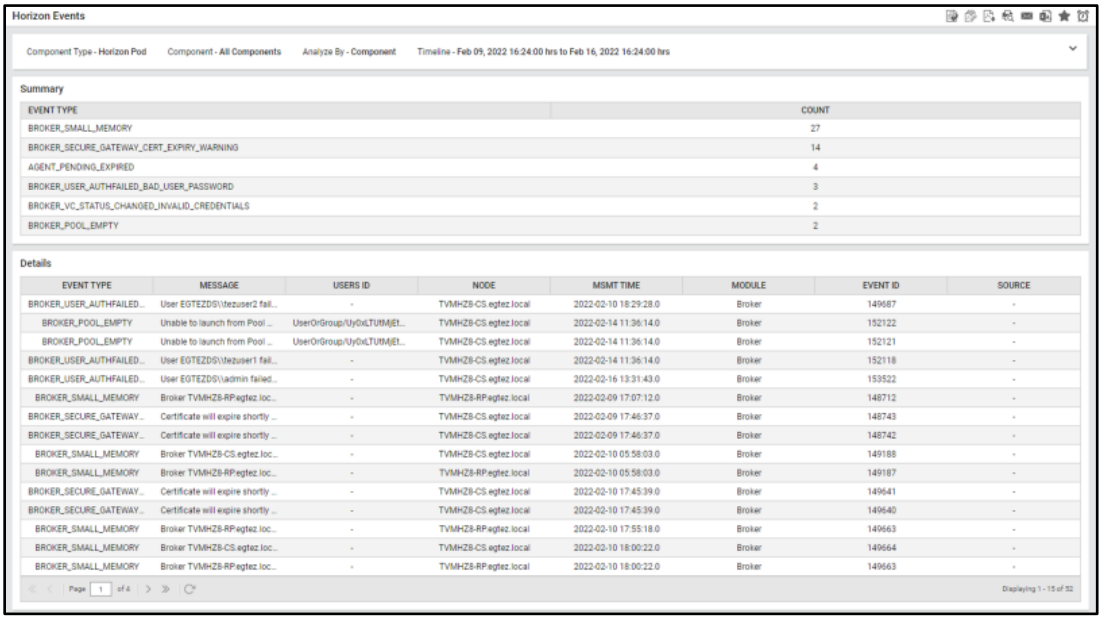


Figure 22: The Horizon Events Report

- **License Usage Report:** This report helps administrators track the license consumption by the target VMware Horizon environment, over time. The farm-level analytics provided by this report reveal whether concurrent and named user licenses have been utilized optimally during the given period, or whether there were any inexplicable and significant spikes in usage during that time. If usage has hit high notes, then administrators can use the component-level analytics to identify the precise VMware Horizon node that has been consistently over-utilizing licenses, and the type of licenses (concurrent / named user) that is consumed excessively. The pointers provided by this report will help administrators prudently plan future license requirements for the farm and for individual nodes in the farm.

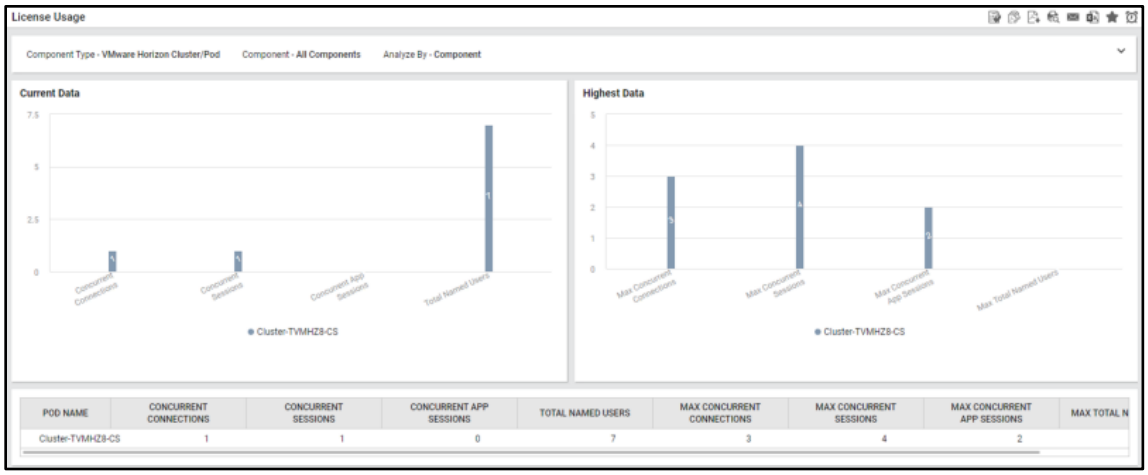


Figure 23: The License Usage Report

- **Client Versions in Use Report:** Whenever a user complains of slowness when accessing applications/desktops launched in a VMware Horizon infrastructure, administrators may want to instantly identify the type/version of the VMware Horizon Client used by the user to connect to the server/infrastructure. This knowledge will ease the troubleshooting pains of administrators as it will clearly indicate if the slowdown occurred owing to the usage of an unsupported or an outdated VMware Horizon Client. The **Client Versions in Use** report offered by eG Enterprise helps administrators figure out the VMware Horizon Client version/type used by each user. By historically analyzing the VMware Horizon clients that were in use, administrators can determine which user logged into the VMware Horizon infrastructure using which client, and in the process, figure out

client-related issues that are contributing to a user's unsatisfactory experience with VMware Horizon.

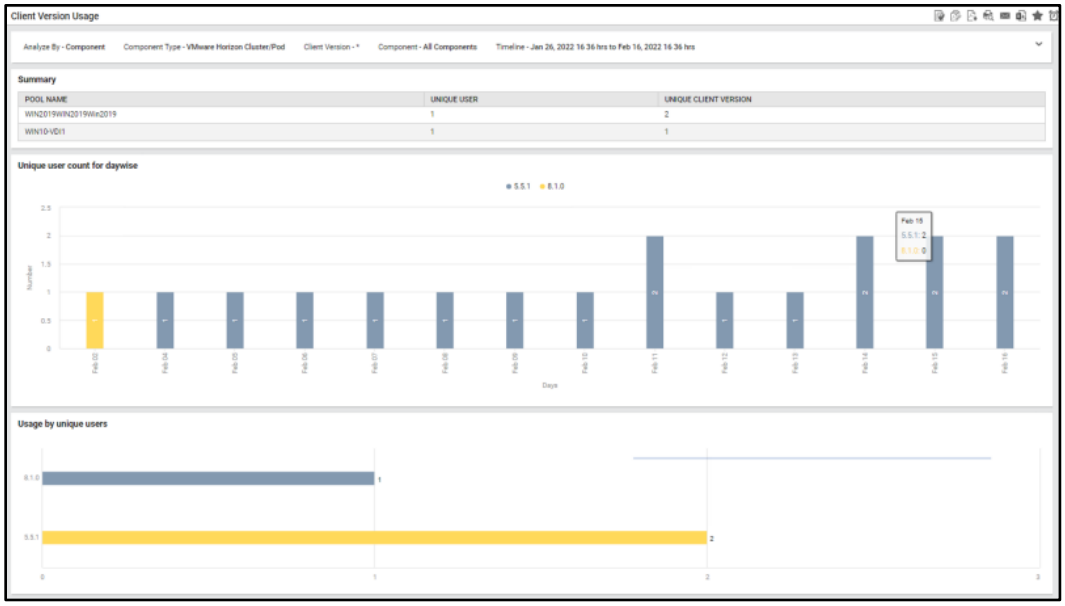


Figure 24: The Client Versions in Use Report

2.3 Microsoft Azure Virtual Desktops Monitoring

Microsoft Azure Virtual Desktop is a popular cloud-hosted virtual desktop service that organizations worldwide are adopting. AVD provides several features including multi-session Windows 10 experience, simplified management, optimizations for Office 365, support for Microsoft RDS and much more at a very affordable price.

eG Enterprise understands the natural need for dedicated cross-vendor, end-to-end management, and monitoring in AVD infrastructures. Therefore, unlike many EUC/Digital Workspace-only vendors, eG Enterprise serves as a whole-of-Enterprise provider of monitoring solutions, covering key components in the customer-managed and Microsoft-managed tiers of the AVD infrastructure; the list includes Microsoft Azure Cloud, AVD Connection Broker, AVD Host Pool, etc.

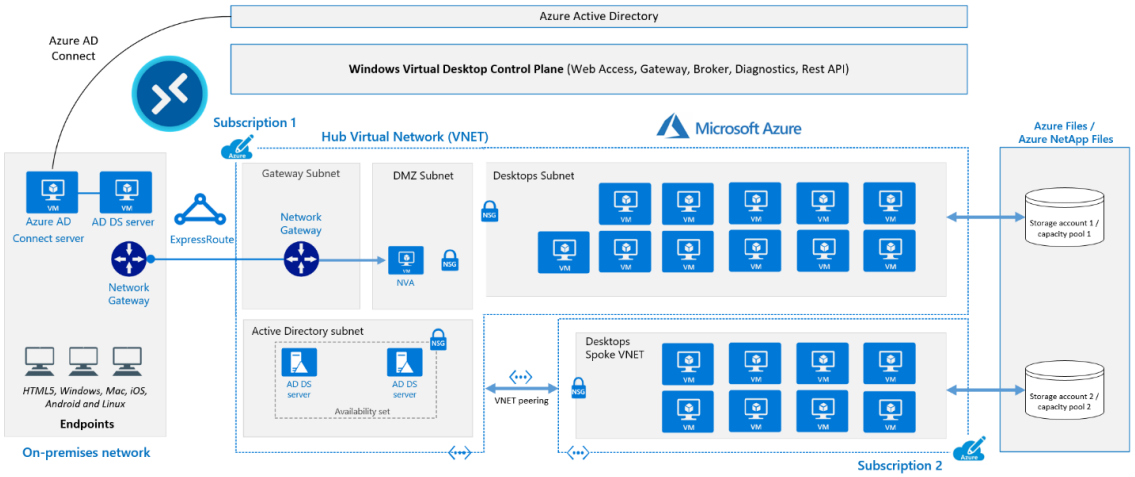


Figure 25: Architecture of Microsoft Azure Virtual Desktop

eG Enterprise v7.2 provides in-depth Microsoft AVD monitoring to help you provide an excellent end-user experience by spotting performance issues before they become real problems. With eG Enterprise you can:

- Monitor all aspects of user experience - logon time, application launch time, frame rate, connection bandwidth - using a combination of synthetic and real user monitoring.
- Get end-to-end visibility into the performance of all the IT tiers supporting Azure - AVD including the Azure cloud infrastructure, network connectivity, virtual desktops, session hosts and host pools and the user endpoints. Get to the root-cause of performance problems in one click.
- Be proactively and accurately alerted to the root-cause of problems using a combination of AIOPS technologies including out-of-the-box configurations of alert thresholds, dynamic automatic baselining of metric thresholds and intelligent dependency-based correlation rules.
- Obtain analytics and insights using which they can determine how to optimize the AVD infrastructure to accommodate more users and thereby deliver greater ROI for the organization.

Let us now briefly discuss on how each key component of Microsoft AVD infrastructure is monitored by eG Enterprise:

- **Monitoring AVD Host Pools:** Host pools are a collection of one or more identical virtual machines (VMs) within Azure Virtual Desktop environments. Each host pool can contain an app group that users can interact with as they would on a physical desktop. You control the resources published to users through app groups. All session host virtual machines in a host pool should be sourced from the same image for a consistent user experience. One of the key factors influencing user experience with an AVD service is the performance of the host pools. Host pool performance largely rests on the session load on the VMs in the pool, and whether/not the VMs are sized commensurate to their load. An under-sized VM will often run into resource crunches, causing applications on the VM to slow down or be unresponsive. Since the applications on a single VM can be used by multiple users, poor VM performance will result in many unhappy users. To avoid this, administrators must continuously monitor the user activity on each VM in a pool to assess its load, and measure resource usage on every VM to understand if the VMs have enough resource capacity to service the load. These insights will help administrators tweak the load-balancing configuration and resource allocations of VMs, so that user complaints related to desktop/application slowness reduce and user satisfaction with the AVD service increases. The FSLogix profile containers created for each user is continuously monitored and alerts are sent out if any user experienced undue slowness while the profile containers were being attached. The disk space allocated to the users attached with profile containers are closely monitored and the user profiles that are currently running out of disk space are promptly reported. This way, eG Enterprise v7.2 is capable of providing useful insights on AVD

host pool performance to administrators!

- **Monitoring Microsoft AVD Broker:** The AVD Connection Broker manages user connections to virtual desktops and remote apps. The Connection Broker provides load balancing and reconnection to existing sessions. This means that even the smallest of issues with the health and operations of the AVD broker service can delay / deny users access to critical apps/desktops. Some common issues that users often complain about include the sudden inaccessibility of the broker service, unexpected unavailability of host pools, desktop connection failures, ill health of session hosts, poor user logon experience with desktops/apps etc. If these issues are not caught and eliminated quickly, they can significantly delay or inexplicably halt the delivery of the AVD service. This is why, it is very important that the AVD broker is monitored. eG Enterprise v7.2 monitors the Microsoft AVD Broker and provides indepth insights into the availability and responsiveness of the AVD service. The diagnostic logs of each host pool are monitored and errors such as connection errors, service errors, management errors and unknown errors are promptly captured and reported. RDP feed and icon feed failures are promptly captured and the AVD host pool/users suffering due to these failures are identified with ease. The availability of each AVD host pool is reported periodically and the session hosts that are added/removed are captured. The configuration changes effected on the AVD service via API/Powershell are captured and the users who made such configuration changes are reported. In addition, the type of configuration change that was frequently made is also revealed. Standard health checks are periodically executed and the health check that failed frequently is identified along with the session host on which the health check failed. The session hosts that are running out of disk, CPU, GPU and memory resources are captured and reported. The applications that are draining the resources on the session host too is identified with ease. The user logins to the session host are periodically monitored and the logon performance measured reveals where exactly performance bottlenecks were noticed during logon. The TCP connection drops, and unusually high TCP retransmits are also promptly captured and reported.
- **eG Enterprise Logon Simulator for Microsoft Azure Virtual Desktop:** eG Enterprise v7.2 also provides a proprietary simulator using which a typical user login to an Azure virtual desktop can be captured and replayed at configured intervals to measure logon performance. This way, the simulator captures logon failures and delays before they occur, pinpoints their root-cause, and enables

administrators to resolve the issue before it impacts the logon experience of real users.

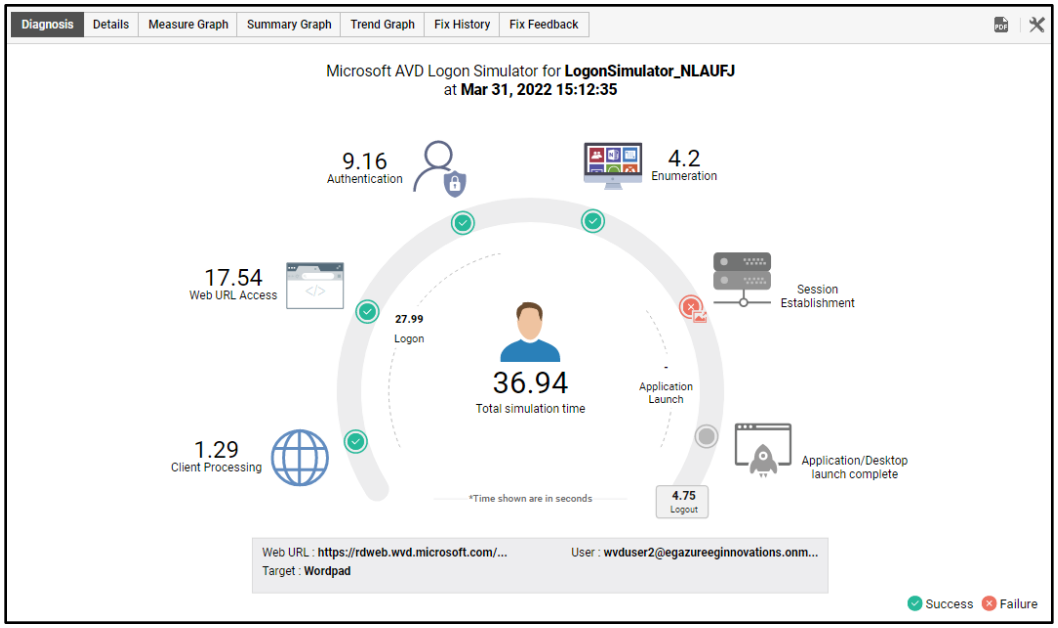


Figure 26: The AVD logon simulator: Identify where exactly slowness/failure occurred during logon simulation

- **AVD User Experience Dashboard:** For Azure AVD to become the preferred means of providing digital workspaces, it must be simple to monitor, diagnose and report on. Though Microsoft's Azure Monitor, the administration tool for AVD can be used for monitoring, setting up monitoring dashboards is tedious and time consuming and the web navigation is not intuitive. Hence, IT operations teams need a simple to use, purpose-built monitoring, diagnosis and analytics solution for Azure AVD. eG Enterprise v7.2 offers purpose-built dashboards which facilitates administrators to spend less time in configuring the dashboards or manually add metrics, event logs and traces to the dashboards. The out-of-the box pre-configured metrics and event thresholds set in the dashboards offer instant intelligent alerting. The AVD User Experience Dashboard helps end-users to view the performance metrics related to their access to the AVD infrastructure.

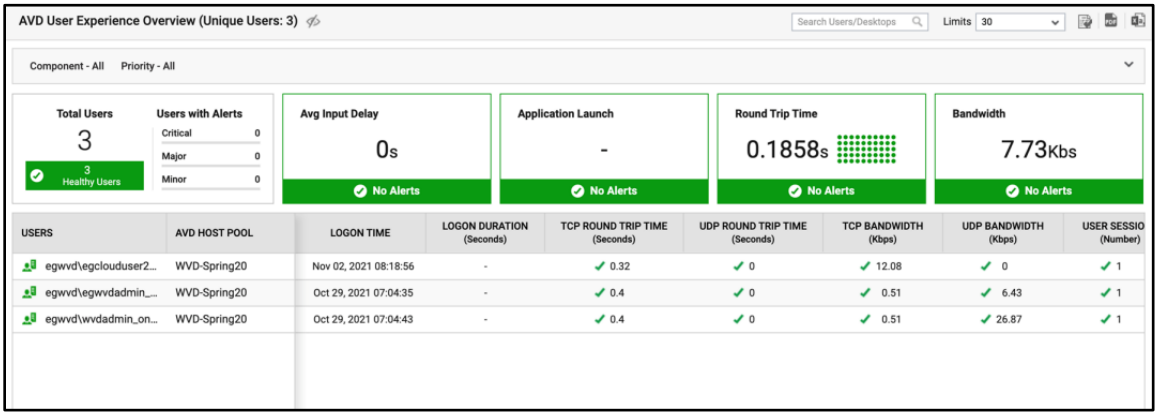


Figure 27: The User Experience dashboard for Microsoft AVD users

Further drilling down a user from Figure 27 reveals where exactly the user experience of the user suffered.

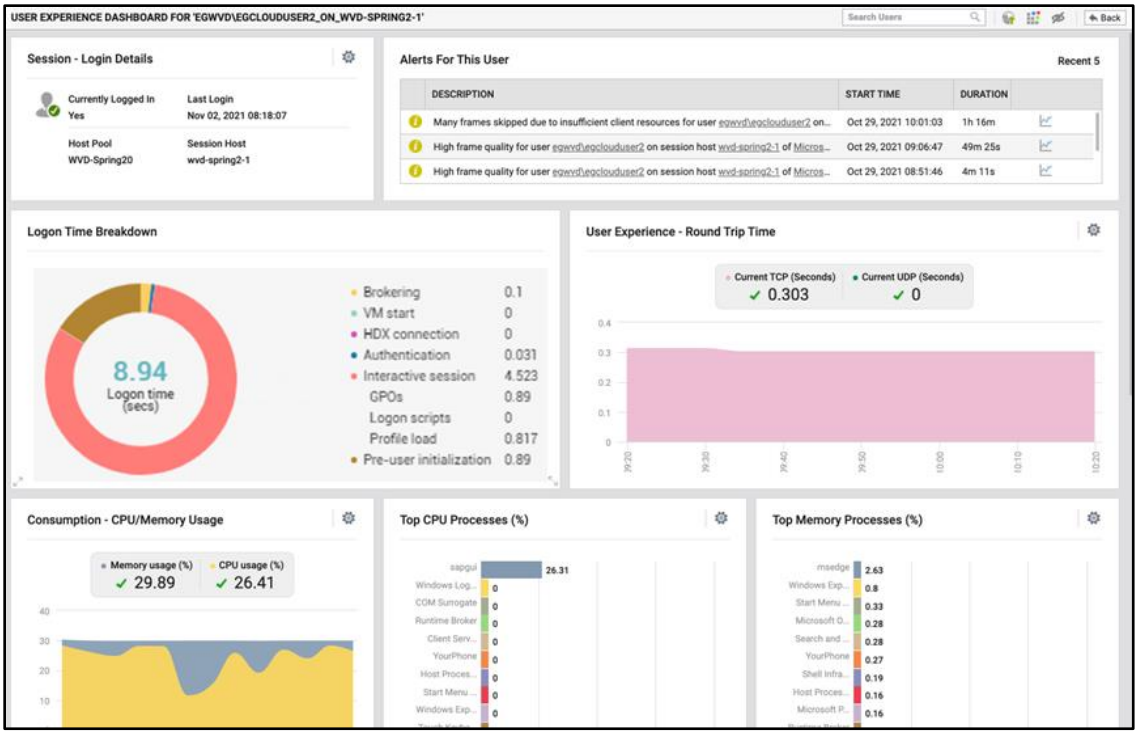


Figure 28: Drilling down to view the experience of a chosen user

- **AVD Infrastructure Dashboard:** To receive an overview of the performance of the Microsoft Azure Virtual desktops in an AVD infrastructure and to quickly spot 'grey areas', administrators can use the AVD Infrastructure Dashboard that eG Enterprise v7.2 offers. Using this dashboard, administrators can:
  - View the overall health and performance of the AVD host pools in an AVD infrastructure, so problematic AVD host pools can be promptly detected;
  - Assess the session load on the AVD infrastructure and identify the sessions hosts that are contributing to the load;
  - Identify the AVD Host pools with maximum number of active sessions, disconnected sessions, idle hosts and session hosts and ascertain the AVD Host pool that is most frequently utilized;
  - Ascertain the count of alerts raised in the AVD infrastructure and identify problem prone

AVD Host pools;

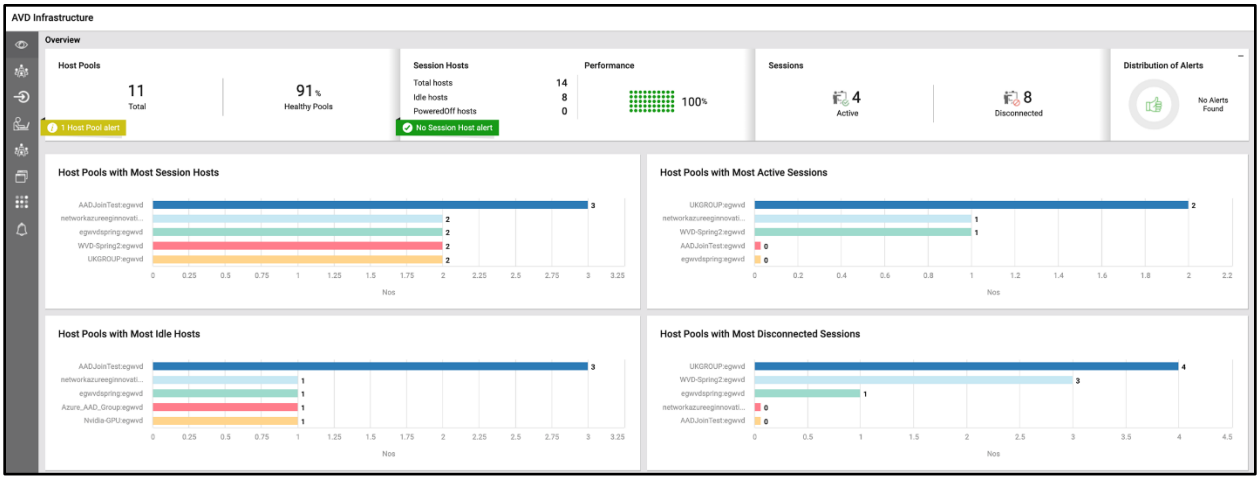


Figure 29: The AVD Infrastructure Dashboard

Upon clicking each icon in the left panel of the AVD Infrastructure dashboard helps administrators:

- Track the logon duration and figure out where exactly the logon time took too long – is it the Logon duration? or User profile duration? or Domain Controller discovery time? or Group Policy processing time? or Average authentication duration?
- Isolate the top 5 users who logged into the AVD infrastructure;
- Track the count of AVD Session hosts in the AVD infrastructure and figure out the count of session hosts that are idle/powered off etc.
- Identify the AVD Sessions hosts that are utilizing maximum physical resources such as CPU, memory, disk etc;
- Analyze the user experience of users by tracking the logon duration and application launch time;
- Isolate the sessions that are currently active and the logon duration of each session;
- Determine the AVD Session host on which maximum number of sessions were established;
- Isolate the top applications that are consuming excessive physical resources;
- Figure out the count of alerts raised in the AVD infrastructure etc

2.3.1 Reports for Microsoft Azure Virtual Desktops

Historical reports provide Microsoft AVD administrators with all the details they need for compliance reporting and infrastructure optimization. eG Enterprise v7.2 offers a bunch of reports that help administrators:

- Report on who logged in, at what times, what applications they accessed, what resources they used and how their digital employee experience (DEX) was. Track active/idle times to report time periods when the user was not active.
- Monitor all aspects of resource usage on the session hosts. Identify bottlenecks including under-sized hosts, applications with resource usage issues, and users generating unusual activity on the shared hosts.
- Get insights to right-size and optimize the infrastructure to deliver better performance and to

enhance the infrastructure to accommodate additional users.

- Report on user sessions, which user sessions were established over a period of time and how was the past trend in session load. Track session hosts on which maximum sessions were established.
- Monitor the slow logons to the AVD infrastructure over a period of time and isolate the users who have been frequently impacted by slow logons in the past.
- Get insights into the users, AVD host pools, session hosts, resources, and sources that frequently suffered connection failures in the recent past.

2.4 AWS DaaS Monitoring

Amazon Workspaces is a cloud DaaS (Desktop as a Service) service, offering persistent digital workspaces hosted in VMs (Virtual Machines) on Amazon infrastructure. Amazon AppStream 2.0 allows organizations to publish individual applications that are then streamed to end users on any device using an HTML5 browser, providing those applications as SaaS (Software as a Service).

A sudden failure of the Amazon Workspaces or the Amazon AppStream in DaaS/SaaS environments may affect hundreds of users simultaneously. With Amazon Workspaces/Amazon AppStream, there are several domains of control that make troubleshooting more difficult. When a user complains that desktop access is slow, you should triage the problem quickly - is the slowness due to the user terminal? or due to their connectivity to AWS cloud? or is it an issue with AWS WorkSpaces? or could it be an issue with one of the applications executing on the desktop? To proactively identify and eradicate such problems, eG Enterprise v7.2 is capable of monitoring both Amazon Workspaces and Amazon AppStream from a single console.

The AWS AppStream fleets are extensively monitored as part of eG's AWS Cloud monitoring and the state, type, and utilization of each fleet in terms of capacity is captured periodically. This way, the fleets that are most extensively utilized are identified. By monitoring the AWS WorkSpaces service, administrators can isolate unhealthy/stopped instances and identify those instances that are under maintenance. The count of session disconnects and sessions with high latency are also periodically monitored and abnormalities if any, are promptly captured and reported.

As with any digital workspace technology, performance monitoring of virtual desktops deployed on the cloud is important. Performance metrics can be collected in different ways:

- Synthetic monitoring using software robots that check if the virtual desktop service is available and responsive.
- Integration with AWS CloudWatch to collect utilization metrics for Amazon WorkSpaces and AppStream 2.0.
- Insights into the virtual desktops obtained using light-weight agents deployed within the desktops. Often these agents are built into the images used to spin up the virtual desktops dynamically.

Since Synthetic monitoring of Amazon WorkSpaces is already performed by eG Enterprise, starting with this version, eG Enterprise can perform synthetic monitoring of Amazon AppStream. Additionally, eG can monitor the virtual desktops hosted on Amazon Cloud using an exclusive monitoring model called "Amazon Cloud Desktops". Let us now discuss each of these capabilities in detail:

- **eG Enterprise Logon Simulator for AWS AppStream:** eG Enterprise 7.2 offers a dedicated logon simulator for AWS AppStream 2.0, which emulates an AWS logon process – from login to the AWS AppStream environment, to application/desktop enumeration, and to application/desktop launch - from designated endpoints. In the process, the simulator measures the logon experience from each endpoint. Since the user login is simulated at pre-configured intervals, administrators need not wait for real users to be actively logged on to the AWS Appstream to spot logon issues. Administrators are proactively alerted to a sub-par logon experience and are automatically lead to the exact step of

the logon process that is failing or slowing down.

The AWS AppStream logon simulator is simple to set up – no recording/replay is necessary, all that an administrator must do is point to the URL used to logon to the AWS cloud and provide the credentials used to simulate the logon.

- **Monitoring Virtual Desktops hosted on Amazon Workspaces:** Many organizations these days are looking to host their virtual desktops on Amazon Workspaces. These virtual desktops are faced with similar management challenges as virtual desktops in VDI infrastructures. eG Enterprise v7.2 seeks to mitigate these challenges by supporting in-depth monitoring of virtual desktops hosted on Amazon Workspaces using an exclusive monitoring model called "Amazon Cloud Desktops". Using the eG VM Agent deployed on each virtual desktop on the cloud, eG Enterprise proactively captures and reports user experience issues, poor session performance, and resource utilization bottlenecks on the Amazon Cloud desktops, and thus enables administrators to promptly initiate remedial measures. If users experience high latency, low frame rate, and serious bandwidth contentions when communicating with their cloud desktops via specific protocols (e.g., Nice DCV, PCoIP and WorkSpaces Streaming Protocol), then these protocols are highlighted. Amazon Cloud Desktops monitoring is licensed by the number of concurrent/named users only.
- **User Experience Dashboard Extends Support to Amazon Cloud Desktops:** Starting with this version, the User Experience Dashboard can be used to measure real-time user experience with Amazon Cloud Desktops as well. One look at the dashboard will pinpoint those cloud desktop users who are experiencing high latency, resource contentions, and I/O processing bottlenecks

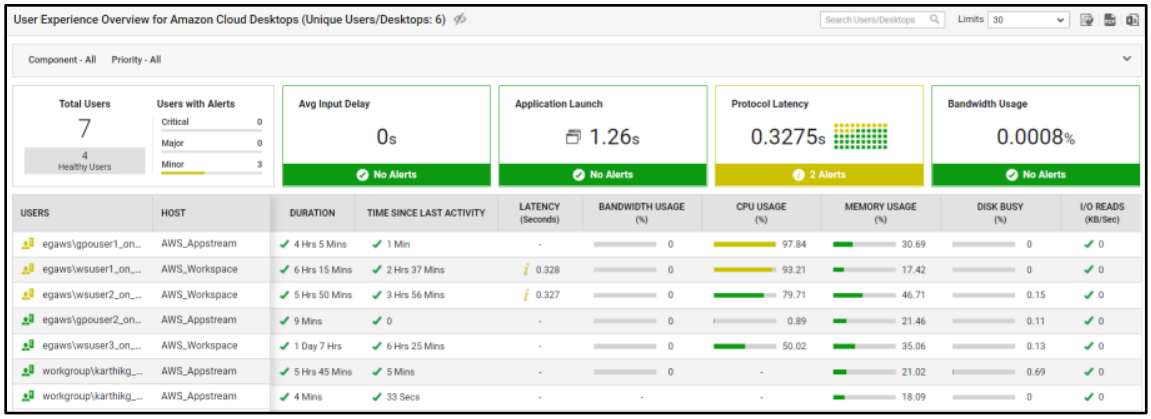


Figure 30: The User Experience Dashboard for Amazon Cloud Desktops

You can even zoom into a user to accurately diagnose why the quality of that user's experience is poor.

2.4.1 Reporter Enhancements for Amazon Cloud Desktops

Historical reports provide Amazon Cloud administrators with all the details they need for compliance reporting and infrastructure optimization. These reports are as follows:

- Report on who logged in, at what times, what applications they accessed, what resources they used and how user experience was.
- A report that tracks active/idle times to report time periods when the user was not active.
- A report that covers all aspects of resource usage; use the report to identify resource usage bottlenecks including under-sized virtual desktops, applications with resource usage issues, and users

generating unusual activity on the virtual desktops.

Let us now discuss a few reports in detail:

- **Active/Idle Time Report:** During and post COVID, many organizations have had to rapidly adapt to a work-from-home or a hybrid work culture. On one end, this culture allowed employees the freedom to work from the comfort of their armchairs. Users could use any device of their choice and connect to their work desktops on the Amazon cloud from any external network. On the flipside however, this change in working style introduced many new security, monitoring, and management challenges for IT administrators. Some of the key challenges faced by administrators during this time were:
    - Verifying employee attendance;
    - Tracking their desktop activity;
    - Measuring their overall productivity;

With the help of the Active/Idle Time Report, administrators can overcome all the aforesaid challenges! For instance, administrators can use this report to quickly ascertain whether all employees/users had logged into their desktops during the given period – i.e., whether/not all employees had reported to work each day during the configured timeline. Employee attendance can thus be verified. The report also reveals how actively users used their desktops during the designated period. If most users were idle on their desktops almost the entire time they were logged in, then the Overview of Active/Idle Time pie chart in the report will alert users to this abnormality. This implies little-to-no desktop activity and poor user productivity during the specified time period. Furthermore, the report also points administrators to the unproductive users and the exact sessions where they were inactive.

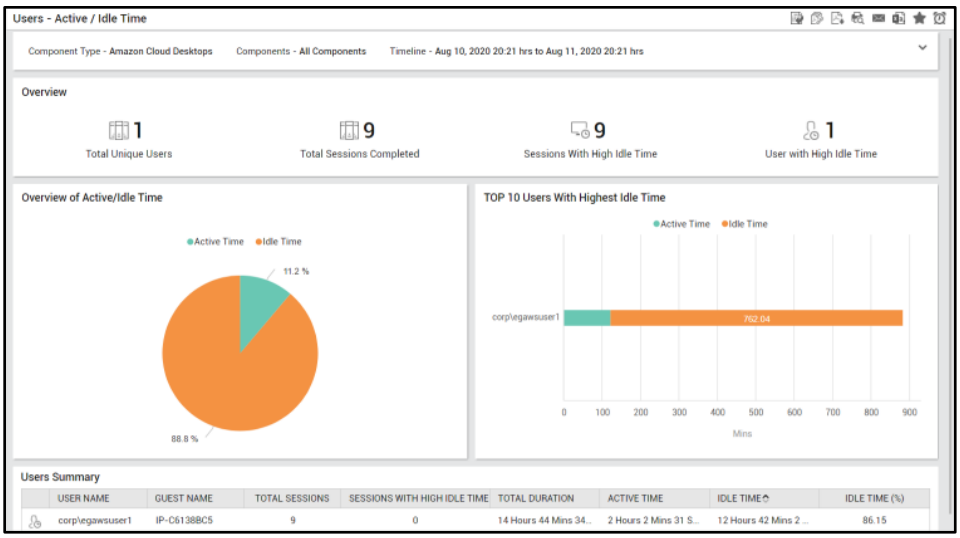
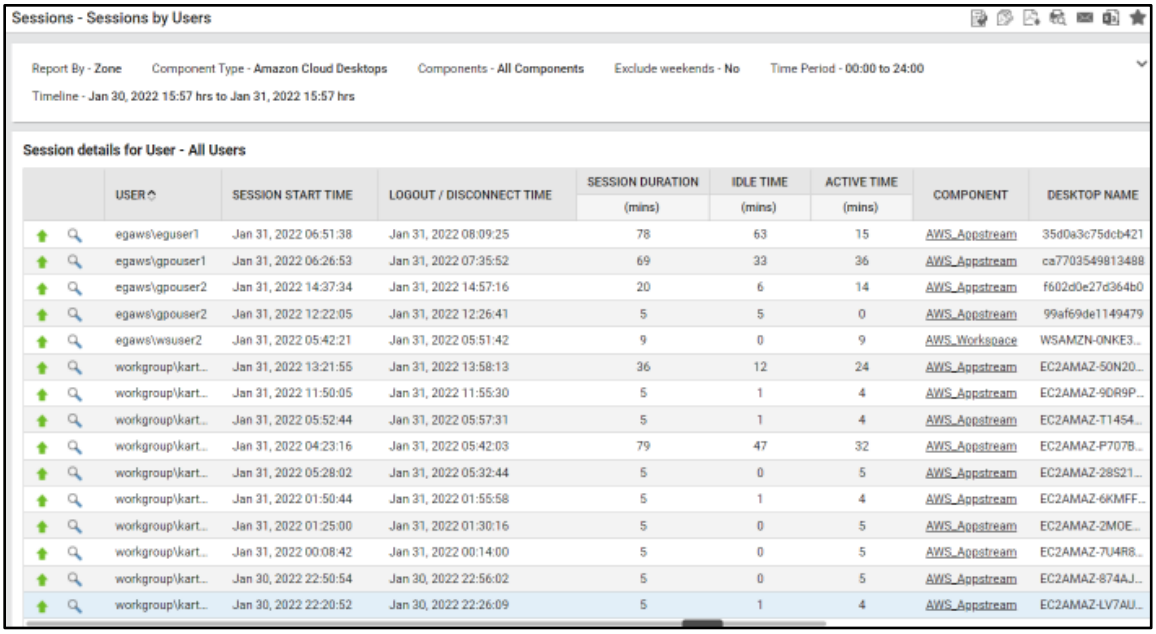


Figure 31: The Users – Active / Idle Time Report

- **Sessions by Users Report:** The key challenge in monitoring AWS Cloud environments is to keep track of the user activity on the cloud desktops. Using the Sessions by Users Report provided by eG Enterprise v7.2, administrators can receive a session-by-session account of the activity of each cloud desktop user, during the given period. With the help of the report, administrators can figure out at what times during the given period each user logged in, when he/she logged out of each session, which desktops were accessed per session and for how long and the active/idle time per session. Like the other reports offered by eG Enterprise, the Sessions by Users Report too permits administrators to customize the view by specifying the measures to be displayed in the report and

computations to be performed on the measures (such as Avg, Max, Min etc.).



USER	SESSION START TIME	LOGOUT / DISCONNECT TIME	SESSION DURATION (mins)	IDLE TIME (mins)	ACTIVE TIME (mins)	COMPONENT	DESKTOP NAME
egaws\eguser1	Jan 31, 2022 06:51:38	Jan 31, 2022 08:09:25	78	63	15	AWS_Appstream	35d0a3c75dcb421
egaws\gpouser1	Jan 31, 2022 06:26:53	Jan 31, 2022 07:35:52	69	33	36	AWS_Appstream	ca7703549813488
egaws\gpouser2	Jan 31, 2022 14:37:34	Jan 31, 2022 14:57:16	20	6	14	AWS_Appstream	f602d0e27d364b0
egaws\gpouser2	Jan 31, 2022 12:22:05	Jan 31, 2022 12:26:41	5	5	0	AWS_Appstream	99af69de1149479
egaws\wsuser2	Jan 31, 2022 05:42:21	Jan 31, 2022 05:51:42	9	0	9	AWS_Workspace	WSAMZN-0NKE3...
workgroup\kart...	Jan 31, 2022 13:21:55	Jan 31, 2022 13:58:13	36	12	24	AWS_Appstream	EC2AMAZ-50N20...
workgroup\kart...	Jan 31, 2022 11:50:05	Jan 31, 2022 11:55:30	5	1	4	AWS_Appstream	EC2AMAZ-9DR9P...
workgroup\kart...	Jan 31, 2022 05:52:44	Jan 31, 2022 05:57:31	5	1	4	AWS_Appstream	EC2AMAZ-T1454...
workgroup\kart...	Jan 31, 2022 04:23:16	Jan 31, 2022 05:42:03	79	47	32	AWS_Appstream	EC2AMAZ-P707B...
workgroup\kart...	Jan 31, 2022 05:28:02	Jan 31, 2022 05:32:44	5	0	5	AWS_Appstream	EC2AMAZ-28S21...
workgroup\kart...	Jan 31, 2022 01:50:44	Jan 31, 2022 01:55:58	5	1	4	AWS_Appstream	EC2AMAZ-6KMFF...
workgroup\kart...	Jan 31, 2022 01:25:00	Jan 31, 2022 01:30:16	5	0	5	AWS_Appstream	EC2AMAZ-2MOE...
workgroup\kart...	Jan 31, 2022 00:08:42	Jan 31, 2022 00:14:00	5	0	5	AWS_Appstream	EC2AMAZ-7U4R8...
workgroup\kart...	Jan 30, 2022 22:50:54	Jan 30, 2022 22:56:02	5	0	5	AWS_Appstream	EC2AMAZ-874AJ...
workgroup\kart...	Jan 30, 2022 22:20:52	Jan 30, 2022 22:26:09	5	1	4	AWS_Appstream	EC2AMAZ-LV7AU...

Figure 32: The Sessions by Users Report

- **Top Users Report:** When managing commercial cloud desktop deployments, it is important for administrators to know who the top resource consumers are and how much virtual resources they usually consume. Based on this knowledge, administrators can recommend the right desktop size and usage plan for the users, so that such users do not complain of resource contentions and related performance deficiencies going forward. This is where the Top Users report helps! This report, when generated for a particular virtual resource, will pinpoint the cloud desktop users who have been hogging that resource consistently, and how much of that resource they have been consuming over time.

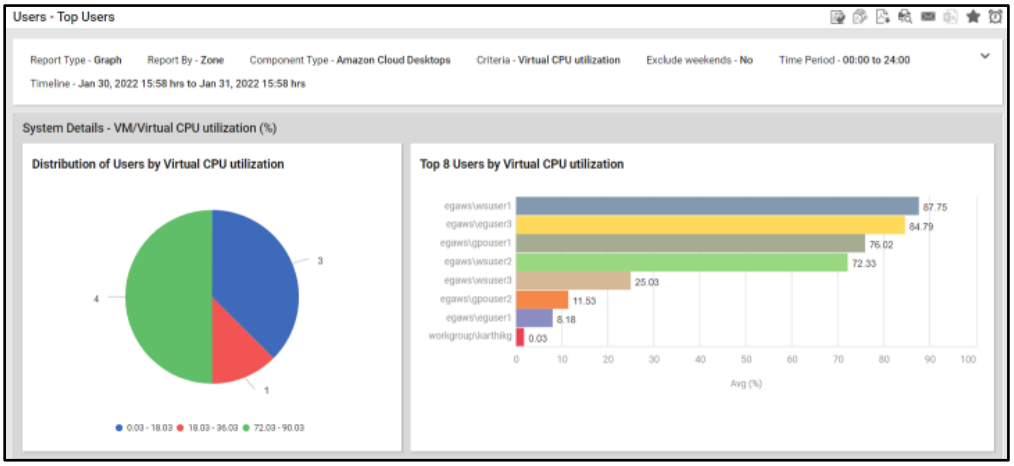


Figure 33: The Top Users Report

2.5 Endpoints Monitoring

2.5.1 IGEL Monitoring

IGEL is a "Next-Gen Operating System" built for secure access to cloud workspaces, such as VDI and Desktop as a Service (DaaS). Built on a highly secure Linux kernel and compatible with any x86-64 device, the IGEL OS is bundled with all the necessary virtual utilities, such as Citrix Workspace App/Receiver, VMware Horizon Client, Windows RDP client, and AWS WorkSpaces client that allow users to securely connect to digital workspaces. A typical IGEL environment comprises of IGEL UMS, IGEL Cloud Gateway and IGEL Endpoints.

- IGEL Endpoint is a thin client - a small-sized desktop terminal without a hard drive. It has a thin footprint, easy to manage, controllable, secure device and does not require high end configurations to run. It has IGEL's "Next generation edge Operating System" which is built for secure access to cloud workspaces such as VDI and Desktop as a Service.
- With IGEL UMS, IGEL Endpoints can be remotely configured and controlled. It supports various OS, database and directory services.
- The IGEL Cloud Gateway extends the UMS via a standard internet connection to Endpoints that are running in Remote branch offices, Home and Anywhere such as cafe, paid workspaces etc.

Most organizations have tools that provide deep visibility into the datacenter components, the servers and virtual desktops. A key missing piece limiting the end-to-end visibility is the endpoint that users connect to their digital workspaces from. If the endpoint is slow or has a resource bottleneck, it will affect the user experience. At the same time, from an administrator's point of view, lack of visibility into endpoint performance hinders troubleshooting. Administrators often spend hours troubleshooting in the datacenter when the real issue is on the endpoint. Therefore, proactive monitoring of IGEL endpoints in an IGEL deployment can help IT administrators take preemptive action to improve user experience to a great extent. eG Enterprise v7.2 offers end to end monitoring of an IGEL deployment with three different monitoring models – IGEL UMS, IGEL Cloud Gateway and IGEL Endpoints.

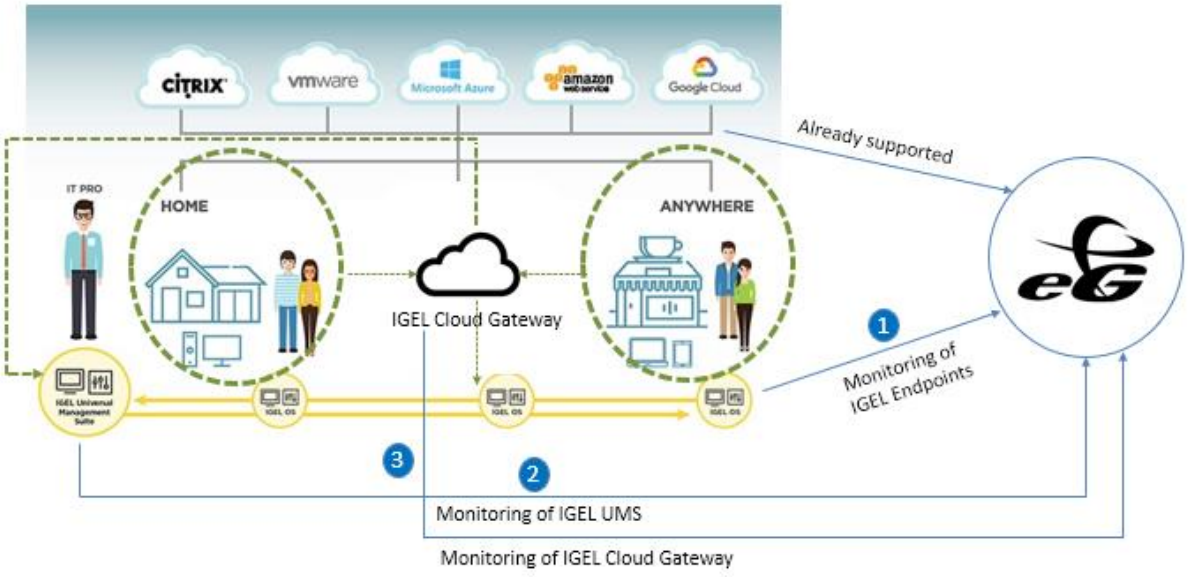


Figure 34: End to End Digital Workspace visibility with eG Enterprise

- **Monitoring IGEL Endpoints:** By monitoring the IGEL Endpoints, administrators can identify the endpoints that are resource-starved and pinpoint the precise process on the endpoint that is hogging resources. Helpdesk staff are provided end-to-end views with drilldowns from a user session to their

IGEL endpoint, thus enabling faster and more accurate diagnosis. Administrators can also benchmark the endpoint resource usage and performance, detect any deviations from normal and take pre-emptive steps based on it.

- **Monitoring IGEL UMS:** For the IGEL Endpoints to seamlessly work, the IGEL UMS should be always available. By monitoring IGEL UMS, you can highlight scalability issues, communication problems and bottlenecks that must be addressed quickly to ensure that all endpoints are working well and are centrally managed.
- **Monitoring IGEL Cloud Gateway:** Since the IGEL Cloud Gateway is the entry point for IGEL Endpoints connected from a remote location, the IGEL Cloud Gateway should always be up and running. If IGEL Cloud Gateway is down, IGEL endpoints from a remote location cannot connect to the IGEL UMS. Users will therefore be denied access to IGEL environment. By monitoring IGEL Cloud Gateway, administrators can leverage the session load on the IGEL Cloud Gateway, accurately identify error messages logged in the log files, and deduce the number of IGEL Endpoints connected to the IGEL Cloud Gateway at any point of time.
- **Licensing:** IGEL Endpoint monitoring is licensed by the number of concurrent endpoints. This is provided as a separate field in the eG Enterprise license. For concurrent licensing, concurrent endpoints in any consecutive 30 minute window are considered just like any Citrix /VDI environment. Though Citrix/VDI can be licensed by server, IGEL endpoints can be licensed by concurrent endpoints.
- **IGEL Endpoints Dashboard:** eG Enterprise v7.2 offers an IGEL Endpoints dashboard as part of IGEL monitoring. This dashboard lists all the IGEL Endpoints reporting to eG Enterprise along with their key performance metrics. By merely looking at the dashboard, administrators will be able to figure out the alerts raised for the IGEL Endpoints and identify resource-intensive IGEL Endpoints.

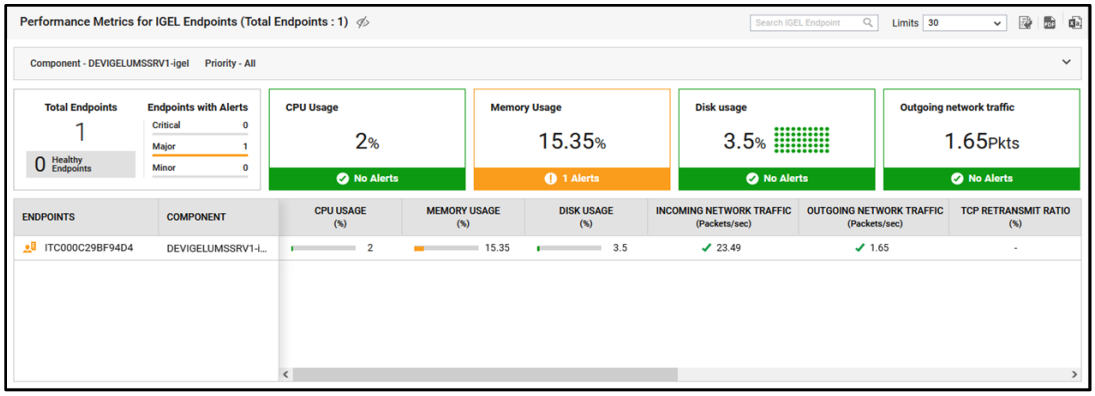


Figure 35: IGEL Endpoints Dashboard

Further, drilling down from an IGEL Endpoint will reveal a detailed performance dashboard which clearly indicates the resource utilization of that IGEL Endpoint, alerts raised on the same, and the TCP connections to the IGEL Endpoint over a period of time. Administrators can also determine, from

a single glance, which process on the IGEL Endpoint is draining its CPU and memory resources.

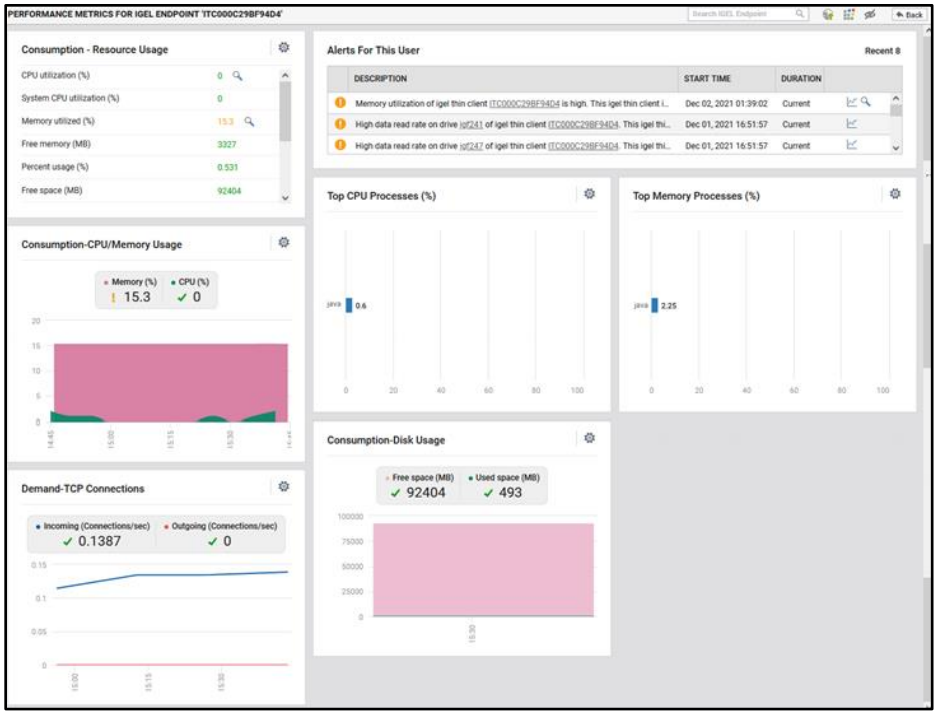


Figure 36: Detailed Performance dashboard of a chosen IGEL Endpoint

- **Drill down to IGEL Endpoint Performance from Citrix User Experience Dashboard:** If a Citrix user accesses his/her environment using an IGEL Endpoint, then, the Session Topology view of that user (accessed by drilling down from the User Experience Overview dashboard) will auto-discover and display the IGEL Endpoint mapped to the user. Zooming into an IGEL Endpoint will reveal the performance of the IGEL Endpoint.

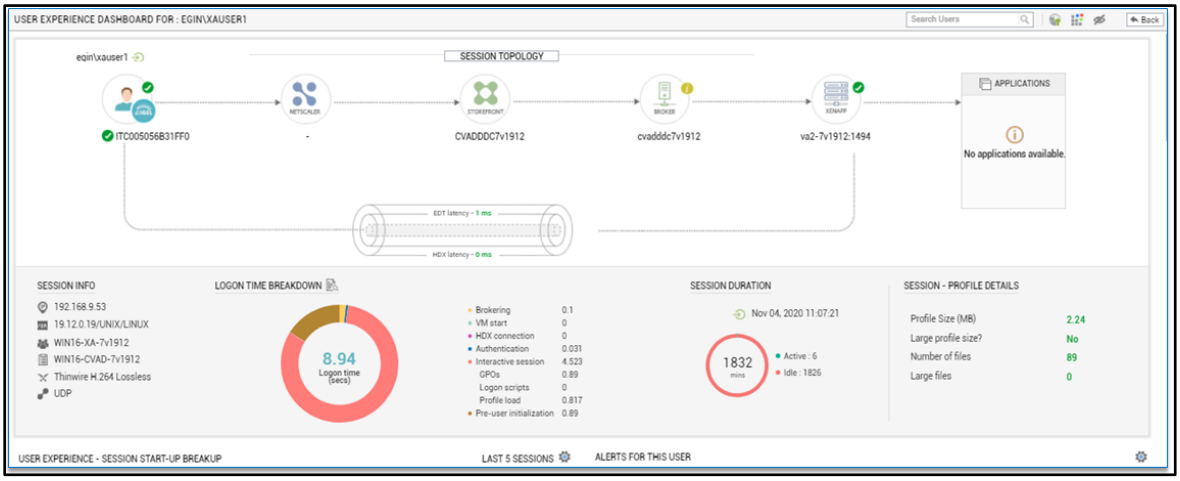


Figure 37: Session Topology of a user logged in through IGEL Endpoint

2.5.1.1 Reporter Enhancements for IGEL

Following are the new reports that are added to eG Enterprise for historical performance analysis of IGEL

components in an IGEL deployment:

- **Endpoint Uptime Analytics Report:** Uptime is a key measure of the general health and availability of the IGEL Endpoints in a typical IGEL infrastructure. Periodic uptime values that the eG agent reports for target IGEL Endpoints can alert you to unscheduled reboots that occurred recently; however, to effectively assess Endpoint availability over time, accurately determine unexpected and prolonged breaks in availability, and accordingly ascertain service level achievements/slippages, a look at the total uptime of an IGEL Endpoint and the total number of reboots it experienced over a period of time is necessary. To enable such an analysis for one/more critical IGEL Endpoints in an IGEL infrastructure, eG Enterprise v7.2 offers the Endpoint Uptime Analytics report.

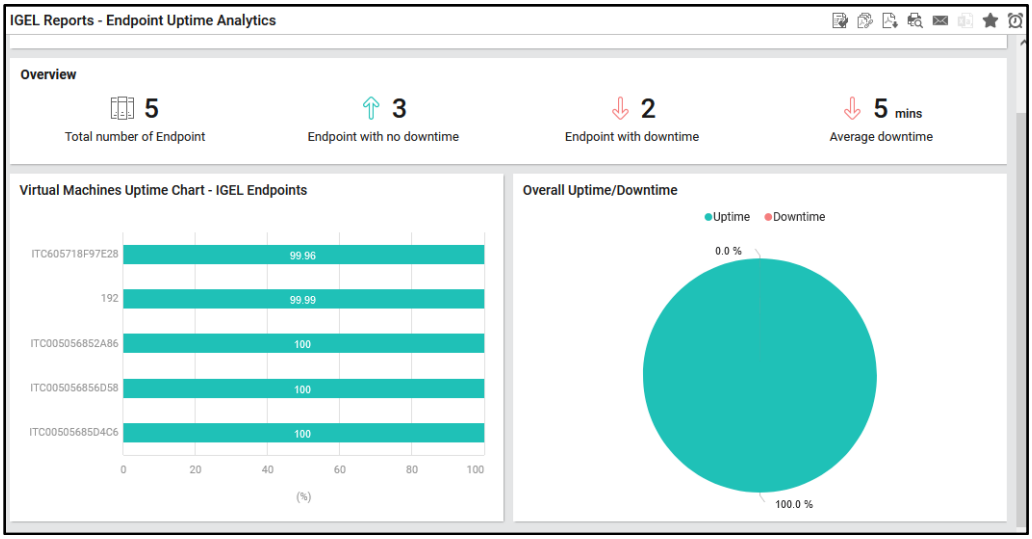


Figure 38: The Endpoint Uptime Analytics Report

- **Endpoint Resource Analytics Report:** This report provides deep insights into the resource utilization of the IGEL Endpoints over a period of time. Using this report, the administrators can easily figure out the following:
  - Is any IGEL Endpoint over-utilizing its memory resources? Are all IGEL Endpoints sized with adequate memory resources?
  - Is any IGEL Endpoint experiencing a sudden/gradual rise in TCP connections?
  - Is any IGEL Endpoint taking too long to read from/write to the disks?
  - Is any IGEL Endpoint rebooted recently?

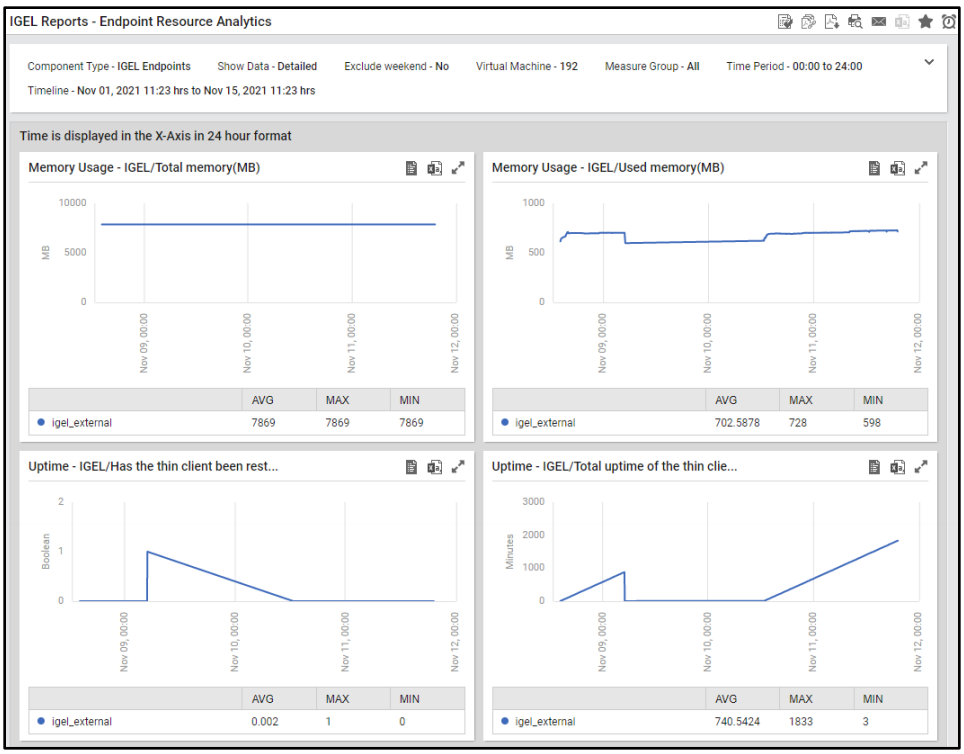


Figure 39: The Endpoint Resource Analytics Report

- **Top IGEL Endpoints Report:** Use this report to historically analyze the memory resource consumption and uptime of the monitored IGEL Endpoints over a period of time. With the help of this report, IGEL Endpoints that are frequently restarting, and those that are consistently draining memory resources can be identified. This report also helps you to identify the IGEL Endpoints that are taking too long to read from or write to the disk.

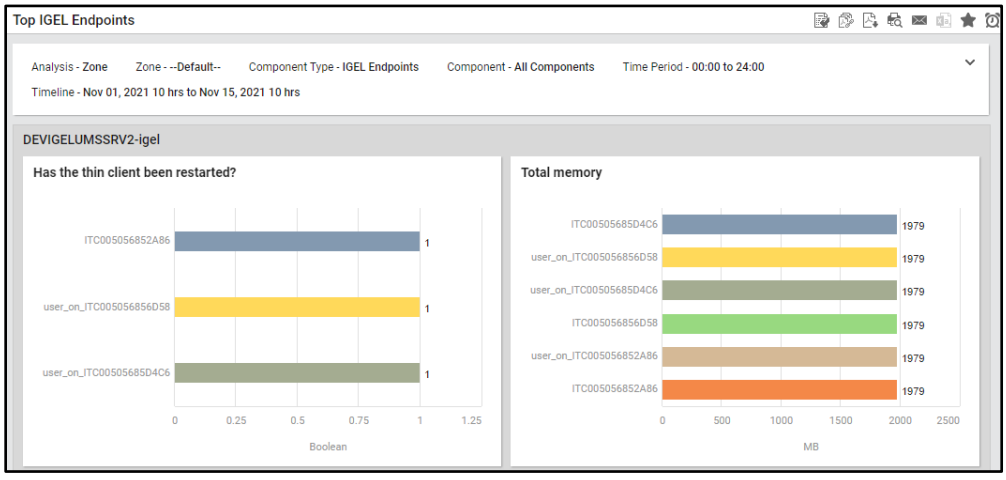


Figure 40: The Top IGEL Endpoints Report

2.5.2 Other EndPoints Monitoring Enhancements

- **Monitoring Physical Desktop Groups:** Many organizations these days deploy a combination of physical desktops and virtual desktops hosted on cloud AWS or Azure clouds to serve their internal and business needs. To ensure that user experience with desktops (physical or virtual) remains

above-par at all times, administrators of such environments need a unified tool that monitors and reports the performance of both types of desktops. Monitoring support for virtual desktops on the cloud is already available in eG. With eG Enterprise v7.2, administrators can now monitor physical desktops as well. To monitor the physical desktops, eG Enterprise requires that you configure a new physical desktop group, where you can group physical desktops based on a region, department, etc. Using the eG VM Agent deployed on each physical desktop, eG Enterprise proactively captures and reports user experience issues, poor session performance, and resource utilization bottlenecks on the physical desktops, and thus enables administrators to promptly initiate remedial measures. The User Experience Dashboard helps administrators quickly analyze the performance of each user logged into the physical desktops that are available within a physical desktop group.

2.6 GPU Monitoring Enhancements

Following are the enhancements included for GPU monitoring in eG Enterprise v7.2:

- GPU monitoring support has been extended to NVIDIA RTX Virtual Workstation Technology, Intel and AMD GPU Adapters.
- Starting with this version, the GPU utilization on Linux VMs can be reported in addition to that of Windows VMs.
- **Monitoring the usage and memory sizing of GPU adapters:** Inadequate memory allocation and inefficient utilization of the GPU adapters can greatly impact the processing performance of the target host/VM. eG Enterprise v7.2 monitors how a target uses each GPU adapter, and how every adapter uses the memory allocated to it. The results reported point administrators to the top-10 applications/processes that are using the maximum amount of GPU resources and those GPUs that are running out of memory.
- **Monitor GPU Usage by User Sessions:** The GPU utilization of user's sessions initiated through Citrix Virtual Apps, Microsoft RDS and VMware Horizon Connection Server can now be periodically tracked and the user/process consuming maximum GPU resources is identified with ease.
- **Analyze GPU Usage by Applications:** The GPU utilization of the applications accessed through sessions initiated on Citrix Virtual Apps, Microsoft RDS and VMware Horizon Connection Server can now be monitored and the process/user consuming maximum GPU resources is identified. This way, users who consistently engage in graphics-intensive operations can be identified, and their GPU requirements accurately ascertained.

3. User Experience Monitoring

3.1 Real User Monitoring Enhancements

Real user monitoring (RUM) captures the real-time user experience of users as they access web applications. RUM breaks down web page load time into various components to help the application owner understand what the potential cause of transaction slowdown could be.

- **Customizing Tolerating Page View Cutoff:** Earlier, if the load time of any web page was between the Slow Transaction Cut off configured for the Web Site test and 4 times the Slow Transaction Cut off', then the eG Real User Monitor automatically counted that page view as a 'Tolerating page view'. Starting with version 7.2 however, administrators are allowed the flexibility to override this default behaviour and custom-define a separate cutoff for tolerating transactions. For this purpose, a **Tolerating Cutoff** parameter has been introduced in the test configuration page for the eG RUM tests. By default, the value specified against this parameter is 16000 milliseconds. Administrators

can increase or decrease this cutoff according to what is 'tolerating', what is 'slow' and what is 'normal' in their environment.

- **Additional Single Page Application Frameworks Supported:** Starting with this version, eG Enterprise extends to monitor the transactions to Single Page Applications built on ReactJS, EmberJS, Vue.js, Meteor and Backbone.js frameworks.

- **Enabling Single Page Application WebSite Monitoring:** In previous versions, to monitor the transactions to a Single Page Application (SPA), administrators had to manually insert application code blocks in the exact location from where the SPA was called from the target web site/web page. This manual process was cumbersome and laborious. To ease the pain of administrators, starting with this version, eG Enterprise has automated the process of instrumenting an SPA for real user monitoring. While adding the Real User Monitor component for monitoring, if the administrators enable the **Capture SPA** and **Capture fetch() requests** sliders, eG Enterprise will automatically inject the application code blocks to monitor SPAs and start capturing relevant metrics.

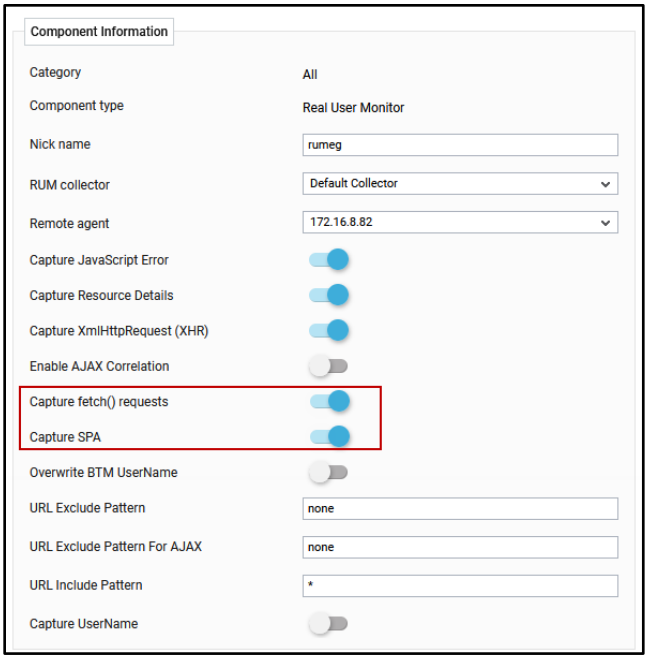


Figure 41: Enabling eG RUM to capture transactions to Single Page Applications

- **User-centric Metrics are now Reported for RUM:** Nowadays, web pages are becoming increasingly complex with rich images, which takes a toll on the page load time. For analyzing the performance of a web site that is both complex and content rich, monitoring the page load time alone may not be sufficient. Sometimes, a web site may load the 'above the fold' content i.e., the content that appears before scrolling down on a web page but may take time to finish rendering. Since users focus on 'above the fold' content, they may not see a delay in accessing the web page. However, many search engines and web sites focus on page speed that includes a plethora of key metrics such as First paint time and First contentful paint time which play a major role in calculating accurate page load time. eG Enterprise v7.2 has been enhanced to provide more granular metrics on page load time, so that administrators can deduce the root-cause of slow page views accurately. For instance, in this version, eG RUM reports the time delay due to events triggered via Onload function or any child events, and thus enable administrators understand how page onload event duration can impact the overall page load time. This way, eG RUM presents to administrators a single pane-of-glass view of all the factors influencing user experience with a web site/application

thus enabling precise root-cause diagnosis.

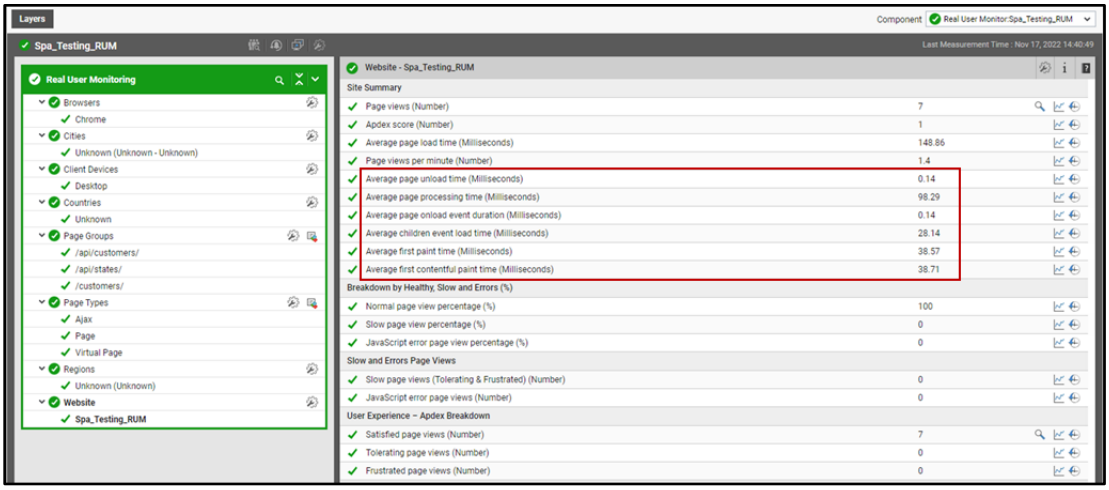


Figure 42: Additional metrics revealing the breakdown of event duration

- **Drilling down from RUM to PHP Transaction Tracing:** Previously, in environments where both RUM and Java/.NET BTM were enabled, an integrated view of RUM and BTM metrics was available as part of detailed diagnosis of the eG RUM tests. This integrated view is now available for environments where eG RUM and eG PHP BTM have been implemented. Administrators can now diagnose the root-cause of slowness in their PHP applications with a single click from the detailed diagnosis page (of eG RUM tests).

- **Utility for Injecting eG RUM JavaScript into SharePoint:** In older versions, to monitor the web pages hosted on a SharePoint site, administrators had to manually insert the eG RUM JavaScript into each web page. This process was tedious if hundreds of web pages hosted on a SharePoint Site or multiple subsites of SharePoint 365 were to be monitored. To save administrators the time and effort involved in this exercise, eG Enterprise v7.2 has introduced a brand new Powershell utility which when executed automatically inserts the eG RUM JavaScript to the web pages on the SharePoint Site/SharePoint 365 automatically.

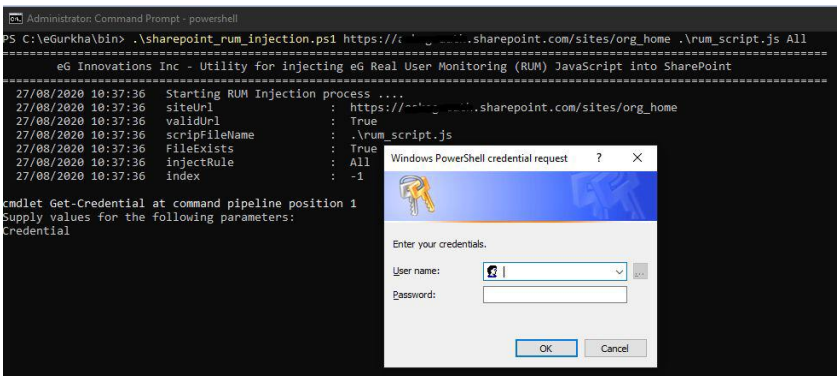


Figure 43: Automatically injecting RUM JavaScript to one/more SharePoint Sites/sub sites

Administrators can also execute this utility to remove the eG RUM JavaScript from one/more web pages of a SharePoint site/SharePoint 365.

- **Self-Guarding the eG RUM Collector from Possible Attacks:** In previous versions, the eG RUM Collector received beacons from websites that were not monitored by eG Enterprise. This was unnecessarily imposing processing overheads on the eG RUM Collector and there was a potential risk

of attack on the RUM Collector. To avoid this, starting with this version, administrators can block requests/beacons from specific websites/client IPs. To this effect, administrators can specify a comma-separated list of websites for which metrics/beacons need not be collected by the eG RUM Collector against the **blocked_sites** option in the **rum.properties** file available in the **<EG_RUM_DATA_COLLECTOR_INSTALL_DIR>\tomcat\webapps\rumcollector\web-inf\lib** directory on Windows; on Unix, this will be the **/opt/rum/tomcat/webapps/rumcollector/WEB-INF/lib** directory). Similarly, to block beacons from certain client IPs, administrators can specify a comma-separated list of client IPs against the **blocked_clients** option in the **rum.properties** file available in the **<EG_RUM_DATA_COLLECTOR_INSTALL_DIR>\tomcat\webapps\rumcollector\web-inf\lib** directory (on Windows; on Unix, this will be the **/opt/rum/tomcat/webapps/rumcollector/WEB-INF/lib** directory). If you wish to avoid collecting RUM Resource Details for specific websites, then, you can specify the website ID against the **ignore_Resource_Details_Data** option in the **rum.properties** file on the **<EG_RUM_DATA_COLLECTOR_INSTALL_DIR>\tomcat\webapps\rumcollector\web-inf\lib** directory (on Windows; on Unix, this will be the **/opt/rum/tomcat/webapps/rumcollector/WEB-INF/lib** directory).

3.2 Web App Simulation Enhancements

Following are the enhancements that are made to the Web App Simulation Recorder in eG Enterprise v7.2:

- **Support for Dynamic 2FA(MFA) using TOTP authentication mechanism:** Two-factor authentication (2FA), often referred to as two-step verification, is a security process in which the user provides two authentication factors to verify who they say they are. In previous versions, the Web App Simulator could not simulate logons fora two-factor authentication enabled user much to the dismay of the administrators. In v7.2 however, the simulator uses the Time-based-One-Time-Password (TOTP) authentication mechanism to lend support to two-factor authentication enabled users who log into the web application/website. For example, you can record a simulation for TOTP enabled users logging into Microsoft O365 site integrated with Microsoft Azure Active Directory.

  To record a simulation, you need to follow the steps below:

  - Register for access to the web application
  - Obtain the secret key from your application
  - Choose any authenticator app that supports TOTP: Google Authenticator, Microsoft Authenticator etc
  - Add your secret key or scan the QR code and provide this to your authenticator app
  - TOTP codes from your authenticator app can be used to login to your web application where you are recording the simulation

  For user authentication using the TOTP code, you need to add a **StoreMFAToken(TOTP) Activity** in the Web App Simulation Recorder and specify the secret code in the **Target** field. Then, you need

to assign a variable to store the generated TOTP passcode.

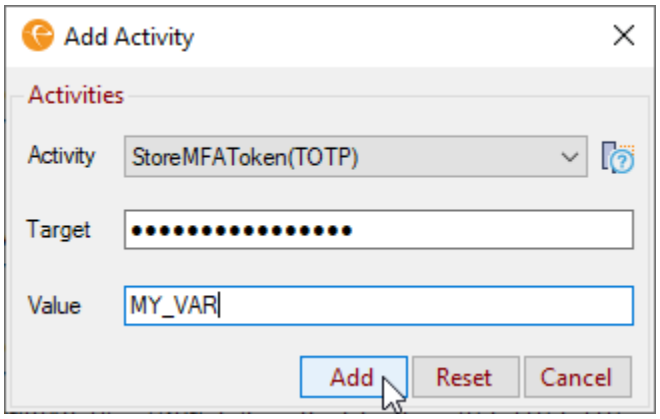


Figure 44: Adding the StoreMFAToken (TOTP) Activity

For the Web App Simulation to generate the TOTP passcode dynamically, you need to add a **Type Activity** in the Web App Simulation Recorder which will input the TOTP passcode as and when required. During playback, the Web App Simulation will automatically generate the TOTP using the secret key and current time and provide this along with user credentials. The generated TOTP is used as a soft token/passcode for user authentication during simulation. After successful authentication, the simulation will report the total time taken for the login.

- **Flexible Recording Options:** Web App Simulation Recording is now more flexible with the introduction of the following options:
  - Cut/Copy,
  - Enable/Disable and
  - Breakpoints

Let us now discuss each of the options in detail:

- **Support to Cut/Copy/Paste a Step/Activity in a Transaction Script:** Earlier, in some environments, administrators had to record one/more steps repeatedly, as such steps were part of multiple transactions. For instance, when simulating interactions with an airline's web site, the login step may be part of the transaction to check flight timings, and the transaction to book a flight. Previously, the login step had to be recorded separately for both the transactions - this was both laborious and time-consuming. Also, once a transaction is recorded, some administrators may want to alter the sequence of recorded steps as per their needs. This could not be achieved earlier. In v7.2 however, these requirements have been addressed. Administrators can now perform Cut, Copy and Paste activities on the recorded steps. Using this capability, administrators can copy a common step from one transaction to another, and even move steps within a transaction.
- **Support for Enabling/Disabling a chosen Step/Activity:** Sometimes, administrators may want to disable the execution of one/more user activities from a transaction script. In earlier versions, administrators had to painstakingly record the script again if they had to disable one/more user activities. However, this is no longer the case now. In v7.2, eG Enterprise offers an Enable/Disable option which can be used to disable one/more user activities from a transaction script. This saves administrators the time and trouble involved in recording the script

all over again.

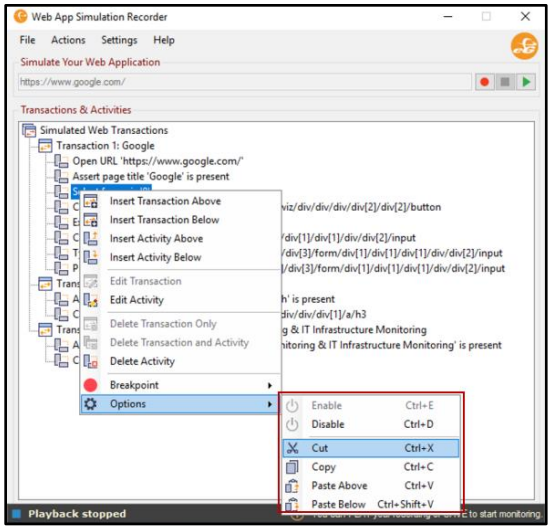


Figure 45: Support for Enable/Disable and Cut/Copy/Paste of a transaction/activity

- **Using Breakpoints to Troubleshoot Recorded Simulations:** Before v7.2, whenever a recorded transaction script failed, administrators had to playback the entire transaction script to identify the exact step that caused the failure. To enable administrators to quickly and accurately determine the reason why a transaction script failed, starting with this version, 'breakpoints' can be included in the script. A breakpoint is an intentional stop, where the execution of the user activity is paused/interrupted until the user continues playback. By introducing breakpoints at strategic stages of script execution, administrators can playback a script piece-meal – i.e., until breakpoints – instead of running the entire script. This eases problem analysis and root-cause isolation.

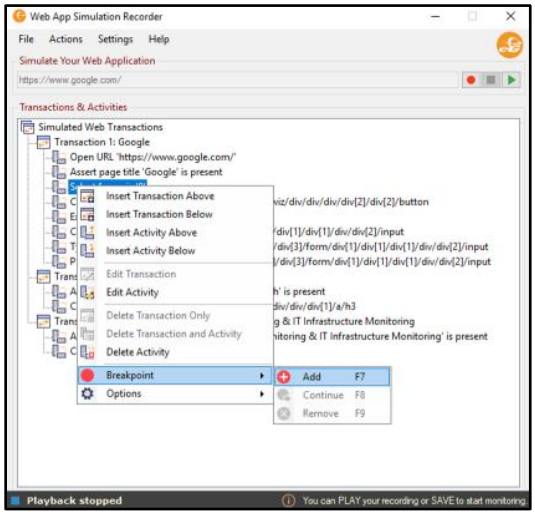


Figure 46:Adding Breakpoints

- **Introduced Additional Recorder Settings:**
  - **Set Default Wait Time Between User Activities:** Typically, when business is transacted over the web, some delay can be expected in page loading, or in performing an action, or when navigating across the pages of a web site. When computing the time taken by each step/user

activity therefore, the simulator should take into account these delays as well. This is why, starting with v7.2, you are allowed to set a default wait time between consecutive steps across the entire simulation. For this purpose, a **Default wait time to perform each activity** parameter has been introduced in the **Recorder Settings** of the Web App Simulation Recorder. Once the simulator is sensitized to such delays, alerts will be raised only if a step takes longer than the configured 'wait time', to execute.

- **Web App Simulation Works on Web Pages Without SSL Certificates**: An SSL certificate error occurs when a web browser cannot verify the SSL certificate installed on a site (e.g., untrusted certificate). Sometimes, you may want the web app simulator to bypass these errors when playing back a recording. To allow this, an additional **Allow browser to ignore certificate errors** flag has been introduced in the **Recorder Settings** of the Web App Simulation Recorder. By default, this flag is set to **No**. You can set this flag to Yes to have the simulator ignore SSL certificate errors.
- **Support to Use the Browser Settings of the User Performing the Simulation:** A typical browser profile is made up of your browsing preferences and history, including the cookies you have accepted; the bookmarks and passwords you have saved; the extensions, add-ons, and toolbar customizations you have added; your security and device SSO settings. In previous versions, whenever a web browser was launched during simulation, it was launched as a new browser window without any default user profile settings. This caused hardship in environments where simulations were performed on applications/desktops enabled with single sign-on. To avoid such hardship, starting with this version, browsers are allowed to load the default user profile settings. To this effect, an **Allow browser to load default user profile settings** flag has been introduced in the **Recorder Settings** of the **Web App Simulation Recorder** which can be set to **Yes**. By default, this flag is set to **No**.
- **Support for Automatic Playback of Script with Time Interval:** In previous versions, soon after recording the script, administrators had to manually playback the script more than once to verify the replay sequence and to look for errors/failures. To automate this process, starting with this version, an additional **Number of playbacks** parameter has been introduced in the **Recorder Settings** of the Web App Simulation Recorder. Administrators can use this parameter to set the number of times the script should be replayed soon after the completion of recording. Also, administrators can custom-define a time interval (in seconds) between two consecutive replays using the **Playback interval (secs)** parameter.

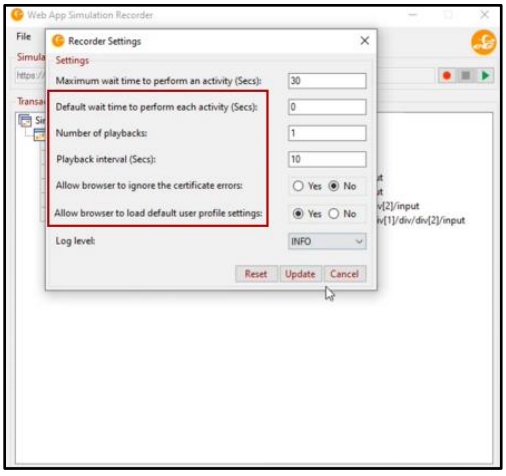


Figure 47: Additional Recorder Settings

- **Additional User Activities/Actions Introduced for Recording a Transaction:** Starting with this version, the user activities/actions introduced in Web App Simulation can help administrators

with the following:

- Verify the availability of a specified text in the target location;
- Verify the availability of a specified text in the Title of the website;
- Verify that the specified text is not present in the Title of the website;
- Verify that the specified text is not present in the target location;
- Verify the availability of a specified text in the URL of the website;
- Verify that the specified text is not present in the URL of the website;
- Assert web page navigation and refresh activities;
- Verify the process running on endpoint machine;
- Verify file-based and windows actions and
- Verify availability of an element and the time taken for it to appear in the web page.

- **Support for recording a transaction on a web page containing Text-based Captcha:** Multiple web sites use text-based captcha for authentication or additional site access. Starting with this version, Web App Simulation can input the dynamically created text captcha values automatically. For this purpose, administrators can pick the **StoreText** and **StoreValue** options from the **Activity** list of the **Add Activity** pop up window. **Note that eG Enterprise does not support capturing image-based captcha**.

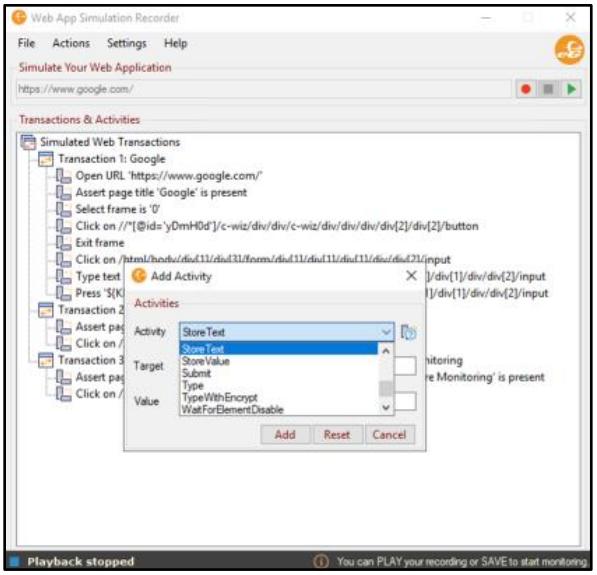


Figure 48: Adding the StoreText Activity

- Starting with this version, for the Web App Simulation to work, ensure that Microsoft .NetFramework

4.5 (or above) pre-exists on the system hosting the web app simulator agent/external agent.

4. Application Performance Monitoring

4.1 Microsoft .Net/Node.js BTM Enhancements

- **New .Net Core Business Transaction Monitoring Capability:** ASP.NET Core is the open-source version of ASP.NET, that runs on macOS, Linux, and Windows. .NET Core is ideal for cross-platform needs. Microservices architecture is supported in .NET Core, which allows cross-platform services to work with .NET Core including services developed with .NET Framework, Java, Ruby, or others.

  An ASP.NET Core app runs with an in-process HTTP server implementation. By default, it ships with a Kestrel web server, which is a cross-platform HTTP server implementation. The Kestrel web server listens for HTTP requests and surfaces them to the app as a set of request features composed into an HttpContext.

  Kestrel can be used by itself or with a reverse proxy server, such as Apache.

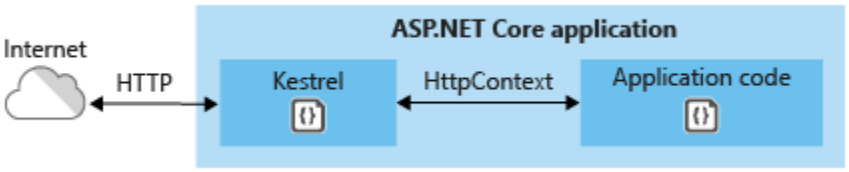


Figure 49: Kestrel used as an internet-facing web server

A reverse proxy server receives HTTP requests from the network and forwards them to Kestrel. Besides Kestrel, IIS web servers too support the .NET Core framework.

The eG .NET Core BTM is currently capable of monitoring transactions to web sites / web applications hosted on Kestrel web servers and IIS web servers.

To be able to track the live transactions to web sites on a Kestrel / IIS web server, eG Enterprise requires that a special eG .NET Core Profiler be deployed on that Kestrel / IIS web server.

If more Kestrel / IIS web servers are in the transaction path, then, the profiler will have to be installed on each of the web servers, for end-to-end visibility.

Typically, the requests to web site transactions are handled by dotnet.exe on a Kestrel / IIS web server. Whenever an end-user requests for a transaction, the Kestrel / IIS web server spawns a worker process (dotnet.exe) to service that transaction request. Upon receipt of a request, the worker process automatically invokes an instance of the .NET Core CLR to process the request. At the same time, the worker process also loads an instance of the .NET Core profiler.

Once the profiler latches on to a worker process, it injects a .NET Core code into the .NET Core application code to trace the complete path of the transaction. By doing so, it auto-discovers the applications the transaction travels through, and automatically ascertains what remote service calls were made by the transaction when communicating with the servers. This knowledge is then translated into an easy-to-understand cross-application transaction flow in the eG monitoring console.

Once the transaction path is determined, the eG .Net Core BTM measures the responsiveness of a transaction by computing the time difference between when the transaction started and when it ended. Using these analytics, the eG .Net Core BTM Profiler precisely identifies the slow, stalled, and

error transactions, and computes the count of such transactions. Intuitive icons and color-codes used in the graphical transaction flow enables administrators to accurately isolate where – i.e., on which Kestrel web server – the transaction was bottlenecked and what caused the bottleneck – is it an inefficient or errored function in the application code? or is it due to a database query that is taking too long to execute? By quickly leading administrators to the source of transaction failures and delays, the eG .Net Core BTM facilitates rapid problem resolution, which in turn results in the low downtime of and high user satisfaction with the Kestrel web server/IIS Web Server.

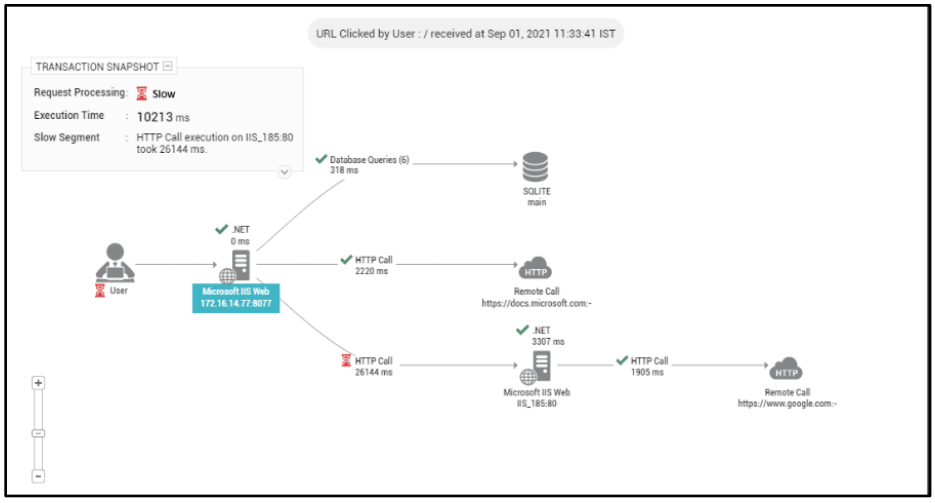


Figure 50: The cross-application transaction flow of a slow transaction captured by eG .Net Core BTM

- **Enhancements to Node.js Monitoring:** The Node.js monitoring model has been improved in eG Enterprise v7.2 to measure the performance of the transaction and provide in-depth code level insights. The eG Node.js Profiler employs an advanced 'tag-and-follow' technique to trace the complete path of each business transaction. When doing so, it auto-discovers the applications the transaction travels through, and automatically ascertains what remote service calls were made by the transaction when communicating with the servers. This knowledge is then translated into an easy-to-understand cross-application transaction flow in the eG monitoring console. Once the transaction path is determined, the eG Node.js Profiler BTM measures the total response time of each transaction, the time spent by the transaction on each application server, and the time taken for processing every external service call (including SQL queries). Using these analytics, the eG Node.js Profiler precisely pinpoints the slow, stalled, and failed transactions to the Node.js application server. Intuitive icons and color-codes used in the graphical transaction flow enables administrators to accurately isolate where – i.e., on which Node.js server – the transaction was bottlenecked and what caused the bottleneck – is it an inefficient or errored function in the application code? or is it due to a database query that is taking too long to execute? By quickly leading administrators to the source of transaction failures and delays, the Node.js application monitoring capability facilitates rapid problem resolution, which in turn results in the low downtime of and high user satisfaction with

the Node.js server.

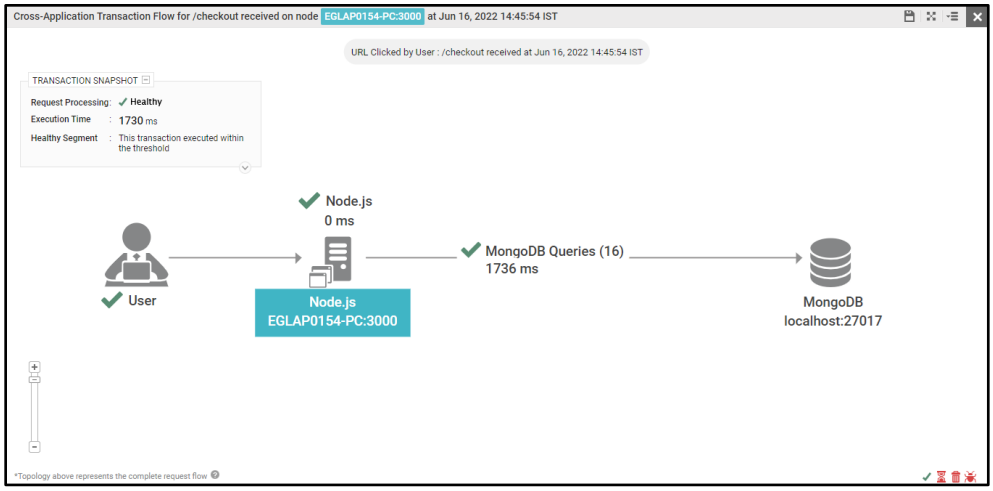


Figure 51: The cross-application transaction flow of a transaction to Node.js application captured by eG

eG Enterprise v7.2 also monitors the worker threads executing on the Node.js server, isolates those worker threads that are up for a lesser duration and reports them. The worker threads that use maximum heap memory are also reported.

- **Monitoring Microsoft .NET Application that uses Managed Windows Services:** Managed Windows Services enable administrators to build applications using .Net Framework. Though these applications lack a user interface, they run in unique Windows sessions and generally run in the background or remote locations. eG Enterprise v7.2 offers a new monitoring model named **Microsoft .NET Application** to monitor the .NET applications or .NET core applications that use Managed Windows Services.

  The eG .Net Profiler/eG .Net Core Profiler employs an advanced 'tag-and-follow' technique to trace the complete path of each business transaction. When doing so, it auto-discovers the applications the transaction travels through, and automatically ascertains what remote service calls were made by the transaction when communicating with the servers. This knowledge is then translated into an easy-to-understand cross-application transaction flow in the eG monitoring console. Once the transaction path is determined, the eG .Net Profiler BTM/.Net Core Profiler measures the total response time of each transaction, the time spent by the transaction on each application server, and the time taken for processing every external service call (including SQL queries). Using these analytics, the eG .Net Profiler BTM/.Net Core Profiler precisely pinpoints the slow, stalled, and failed transactions to the .NET application/.NET core application. Intuitive icons and color-codes used in the graphical transaction flow enables administrators to accurately isolate where – i.e., on which .NET application/.NET core application – the transaction was bottlenecked and what caused the bottleneck – is it an inefficient or errored function in the application code? or is it due to a database query that is taking too long to execute? By quickly leading administrators to the source of transaction failures and delays, the Node.js application monitoring capability facilitates rapid problem resolution, which in turn results in the low downtime of and high user satisfaction with the .NET application/.NET core application.

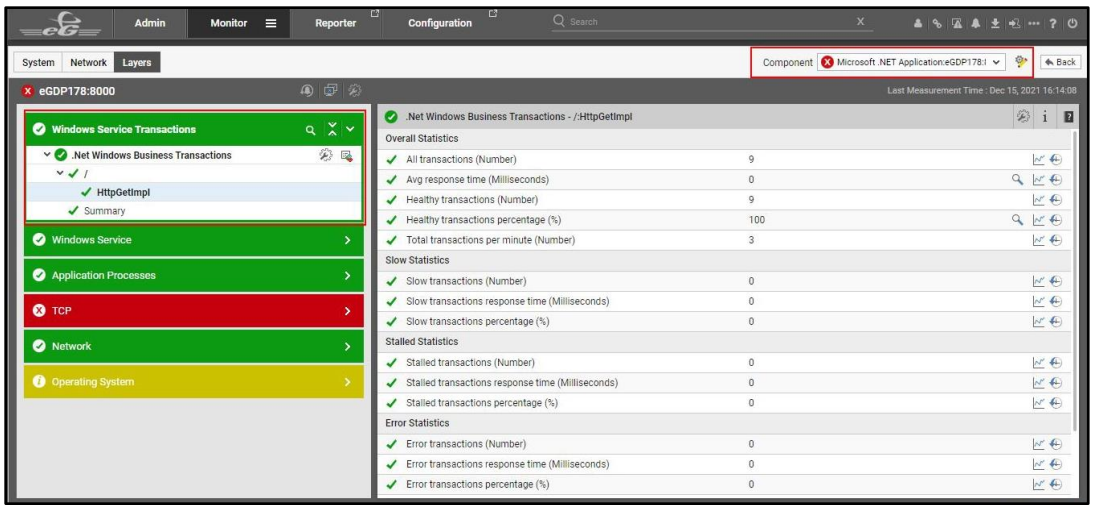


Figure 52: Monitoring the Microsoft .Net Application that uses Managed Windows Services

- **New Exit Call and Point Cut Support:** Starting with eG Enterprise v7.2, monitoring support is available to the following:
  - The eG PHP BTM now captures the time taken by NuSoap Webservice exit calls and Memcache exit points.
  - The eG .Net BTM now reports the time taken by external calls/queries to Azure Queue storage and NLog logger
  - The eG Java BTM now reports the time taken by external calls/queries using RabbitMQ AQMP protocol and JMS queues that use Jakarta JMS/Spring JMS. You can now trace transactions passing through Jakarta message queues and RabbitMQ message queues and topics.
  - The eG Java BTM now captures the time taken by Synapse Mediate Webservice calls and API calls to WSO2 API manager
  - The eG Node.js Profiler now captures the time taken by external calls/queries to Microsoft SQL Database and RabbitMQ AQMP protocol.

  The addition of these exit calls and point cuts provides administrators with more diagnostics related to where a transaction spends time (pinpoints the servers that are slow) and thus enables accurate root-cause identification of a transaction slowdown.

- **Support for New Point Cut:** Starting with this version, eG Node.js Profiler is capable of accurately capturing the time taken by the external calls/queries to RabbitMQ. Also, using eG Java BTM / eG Node.js Profiler, you can now trace transactions passing through RabbitMQ message queues and topics. The addition of these point cut provides administrators with more diagnostics related to where a transaction spends time (pinpoints the servers that is slow) and thus enables accurate root-cause identification of a transaction slowdown.

- **eG Java/.Net BTM now Captures Transaction Slowness Due to Asynchronous Thread/Task calls:** Starting with v7.2, the eG .Net BTM captures the execution time of the asynchronous calls (both asynchronous thread calls and asynchronous tasks) made by the .Net application. These calls and their duration also find a place in the Cross Application Transaction Flow

representation.

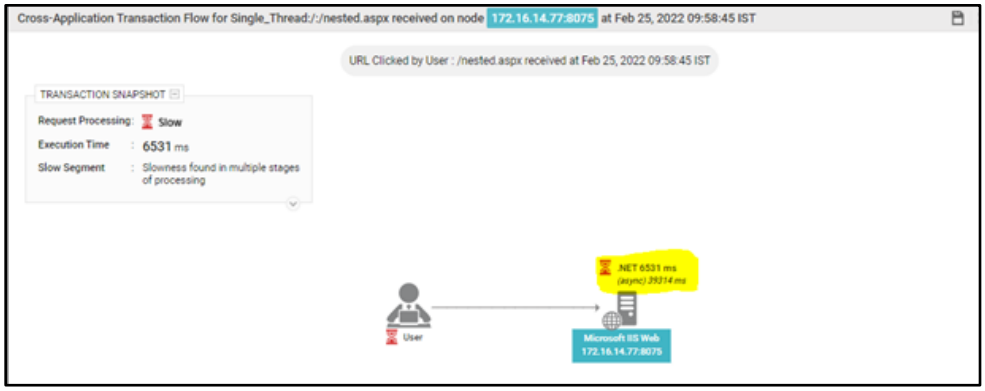


Figure 53: Slowness captured by eG .Net BTM due to asynchronous calls

Further drilling down an asynchronous call in the Cross Application Transaction flow, will reveal the exact thread/task that caused a delay in the transaction.

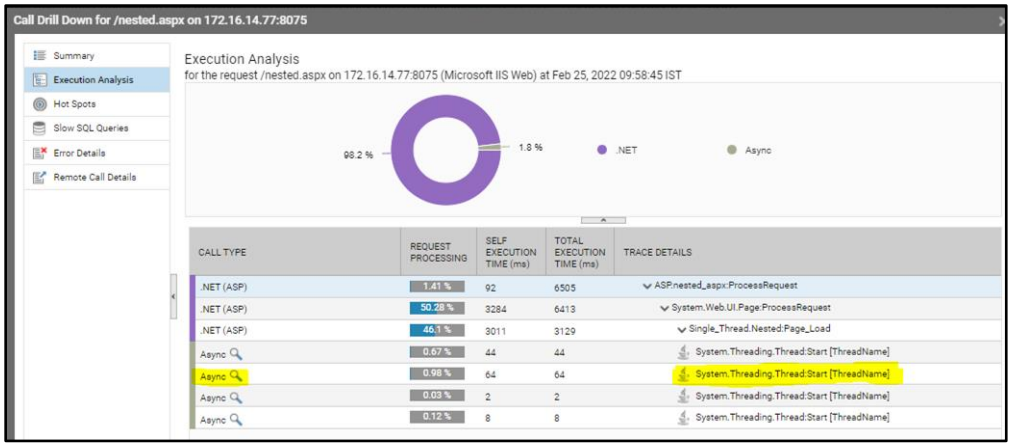


Figure 54: Tracing the exact asynchronous thread/task that was causing transaction slowness

- **Enabling/Disabling RUM-BTM Correlation:** Starting with this version, RUM-BTM correlation can be enabled for the eG PHP Business Transaction. For this, administrators need to set the **RUM_BTM_CORRELATION** flag available in the **eG_PHPBtm.ini** file (available in the **<eG_INSTALL_DIR>/agent/config** file) to **1**. By default, this flag is set to 0.

4.2 Enhancements to Java Business Transaction Monitoring

- **Configuring User Name and Business Context for Java Business Transactions Made Simpler:** As part of detailed diagnostics, eG BTM displays two columns, namely - User Name and Business Context. By default, these two columns will not display any values. This has been done so that administrators can use these columns to display any additional information that they deem useful for troubleshooting transaction slowness. In previous versions, administrators had to manually configure the rules for capturing usernames and business context for different URLs/URL patterns. This process was tedious, laborious, and error-prone. To help administrators save time, effort, and minimize errors when configuring these rules, a special page is now available in the eG administrative interface. This page appears if you click on the icon alongside the newly-introduced

USERNAME/BUSINESS CONTEXT CONFIGURATION parameter of the **Java Business Transactions** test. Once the special **Username/Business Context Configuration – Rule List** page appears, you can use the intuitive fields and smart controls in the page, and quickly build rules for capturing usernames and business context for different URLs/URL patterns.

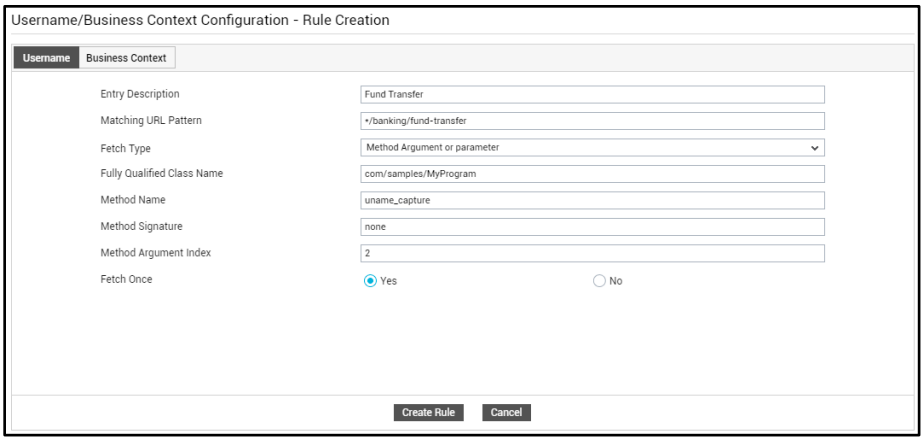


Figure 55: Configuring a rule for capturing user name

- **Accurately Diagnosing the Root-cause of a Database Query Failure/Slowness , which Lead to Poor Transaction Performance:** In previous versions, the **Slow SQL Queries** section of the **Call Drill Down** page (that appears when you drill down from a problematic database server in the **Cross Application Transaction Flow** page) listed the database queries that may have caused a transaction to slow down From this list, you can figure out which queries run by the slow transaction were slow or simply failed to execute. Sometimes, a persistent, underlying database server issue may manifest as a query failure or slowness. For instance, if the database server is rapidly running out of tablespace, then queries run on that server will fail for want of space. Administrators will be able to quickly and effectively troubleshoot transaction slowness only if they know what is impeding query execution. For this purpose, in v7.2, an additional **RELATED ALERTS** column has been introduced in the **Slow SQL Queries** section. If the database server in question is also managed by eG Enterprise, then clicking the **Diagnosis** icon in the **RELATED ALERTS** column will reveal the alerts that were raised by eG Enterprise for that database server when the transaction was recorded. By analyzing these alerts, administrators can swiftly and accurately diagnose the root-cause of transaction slowness.

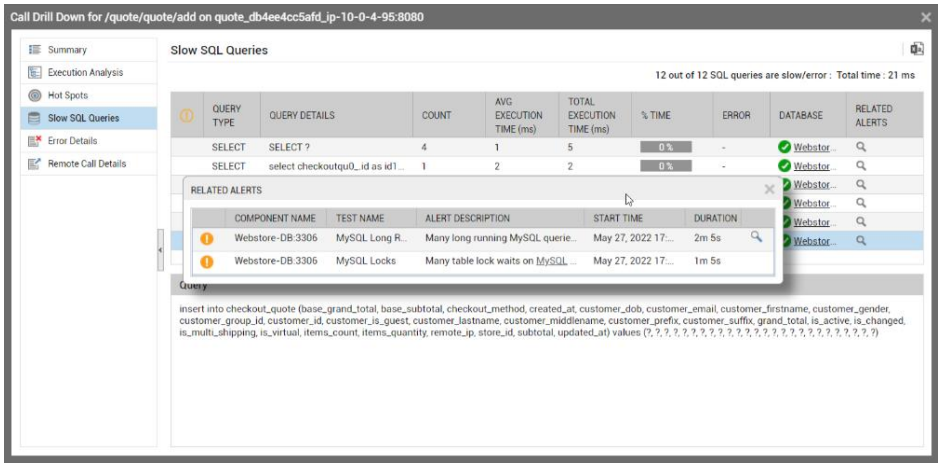


Figure 56: Displaying alerts for the database on which a query that caused slow transaction was executed

4.2.1 New Reports for eG Business Transaction Monitor

Following are the new reports that have been included in eG Enterprise v7.2 with respect to Business Transaction Monitoring:

- **Problem Analysis Report:** In today's era, user experience is key to the success of business-critical web services that an enterprise offers to its customers. Frequent complaints from end-users regarding web transaction failures, errors, or slowness, if left unnoticed/unattended, can escalate support costs, lengthen the troubleshooting curve, increase service downtime, reduce revenue, and damage the reputation of an enterprise. To avoid this, administrators should be able to proactively detect poor transaction performance well before users complain, and accurately pinpoint where the bottleneck is – is it in the client-side? the server-side? the JVM/container? the network? or in the backend infrastructure supporting the application? To help administrators in this regard, eG Enterprise v7.2 offers the Problem Analysis report. This report helps administrators historically analyze the end-to-end performance of a web service, instantly determine whether/not users are 'happy' with the service and isolate the broad problem areas at-a-glance.

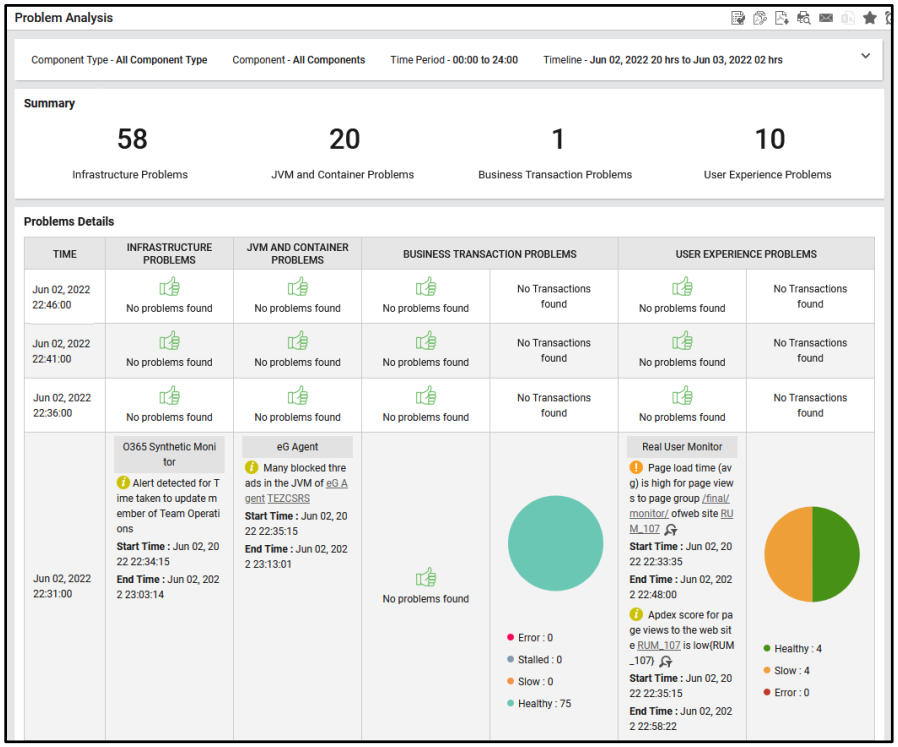


Figure 57: Problem Analysis Report

- **SQL Performance Report:** Sub-optimal / erroneous SQL queries are common causes for poor web transaction performance. If a web transaction frequently runs an inefficiently structured SQL query on its backend database server, that transaction will always be lethargic. Likewise, if a web transaction often runs SQL queries that use poor/incorrect syntax, then such queries will fail frequently, causing the web transaction to fail as well. As a result of these abnormalities, such a web transaction will consistently deliver a sub-par experience to users. To always assure web application users of a superlative experience, administrators should:
  - Look back at the web transactions processed by a target web application in the past;
  - Identify those transactions that consistently spent too much time in the database tier

processing SQL queries;

- Isolate those queries that often threw errors or were regularly slow in execution, and optimize them for better performance;

This is where the SQL Performance Report of v7.2 helps! This report helps administrators historically analyze the performance of business transactions based on SQL queries they execute. In the process, administrators can:

- At-a-glance, identify those business transactions that were consistently slow in SQL query execution;
- Isolate the precise SQL queries that often took too much time to execute;
- Identify the exact queries that frequently executed with errors.

By closely reviewing the result-set of this report, administrators can pick those queries that should be optimized, so that web transaction performance improves, and user experience remains above-

par thus gaining more 'happy' users.

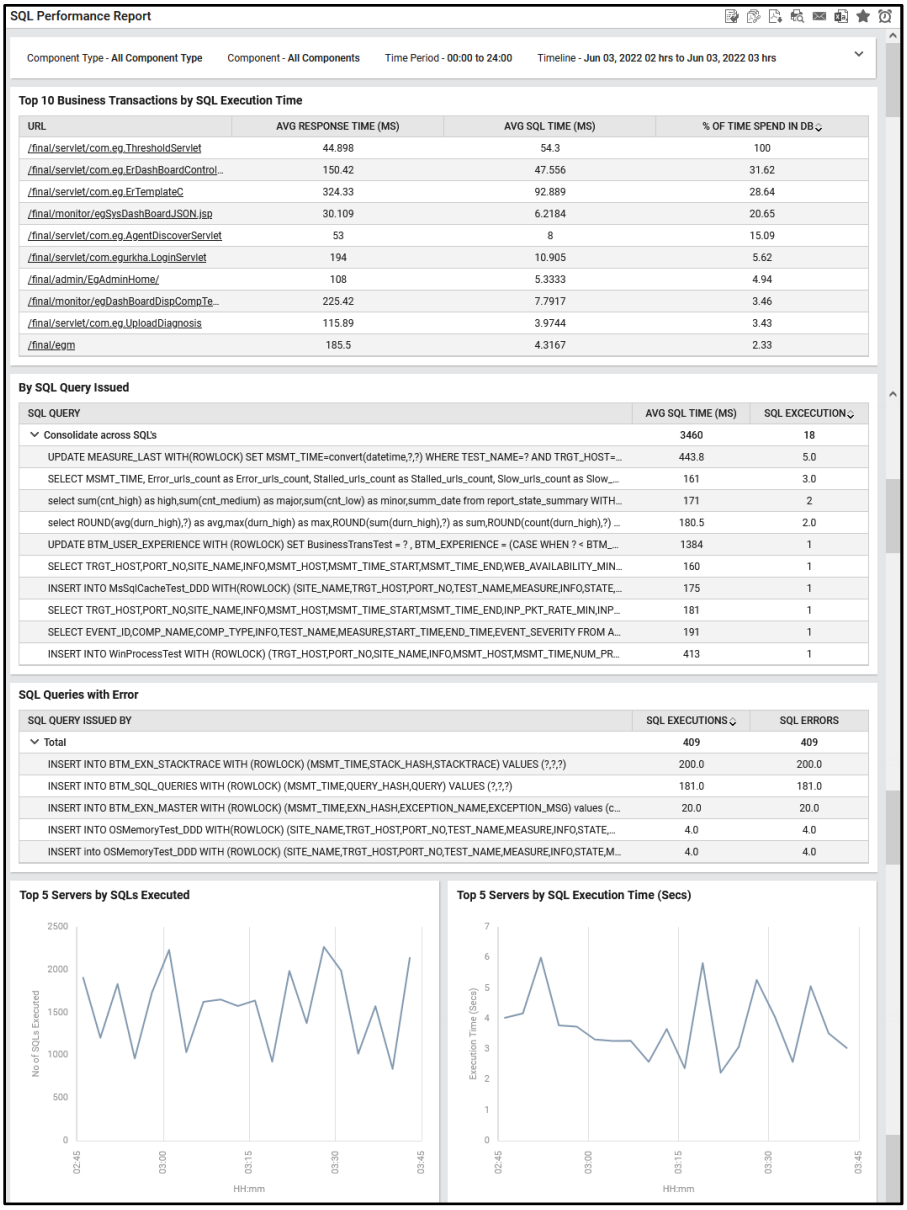


Figure 58: The SQL Performance Report

Exceptions Trend Report: The Code-Level Exceptions report offered by eG Enterprise helped administrators understand which URLs were affected due to a code-level exception and what were the exceptions that were frequently encountered by a business transaction. While this report helped in identifying the affected exceptions and URLs, administrators were still left in large in identifying how well the exceptions fared over a period of time. To historically analyze the trend of exceptions over a period of time, eG Enterprise v7.2 offers the **Exceptions Trend** report. By carefully analyzing this report, administrators can identify the top exceptions based on the number of occurrences, the time elapsed since each exception lastly occurred and compare if each exception is trending up or down for a selected look back period. Also, administrators can visually identify the trend of all exceptions over time. Administrators are also directed to the top tiers or JVM

instances that experienced the exceptions frequently.

Figure 59: The Exceptions Trend Report

4.3 Java Application Servers Monitoring Enhancements

- **Monitoring Jetty Application Servers:** Jetty is an open-source Java web server, as well as a servlet container, that provides an application with the features required to launch and run an application servlet or API. eG Enterprise v7.2 monitors the Jetty Application server, checks its operating system and JVM for resource contentions, and alerts administrators if the OS/JVM should be right-sized. Business transactions to the Jetty Application server too can be monitored and the transactions that are slow/stalled/error-prone can be isolated. eG Enterprise v7.2 also monitors the Jetty Application server that is installed as an embedded servlet container used by the Spring Boot web starter.
- **Identifying the Web Applications that are stopped on an IBM WebSphere Application Server:** Sometimes, a web application deployed on a WebSphere Application Server may be stopped for maintenance or for debug activity. During such times, users may not be able to access the application. Also, in some environments, the web application would have stopped abruptly.

Regardless, the unavailability of the web application can scar user experience with it. To enhance user experience with critical web applications on WebSphere, it is important to promptly identify the applications that have stopped running. This is now possible with eG Enterprise v7.2! Starting with this version, eG Enterprise reports the status of each web application deployed on the IBM WebSphere Application server. The web applications that are in 'Stopped' state can be isolated and the reason for the same can be determined. This way, the problem can be rapidly fixed, so that the web applications become operational and accessible again.

- **Identifying Failed and Overloaded Web applications on Oracle WebLogic Application Servers:** When a web application fails, the users may not be able to access that web application leading to poor user experience. Similarly, when a web application is overloaded, users may experience slowness. To improve the user experience, administrators should identify those web applications that have failed or are overloaded. Starting with this version, the count of web applications that are in various states such as Warning, Critical, Failed and Overloaded are captured and reported. The detailed diagnostics reveals the exact name of the web applications that are in different states.

- **Automatically Discovering the Name of Oracle WebLogic Server Instance to be Monitored:** An Oracle WebLogic Application server hosted on a containerized environment can be auto-discovered and auto managed by eG Enterprise by default. Previously however, to collect metrics from an auto-managed WebLogic server, administrators had to first reconfigure its tests and manually specify the exact server instance to be monitored in the test configuration page. Version 7.2 dispenses with the need for this manual intervention! To ensure that an auto-managed Oracle WebLogic Application server starts reporting metrics immediately the SERVER parameter of the eG tests is now set to *EG_ENV_SERVER_NAME* by default. This ensures that eG Enterprise automatically discovers the server instance name of the auto-managed WebLogic server, and auto-configures the SERVER parameter with that name.

- **Enhancements to Tomcat Monitoring:** Starting with this version, eG Enterprise reports the number of connections that are available (connections that are not used/idle) in each connection pool configured on the Tomcat server and the percentage of connections that are available. By carefully analyzing these measures, administrators can turn the spotlight on connection pools that are incorrectly sized and could hence be a threat to application performance. eG Enterprise also captures useful metrics related to different connection pool types such as C3P0, Hikari, Druid and BoneCP.

- **In-depth Monitoring of WAR files deployed on Wildfly/JBoss Servers:** In previous versions, when a war file deployed on a Wildfly/JBoss server failed, administrators could not instantly figure out which war file failed. To troubleshoot WAR file failures at a faster pace, starting with this version, eG Enterprise auto-discovers the WAR files deployed on a target Widfly/JBoss server and reports the WAR file that failed/stopped.

- **Identifying Memory Leaks Caused by Objects that are Pending Finalization:** A Garbage collector reclaims memory from only those objects that are unreachable, abandoned, or unwanted. Unreachable objects are those that are not referenced by any other live objects in JVM. Sometimes, GC may find that an object is 'unreachable', but that it continues to be associated with certain native resources such as, file handles, images, fonts etc. In such cases, GC adds the object to the finalization queue. Finalization performs final operations or cleanup operations on objects to reclaim the native resources associated with those objects, before those objects are garbage collected. If too many objects are pending finalization, then it indicates that the objects are still occupying the JVM memory space and are unable to be reclaimed by the GC. This may result in memory leaks if left unattended and may cause application failures/crashes. To ensure that the memory leaks are detected at the earliest, starting with this version, eG Enterprise offers a brand-new **JVM Summary** test which when executed reports the count of objects that are pending finalization. Also, JIT compilation time is also reported which helps administrators in optimizing memory usage and reducing page faults.

5. Enterprise Application Monitoring

5.1 Enhancements for SAP Monitoring

eG Enterprise v7.2 has expanded its SAP monitoring capabilities to support new SAP applications such as SAP BTP Neo and SAProuter. SAP BOBI monitoring has also been enhanced.

- **Monitoring SAP BTP Neo:** SAP Business Technology Platform (SAP BTP) brings together intelligent enterprise applications with database and data management, analytics, integration, and extension capabilities into one platform for both cloud and hybrid environments, including hundreds of pre-built integrations for SAP and third-party applications. If application performance degrades or if database access slows down, user experience will be adversely impacted. As a result, help desk will be flooded with complaints and support requests from users, troubleshooting costs and time will soar, and critical business opportunities will be lost. To avoid this, eG Enterprise v7.2 monitors the SAP BTP Neo platform, proactively alerts administrators to potential issues in the availability, resource usage, and overall health of the platform, and enables them to initiate appropriate remedial action, before users complain. This eG Monitor:
    - Reports the availability and status of each Java application and SAP HANA XS application, and promptly sends out alerts if any application is unavailable;
    - Tracks the status of the processes executing on the Java applications , and promptly captures and reports the processes that have stopped;.
    - Pinpoints Java applications that failed to be uploaded and reveals the reason for upload failures, so as to ease troubleshooting;
    - Periodically checks the status of the files in the Java applications , and highlights the unavailable files.
    - Monitors the disk space usage of the Java applications , and points to those file directories that are hogging disk space
    - Sheds light on resource-intensive processes;
    - Verifies the status of the services of each SAP ASE database and SAP HANA database, pinpoints services that are in a 'critical' state, and reveals the reason for the abnormal state;
    - Alerts administrators to databases that are running out disk space, or are engaged in I/O-intensive processing;
    - Isolates VMs that have stopped / failed;
    - Turns administrator attention to error-prone VMs / volumes / snapshots;

  eG Enterprise v7.2 also offers a One Click SAP Neo Dashboard that reports key performance metrics such as the status of Java Applications, HTML5 Applications and HANA XS Applications. This dashboard helps administrators assess the performance and resource utilization of the applications and identify those applications that are experiencing slowdowns at a single glance.

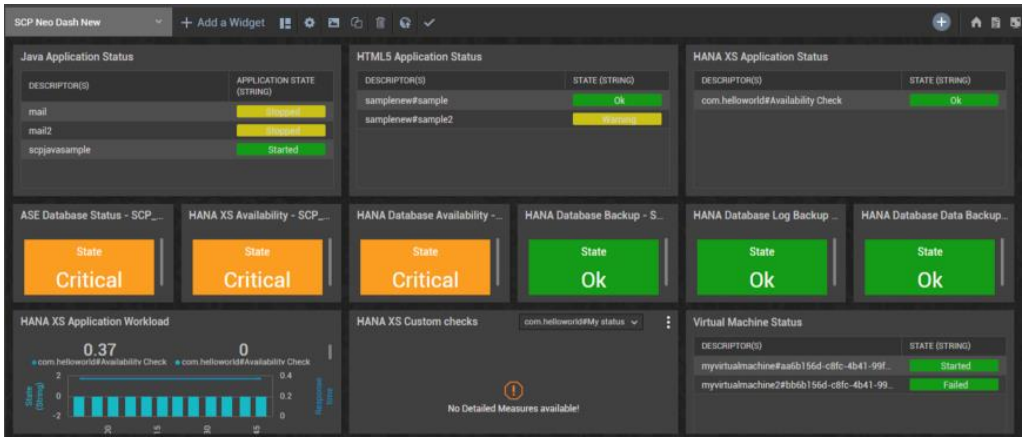


Figure 60: One Click SAP Neo Dashboard

- **Monitoring SAProuter:** SAProuter is a standalone program that protects your SAP network against unauthorized access. Since issues in the availability and overall performance of the SAProuter can threaten the safety and security of the SAP network, eG Enterprise v7.2 offers a dedicated SAProuter monitoring model, which promptly captures such issues, brings them to the notice of administrators, and enables them to take action before network security is compromised. The availability and uptime of the SAProuter is monitored, and administrators alerted if there is any break in availability. The validity period of SSL certificates is periodically checked, and certificates nearing expiry are highlighted, so that administrators can rapidly initiate measures to prevent certificate expiry and resultant connectivity issues. The logs on the SAProuter are periodically monitored and log files on which maximum errors were logged are identified. The count of client connections to each host is reported and the host with maximum number of connections is determined.

  eG Enterprise v7.2 offers an exclusive One Click SAProuter Dashboard that helps administrators obtain an at a glance view of the number of client connections, log errors, SSL Connection validity time etc.

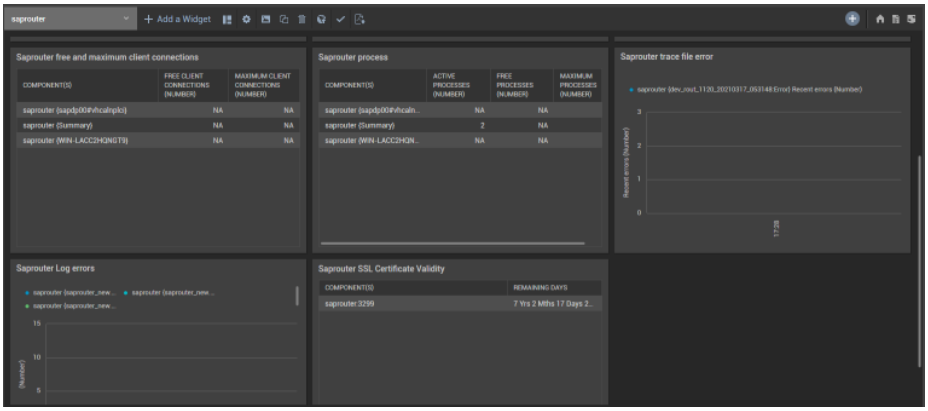


Figure 61: One Click SAProuter dashboard

- **Enhancements to SAP BOBI:**

  Following are the enhancements made to SAP BOBI monitoring in eG Enterprise v7.2:

  - SAP Lumira is a self-service data discovery and visualization tool that allows users to find and analyze relevant business data and create custom interactive dashboards and analytics applications. eG Enterprise v7.2 is capable of monitoring SAP Lumira when integrated with SAP BOBI. eG Enterprise v7.2 provides in-depth insights into the status and overall performance of each Lumira server process. Log files of each Lumira server process are periodically parsed for

error messages, This enables administrators to accurately isolate error-prone server processes, closely study the errors they encounter frequently, and rapidly troubleshoot those errors

- The health of each service running on a specific SAP BOBI node is monitored and the services that failed are promptly captured and reported.

5.2 Other Enterprise Application Monitoring Enhancements

➢ **Enhancements to Siebel Application Server Monitoring:** Starting with this version, eG Enterprise captures the count of tasks that are executing for each type of task on the target Siebel Application server for a duration beyond a specified cutoff time. The task ID and the start time of the task is promptly reported as part of the detailed diagnostics.

6. Cloud Monitoring

6.1 AWS Monitoring Enhancements

➢ **New Dashboard Introduced for AWS / Microsoft Azure Monitoring:** eG Enterprise v7.2 provides an AWS Dashboard / Azure Dashboard, using which, administrators can figure out the answers to the following questions:

- Is the service healthy?
- Are there any EC2 Instances/VMs in powered off state? If so, how many EC2 instances/VMs are powered off?
- Are there any alerts raised based on the resource utilization on the EC2 instances/VMs? If so, which type of resource utilization was the major reason behind such alerts – is it CPU? or Disk? or Network?
- Is the distribution of EC2 instances/VMs consistent? How many large/xlarge/medium EC2 instances are currently distributed across the target environment?
- Are there any powered off EC2 instances/VMs across different geographic locations? If so, which geographic location contains maximum number of powered off Ec2 instances/VMs?
- Are EC2 instances/VMs newly added/removed from a specific region during the last 7 days? If so, which regions gained/lost the maximum number of EC2 instances/VMs?
- Are specific EC2 instances/VMs draining the resources allocated to them over a period of time? If so, which are those EC2 instances/VMs that are constantly topping the resource utilization graphs?

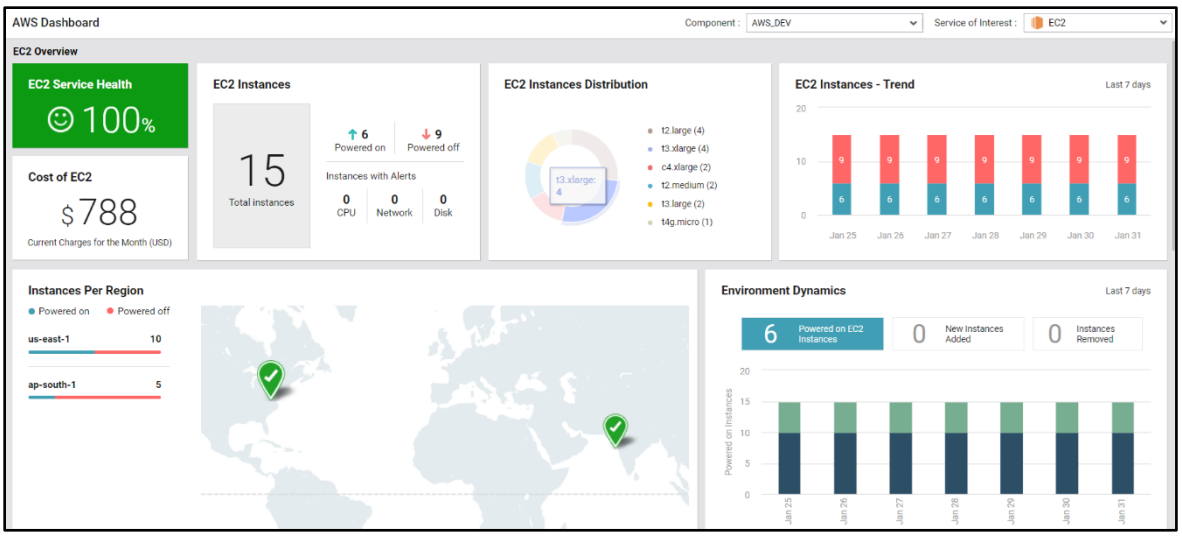


Figure 62: The AWS Dashboard

The AWS Dashboard also provides in-depth insights into Amazon RDS service and Amazon EBS.

- **Use Roles for AWS Monitoring:** In previous versions, eG Enterprise used the AWS Access Key and AWS Secret Key to connect to the AWS Cloud and make API calls to pull metrics. These keys were passed as input parameters for eG tests run on the Amazon Cloud. Though this monitoring approach was hassle-free, cloud administrators often found themselves having to change these keys frequently, owing to security mandates from Amazon. As a result, administrators had to reconfigure the eG tests, every time the key values changed. This was proving to be painful for administrators! To avoid this rigmarole and unburden administrators, eG Enterprise v7.2 is capable of monitoring the AWS Cloud using the **AWS Role** and **AWS Account ID** besides using the AWS Secret Key approach. For this purpose, an **ACCESS TYPE** flag has been included in the Test Configuration page. By default, the **Role** option is chosen against this flag. Upon providing the **AWS ACCOUNT ID TO MONITOR** and **AWS ROLE NAME**, the eG agent starts collecting the required metrics from the AWS Cloud. This approach is more secure and convenient for administrators. Administrators are even allowed to define an AWS Role exclusively for monitoring purpose. However, if you still wish to make use of the AWS Access Key and AWS Secret Key to connect to the AWS Cloud and pull the metrics, you can do so by choosing the **Secret** option against the **ACCESS TYPE** parameter.

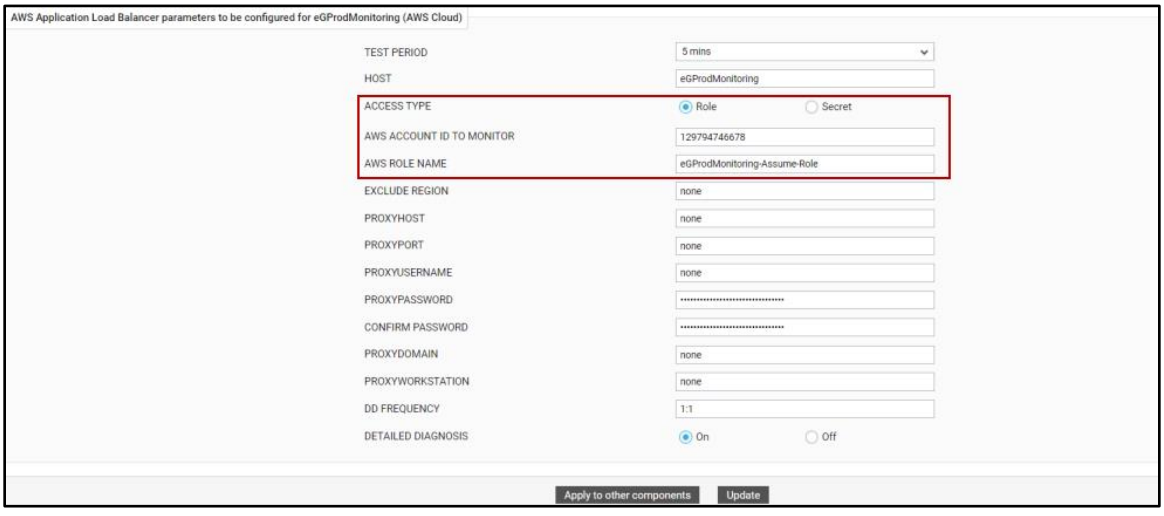


Figure 63: Specifying the AWS Role to monitor AWS Cloud

- **Support for Additional metrics:** Version 7.2 of eG Enterprise provides enhanced monitoring of AWS Cloud. The AWS Trusted Advisor feature of the Amazon Web Services Support service is monitored, and the estimated monthly savings is tracked. The action recommendations obtained helps administrators in cost optimization of the AWS Cloud environment. By monitoring the AWS S3 service, administrators can track the uploads/downloads to each S3 bucket and in the process, accurately identify the S3 bucket that is degrading the quality of the S3 service. The billing of each organization account is tracked, and the alerts are sent out when the bills grow beyond an expected limit. The billing of each AWS service/EC2 component is monitored and the AWS service/EC2 component with maximum bill amount is identified. Also, the detailed diagnostics further reveals the top EBS Volumes, Snapshots, Elastic Ips that are contributing to the billing cost. The AWS Lambda functions available on an AWS account is closely monitored and the functions that are recently added/deleted are promptly reported. The detailed diagnostics further reveals the name of the Lambda function and the date on which the function was modified. Each AWS API Gateway is monitored, and the count of client-side errors are promptly captured and reported. This way, the API Gateway that is prone to errors is identified. The time elapsed when each API Gateway routes/receives a request/response to/from the client/backend client is periodically monitored and the API Gateway that is experiencing abnormal latencies is isolated.
- **Monitoring Amazon Connect:** Amazon Connect is an easy-to-use omnichannel cloud contact center that helps you provide superior customer service at a lower cost. eG Enterprise v7.2 is capable of monitoring Amazon Connect and reports useful performance metrics. Using the eG Monitor for Amazon Connect, administrators can figure out whether/not the Amazon Connect Instance is active and whether/not inbound and outbound calls are enabled. The status of the agents is monitored and the agents in 'Error' and 'Offline' status are identified. The overall performance of the contact center is monitored and discrepancies in call/chat handling between the agent and contact are brought to light. Real-time metrics on chats/calls/tasks are monitored and the performance of the agents are evaluated periodically. By studying the variations to these metrics over time help administrators assess the overall performance of the agents and identify where exactly customers are dissatisfied – is it owing to the average call handling time? or is it due to agent interaction time? or queue time? or hold time? The data sent to Cloudwatch from Amazon Connect is also periodically monitored, and alerts are sent out if there are missed calls, throttled calls, and packet loss.

6.2 Microsoft Azure Monitoring Enhancements

With eG Enterprise's v7.2 Microsoft Azure monitoring capabilities have been significantly enhanced. Also, a host of new Microsoft Azure components have been included in the scope of monitoring. Let us now discuss each of the enhancements in detail:

- **Enhancements to Monitoring Microsoft Azure Subscription:** Starting with this version, the existing Microsoft Azure component has been renamed as Microsoft Azure Subscription. This is because, eG Enterprise maps the Azure component with an Azure subscription. This way, it is easier to align monitoring users and entities with subscriptions. The monitoring capabilities of Microsoft Azure Subscription have also been enhanced significantly to report a host of additional metrics.
    - Each configured Azure Firewall is monitored, and the status and health are reported periodically. Alerts are also sent out if the firewall's ability to differentiate between malicious and non-malicious traffic is compromised.
    - Each VPN Gateway is periodically monitored, and the bandwidth/throughput used by the tunnels of the gateway in real-time is closely computed. The incoming/outgoing traffic through each VPN Gateway is measured round the clock and administrators are alerted to abnormal traffic levels. Issues that can impede smooth communication over the network such as unexpected gateway failures, packet drops, sudden route disconnects, and revoked certificates are also promptly captured and reported.
    - The resource utilization and status of each Azure VM is periodically captured and the resource-

hungry VMs are promptly isolated.

- Azure Activity log monitoring has been improved to report the events belonging to Autoscale and Recommendation categories. The write operations that failed are also captured promptly by reading the Activity logs.
- The health of the services offered by Microsoft Azure is periodically monitored and the count of services in warning and critical states are reported. Further, the detailed diagnostics reveals the services that are in critical state.
- Each capacity pool created in each NetApp account configured for the target Azure subscription is periodically monitored and the capacity pool that is experiencing a space crunch is identified. The service level configured for each capacity pool is revealed using which administrators can figure out which service level, QoS type, and capacity combination will help maximize the throughput and overall performance of their capacity pools.
- Each volume configured for each Resource group is monitored and the volume that has exhausted the allocated capacity is identified. Administrators are also promptly alerted to high latencies noticed in I/O processing on any volume. The replication activity on each volume is scrutinized to eliminate replication bottlenecks and to avoid data loss during disaster recovery.
- The status of the backup jobs that have been triggered for an Azure Subscription is monitored and the count of jobs in each state is reported. The jobs that have failed and those that are running for a longer duration are highlighted.
- Resource usage of each resource (that Azure services subscribed to) is tracked, and administrators are alerted if actual usage is dangerously close or has exceeded the usage limit set for each resource.
- The CPU, memory, network, and disk I/O resources used by each scale set is monitored and the scale sets that are running resource-intensive applications are promptly isolated.
- The Azure subscription is monitored periodically to identify unused, wasted and orphaned resources (disks, network interfaces, load balancers, resource groups etc). This helps administrators in reducing the cost spent unnecessarily on Microsoft Azure.

- **Monitoring Microsoft Azure Active Directory:** In previous versions, Microsoft Azure administrators monitored the users, groups, directory role and audit logs that are part of the Azure Active Directory by managing the Microsoft Azure component offered by eG Enterprise. In recent times, many organizations are focusing more on cloud-based infrastructures and hence, the requirement to perform in-depth monitoring of those cloud-based infrastructures had reached a new high! To meet the needs of such organizations, eG Enterprise v7.2 has introduced an exclusive monitoring model to monitor Microsoft Azure Active Directory. Besides monitoring the users, groups, directory role and audit logs that are part of the Azure Active Directory, eG Enterprise v7.2 focuses on tracking the devices that are stale and are removed from the Azure Active Directory. Alerts are also raised when issues such as certificate expiry, client-secret expiry are detected and reported. Administration activities such as adding/removing users, groups, app registrations etc are periodically monitored and abnormalities are promptly reported and rectified. The Azure Active Directory sign-in logs are periodically monitored, and alerts are raised whenever a suspicious activity is captured and reported. Non-interactive user sign ins which are often associated with critical key services and targeted by malicious third-parties are periodically monitored and anomalies are identified at the earliest. The logins are monitored based on IP addresses, geo location and users so that common attack patterns are identified with ease.
- **Monitoring Microsoft Azure AD Connect:** Azure AD Connect is an on-premises Microsoft application that's designed to meet and accomplish your hybrid identity goals. eG Enterprise v7.2 monitors the Microsoft Azure AD Connect and reports a slew of metrics. Errors and configuration issues of the AD Scheduler are captured, and alerts are raised periodically. Authentication failures, synchronization cycle progress failures, and synchronization delays are periodically captured and

reported. Errors and Warning messages logged in the event logs of the Microsoft Azure AD Connect are promptly captured and reported. The Azure AD Federation Services are periodically monitored and unhealthy services as well as federation servers connected to such services are highlighted in the process. The health of the Azure AD Domain services is monitored, and administrators are notified of failures (if any). Synchronization errors are promptly captured and reported along with the type of error – is it duplicate attributes? or data mismatch? or data validation failure? or large attributes?

- **Monitoring Microsoft Azure Load Balancers:** Azure Load Balancer operates at layer 4 of the Open Systems Interconnection (OSI) model. It's the single point of contact for clients. Load balancer distributes inbound flows that arrive at the load balancer's front end to backend pool instances. These flows are according to configured load-balancing rules and health probes. The backend pool instances can be Azure Virtual Machines or instances in a virtual machine scale set. With Azure Load Balancer, administrators can scale the applications and create highly available services. Load balancer supports both inbound and outbound scenarios. Load balancer provides low latency and high throughput and scales up to millions of flows for all TCP and UDP applications. eG Enterprise v7.2 auto-discovers the Microsoft Azure Load Balancers that are available in the target Microsoft Azure environment. For each Managed Azure load balancer, eG reports a variety of useful metrics. The provisioning status and the health of each load balancer is reported. Statistics on the data transmitted through each load balancer helps administrators isolate the time periods when load peaked. The SYN ports are also periodically monitored and abnormal utilization of the SYN ports is promptly captured. By analyzing the count of outbound/inbound NAT rules, load balancing rules, backend pools and health probes, administrators can figure out if load balancer is adequately configured to handle high volume traffic in a swift manner.
- **Monitoring Azure Traffic Managers:** Azure Traffic Manager is a DNS-based traffic load balancer. This service allows you to distribute traffic to your public facing applications across the global Azure regions. Traffic Manager also provides your public endpoints with high availability and quick responsiveness. eG Enterprise v7.2 automatically discovers Microsoft Azure Traffic Managers in the target environment and reports a host of useful performance metrics. The status of each Traffic Manager profile is extensively monitored and the profiles that are disabled are isolated. The count of endpoints i.e., application deployments supported by each profile is reported. The detailed diagnostics offered by eG Enterprise helps isolate the endpoints that are degraded. The queries processed by each profile is carefully analyzed and the profile that is busy processing maximum number of queries is identified.

6.3 Other Monitoring Enhancements for Cloud / SaaS Applications

- **Monitoring Panzura Cloud File System:** Panzura's global cloud file system CloudFS transforms cloud storage into high-performance, high intelligence data management environment by giving distributed teams rapid, secure file access to a single, authoritative data source. By delivering a single file system across hundreds of offices, CloudFS™ allows users to work together as if they were in the same room. eG Enterprise v7.2 offers to monitor the Panzure Cloud File System and reports a host of metrics. The CPU, memory and space utilization of the Panzura Cloud File System is periodically monitored and resource contentions, if any are brought to light. Each hard disk of the Panzura Cloud File System is monitored and the hard disk that is running out of storage space is identified. The performance of the Panzura Cloud File System is periodically assessed and file upload and download failures are promptly captured and reported. The efficiency of the caches is periodically monitored and the cache that is experiencing slowdowns/delays is identified. The load on the Panzura Cloud File System is measured by constantly monitoring the count of users connected to the file system. This way, malicious attack on the cloud file system can be proactively averted.
- **Enhancements to Salesforce monitoring:** In previous versions, sometimes, the tests executed for monitoring Salesforce failed to report metrics. This was noticed in environments where the IP

address of the eG remote agent monitoring Salesforce was not within the trusted IP range specified by the target environment. For uninterrupted monitoring of Salesforce in such environments, a security token had to be appended to the password of the user who is authorized to execute API commands on Salesforce to pull the required metrics. To this effect, a **SECURITY TOKEN** parameter has been included in the test configuration page for the tests pertaining to Salesforce, in v7.2.

7. Virtualization and Container Monitoring

7.1 Monitoring Container Environments

Following are the enhancements that have been made to monitor the Container environments in eG Enterprise v7.2:

- **Monitoring Container Engines:** CRI-O is an open source, community-driven container engine. Its primary goal is to replace the Docker service as the container engine for Kubernetes implementations, such as OpenShift Container Platform. The CRI-O container engine provides a stable, more secure, and performant platform for running Open Container Initiative (OCI) compatible runtimes. eG Enterprise v7.2 monitors the RHEL CoreOS/CRI-O Container engines and reports the current status of the container engine. The uptime of each container/pod is periodically monitored, and abnormalities (if any) are reported. The number of containers is tracked, and administrators are alerted if any container has stopped running or has been removed/paused. The images are periodically monitored and if any image is not mapped to the containers, administrators are duly notified. The resource utilization of each container is tracked periodically, and the resource hungry containers are isolated.
- **Monitoring Podman:** Podman is a daemonless container engine for developing, managing, and running OCI Containers on your Linux System. Podman manages the entire container ecosystem which includes pods, containers, container images, and container volumes. eG Enterprise v7.2 monitors Podman, checks whether/not the Podman service is installed, and if it is, verifies the status of the Podman service. Administrators are alerted if the service is down. The uptime of each container/pod is periodically monitored, and abnormalities (if any) are reported. The uptime of each container/pod is periodically monitored, and abnormalities (if any) are reported. The number of containers is tracked, and administrators are alerted if any container has stopped running or has been removed/paused. The images are periodically monitored and if any image is not mapped to the containers, administrators are duly notified. The resource utilization of each container is tracked periodically, and the resource hungry containers are isolated.
- **Enhancements to Kubernetes Monitoring:** Starting with this version, the network data sent from/received on each node/Pod in the Kubernetes Cluster is tracked and reported. This will point administrators to those nodes/Pods that are sending / receiving unusually large volumes of data. Such nodes/Pods will naturally be isolated and subjected to further analysis to identify the root cause of abnormal data traffic. By periodically monitoring the network data traffic, administrators can avert malicious attacks on the nodes/Pods well in advance.

7.2 Nutanix Monitoring Enhancements

- **Monitoring Nutanix Prism Center:** Nutanix provides an option to monitor and manage multiple clusters through a single web console. This multi-cluster view, known as Prism Central, is a centralized management tool that runs as a separate instance comprising either a single VM or a set of VMs. eG Enterprise v7.2 offers a specialized monitoring model called Nutanix Prism Center. The eG monitor for Nutanix Prism Center reports the count of clusters, containers, storage pools and virtual machines in all Nutanix Prisms managed by Nutanix Prism Central. This overview helps

administrators easily figure out how many storage pools/virtual machines have been added to /removed from each Nutanix Prism managed by the Nutanix Prism Central recently. In addition, the VMs that are powered on and powered off can be determined by the administrators at a single glance.

- **Enhancements to Nutanix Prism Monitoring:** eG Enterprise v7.2 is now capable of reporting in-depth metrics on Nutanix File Servers and File Shares. The Nutanix File servers that are bandwidth-intensive and space-hungry, and those with maximum ICAP quarantined files are identified and reported. Similarly, the Nutanix File Shares that are running out of space are also reported.
- **Grid GPU Monitoring Support for Nutanix Acropolis Hypervisor:** Starting with this version, eG Enterprise is capable of monitoring those vGPUs of Nutanix Acropolis Hypervisors that are configured in 'shared' mode. eG Enterprise now provides an overview of GPU capacity and usage at the hypervisor-level, so as to enable administrators to figure out inconsistencies in GPU sizing at the hypervisor and VM level. The encoder and decoder utilization on each GPU is now reported, and administrators promptly alerted to situations where graphics processing is a bottleneck. The GPU memory is periodically monitored so that administrators can determine whether/not the hypervisors are adequately sized to support graphic displays.
- **In-depth Monitoring of VMs on Nutanix Acropolis Hypervisor:** One of the key statistics that administrators use to determine overall health in a virtualized environment is CPU ready time. This is the amount of time a virtual machine is ready to use CPU but was unable to schedule time because all CPU resources (on a Nutanix Acropolis hypervisor) are busy. A high CPU ready time is a sign of CPU contention which can cause serious performance issues for many applications. eG Enterprise v7.2 monitors the CPU ready time of each guest VM and reports those VMs with high CPU ready time. Also, eG Enterprise is now capable of reporting those VMs that directly read data from SSDs.

7.3 Other Monitoring Enhancements

- **Monitoring OpenStack:** OpenStack is a collection of modules and tools that provides a framework to create and manage public cloud and private cloud infrastructure. OpenStack delivers infrastructure-as-a-service functionality -- it pools, provisions, and manages large concentrations of compute, storage, and network resources. These resources, which include bare metal hardware, virtual machines (VMs) and containers, are managed through APIs / an OpenStack dashboard. KVM (for Kernel-based Virtual Machine) is a full virtualization solution for Linux on x86 hardware containing virtualization extensions (Intel VT or AMD-V). OpenStack enables you to launch virtual machines on a bare-metal through KVM Hypervisor. Though this approach is beneficial, for a seamless operation, administrators need to continuously track the performance of OpenStack. This way, administrators can identify and triage performance anomalies quickly, and ensure the smooth operation of business services. eG Enterprise v7.2 monitors the OpenStack deployment using two different components namely OpenStack KVM and OpenStack Controller. By monitoring the OpenStack deployment, eG Enterprise offers visibility into the performance of the OpenStack Hypervisors, the VMs on each hypervisor, virtual machine status and resource usage levels.
- **Enhancements to IBM pSeries Monitoring:** Starting with v7.2, the HMC REST API is used to collect the outside view of LPARS on IBM pSeries v9 and above. For this, administrators are simply required to specify the console credentials of the HMC server alone. This approach eliminates the need to connect individually to each LPAR to collect the required metrics.
- **Enhancements to VMware vCenter Monitoring:** Starting with this version, eG Enterprise monitors and reports the storage capacity of each ESX cluster and alerts administrators to potential storage issues, if any on the cluster. The storage capacity of each datacenter is closely monitored and the datacenter that is utilizing the storage to the maximum is isolated. eG Enterprise v7.2 also monitors the alarms triggered and detected by vCenter in response to an event, a set of conditions,

or the state of an inventory object on a VMware vCenter server.

8. Unified Communications Monitoring

8.1 Enhancements to Office365 Monitoring

eG Enterprise v7.2 is one of the few tools in the market that provides complete monitoring of Microsoft Office 365 (O365) environments. With these enhancements, O365 customers do not have to just rely on status updates posted by Microsoft about the performance of the overall O365 services, but they can see in real-time the real performance that their users are seeing. Broadly, eG Enterprise v7.2 offers the following capabilities for O365 customers:

- **Enhancements to Microsoft Teams Monitoring:**
  - **Analyzing Service Level of Microsoft Teams by emulating Team, Channel and Chat Operations:** Microsoft Teams enables users to communicate with their peers quickly and securely. Microsoft Teams also helps users retrieve/update the properties of the chat/channel/team securely, list/retrieve one/more members, and update the role of a member in a chat/channel/team through any desktop/device. However, if Microsoft Teams is unable to deliver the high-quality experience it promises when performing the aforesaid operations, users are going to be frustrated. Consistence slowness when performing retrievals/updates can force IT administrators to hunt for alternatives. To avoid such an outcome, administrators should make sure that the guaranteed Microsoft Teams service levels are always delivered. For this, administrators should periodically check the time it takes to retrieve properties of / update chat/team/channel, and to list and update the role of the members in the chat/team/channel, isolate bottlenecks proactively, and plug the holes before users complain. eG Enterprise v7.2 helps administrators in this regard. The eG agent emulates a user updating the properties of, retrieving the member collection of, and updating the role of members in the chat/team/channel. In the process, the agent reports the time it takes to perform each of these operations. This provides administrators early indicators of problems and helps them resolve those problems at the earliest. This way, the service level of Microsoft Teams can be maintained at its peak at all times.
  - **Analyzing Audio/Video/VBSS Streams per User:** In previous versions, eG Enterprise analyzed the overall performance of the VBSS streams, Video streams and Audio streams by monitoring Microsoft Teams. Though this approach was helpful to isolate which type of stream was frequently classified as 'poor', administrators had to drill down to the detailed diagnosis to figure out the exact users who were affected due to poor streams. In environments where thousands of users were logged in Microsoft Teams, administrators felt the pain to drill down to the detailed diagnosis to figure out the users whose user experience suffered due to poor streams. To ease the pain of such administrators, eG Enterprise v7.2 offers to monitor the VBSS/Video/Audio streams initiated by each user. Alerts are promptly sent out to the administrators if the streams initiated by the users are classified as 'poor'. This way, administrators can immediately isolate the users experiencing poor user experience.
  - **Analyzing Service Level of Calendar by Emulating Operations:** In most environments, users use the Calendar application in Microsoft O365 to keep track of their meetings, tasks and appointments. If the user is unable to use the Calendar application to perform certain basic operations such as creating an event, updating/deleting scheduled events, users may become frustrated. If a consistent slowness is noticed while performing such basic operations on the Calendar application, administrators may be forced to look for other alternative applications. To avoid such an outcome, administrators should make sure that the guaranteed Microsoft Teams service levels are always delivered. For this, administrators should periodically check the time

it takes to create/update/list/read/delete events from the Calendar, isolate bottlenecks proactively and fix them before users start complaining. eG Enterprise v7.2 helps administrators in this regard. The eG agent emulates a user creating/deleting/updating/listing/reading an event from the Calendar application. In the process, the eG agent reports the time it takes to perform each of these operations. This provides administrators early indicators to problems and helps them resolve the problems at the earliest.

- **Real-time Call Quality Analytics Collected Using Webhooks:** In previous versions, eG Enterprise used Microsoft API to pull metrics on call quality. The Audio Streams test, the Video Streams test, Call Quality Check test, VBSS Streams test, and Network Quality Summary test relied only on the API for measuring the quality of Teams calls and the overall end user experience with them. One of the key limitations of the Microsoft API is its inability to provide real-time analytics on calls. The prime reason for this is that APIs do not run automatically; they need to be manually polled for metrics. Secondly, Microsoft publishes call records at 4-hour intervals; the API accesses these published records only. Because of the delay in data access, problem identification took a lot of time, and troubleshooting became iterative. This left the users frustrated.

  To overcome the shortcomings of the API, Microsoft introduced Webhooks. Webhooks can be thought of as automated API response, without the request. It is a mechanism used by the Microsoft Graph API to deliver change notifications to clients. No manual polling is required for Webhooks to work. Via Webhooks, data is automatically passed to the clients when an update is made. Webhooks assure administrators of real-time metrics, and greatly ease troubleshooting. Starting with this version, the eG agent leverages the capabilities of Webhooks. The agent is now capable of running additional tests that pull real-time call quality analytics using Webhooks. The below figure depicts how the eG agent runs these tests and collects diagnostics.

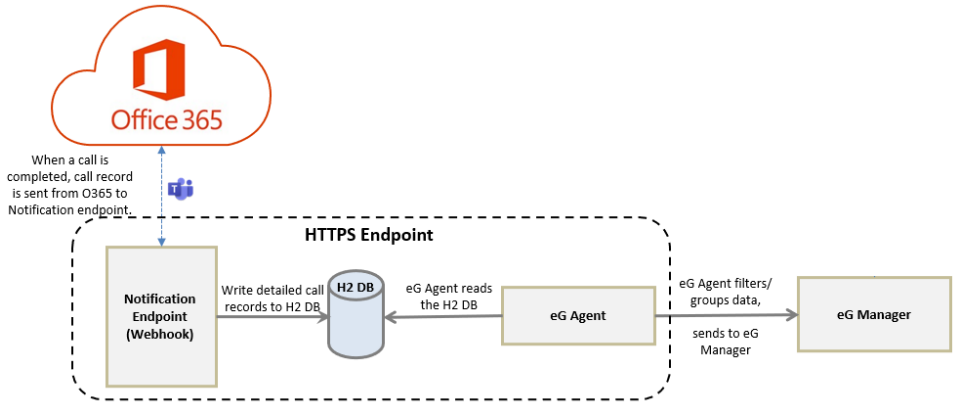


Figure 64: Representation of how the eG agent uses Webhooks to pull call quality analytics

1. Whenever a call is completed in Microsoft teams, a new call record is sent from Microsoft office 365 to the Notification endpoint. A notification endpoint is a URL which is publicly accessible via HTTPS so that Microsoft can send call records to the endpoint.
2. The key information in the call record is call record ID. Notification endpoint will query Microsoft for details of the call record using the 'call record ID' received and tenant properties. In return, call record details will be sent in JSON format to notification endpoint.
3. Call record response - i.e., the JSON response - received by the notification endpoint is parsed, written to CSV files, and stored in the H2 database.
4. The eG agent queries the H2 database and reads the call quality measures.

5. The eG agent also filters/groups the metrics so read, and sends them to the eG manager.

6. The eG manager publishes the metrics to the eG web console.

This way, call quality metrics of Microsoft Teams can be pulled in near real-time using Webhooks.

- **Microsoft 365 User Dashboard:** eG Enterprise v7.2 includes a brand-new Microsoft 365 User Dashboard that provides an overview of the usage of O365 services by all users who are registered with a chosen O365 tenant. From this dashboard, O365 administrators can quickly glean which user is using which service, understand what operations he/she performed using that service, and track the resources consumed by each user in the process. These insights will help administrators proactively identify users who have subscribed to a service but are not using it optimally, and users who may not be able to use a service for too long owing to potential resource crunch. You can even zoom into a problematic user in the dashboard to closely study the activities of that user, service-wise. With the help of these granular details, O365 administrators can tell whether/not the user is actively utilizing all the services they are licensed to use. Under-utilized services can be quickly identified this way, and the reason for the inactivity can be investigated. The 'per-service' insights will warn administrators of probable capacity bottlenecks that can impact service usage in the future, so that administrators can promptly take pre-emptive action. They also alert administrators to service operations / operational levels that may be 'suspect' – for instance, administrators can rapidly detect if an Exchange Online user is sending / receiving more mails than he/she should. Malicious attacks can thus be captured before any permanent damage is done.

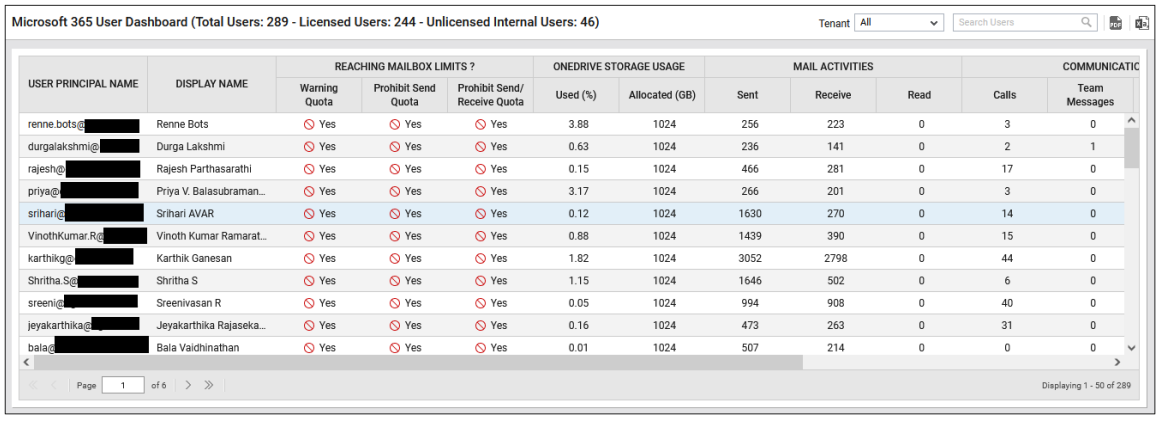


Figure 65: The Microsoft 365 User Dashboard

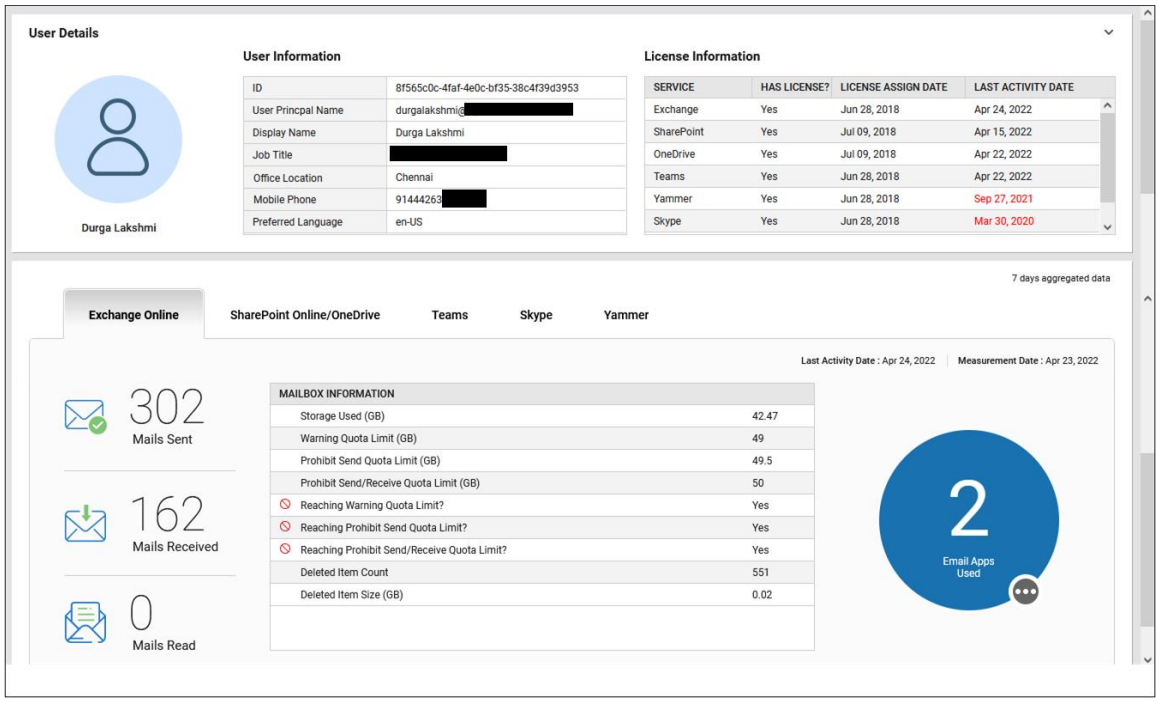


Figure 66: Drilling down to the dashboard of a specific user

- **Enhancements to Microsoft Yammer Monitoring:** Using eG Enterprise v7.2, administrators is can assess the performance levels achieved by Microsoft Yammer. By emulating user logins, message posts/likes, file uploads and deletes in Microsoft Yammer , eG measures the time taken to perform each of these operations . This way, administrators are alerted to problem conditions well in advance, which helps them resolve the issues before user experience starts deteriorating.
- **The new Microsoft Yammer Dashboard:** The Office 365 dashboard has been enhanced to report the real-time experience of users logging into Microsoft Yammer and measure user satisfaction levels. In-depth visibility into the health and activity levels of the Microsoft Yammer service can be obtained. Real-time user experience can be ascertained from this dashboard by analyzing the user operations that were emulated at regular intervals on Microsoft Yammer. The user operation that is failing frequently (Message Post, Message Like, Message Delete etc) can be easily ascertained. The device that is most widely used by the users to login to Microsoft Yammer can be ascertained along with the user load on the Microsoft Yammer.

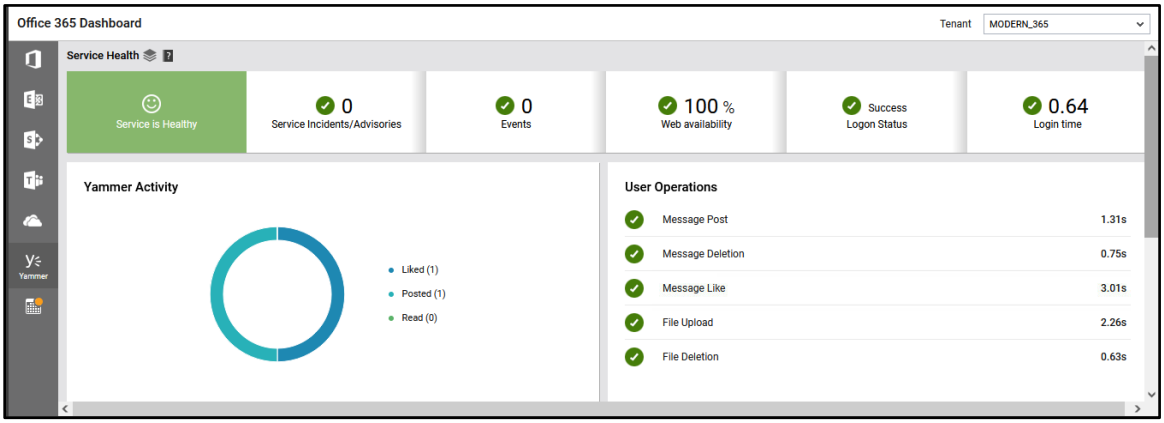


Figure 67: Microsoft Yammer Dashboard

- **Email Path Flow Visibility for Microsoft O365 products:** Organizations rely heavily on emails for both their business and internal correspondence. If delivery of important emails fails / is slow, it can cause irredeemable business losses, To avoid such a disastrous outcome, administrators should monitor the email path flow to and from their organization, proactively identify mail routing issues, and resolve them well before it affect. This is why, eG Enterprise periodically simulates email path flow.

  Email Path Flow simulation, helps administrators:

  - Capture mail transmission/reception failures, without waiting for users to actually send/receive mails;
  - Monitor the entire email flow to proactively detect a probable delay in mail delivery, and isolate the source of the delay – is it the mail sender? Or mail receiver?
  - Measure mail delivery SLAs for specific or all domains;
  - Check if the SMTP server or mail filters are causing any slowness
  - Complete mail delay details covering all the hops

  Email flows can be simulated for the following:

  - Microsoft Exchange <-> Microsoft Exchange
  - Microsoft Exchange <-> SMTP (Gmail, Yahoo etc)
  - Microsoft Exchange Online <-> Microsoft Exchange
  - Microsoft Exchange Online <-> Microsoft Exchange Online
  - SMTP <-> SMTP
  - SMTP <-> Microsoft Exchange Online

  The Synthetic Monitoring dashboard offered by eG Enterprise displays relevant statistics captured for the configured email paths.

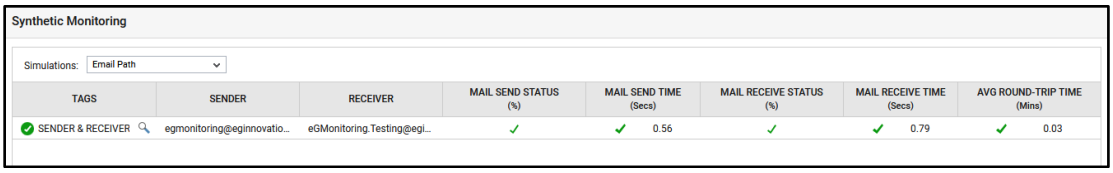


Figure 68: The Synthetic Monitoring Dashboard

Drilling down from an email path will help administrators detect and troubleshoot email delay issues

well before end users notice.

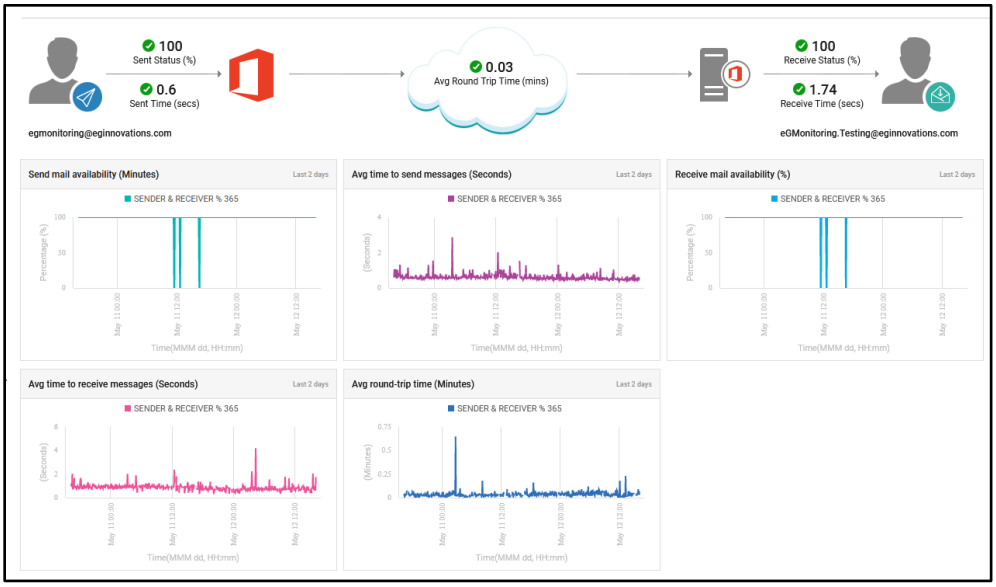


Figure 69: Detailed analysis on a trouble-prone email path

- **Daily Performance Overview Email for Microsoft O365:** By default, every day, eG Enterprise emails a report to those eG users who have been assigned one/more Microsoft O365 products/components (e.g., SharePoint Online, Exchange Online etc.) for monitoring. For a user, this report reveals the health of a set of pre-configured KPIs related to the Microsoft O365 products assigned to that user. A quick look at this report will point users to problem areas in their O365 infrastructure. Also, by comparing one day's report with that of another, you can track variations in the values of the KPIs, and quickly detect abnormalities. This report can be viewed/accessed by the

administrators from any mobile device without the need for logging into the application directly.

Figure 70:The Daily Performance Overview Emailer for Microsoft O365

- **Support for Modern Authentication in Microsoft Office365:** Modern Authentication is not a single authentication method, but instead a category of several different protocols that aim to enhance the security posture of cloud-based resources. Some examples of Modern Authentication protocols are SAML, WS-Federation, and OAuth. eG Enterprise v7.2 supports Certificate based authentication (CBA) or app-only authentication which enables modern authentication in unattended scripts/automation scenarios by using Azure AD apps and self-signed certificates. In environments where Microsoft Office 365 products are extensively monitored, administrators can use Modern Authentication to provide a higher level of security.

  Following are the brief steps on how to enable modern authentication in eG Enterprise's O365 monitoring:

  - Create/register an app in Azure AD and assign appropriate permissions
  - Generate a certificate and upload it in Azure AD
  - Install/place the certificate in eG agent system as well
  - Specify the name of the Tenant as an input while configuring all the O365 tests

  Upon providing the name of the Tenant, administrators can refrain from providing the credentials of

an O365 user while configuring the tests. This will enhance the security of their O365 environment.

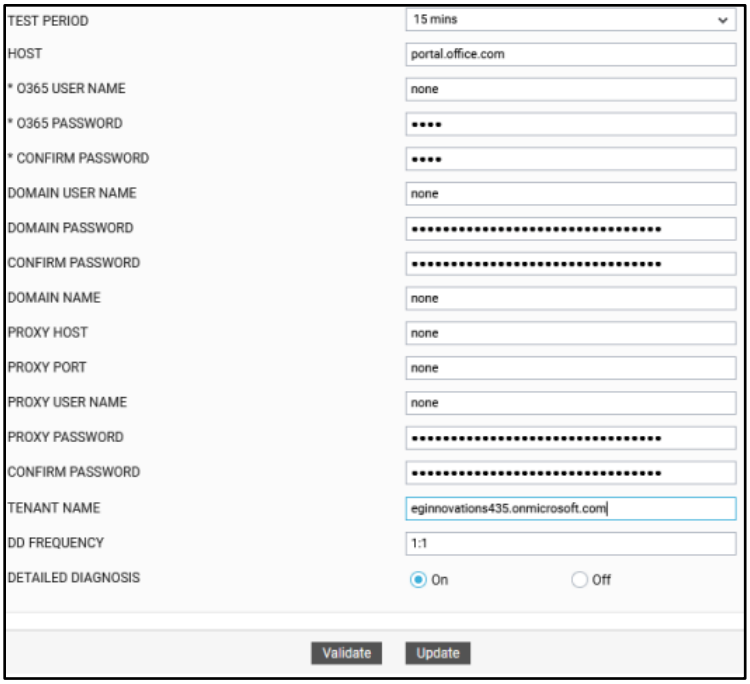


Figure 71: Specifying Tenant Name to support Modern Authentication

- **Unlicensed External Users in Office 365 Environments can now be Tracked:** Sometimes, users belonging to other domains are allowed restricted access to an Office 365 environment. For example, users from a domain are allowed to view the documentation hosted via Microsoft SharePoint in Office 365 environment. For such users, administrators are not required to allocate a valid Office 365 license and hence, they can remain unlicensed in the target Office 365 environment. eG Enterprise v7.2 helps administrators keep track of the count of users from different domain who are accessing the target Office 365 environment. The detailed diagnostics further reveals the name of such unlicensed external users.

➢ **Automating Microsoft O365 Pre-requisites Installation:** In previous versions, administrators had to manually configure the target Microsoft O365 environment for monitoring by following a long list of pre-requisites and related procedures. Besides being tedious, errors and misconfigurations also became inevitable during this manual process. Moreover, troubleshooting these incorrect configurations was also a challenge. To ease the administrator's pain in this regard, eG Enterprise automates the fulfillment of pre-requisites in version 7.2. A proprietary Powershell script is provided, which eG when run, automatically performs the following:

  - Installs the Powershell modules/packages required for monitoring Microsoft O365 products
  - Creates a user with required roles and permissions to execute Powershell cmdlets, or, assigns the requisite roles and permissions to existing users
  - Creates MS Graph App and assigns required permissions
  - Checks if the pre-requisites are in place

This script when executed, also writes the progress/status of the automated steps to a log file. These log files are useful for troubleshooting when the Microsoft O365 products are not reporting metrics

as expected.

- **Office 365 Pre-requisites now requires Lesser Privileges:** Earlier, to monitor Microsoft O365 environments, administrators required a Microsoft O365 account with 'Global Admin' privileges. A few organizations were unwilling to grant this privilege citing compliance issues. To aid such organizations monitor Microsoft O365 products, starting with this version, eG Enterprise does not require 'Global Admin' privileges for O365 monitoring account.
- **Proxy Support for Monitoring Microsoft Office 365:** In previous versions, the eG remote agent failed to collect metrics from Microsoft O365 when placed behind a proxy server. This is not the case any longer. Because, starting with this version, the eG agent can communicate with Office 365 via a proxy server and pull metrics. To enable this communication, the eG tests should be configured with the details of the proxy server.
- **Monitoring Domain - Microsoft Teams and Domain- Exchange Online:** In large enterprises, domains may be created for different user groups and departments. A Domain administrator will be concerned only about the activities specific to his/her domain. Such administrators may be interested in only monitoring how the users in their domain are using Microsoft O365. To cater to the needs of such administrators, eG Enterprise v7.2 offers **Domain – Microsoft Exchange and Domain – Microsoft Teams** monitoring models. Once the eG tests for these models are configured with the domain to be monitored, eG pulls a wide variety of metrics related to that domain. Using these metrics, administrators can figure out the overall performance of the users of that domain with respect to Microsoft Exchange and Microsoft Teams in detail, identify pain-points experienced by the users of that domain and rectify them at the earliest.
- **Ability to view Domain-wise Microsoft O365 Dashboards and Reports:** By default, the Microsoft Office 365 dashboard offers administrators with an extensive view of the services that are subscribed by each tenant and reports the health of the services. However, in some environments there may be multiple administrators overlooking the performance of the services offered by Microsoft O365 and they may be interested to review the performance of the services of their interest alone. In previous versions of eG Enterprise, administrators viewed the Microsoft O365 dashboard for all the services (Microsoft O365, Microsoft Exchange Online, Microsoft Teams etc) irrespective of their area of interest. To offer more granularity and to ensure that the administrators are provided with the dashboard relevant to their field of expertise, eG Enterprise v7.2 offers a **Microsoft O365 Tenants** page. Administrators are allowed to configure the tenants of their interest and view the Microsoft O365 dashboard based on the configured Tenant. Also, this page aids administrators create a tenant for each domain so that they can concentrate on issues that arise in their domain alone.

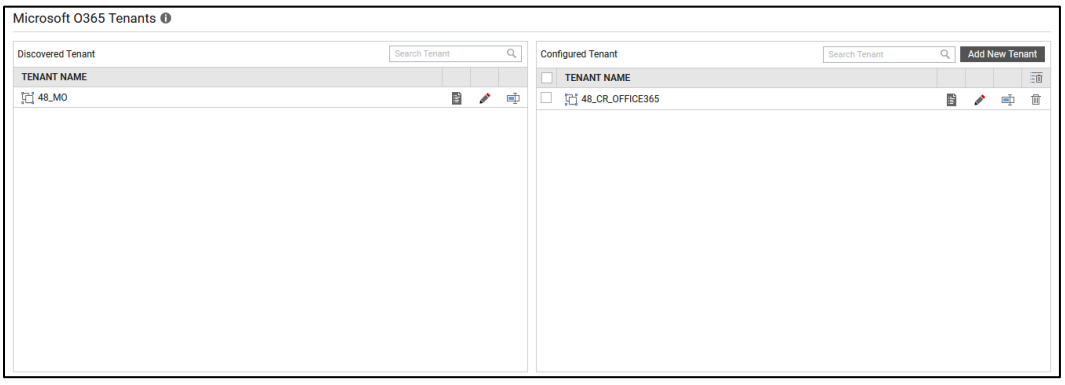


Figure 72: The Microsoft O365 Tenants page

- **Identifying the Mailboxes that are nearing Recoverable Item Quota in Exchange Online Environments:** The Recoverable Items folder contains items deleted by Microsoft Outlook and Microsoft Office Outlook Web App users or by the Mailbox Assistant. The duration that deleted items remain in this folder is based on the deleted item retention settings configured for the mailbox

database or the mailbox. If the recoverable items limit for a user's mailbox is reached, that user will no longer be able to delete items from his/her mailbox. As a result, the mailbox will keep growing in size, soon exhausting the mailbox quota that is set. Once this happens, the user will not be able to send/receive mails. To avoid this, administrators should know that the recoverable items limit is about to be reached, well before it is actually reached. Towards this end, eG Enterprise v7.2 monitors the recoverable items folder attached to each user's mailbox, and proactively alerts administrators if any folder is filling up fast and is about to exhaust its limit. Based on this warning, administrators can fine-tune the retention settings of the recoverable items folder, so that it keeps purging its contents at regular intervals, and thus prevents the user's mailbox from growing uncontrollably.

- **Track Licenses Consumed by Microsoft O365 Users:** Microsoft Office 365 monitoring is licensed based on the number of concurrent users accessing Microsoft Office 365 products. The eG Enterprise license tracks the license utilized by all the Microsoft O365 users in the target environment and reports the same in the **Total License Usage** tab of the **LICENSE INFORMATION** page in the eG administrative interface. You can even figure out the Microsoft O365 users who are currently utilizing the licenses from the **O365 USERS REPORT** page. You can even generate an hour-wise/day-wise distribution of the licenses utilized by the Microsoft O365 users.

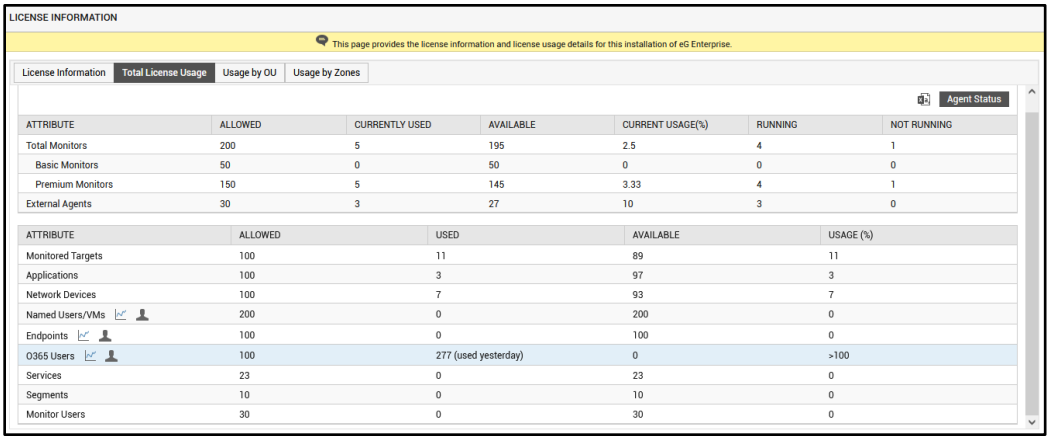


Figure 73: Tracking the license utilization of O365 users

8.1.1 Reporter Enhancements for Microsoft Office365

Following are the new reports that are introduced in eG Enterprise v7.2 with respect to Microsoft O365:

- **User Logins Report:** Administrators can use this report to historically analyze the pattern of user logins to the Microsoft Office 365 environments and identify the accounts/users with maximum number of logon failures. This will help administrators analyze if the account of the user is under any malware attack or if the user account needs a password reset. This report also helps administrators to track the Client IP addresses with maximum logon failures. By periodically analyzing such Client IP addresses, administrators can decide whether/not such IP addresses that are attempting brute

force/bot attacks need to be blocked.

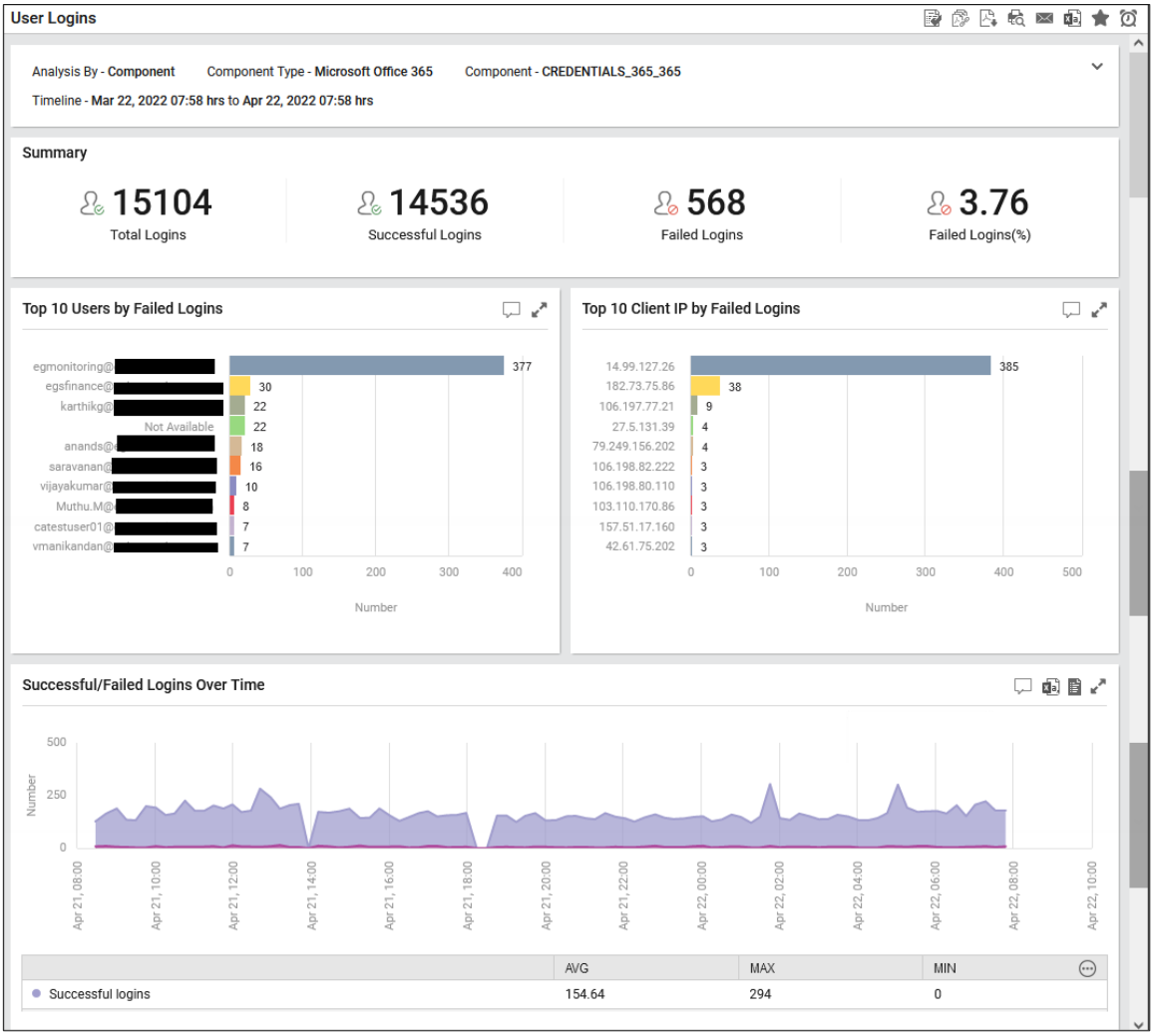


Figure 74: The User Logins Report

- **Least Active Users Report:** This report helps administrators identify the users who are least active on each service/application offered by Microsoft Office 365. Using this report, administrators can figure out the applications/services that are less popular among users and decide on the renewal of license for those services/applications. Using this report, administrators can also identify dormant user accounts and delete the same so that licenses can be made available to genuine users who are

in need.

Figure 75: The Least Active Users Report

- eG Enterprise also offers reports to identify Licensed/Unlicensed Users logged into Microsoft Office365 environment, the top users accessing the services offered by Microsoft Office 365 and the Top groups that are accessible in Microsoft Office 365. These reports help administrators leverage the utilization of Microsoft Office 365 products in their environment.

8.1.2 Reporter Enhancements for Microsoft Teams

Following are the new reports introduced in eG Enterprise v7.2 with respect to Microsoft Teams:

- **Service Health Report:** As with any cloud-hosted service, service disruptions, downtime and slow

connectivity issues are bound to affect business continuity and Microsoft Teams administrators require actionable insight to proactively alert them when performance starts to degrade and to help them resolve problems quickly. eG Enterprise v7.2 helps Microsoft Teams administrators generate a Service Health report which throws light on health, connection status and the trend of packet loss noticed while calls were initiated by the users using the Microsoft Teams service over a period of time. This report also helps administrators in post-mortem analysis of the data which in turn would help administrators in understanding the pattern of Microsoft Teams performance problems.

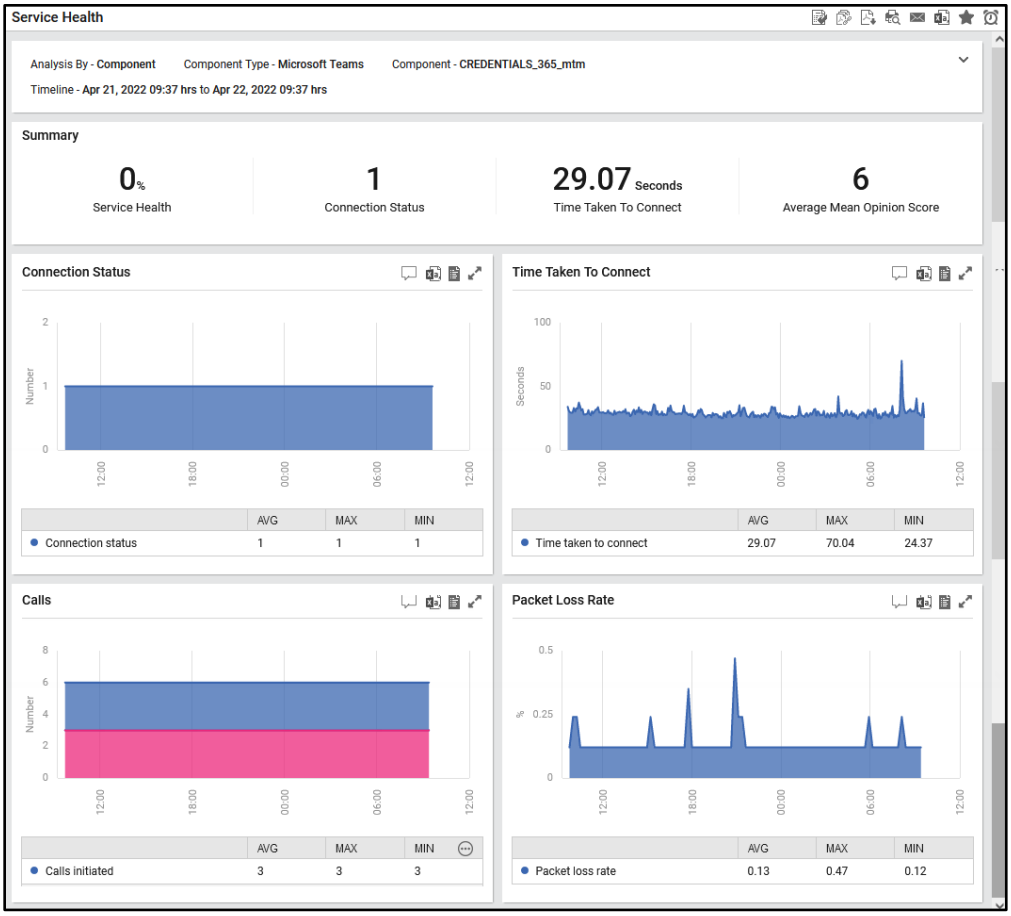


Figure 76: The Service Health Report

- **Users/Devices Report:** Administrators can use the Users/Devices report offered by eG Enterprise v7.2 to analyze Microsoft Teams usage in terms of users connecting to them, and devices from which they are connecting. By closely observing the generated report, administrators can figure out how actively Microsoft Teams has been used over a period of time, the most/least popular devices, and the unique users who were most/least active on Team chats during the given period. Administrators may want to pay more attention to the devices and users who are not very active on Teams and investigate why their Teams usage is poor. This path may lead them to performance, connectivity, or compatibility issues that may have to be resolved to ensure the organization-wide usage of Teams.

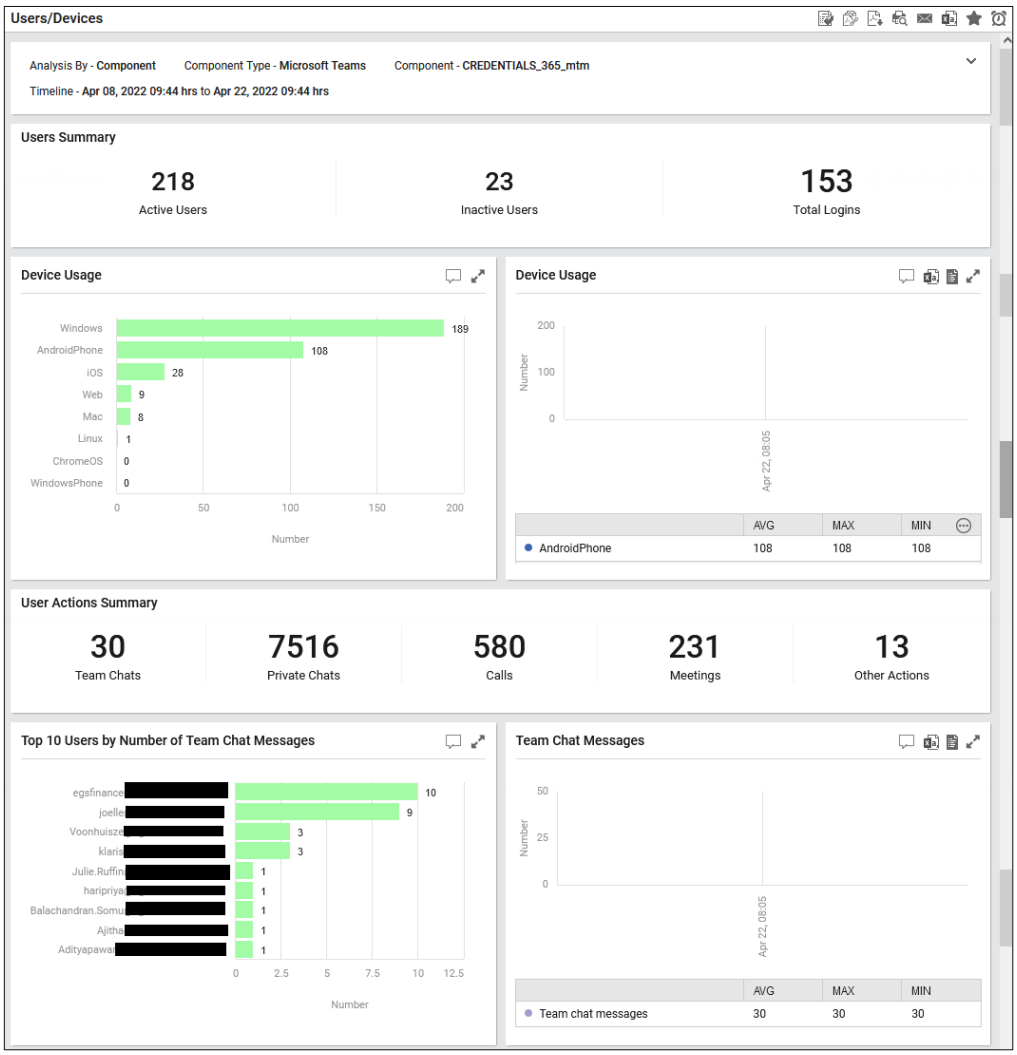


Figure 77: The Users/Devices Report

- **Call Quality Analytics Report:** The Call Quality Analytics report offered by eG Enterprise v7.2 helps administrators historically analyze the quality of calls handled by Microsoft Teams, so that they can determine the following:
    - Did calls consistently fail? If so, what were the common causes of the failure – call drops? incorrect call setup? media failures?
    - Were audio / video / VBSS streams unhealthy during the given period? What frequently caused the quality of the streams to degrade?
    - Were calls consistently slow?

With the help of these analytics, administrators can understand why user experience with Teams

calls is poor, and what they should do to deliver a superlative experience to users.

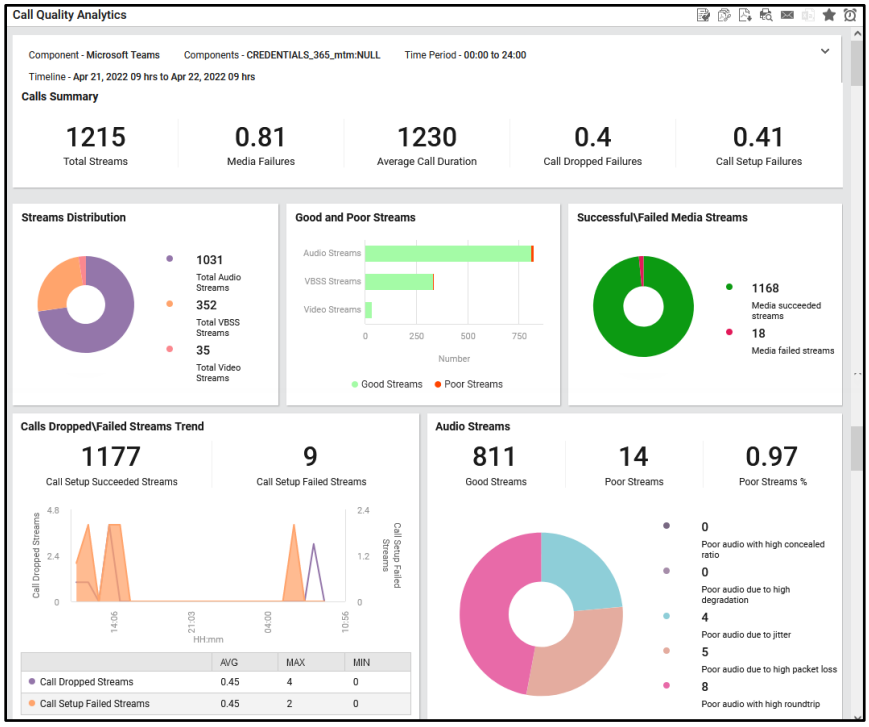


Figure 78: The Call Quality Analytics Report

- **User Experience Report:** Use this report to historically analyze the operations performed by an emulated user on Microsoft Teams. By closely analyzing the generated report, administrators can figure out which operation (for e.g., updating chat, updating channel, updating team etc) is the key contributor in degrading the user experience on Microsoft Teams over a period of time.

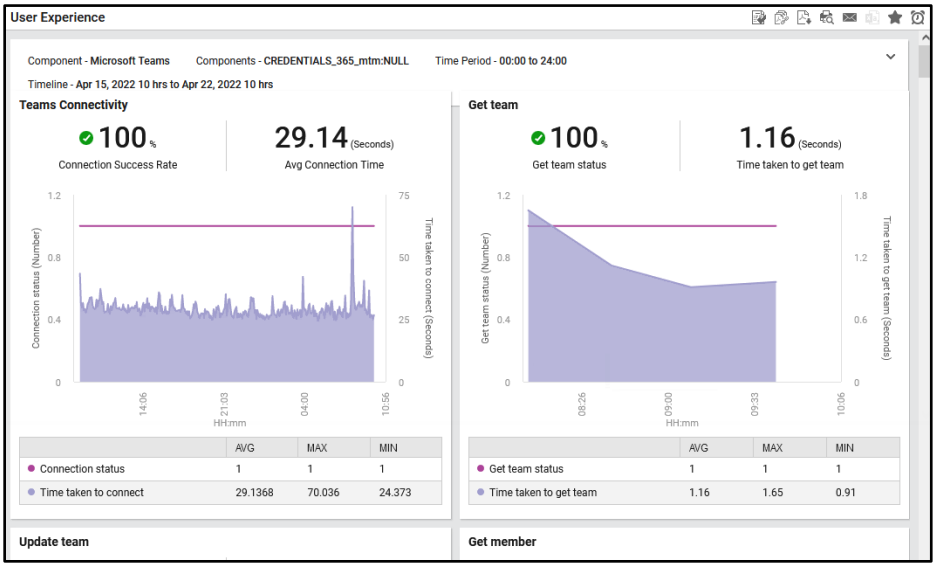


Figure 79: The User Experience Report

8.1.3 Reporter Enhancements for Microsoft Yammer

Following are the new reports that are introduced in eG Enterprise v7.2 with respect to Microsoft Yammer:

- **Service Health Report:** This report helps Microsoft Yammer administrators audit the status and overall performance of the Yammer service during a designated period. Poor activity levels, consistent connectivity issues, sluggish Yammer operations, sub-par login experience, and frequent breaks in service availability are brought to administrator attention through this report.

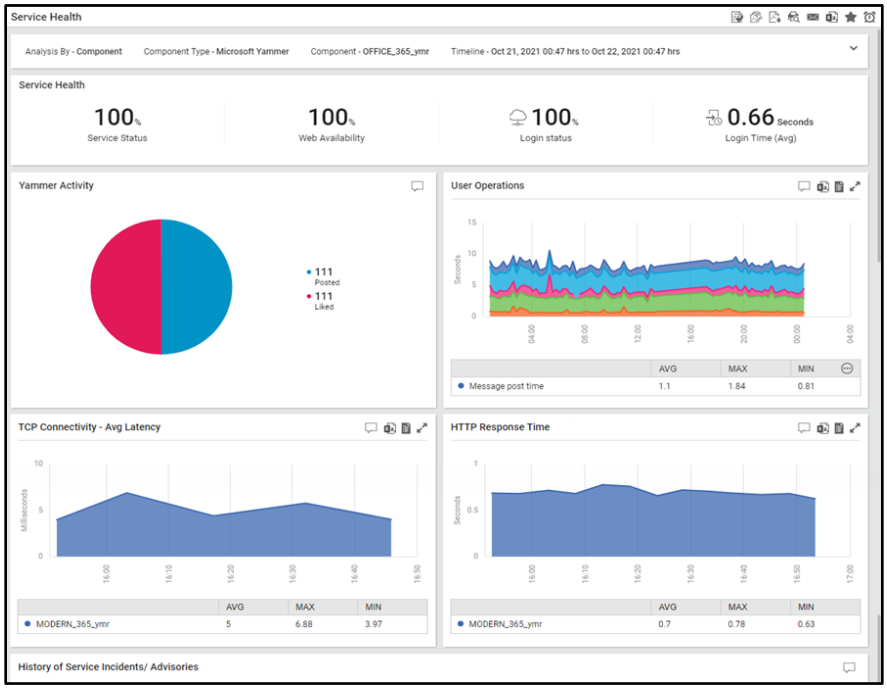


Figure 80: The Service Health Report

- **User Experience Report:** Use this report to historically analyze the operations performed by an emulated user using Microsoft Yammer. By closely analyzing the generated report, administrators can figure out which operation (for e.g., like/post/delete messages, upload files etc) is the key

contributor in degrading the user experience on Microsoft Yammer over time.

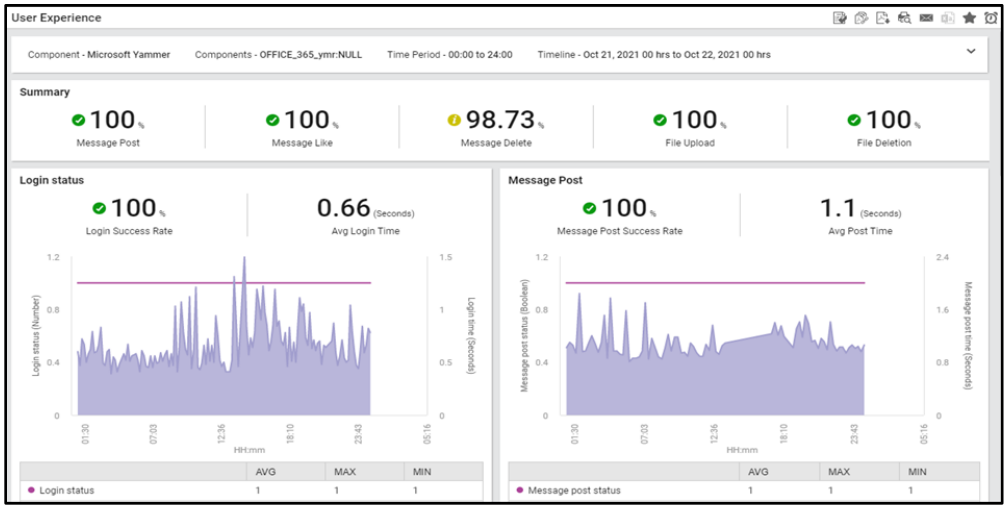


Figure 81: The User Experience Report

- **Users/Groups Report:** Administrators can use the Users/Groups report offered by eG Enterprise v7.2 to study past trends in Yammer usage. Using the report, administrators can determine whether/not individual users and user groups are actively using Yammer. If not, the reasons for the same should be ascertained. The report also points administrators to the devices that are popular in terms of the number of users using them to connect to Yammer. Unpopular devices may hint at compatibility issues that administrators may have to resolve to improve Yammer usage and hasten its adoption across the organization.

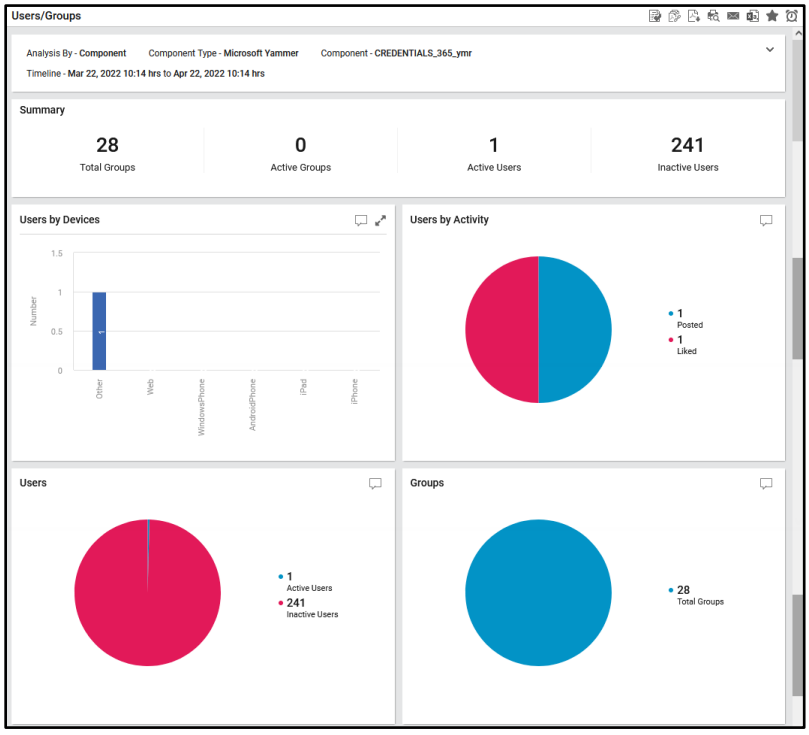


Figure 82: The Users/Groups Report

8.1.4 Reporter Enhancements for Microsoft OneDrive

eG Enterprise v7.2 offers a wide range of reports for in-depth analysis of OneDrive performance. Following are a few key reports that are discussed in detail:

- **Synchronization Activities Report:** The Synchronization Activities Report offered by eG Enterprise v7.2 helps administrators effectively audit the synchronization activities that users perform on files in Microsoft OneDrive. This reveals the top users and clients who performed the maximum number of synchronization activities during a given period of time. Administrators can also assess which type of operation (e.g., uploads, downloads etc) was frequently performed as part of synchronization, the unique users performing synchronization etc. By closely observing the generated report, administrators can detect anomalous activities with ease and ensure that only legitimate users/teams are accessing Microsoft OneDrive.

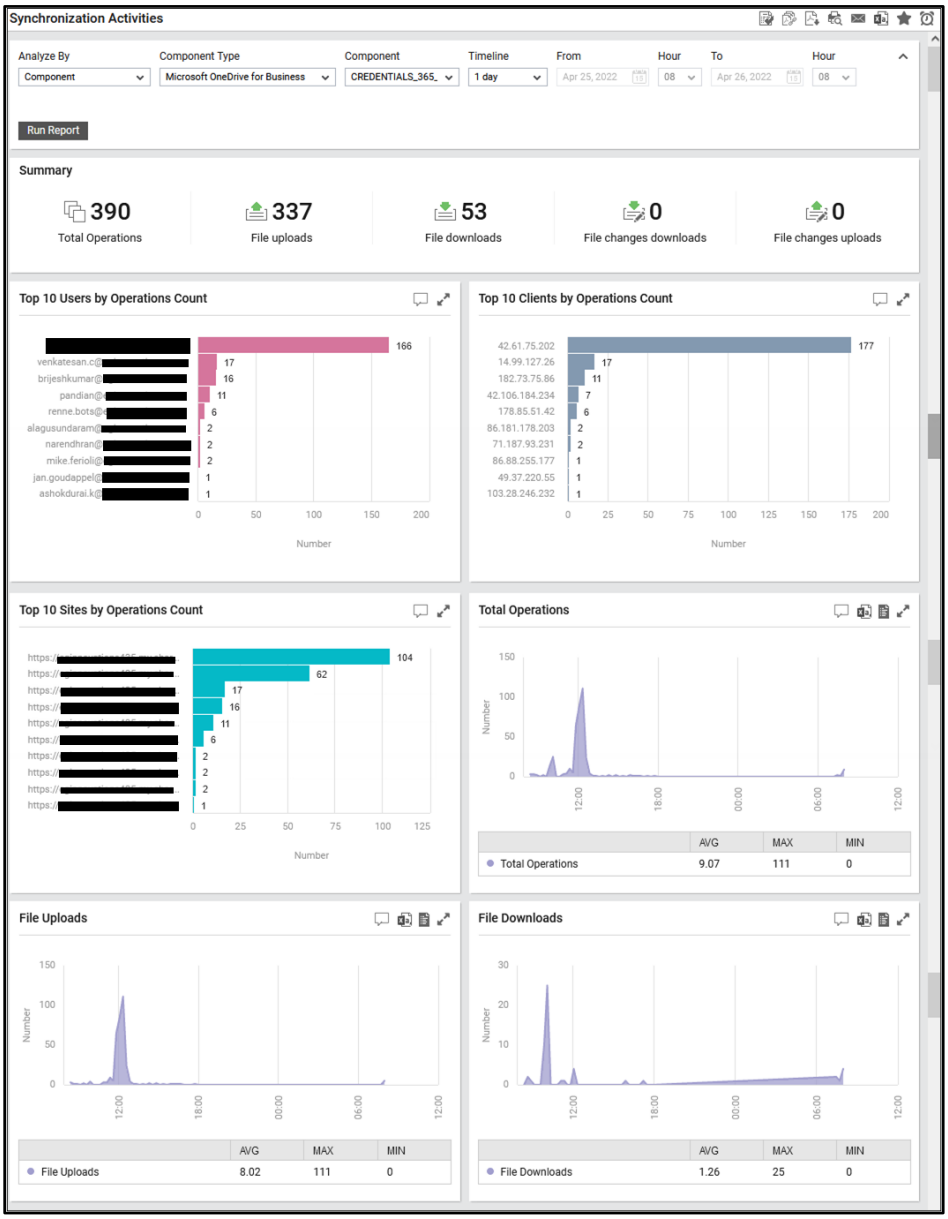


Figure 83: The Synchronization Activities Report

- **Folder Activities Report:** To historically analyze the folder operations performed by users on Microsoft OneDrive, administrators can use the **Folder Activities** report offered by eG Enterprise v7.2. Use this report to identify who performed the maximum number of folder operations during the given period and what type of operations (delete, upload etc) they were. This will reveal if folder operations were performed by authorized personnel only.

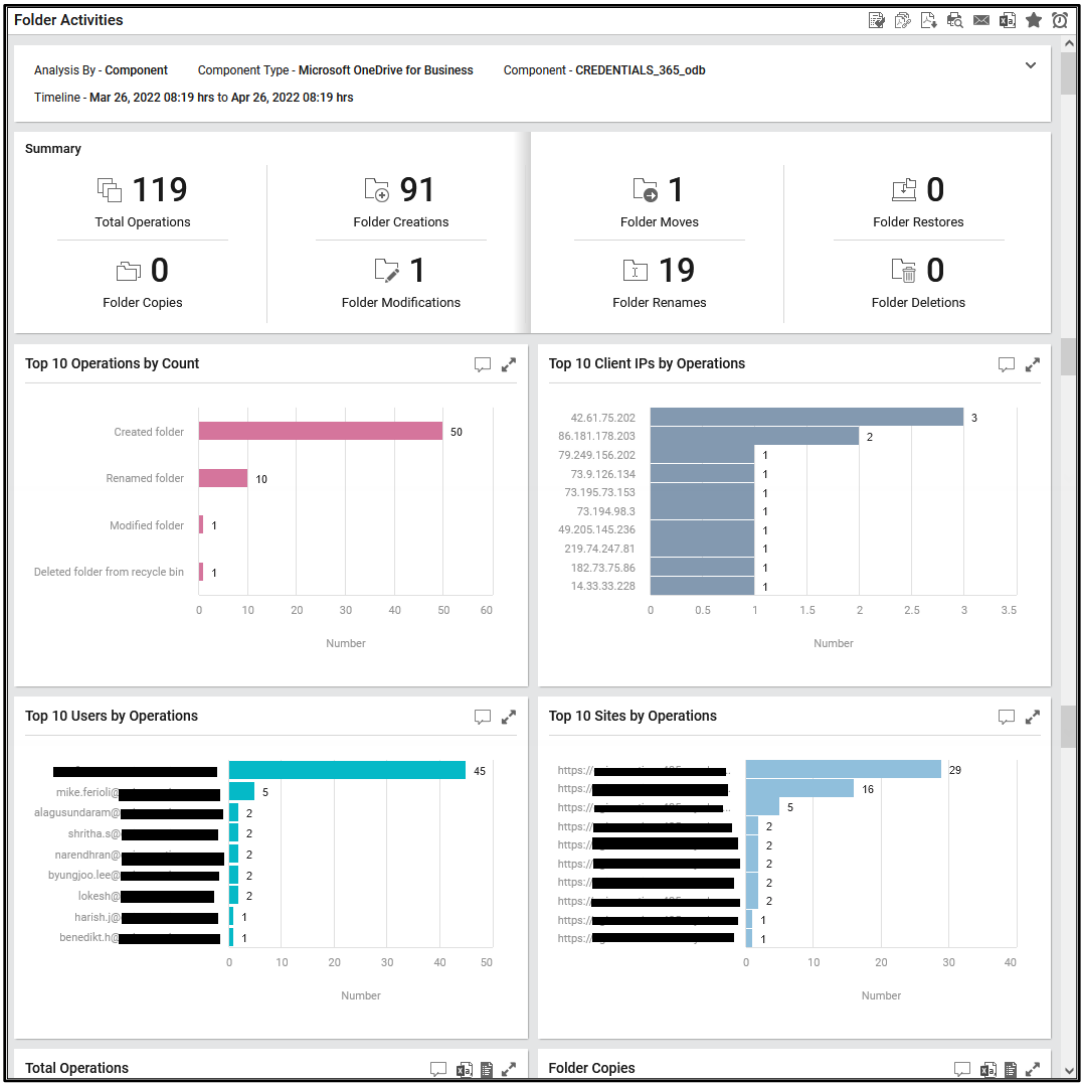


Figure 84: The Folder Activities Report

- **File and Page Activities Report:** Use the File and Page Activities report offered by eG Enterprise v7.2 to analyze the file and page operations performed by the users on Microsoft OneDrive over a period of time. The top users performing the file and page activities, the operations that were frequently performed on the files and pages, the client IPs that were frequently used in accessing the files and pages can be ascertained with ease. This will reveal operations that are 'suspect', and

the users/clients who performed them.

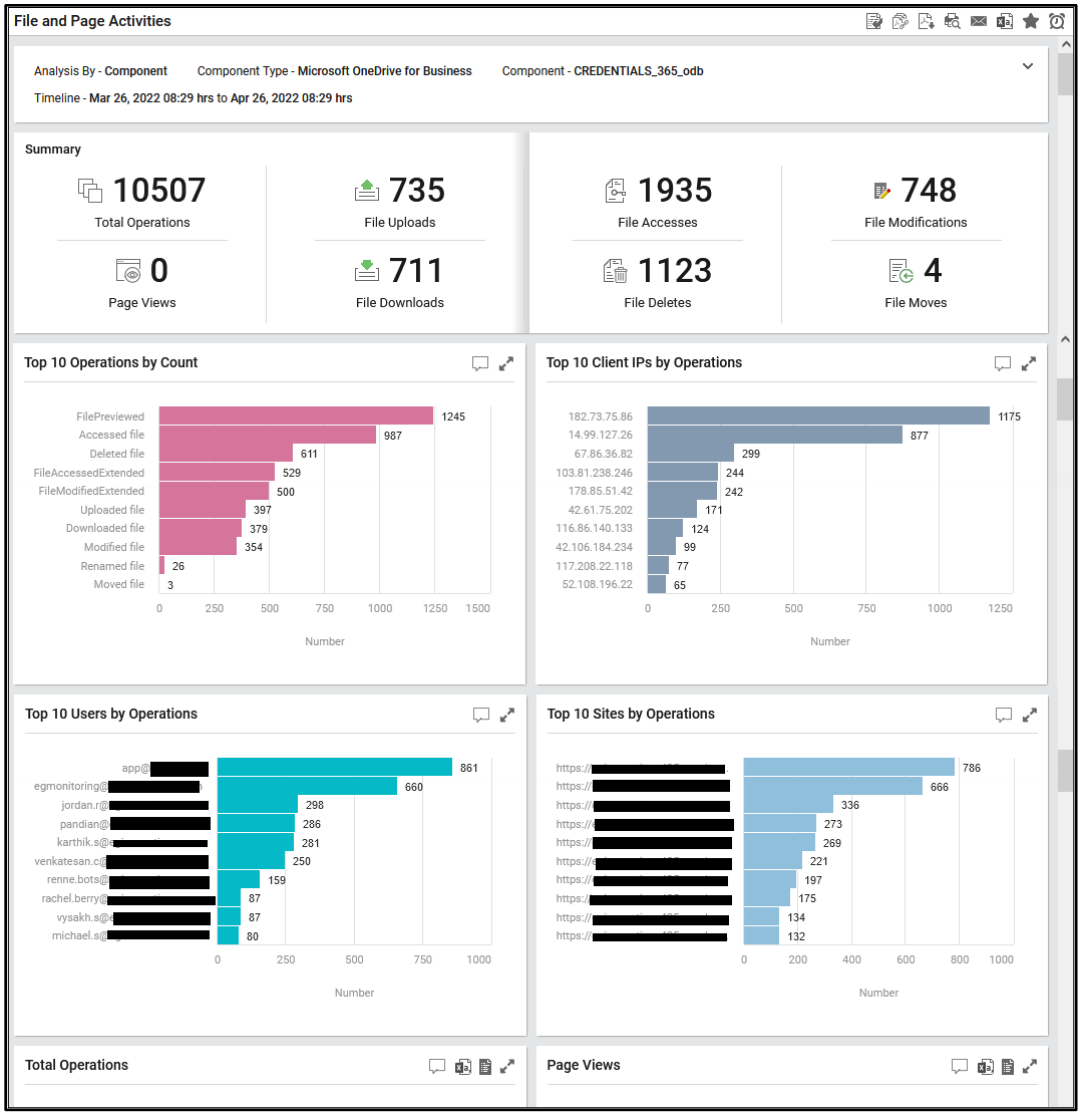


Figure 85: The File and Page Activities Report

8.2 Other Unified Communications Monitoring Enhancements

- **Monitoring BlackBerry UEM 12.x:** BlackBerry® UEM delivers complete, unified endpoint management and policy control for your diverse and growing fleet of devices and apps. eG Enterprise v7.2 monitors the BlackBerry UEM 12.x and reports if connections were established through the BlackBerry Dispatcher. The load on the BlackBerry Dispatcher is periodically monitored and administrators are proactively alerted to potential delays in the Dispatcher's responsiveness to requests from devices. The load on the MDS connection service is periodically monitored and irregularities if any, are brought to light. SRP connection failures, invalid SRP connections and socket connection errors are captured and reported well in advance. The responsiveness of the Affinity Manager is measured, and, in the process, administrators are alerted to errors and delays in request processing by the Affinity Manager. The RCP connection load from the Internal servers to the Affinity

Manager and the RCP connection load to the external servers from the Affinity Manager are monitored and data transmission/reception irregularities if any, are promptly captured and reported.

- **Monitoring Cisco Unified Communication Manager:** Cisco Unified Communication Manager (Unified CM) is an IP-based communications system that allows you to contact your co-workers or customers through audio or video regardless of their location. Unified CM provides reliable, secure, scalable, and manageable call control and session management. eG Enterprise 7.2 extends monitoring support for Cisco Unified Communication Manager. The status of each local call manager is tracked, and abnormalities promptly reported. The Computer Telephony Integration (CTI) devices and media devices that are not registered with and are rejected by the local call manager are highlighted, so that administrators can reason for the same. Unregistered gatekeepers and the ones in an 'unknown' state can be identified. Alerts are also sent out if any gateway / D-channel is in an abnormal state, if unregistered / partially registered phones are detected, and if any phones are rejected by Unified CM. Gateway trunks are closely monitored and the gateway trunks that are in an unknown/busy/inactive state are isolated. The administrator is notified if there are one/more unregistered, inaccessible, or rejected voice messaging devices, if any failures (e.g., phone / gateway / call manager failures) are detected, or if any malicious calls are captured.
- **Monitoring SBC AudioCodes:** AudioCodes' Mediant session border controllers (SBCs) deliver seamless connectivity, enhanced security and quality assurance for enterprise and service provider VoIP networks. A session border controller (SBC) is a dedicated hardware device or software application that governs the way phone calls are initiated, conducted, and terminated on a voice over Internet Protocol (VoIP) network. eG Enterprise v7.2 offers a dedicated monitoring model to monitor Session Border Controllers called SBC AudioCodes. The overall DSP channel utilization is periodically reported, and administrators are promptly alerted to drops noticed in the utilization of active DSP channels. The messages sent/received over control protocol by the appliance is periodically monitored and administrators are alerted to the count of messages that failed to be sent/received. Packet loss and packet transmission delays over Real-time Transport Protocol (RTP) and RTP Control Protocol (RTCP) are duly captured and reported. The trunk groups are closely monitored, and the calls established from/to IP and telephone through SIP are tracked and reported. Calls that were dropped/released due to lack of resources too are reported based on the trunk group. Voice call connected through the SBC appliance helps administrators determine the load on the appliance. By closely monitoring the SIP dialogs to the IP groups, administrators can determine whether there was a sudden surge in the count of incoming INVITE/SUBSCRIBE dialogs or outgoing INVITE/SUBSCRIBE dialogs. The calls from IP to telephone and vice versa over SIP protocol are periodically monitored and administrators are alerted to a sudden surge in the count of not answered calls and non-routed calls. FAX calls are also periodically monitored and reported. The calls established through the SIP interface also helps administrators determine the load on the SIP interface.
- **Monitoring Zoom:** Zoom is a communications platform that allows users to connect through video, audio, phone, and chat. To ensure that user experience with Zoom remains above-par all the time, eG Enterprise v7.2 monitors Zoom and reports the call quality of various Zoom services like audio, video, screen sharing, and more. The videos or calls that are streaming poorly or failing can be identified and the root cause of such a poor show can be diagnosed. User activities such as chats, calls, webinars and meetings are monitored, so that administrators can assess the level of activity on Zoom. The users accessing Zoom are continuously monitored and administrators are alerted to the users who are deleted/disassociated/deactivated from the Zoom platform. The file recordings are monitored periodically and the recordings that are stopped/paused/deleted are identified. The storage space utilized by the Zoom account is periodically monitored and abnormalities, if any are promptly reported.

9. Operating Systems Monitoring Enhancements

- **Enhancements to AS400 server Monitoring:** Starting with this version, the jobs executing on the AS400 servers with different status are captured and the count of jobs for each job status is reported. The CPU usage of the jobs are carefully scrutinized and the jobs that exceed the maximum CPU usage are reported. The I/O activity of each disk is monitored and request processing latencies if any are promptly captured and rectified.
- **Windows Defender Event Logs can now be Monitored**: Microsoft Windows Defender aims to keep your PC safe with built-in, real-time protection against viruses, ransomware, spyware, and other security threats. The event logs of Microsoft Windows Defender captures information related to such threats. By periodically monitoring the event logs, eG Enterprise v7.2 promptly captures critical problem events / warnings, and thus enables administrators to fix the problems before any permanent damage is done.
- **Identifying the Linux Processes to which Swap Space is Allocated:** In older versions, when the percentage of swap space on a Linux system was nearing 100%, administrators did not know the exact processes for which swap space was allocated/reserved. Sometimes, a process that is less frequently utilized may be sized with more swap space than it needs. To optimize the allocation of swap space across the processes, starting with this version, detailed diagnostics is offered for the Swap test executing on Linux systems. The detailed diagnostics reveals the processes for which swap space is allocated/reserved. Using this information, administrators can isolate the process for which maximum swap space is allocated/reserved.
- **Monitoring Entropy on Linux Servers:** When building secure systems, having a source of random numbers is essential. Without them, most cryptographic systems break down and the privacy and authenticity of communications between two parties can be subverted. For example, if you are accessing an SSL-enabled website/URL, then, the SSL connections that you are using would require random numbers to ensure a secure connection. Entropy is the measure of the random numbers available from */dev/urandom* on a Linux server, and if users run out of random numbers, they will not be allowed to make SSL connections. Similarly, many applications too need random numbers for their operations for e.g., encryption. An entropy pool is a store of randomness which gets built up by the keystrokes, interrupts, etc. and drained by the generation of random numbers. If the entropy pool has fewer entries, random numbers could not be generated and hence may hamper the functioning of the applications as well as their security. Therefore, it is necessary to keep a vigil on the entries in the entropy pool. eG Enterprise v7.2 helps administrators in this regard. The availability of the entropy pool and the size of the entropy pool is continuously monitored, and administrators are promptly alerted if the count of entries in the pool keeps depleting at a rapid pace.
- **Support Provided to Monitor NTP with Chrony:** In previous versions, eG Enterprise used *ntpd* daemon to report the time difference between the local clock and the designated reference clock. In environments where systems were not permanently connected, or not permanently powered on, the systems took a relatively long time to adjust their system clocks with *ntpd*. This caused a huge difference in the reported NTP offset measure. To avoid such error-prone reporting and ensure that only the actual value of the NTP offset measure is reported always, starting with this version, eG Enterprise v7.2 offers an option to use *chronyd* daemon to report the time difference. Administrators can set the **USE CHRONY** flag to **Yes** in the test configuration page of the **Domain Time Sync** test if the systems in their environment are intermittently accessible.
- **Monitoring Linux services:** In previous versions, eG Enterprise reported the status of services that are configured for automatic startup on Microsoft Windows operating system. Starting with this

version, eG Enterprise is capable of reporting the status and availability of the services executing on Linux operating system.

- **Introduced Security Checks on Windows Operating System:** Nowadays, many environments face frequent security breach which impacts their business significantly. Administrators are, therefore, more concerned about their environment, from a security perspective. To proactively alert administrators on security violations or potential breach, eG Enterprise v7.2 performs the following security checks on Windows operating systems:
    - File/Folder Modification Checks
    - Root/System Folders Checks
    - Service Checks
    - OS Modification Checks
    - Suspicious Process Checks

  By periodically performing these checks, eG Enterprise alerts administrators to the files/folders that were modified, files included to the root/system folders, malicious services that are executing, suspicious tasks and user accounts and suspicious process executing on the Windows operating system.
- **Troubleshooting Server Reboots is now Easy:** In previous versions, administrators were able to figure out when exactly the server rebooted, and how long the server was shut down before it was restarted. However, they were unable to figure out the reason behind reboots –was it due to any maintenance activity? or was it planned as part of system upgrades? To proactively identify the reason behind system reboots, eG Enterprise v7.2 captures the possible shut down reason of a reboot and reports the same as part of the detailed diagnostics of the **Uptime** test. This way, administrators can spend less time troubleshooting unexpected reboots.
- **Enhancements to TCP Traffic Monitoring:** Starting with this version, TCP protocol traffic/retransmission monitoring has been extended to **AIX** and **HPUX** host systems.

10. Database Monitoring Enhancements

Following are the enhancements made in v7.2 with respect to eG Enterprise's capability to monitor databases:

- **Monitoring Snowflake:** Snowflake's Data Cloud is powered by an advanced data platform provided as Software-as-a-Service (SaaS). Snowflake enables data storage, processing, and analytic solutions that are faster, easier to use, and more flexible than traditional databases. The status, availability and statements running on each warehouse is promptly captured and monitored. The query load on each warehouse is monitored and the warehouse that is overloaded is determined. The data load is periodically monitored to determine failures while loading data in bulk and through snowpipe. The tasks executing on Snowflake are monitored, and task failures are captured at the earliest. The usage of Snowflake credits by each service/warehouse is tracked, and the service/warehouse that is utilizing maximum number of credits is identified. The queries executing on each database instance is monitored and the database instance on which maximum queries were blocked or failed with errors is identified. Also, the database instance that is slow in executing the queries can be identified. User connections to Snowflake is periodically monitored and the user with maximum login failures is identified. The replication status of each database instance is monitored and the regions to which data is replicated from a database instance is identified. A built-in One Click Dashboard template is also offered to view the key performance metrics of Snowflake.

- **Monitoring Amazon Aurora Database:** Amazon Aurora is a relational database management system that combines the speed and availability of high-end commercial databases with the simplicity and cost-effectiveness of open-source databases. Aurora is fully compatible with MySQL and PostgreSQL, allowing existing applications and tools to run without requiring modification. eG Enterprise v7.2 is capable of monitoring Amazon Aurora Database. If you have created your Amazon Aurora Database using MySQL DB snapshot, then you can monitor the database using **MySQL on Cloud** monitoring model. Likewise, if you have created your Amazon Aurora Database using PostgreSQL DB snapshot, then you can use the **PostGreSQL on Cloud** monitoring model. The metrics reported for MySQL on Cloud and PostGreSQL on Cloud are extended to Amazon Aurora Database based on the snapshot used to create the Amazon Aurora Database.

- **Monitoring Maria Cluster:** MariaDB Cluster is a Multi Master replication system built from MariaDB Server, MySQL wsrep patch and Galera wsrep provider. MariaDB Galera Cluster is a virtually synchronous multi-primary cluster for MariaDB. It is available on Linux only, and only supports the InnoDB storage engine. eG Enterprise v7.2 monitors the Maria Cluster. The availability and responsiveness of the cluster is periodically monitored, and administrators promptly alerted to the unavailability or poor responsiveness of the cluster. The memory utilization of each cluster node is monitored, and the memory-hungry nodes are identified. The locking activity on each cluster node and the I/O usage of the buffers on each node are monitored and abnormalities (if any) are reported. The queries serviced by the cache are monitored periodically to check whether/not the cache is utilized effectively. The threads, buffers, tables and transactions on each cluster node are also monitored to ascertain the performance of the cluster node. The queries that are running for a longer duration on each cluster node are isolated, so that the reason for their prolonged execution can be investigated. The count of errors encountered while connections to each cluster node were initiated by the hosts are monitored and reported so that administrators can identify the type of errors that are frequently noticed – is it Transient errors? or Permanent errors? or Reverse lookup DNS errors? or Authentication errors? or Handshake errors? etc.

- **Monitoring MongoDB Cluster:** MongoDB Atlas Cluster is a NoSQL Database-as-a-Service offering in the public cloud (available in Microsoft Azure, Google Cloud Platform, Amazon Web Services). eG Enterprise v7.2 monitors the MongoDB Cluster and provides in depth insights into the availability and responsiveness of the cluster. Each node in the cluster is monitored, and the availability and responsiveness of the nodes are reported and those nodes that are in an abnormal state are also highlighted. The status of the cluster processes is monitored periodically and the processes that were stopped and those processes that failed are identified. The memory utilization of each cluster node is monitored, and the memory-hungry nodes are identified. The locking activity on each cluster node and the I/O usage of the buffers on each node are monitored and abnormalities (if any) are reported. The queries serviced by the cache are monitored periodically to check whether/not the cache is utilized effectively. The threads, buffers, tables and transactions on each cluster node are also monitored to ascertain the performance of the cluster node. The queries that are running for a longer duration on each cluster node are isolated, so that the reason for their prolonged execution can be investigated.

- **Enhancements to Oracle Cluster Monitoring:** eG Enterprise's Oracle Cluster monitoring has been significantly enhanced in v7.2. eG Enterprise is now capable of monitoring the database instances on the Oracle Cluster on which the Oracle DataGuard feature is enabled. Administrators are promptly alerted to the abnormal state of the primary/secondary database servers, a wide archive gap between the primary and secondary servers, and errors encountered. The Explain plans executing on each database instance in the Cluster is closely monitored and the explain plans that were changed during query execution are tracked. The sessions and processes executing on each database instance on the Oracle Cluster is periodically monitored and the sessions/processes that are consuming excessive resources are identified. Oracle RAC 11g release 2 has introduced the Single Client Access Name (SCAN), which provides a single name for clients to access Oracle Databases running in a cluster and simplify the database connection strings that an Oracle Client uses to connect. The status of each SCAN listener is monitored and the SCAN Listeners that are not enabled

and are not running are identified. To evaluate the load balancing ability of the SCAN listeners in a cluster, the connection traffic to each node in the Oracle cluster is monitored and reported. The SCAN VIPs that are not running are promptly identified along with the SCAN VIPs that were relocated on each node due to failover.

- **Troubleshooting Oracle Root Blocker Processes is now easier:** eG Enterprise is capable of capturing root blocker processes (of the Oracle Database server) and reporting the queries issued by these processes as part of detailed diagnostics. An administrator will have to optimize these queries to remove the blocks and improve database performance. For query optimizations, administrators need to study the execution plan. An execution plan is a set of steps that are executed to complete a query. By analyzing the execution plan, administrators can drill down to the exact step that either took too long to execute or is executing in a loop. By addressing the lapses indicated by the execution plan, administrators can build better queries and eliminate root blockers. This is why, starting with eG Enterprise v7.2, the detailed diagnostics of the **Oracle Root Blockers test** includes an Execution Plan column, which will detail the steps that were executed to complete the query.

- **Troubleshooting Long Running Queries is now easier:** eG Enterprise is capable of capturing the count of queries that are running for a duration longer than the configured time and reporting the exact long running queries as part of detailed diagnostics. An administrator will have to optimize these queries to reduce the execution time and improve database performance. For query optimizations, administrators need to study the execution/explain plan. An explain/execution plan is a set of steps that are executed to complete a query. By analyzing the explain plan, administrators can drill down to the exact step that either took too long to execute or is executing in a loop. By addressing the lapses indicated by the execution/explain plan, administrators can build better queries and reduce the query runtime. This is why, starting with eG Enterprise v7.2, the detailed diagnostics of the Oracle Long Running Queries test, **Maria Long Running Queries** test and **MySQL Long Running Queries** test includes an Explain Plan column, which will detail the steps that were executed to complete the query.

- **Enhancements to PostgreSQL Monitoring:** Starting with eG Enterprise v7.2, the replication mechanism of the PostgreSQL database server is monitored, and a host of useful metrics are reported. The replication status is reported along with the count of replica servers attached to the database server. Administrators can also determine the amount of data that is yet to synced with the replica servers and the time lag noticed in the transport of logs during replication. In the process, administrators can figure out if the data on the replica server is in sync with the primary server at all times. Root blocker processes are captured, and queries issued by those processes are reported as part of detailed diagnostics. Each wait event on the PostgreSQL database server is monitored, and the wait event with maximum wait time is captured and reported. Deadlocks are promptly captured, and queries affected by those deadlocks and the user who issued the queries are reported as part of the detailed diagnostics.

- **Enhancements to Db2 UDB Monitoring:** eG Enterprise v.7.2 is loaded with significant enhancements to monitor Db2 UDB servers. The applications running on each DB2 UDB server are monitored and the applications that are utilizing maximum CPU time and performing maximum reads/writes are identified. The status of each database instance in the target Db2 UDB server is monitored, and the standby databases are quickly identified. The databases that are running out of space can also be determined with ease. The space utilized by the transaction log is closely monitored and abnormal growth in size of the transaction log promptly captured and reported. Queries that are executing for a longer duration are isolated and reported so that administrators can optimize such queries and improve the overall performance of the database. The replication mechanism is monitored, and the replication status is reported. Administrators can also figure out if the secondary database server is active or not in a high availability setup. Administrators can also determine the amount of data that is yet to be synced with the secondary servers and the time lag noticed in the transport of logs during replication. In the process, administrators can figure out if the data on the secondary database server is in sync with the primary at all times. The replication heartbeats are also closely monitored, and heartbeat failures are captured proactively.

- **Enhancements to MySQL Monitoring:** With v7.2, eG Enterprise's MySQL Database server monitoring capabilities have been significantly enhanced to report a slew of metrics relating to deadlocks, tablespaces, logs and many more. The MySQL database instances on which deadlock detection is enabled are identified and the count of deadlocks are reported. The error log and general query log are monitored, and the log size is reported. In the process, abnormalities noticed in the growth rate are promptly detected and averted. Root blocker processes are captured, and queries issued by those processes are reported as part of detailed diagnostics. Each wait class on the MySQL Database server is monitored, and the wait class with maximum session waits is captured and reported. Slow queries are promptly reported by analyzing the slow query log. Abnormal growth rate of the slow query log is also captured. Full table scans that happened on the database are proactively captured and the root-cause of such scans is identified. The temporary tables and the wait time for locks are also periodically monitored to ensure that the performance of the database server is at its peak always. Starting with this version, eG Enterprise is capable of monitoring SSL-enabled MySQL database servers.

- **Enhancements to MySQL Cluster Monitoring:** eG Enterprise's MySQL Cluster monitoring capabilities have been enhanced in v7.2 to provide in-depth insights into the deadlocks encountered by the InnoDB engine and the workload of the cluster. The queries executing for a longer duration are identified and inefficient queries are isolated for optimization. The status of each tablespace in the database instances on the MySQL Cluster is monitored and corrupted tablespaces are promptly identified and removed. The space utilization of each tablespace is closely monitored and the tablespaces that are running out of space are promptly detected. The tables that have outgrown based on their configured size and table rows are also promptly identified and reported.

- **In-depth Analysis of Threads executing on Microsoft SQL Database Server:** v7.2 of eG Enterprise is capable of capturing metrics related to the utilization of threads executing on the target Microsoft SQL server. Active threads and threads waiting in queue serve as good indicators of the workload on the server, and whether the server has adequate processing power to handle the load. Idle threads are also captured and reported.

- **Capturing Additional Memory Allocated to PGA is now possible:** If the PGA runs out of memory space, certain critical server processes may not run. To ensure uninterrupted execution of the server processes, in some scenarios, Oracle Database, by default, allocates additional PGA memory to the originally allocated PGA memory. eG Enterprise v7.2 captures this additional memory that was allocated and reports the same. By continuously monitoring the PGA memory that was additionally allocated, administrators can decide if they should consider resizing the PGA memory region.

- **Enhancements to SAP HANA Database server:** eG Enterprise v7.2 is capable of monitoring SAP HANA Multitenant Database structures. When monitoring a multi-tenant SAP HANA Database structure using eG Enterprise, make sure you manage each instance/database of the setup as a separate SAP HANA Database server component.

  eG Enterprise v7.2 is now capable of monitoring SAP HANA Extended Application Services integrated into the SAP HANA Database server. eG Enterprise offers in-depth insights into the status of the SAP HANA XS service and overall performance of the XS service by reporting the count of applications and instances. Each application is monitored, the count of crashed instances and stopped instances are promptly captured, and the failure reason is duly reported. The actual state of each application is tracked and reported along with its memory utilization. The log file is periodically monitored, and error-prone applications are isolated by tracking the error messages recorded for those applications.

- **Enhancements to Microsoft SQL Azure Database Monitoring:** eG Enterprise's Microsoft SQL Azure Database server monitoring capabilities have been enhanced in v7.2 to provide the following insights:

  - Tracks the resource usage of the sessions to Microsoft SQL Azure Database server. In the process, it turns the spotlight on resource-intensive sessions and the queries executed by

such sessions that may require fine-tuning. Additionally, it also reports the average wait time of sessions, leads you to that session that has been waiting for the maximum time, and points you to the exact query that the session has been taking too long to execute. Inefficient queries are thus revealed, enabling you to quickly initiate query optimization measures.

- Monitors the uptime of the Microsoft SQL Azure Database server and in the process, captures sudden breaks in server availability and unscheduled server reboots.
- Monitors the locking activity on the Microsoft SQL Azure Database server and in the process, reveals the lock type for which maximum number of lock events were registered.
- Reports the queries that have been running for a longer duration so that such queries can be optimized.
- Monitors the processes running on the Microsoft SQL Azure Database server and in the process, reports the processes that are blocked and suspended.
- Monitors the indexes on the database server and reveals the indexes that are unused. This way, the performance of the database server can be substantially improved.
- Tracks the growth of the tables periodically and in the process, identifies and reports the tables that have recorded tremendous growth in recent times.

- **Support to Monitor Multiple Listeners listening to a Single Oracle Database Instance:** In some environments, administrators may configure multiple listeners that listen to a single Oracle database instance so that the incoming connections can be load balanced and high listener availability can be ensured. To ensure that more than one listener is monitored in a hassle-free manner, eG Enterprise has improvised the **Oracle Listener** test. Setting the **Is Multiple Listeners** flag to **Yes** will ensure that all the listeners listening to the same Oracle database instance are auto discovered and metrics are collected and reported for each listener.
- **Monitoring SSL-enabled IBM Db2 UDB Servers:** Starting with this version, eG Enterprise is capable of reporting metrics for SSL-enabled IBM Db2 UDB servers.

10.1 Reporter Enhancements for Microsoft SQL Database Servers

For a database administrator, one of the foremost tasks is to track the performance of the database and maintain the database servers at optimal performance levels. For this purpose, G Enterprise v7.2 offers extensive reports that help administrators analyze the trend on the following:

- Missing Indexes
- Unused Indexes
- Overall Instance Performance
- Uptime
- Databases
- Query caches
- Root blockers
- Top queries
- Long Running Queries
- Errors etc

Following are a few reports that are explained in detail:

- **Instance Performance Report:** Use the Instance Performance report to perform periodic service level audits on a chosen database server, and isolate the exact dates during the given period when the guaranteed availability and response time levels were not met. The report also reveals the total

number of alerts that were raised during the given period owing to availability and response time issues. Administrators can even zoom into these alerts to understand when they occurred, and what might have caused them. This information also enables them to determine how frequently such issues occurred, and whether there is cause for concern.

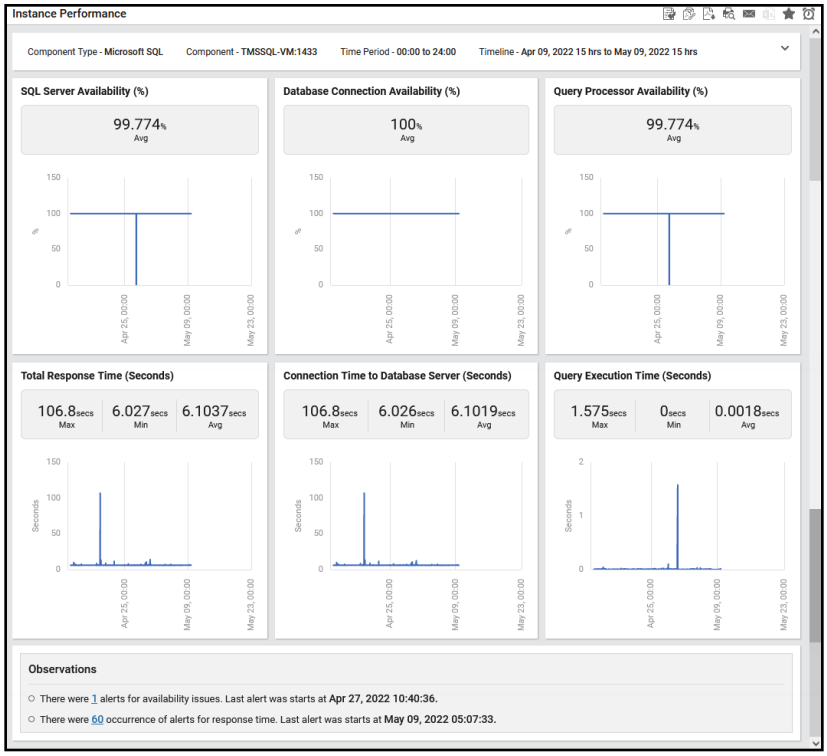


Figure 86: The Instance Performance Report

- **Missing Indexes Report:** Using this report, administrators can closely study the time-of-day variations in the count of indexes that are missing on a chosen database server, during a specified timeline. This will reveal if the query optimizer frequently spotted indexes it would have liked to see in the tables but could not find. This in turn implies that inoptimal queries are often run on the server. The report also points administrators to the precise database on which many queries missing indexes are run. Additionally, you can use the report to quickly get to the exact tables and table columns that are missing indexes. This way, the report helps administrators to go from problem symptom to problem source in no time! Administrators can use the statistics provided by the report to decide on the ideal approach to improving query performance – should new indexes be created? or should

queries be optimized to use existing indexes?

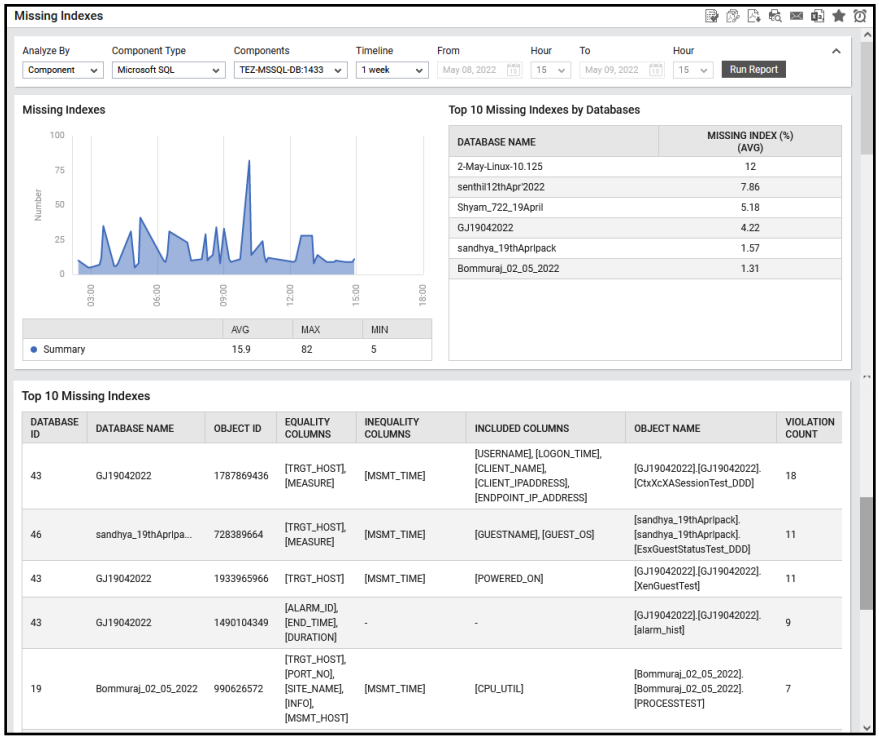


Figure 87: The Missing Indexes Report

- **Databases Report:** Use the Databases report offered by eG Enterprise to historically analyze the transaction load on each database instance on the target database server. Using this report, administrators can identify those databases that were online/offline as well as isolate the databases that experienced an influx of transactions over a period of time. By carefully analyzing this report, administrators can fine tune the memory allocated to the databases based on the transaction log size and the wait time to flush the log files. eG Enterprise also offers an **Observations** section in the generated report which quickly helps administrators to identify the databases that encountered

high transaction log usage and log flush wait time over the chosen time period.

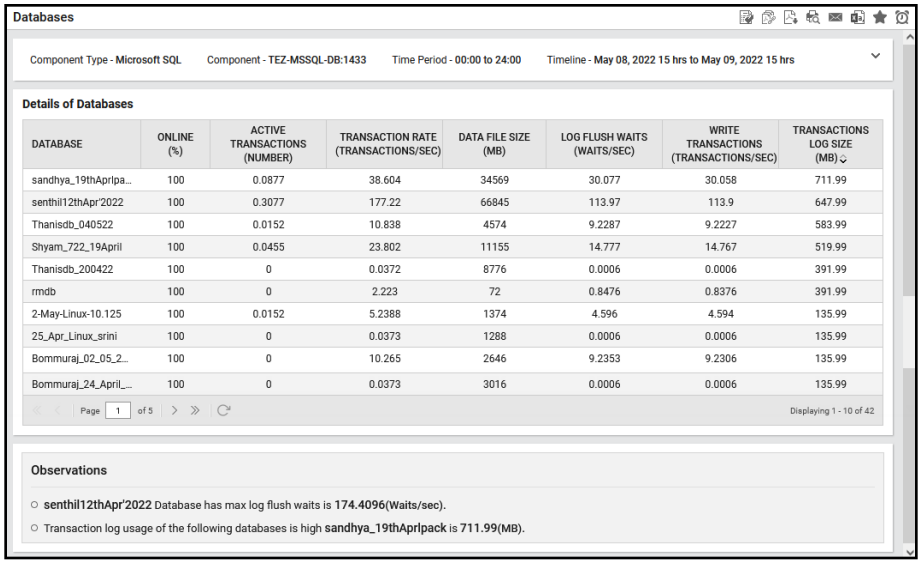


Figure 88: The Databases Report

- **Workload Report:** Use this report to assess cache usage over time and analyze its impact on the query processing ability of the chosen database server. By enabling administrators to compare the rate of physical and logical reads during the selected timeline, the report reveals how most of the queries were serviced in that time period – by directly accessing the disk or by using the cache. A low rate of logical reads is indicative of poor cache usage. The report also tracks the CPU usage of the queries during the given timeline. From this, administrators can determine if the queries were consistently hogging the CPU resources of the server. Excessive CPU usage can indicate that the query load on the server was high during the said period, or that many sub-optimal queries were processed in that timeline. Also, using the report, cache usage levels between the chosen time period and the week before it can be quickly compared, and significant spikes/drops in usage can be detected. Administrators may then want to investigate the reason for the unusual highs and lows (if

any) in cache usage.

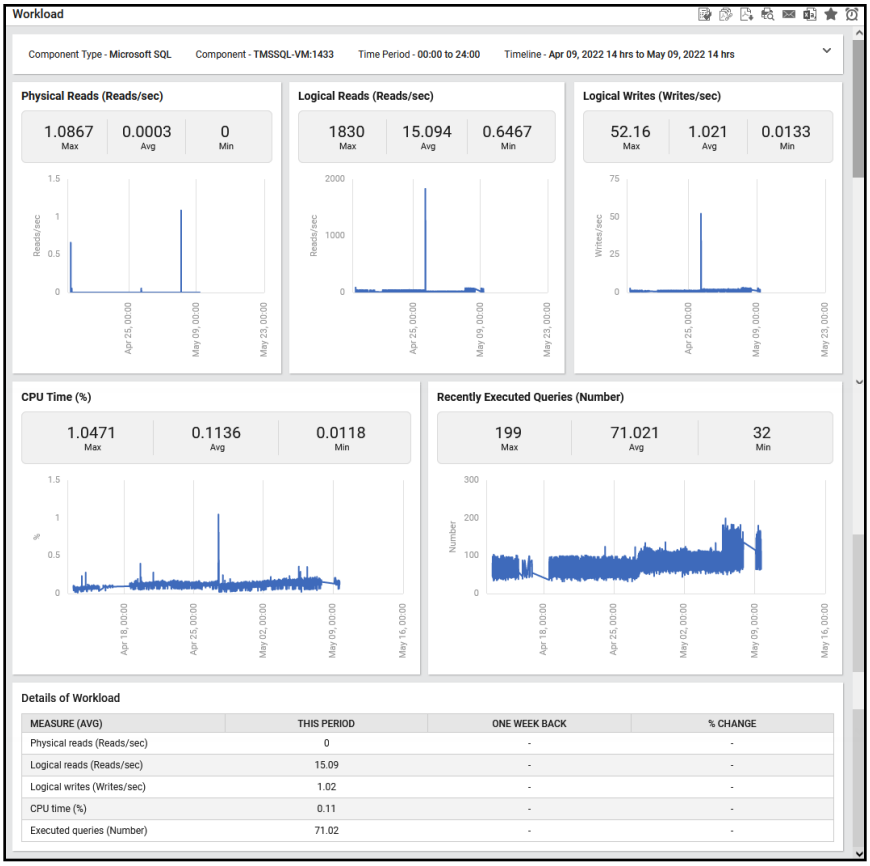


Figure 89: The Workload Report

- **Query Blocking Report:** One of the most common problems encountered with databases is blocking. What matters to a database administrator is identifying when blocking is a problem and how to deal with it effectively. When blocking is bad enough, users will notice slowdowns and complain about it. With many users, it is common for tens or hundreds of processes to be blocked when slowdowns are noticed. When you have lots of blocking that is not resolved in a reasonable amount of time, you need to identify the root blocker, or the process at the top of the tree of blocked processes. To historically analyze blocking and the root blockers responsible for it, administrators can use the Query Blocking Report. This report helps administrators study past trends in blocking. The trend analysis reveals whether/not the count of blocking processes spiked every time the count of root blockers did. The report also pinpoints the exact day on which the root blockers and blocked processes were at their peak. Additionally, the report enables administrators review the queries that are blocking other queries, so that they can figure out the reason on why the queries are blocking

and optimize the query line so that it no longer blocks.

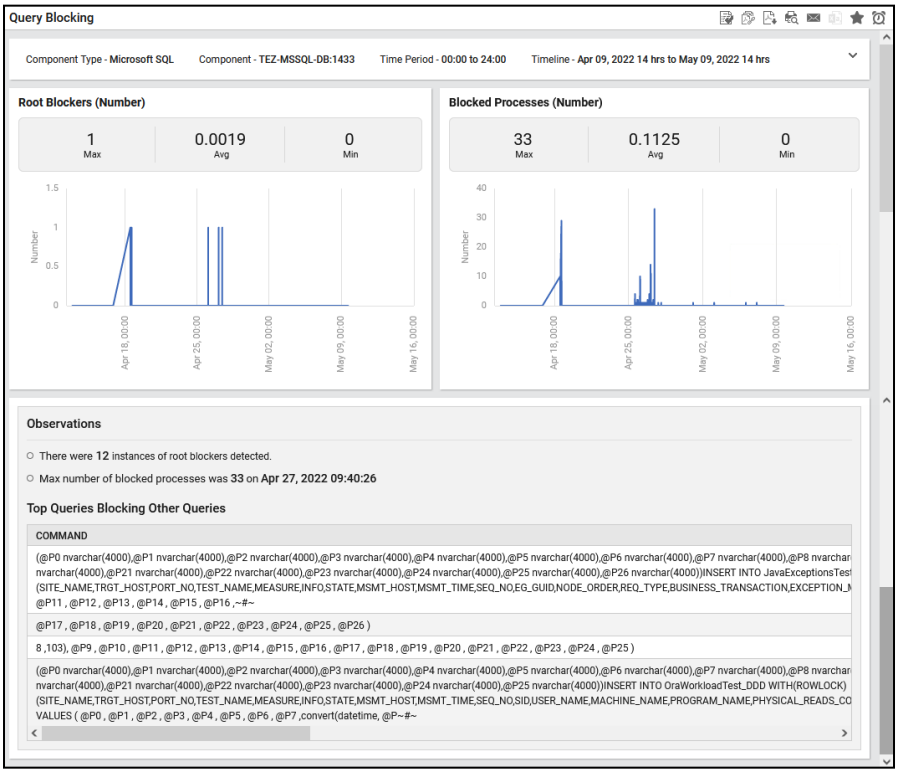


Figure 90: The Query Blocking Report

11. Mobility Monitoring Enhancements

- **Monitoring VMware Airwatch:** Mobile Device Management (MDM) is the foundation of a comprehensive Enterprise Mobility Management (EMM) platform. VMware AirWatch Mobile Device Management provides a simplified, efficient way to view and manage a diverse fleet of devices from a central admin console. EventTracker collects the logs, helps administrators to analyze the events and generate the reports. eG Enterprise v7.2 is now capable of monitoring VMWare Airwatch. The events recorded for each event type is monitored and the event type with maximum number of events is isolated for further analysis.

12. Enhancements to Monitoring Messaging Servers

- **Monitoring Apache Kafka Message System:** Apache Kafka is an open-source distributed event streaming platform used by thousands of companies for high-performance data pipelines, streaming analytics, data integration, and mission-critical applications. eG Enterprise monitors the Apache Kafka Message System and provides a wide range of useful performance metrics. The status of Apache Kafka's connection to Apache Zookeeper is monitored and authentication failures, disconnected clients, and expired clients to the Apache Zookeeper are promptly captured. The count, I/O

Operations, and throughput of the Apache Kafka consumers are monitored, and discrepancies brought to light. The I/O operations, request processing capability and response time of the Apache Kafka producers are monitored and discrepancies in authentication failures and errors are proactively identified. The Kafka coordinator groups are monitored and groups that are dead and are empty are promptly reported. The state of the Kafka Controller, the topics to be deleted from the controller are monitored periodically and reported. The I/O processing ability and request/message processing ability of the Broker topics are monitored, and discrepancies brought to light.

- **Monitoring AWS MSK:** Amazon Managed Streaming for Apache Kafka (Amazon MSK) is a fully managed, highly available Apache Kafka service that enables administrators to build and run applications that use Apache Kafka to process streaming data. eG Enterprise v7.2 offers a specialized monitoring model that provides deep insights into the performance of the Amazon MSK and proactively alerts administrators to probable performance lags. The network availability and responsiveness of AWS MSK are periodically checked, so that the unavailability and poor responsiveness of MSK can be promptly captured. The CPU and broker memory utilization of the Amazon MSK is continuously monitored, and administrators are alerted to potential resource constraints. The health of the network connection to/from the AWS MSK is determined by looking out for packets dropped and errors encountered during transmission/reception. Critical statistics related to partitions, swap memory, request processing ability, bandwidth overflow, and thread handlers on the cluster are periodically reported, and administrators alerted to potential abnormalities. Alerts are also sent out, if:
    - The cluster is in an abnormal state;
    - Data logs are occupying excessive space in the cluster;
    - The Apache Zookeeper is unreachable or is taking too long to receive requests from the broker;
    - Abnormal I/O activity is noticed on one/more volumes;
    - Read operations are slow on one/more volumes etc.
- **Monitoring Apache Qpid Java Broker:** Apache Qpid Broker-J is a message broker written in Java that stores, routes, and forwards messages using Advanced Message Queuing Protocol (AMQP). Apache Qpid Broker-J acts a middleman for various applications (e.g., web application). eG Enterprise offers a dedicated Apache Qpid Java Broker monitoring model to monitor the Apache Qpid Broker-J. The status of each Control Provider and Authentication Provider is monitored and error-prone and stopped providers are identified. Logs are scanned periodically, so that errors/warnings logged can be promptly captured. The state of each connection and data transmission through each connection is monitored, and administrators alerted to abnormalities. The sessions initiated by each connection reveals the load on the connection. The queues on the message broker are periodically monitored and the queues that are stopped/error-prone/uninitialized are identified. Administrators are also pinpointed to the queue that is handling maximum number of messages and the queue that holds maximum number of expired messages. The status of each port is determined periodically and the ports that are stopped/unavailable/uninitialized/error-prone are promptly detected and reported. The port through which maximum number of connections were established is also identified with ease. The status of each virtual host and the data transmission through each virtual host is monitored and the virtual host that is error-prone/stopped is identified.
- **Enhancements to IBM WebSphere MQ Monitoring:** Starting with this version, eG Enterprise offers an improvised capability to monitor IBM WebSphere MQ servers. The status of MQ File transfer agents is periodically monitored, and the agents that are stopped/unreachable/problematic are isolated. The status of file transfer is periodically assessed and the files that failed during transfer are easily identified. MQ event messages are continuously monitored, and administrators are alerted to the event messages (for e.g., Alias base queue type error, Channel SSL error etc) that are frequently noticed. Dead letter queues are monitored and the dead letter queue holding maximum number of undelivered messages are identified. The transmit queues are periodically monitored and

the transmit queue with maximum number of messages are identified.

- **Monitoring Solace Message Broker:** Solace Message Broker is a complete event streaming and management platform for real-time enterprises. It helps enterprises design, deploy, and manage event-driven architectures (EDAs) across hybrid cloud, multi-cloud, and IoT environments, so that they can be more integrated and event-driven. Starting with eG v7.2, eG Enterprise monitors the Solace Message Broker and reports wide range of useful performance metrics. Hardware components such as fans, power supplies, voltage sensors and temperature sensors of the broker are periodically monitored, and the hardware component failures are proactively captured and reported. The memory utilization of the broker is monitored round the clock and abnormal memory usage patterns are promptly captured. The Message VPN clients are closely monitored and the Message VPN Clients that are handling maximum ingress and egress byte traffic are identified. The status and resource utilization of the message spool is monitored periodically, and abnormalities are brought to light. The status and resource utilization of the message spools are monitored periodically, and abnormalities are brought to light.
- **Enhancements to RabbitMQ Clusters:** Starting with this version, eG Enterprise is capable of monitoring Rabbit MQ Clusters enabled with Mutual TLS authentication. In order to collect metrics from such RabbitMQ clusters, the eG agent should be configured with the exact path to the TrustStore file and the Private Key File. To this effect, additional parameters such as **TIMEOUT**, **TRUSTSTORE FILE**, **PRIVATE KEY FILE**, **PRIVATE KEY FILE PASSWORD**, **CONFIRM PASSWORD** and **TLS VERSION** have been introduced in the test configuration page. The disk space utilization of each node in the RabbitMQ Cluster is also monitored and the node that is running out of disk space is highlighted.

13. Application Middleware Monitoring Enhancements

Big Data is a collection of data that is huge in volume yet growing exponentially with time. Few environments where Big Data plays a major role are Stock exchanges, Social Media websites, Air Traffic Control sites etc. To handle Big Data and perform Big Data Analytics, a lot of new technologies have been introduced in the market in recent times. eG Enterprise v7.2 adds out-of-the-box monitoring support for a few popular Big Data technologies that are enumerated below:

- **Monitoring Apigee Edge:** Apigee Edge is a platform for developing and managing APIs. Apigee Edge enables you to provide secure access to the services with a well-defined API that is consistent across all services, regardless of service implementation. The request processing ability of each API/API product/API program/API resource is monitored, and error-prone APIs/API products/API programs/API resources are isolated. Also, the API products/API programs/API resources with maximum request processing latencies are identified. The performance of each developer is closely monitored by tracking the count of application registered by each developer and the end users associated with each developer. Each application is periodically monitored, and the most sought-after application is identified. In the process, administrators are also pinpointed to the application that is slow in processing requests and that is frequently prone to errors.
- **Monitoring Apache Zookeeper:** Apache Zookeeper is an open-source Apache project that provides a centralized service for providing configuration information, naming, synchronization, and group services over large clusters in distributed systems. The status of the Apache Zookeeper, packet transmission, count of znodes and ephemeral nodes, and pending synchronization operations are monitored, and abnormalities promptly brought to the attention of administrators. The resource utilization of the Apache Zookeeper is periodically monitored, and unusual resource usage patterns are highlighted. For each client, the packet transmission, open connections , and request processing

latency of that client are monitored. In the process, the client who is overloading the server, and whose requests are processed sluggishly are revealed.

- **Monitoring Apache Solr:** Apache Solr is one of the most popular, blazing-fast, open-source enterprise search platforms built on Apache Lucene. Apache Solr is reliable, scalable and fault tolerant, providing distributed indexing, replication and load-balanced querying, automated failover and recovery, centralized configuration and more. Apache Solr powers the search and navigation features of many of the world's largest internet sites. To periodically check the efficiency of this search engine and to proactively alert administrators to inconsistencies in its performance, eG Enterprise v7.2 offers a specialized monitoring model for Apache Solr. Using the eG Monitor for Apache Solr, administrators can monitor the Lucene index. The administrative task handlers, update handlers, and search queries on the Lucene index are monitored periodically. Alerts are sent out if any handler and/or search query is error-prone and is taking too long to process requests. The count of cache indexes and the number of documents added to the cache indexes can be measured. eG Enterprise also reports whether replication is enabled on each index. If it is, eG additionally measures the request processing capability of every index. Those indexes experiencing processing bottlenecks are thus highlighted.

- **Monitoring Apache Hive:** Apache Hive is a distributed, fault-tolerant data warehouse system that enables analytics at a massive scale. A data warehouse provides a central store of information that can easily be analyzed to make informed, data driven decisions. eG Enterprise v7.2 monitors Apache Hive and provides in-depth insights into the active and open sessions on the Hive. The Hive cache is monitored, and the count of cache misses are reported, so that administrators can determine whether/not the cache is effectively used. Connection requests and the count of connections that are available in the connection pool are promptly captured and reported. With the help of these statistics help administrators in connection pool sizing. Space utilization of the memory pools are monitored and memory pools with space constraints are identified and reported at the earliest. The buffer pools are periodically monitored and buffer pools with memory constraints are identified. Anomalies are brought to light by monitoring the error messages logged in the logs of Apache Hive.

- **Monitoring Apache Zeppelin:** Apache Zeppelin is a web-based notebook that enables data-driven, interactive data analytics and collaborative documents with SQL, Scala, Python, R and more. eG Enterprise v7.2 monitors the Apache Zeppelin and reveals the number and state of notebooks and paragraphs. This way, it turns the spot light on notebooks and paragraphs that are in an abnormal state.

- **Monitoring Apache Ignite:** Apache Ignite is a distributed database for high-performance computing with in-memory speed. Apache Ignite helps deliver projects faster while giving companies a foundation for a more real-time, responsive digital business model and the ability to be more flexible to change. eG Enterprise v7.2 monitors the Apache Ignite and provides insights into the hits and misses of the cache entry processor and cache off-heap. The cache rebalancing ability of the Apache Ignite is continuously monitored to find out how well the rebalancing activity is performed on a node. The Write-Behind Caching capability of the Apache Ignite is monitored, and the count of entries to be flushed, the flushing interval and the maximum size of the Write-Behind Cache are reported. The job processing ability of the cluster is monitored and reported. The metrics also reveal how well the RAM space allocated for data region is utilized, and thus sheds light on potential RAM contentions. The growth of the outbound message queue is tracked, and any abnormal growth rate is brought to the attention of administrators. The TCP/IP Discovery ability is measured based on factors such as the health of the Discovery SPI, whether/not any nodes have failed / have left the cluster, and the message processing speed. The count of transactions committed to and rolled back from each node and the count of transactions holding locks on the node are proactively reported. The main cache is monitored to figure out if the cache is enabled with different features. The efficiency of the cache is gauged by measuring the hits and misses to the cache, the transactions

committed to and rolled back, and the time taken to execute the transaction.

- **Monitoring Apache Impala:** Apache Impala is a modern, open source, distributed SQL query engine for Apache Hadoop. eG Enterprise v7.2 provides deep dive insights into the performance of Apache Impala. The uptime of each Impala daemon is measured. In the process, unexpected restarts and unscheduled reboots are brought to light. The queries are continuously monitored and the queries with exceptions are promptly identified and reported. The overall performance of the queries is measured periodically to ensure that the query spillage and query fragmentation is kept under control. The sessions initiated by each client type are closely monitored and the count of sessions that are inactive/expired/closed are identified. The throughput of the IO Manager is periodically assessed and discrepancies if any, are brought to light. The count of remote procedure calls made by servers such as backend server, beeswax server, catalog daemon server etc to each endpoint service is monitored and the endpoint service to which maximum number of remote procedure calls are made is identified. The JVM memory utilized by each JVM memory area that runs the Impala daemon and Catalog daemon is periodically monitored, and the JVM memory area that is running out of memory is promptly identified.

- **Monitoring Apache Storm:** Apache Storm is a distributed real-time big data-processing system. Storm is designed to process vast amount of data in a fault-tolerant and horizontal scalable method. eG Enterprise v7.2 provides insights into the performance of Apache Storm so that administrators are proactively alerted to probable performance issues. The resource (memory and CPU cores) utilization is periodically monitored and resource constraints if any, are proactively detected. The count of supervisors, topologies and worker slots in a Storm cluster help administrators assess the sizing of the cluster. Each Storm worker is monitored and the storm worker that is assigned with maximum on/off heap memory is identified. The Storm worker that is up for the longest duration too can be isolated. The status, uptime and resource utilization of each Storm topology is monitored and the topology that is offline and utilizing maximum resources can be identified. The resource utilization of each owner is periodically monitored and the owner who is consuming maximum resources is identified. By periodically monitoring the uptime and resource utilization of each Storm supervisor, administrators can isolate the supervisor that is consuming maximum resources. The status and uptime of the Storm Nimbus is also tracked and reported.

- **Monitoring IBM Cognos Business Intelligence:** IBM® Cognos® Business Intelligence is an integrated business intelligence suite that provides a wide range of functionality to help you understand your organization's data. IBM Cognos BI can be used to view or create business reports, analyze data, and monitor events and metrics so that the organization can make effective business decisions. eG Enterprise v7.2 monitors each service started by the dispatcher of the IBM Cognos Business Intelligence and reports a host of performance metrics. The request processing ability of each service is monitored and the service where request processing failed often is identified. The space used by the Content manager service is continuously tracked, and administrators proactively alerted to a potential space crunch. The Graphics service, Report service and MetaData service are periodically monitored, and abnormalities (if any) in their operations are promptly captured.

- **Enhancements to Monitoring Mule ESB:** Mule ESB is a widely used integration platform for connecting enterprise applications on-premises and in the cloud. Starting with this version, the scope of monitoring Mule ESB has been extended to report a variety of metrics that offer insights into the applications executing on Mule ESB. The memory utilized by each application is monitored periodically and the application that is consuming maximum memory resources is isolated. The application flows that are processing slowly, that are overloaded, and those that are error prone can be pinpointed with ease.

- **Monitoring Mule ESB Cloud:** eG Enterprise v7.2 is capable of monitoring Mule ESB hosted on cloud and provides a wide range of metrics that help administrators assess the overall Mule infrastructure by scrutinizing the count of load balancers, static IP consumption, sandbox applications etc. The applications deployed on the CloudHub are periodically monitored and the applications that are stopped/not deployed/failed are isolated. The log of each application instance is carefully

analyzed to quickly capture errors/warnings. This way, administrators can be proactively pointed to application instances that are troublesome. The resources utilized by each worker accessing the applications are monitored and the worker who is over-utilizing the resources are identified with ease. The application queues are periodically monitored, and abnormal queues are isolated.

- **Enhancements to Redis Monitoring:** Starting with this version, eG Enterprise is capable of monitoring the Redis streams in a Redis Cluster and provides the overall performance of the Redis streams. Memory utilization of each Redis stream is periodically monitored so that administrators are alerted to potential memory crunch on the streams. Pending entries on each Redis stream group helps administrators isolate the stream group with maximum number of entries. In previous versions, the eG agents collected performance metrics from the Redis servers that do not require authentication as well as from the Redis servers that are password protected. However, with the advancement of technology, newer versions of Redis server require users to be authenticated via Access Control List. To collect metrics from the newer versions of Redis servers, starting from this version, the eG agent requires the credentials of a user with read-only privilege to connect to the Redis server and collect metrics. To this effect, a **USERNAME** parameter has been included in the Test configuration page.
- **Monitoring Regex Log:** Regular expression (regex) is widely used to identify character patterns. Regex can be used to validate the text input such as passwords and phone numbers or parse text data into a more structured format. eG Enterprise v7.2 offers an exclusive Regex Log Monitor monitoring model to monitor the Regex. Each log file parsed by the Regex Log Monitor is meticulously monitored and the count of lines that match each priority message type is reported. In the process, the lines that were discarded/duplicated for each priority message type is also captured. By carefully analyzing the lines in the log files, administrators are also pointed to the error messages so that they can further analyze the root cause of issue highlighted in the log file.

14. Storage and Backup Monitoring Enhancements

14.1 Storage Enhancements

The following enhancements have been made to eG Enterprise's storage monitoring capabilities in v7.2:

- **Monitoring EMC Centera:** EMC Centera is the world's first content addressed storage (CAS) solution specifically designed to meet the unique requirements of "fixed content" - unchanging digital assets retained for active reference and long-term value. eG Enterprise v7.2 monitors EMC Centera, and proactively alerts administrators to probable issues in its performance. The capacity of the Centera Cluster is periodically monitored, and alerts are raised when the capacity increases at an alarming rate. The status and capacity of each node is monitored, and faulty nodes are isolated. The read/write transactions on the EMC Centera are closely monitored using which the efficiency and throughput of EMC Centera is ascertained. The capacity of each Centera pool is monitored and alerts are raised when the capacity of the pool exceeds a pre-configured limit.
- **Monitoring EMC PowerVault ME:** The Dell EMC PowerVault ME storage system is a high-performance storage solution that provides direct attached, external shared storage services. To continuously monitor the availability and overall performance of the Dell EMC PowerVault ME storage system, promptly detect sensor failures, disk failures, and I/O overload conditions, and proactively alert administrators to such anomalies, eG Enterprise v7.2 offers the Dell EMC PowerVault ME monitoring model. This model monitors the storage system inside-out and sheds light on current or probable performance dips that the storage system suffers. Slow vDisks, and volumes, controllers

hogging CPU, and unhealthy disks and host ports can be isolated in the process.

- **Enhancements to HP 3PAR Storage Server Monitoring:** A Common Provisioning Group (CPG) is a virtual pool of Logical Disks that allocates space to virtual volumes (VV) on demand. A CPG allows VVs to share the CPG resources. Starting with this version, eG Enterprise auto-discovers the CPGs, and monitors how each CPG uses the storage space allocated to it. In the process, the snap storage space and admin storage space are reported for every CPG. This way, administrators can identify which CPG is running out of space. The space utilized by each disk is monitored and the disk that is running out of space is identified with ease. Administrators are also alerted to failed /degraded disks. The LUNs are periodically monitored and the LUN that is utilizing maximum amount of snapshot administration space, snapshot data and user space is reported.

14.2 Monitoring Backup Technologies

- **Monitoring Cohesity Backup:** Cohesity provides a backup and recovery solution that converges multiple point products and backs up data whether it is stored on-prem, at the edge, or in the public cloud on a single multi-cloud data platform. Cohesity Data Platform provides scale-out, globally deduped, highly available storage to consolidate all your secondary data, including backups, files, and test / dev copies. eG Enterprise v7.2 is capable of providing deep-dive insights into the performance of and problems encountered by the Cohesity Backup solution. The status of the hardware components such as fans, power supplies and CPUs are periodically monitored and the hardware components that are 'down' are promptly isolated. Fans and CPUs operating at an abnormal speed can be pinpointed, so they can be repaired. eG Enterprise also measures how each cluster is utilizing the space available to it, thus turning the spotlight on those clusters that are running out of space.
- **Monitoring ExaGrid Backup Server:** The ExaGrid system is a disk backup appliance with data deduplication that works with existing backup applications. ExaGrid uses compression and data deduplication (sometimes called Capacity optimization) to minimize the amount of data stored. eG Enterprise v7.2 can perform specialized monitoring of ExaGrid Backup Servers. This Monitor alerts administrators if any slowness in noticed when data is read from the retention repository disk, when it is written to the disk landing zone, or when deduplicated. Administrators are also notified if space in the retention repository disk and disk landing zone are being rapidly drained. Irregularities in the backup operations can thus be detected and repaired.

15. Hardware and Networking Technologies Monitoring Enhancements

The following enhancements have been made to eG Enterprise's network monitoring capabilities in v7.2:

- **Monitoring IBM DataPower:** IBM DataPower Gateway is a single multichannel gateway that helps provide security, control, integration, and optimized access to a range of mobile, web application programming interface, service-oriented architecture, B2B and cloud workloads. eG Enterprise v7.2 monitors IBM DataPower and reports a slew of performance metrics. The temperature of the hardware components such as CPU, power supply units is monitored, and abnormal temperature fluctuations are brought to light. The CPU, memory and space utilization of the File System and each Power raid is monitored, and abnormal resource usage patterns are proactively captured. The connection requests received by each XML manager, the connections that were created and reused are monitored and the XML manager that received the maximum number of connection requests is identified. The number of users accessing the IBM DataPower gateway is monitored and

disconnected users are identified instantly.

- **Monitoring DELL EMC S-Series OS10 Switch:** Starting with this version, eG Enterprise is capable of monitoring Dell EMC S-Series Switch with Operating System 10. To this effect, Dell EMC S-Series OS10 Switch monitoring model has been introduced. The metrics collected for Dell EMC S-Series Switch has been extended to report for Dell EMC S-Series OS10 Switch.
- **Monitoring Lenovo XClarity:** Lenovo XClarity Controller is the embedded management engine in ThinkSystem servers designed to standardize, simplify, and automate foundation server management tasks. Using eG Enterprise v7.2, administrators can perform extensive monitoring of Lenova XClarity. The status of the hardware components such as fans, disks, power supply and temperature sensors are tracked, and abnormalities brought to administrator's attention. The resource utilization of the fuel gauge is closely monitored, and abnormal resource usage patterns are highlighted.
- **Monitoring Arista Switch:** Arista switch offers high density, non-blocking ethernet ports controlled through an extensible modular Linux based network operating system. This switch offers true innovation for high performance data center switches delivering support for a programmable forwarding pipeline, flexible profiles, dynamic packet buffer and a choice of interface types in a set of power efficient compact systems. Using eG Enterprise v7.2, you can monitor the CPU and memory usage of the switch to proactively spot resource contentions. The status of the hardware components such as fan and PSUs of the switch are periodically monitored and reported. The temperature of the sensors in the switch is continuously monitored and sensor failures are promptly captured. The count of users accessing the switch is captured periodically, and administrators are alerted to potential overload conditions.
- **Monitoring Cisco Wireless LAN Controller:** WLAN controller manages wireless network access points that allow wireless devices to connect to the network. A Wireless Access Point takes the bandwidth coming from a router and stretches it so that many devices can go on the network from farther distances. eG Enterprise v7.2 offers complete monitoring support to Cisco Wireless LAN Controller. Using the metrics collected, the resource utilization (CPU and memory) levels of the WLAN can be ascertained. The count of access points connected to / disconnected from the WLAN is reported. By periodically monitoring the resource utilization (CPU and memory) of each access point, administrators can identify the access point that is abnormally consuming resources.
- **Monitoring Infiniband Switch:** InfiniBand technology works by connecting host-channel adapters (HCAs) to target channel adapters (TCAs). The InfiniBand switch allows links to create a uniform fabric environment. The InfiniBand switch allows managing packets of information (or data) based on variables, such as service level agreements and a destination identifier. With eG Enterprise v7.2, you can monitor the availability of the element manager to each fabric element. The performance of the switch is also monitored and reported so that administrators can be instantly alerted to performance issues. The data transmission and packets transmission through each PMA extended port is monitored and the port that is handling maximum traffic is identified. Error-prone PMA ports are proactively identified and rectified periodically. Administrators can also keep a vigil on the count of dropped packets to ascertain if network connectivity to PMA ports is flaky. The physical status, link state and speed of SMA link of each SMA port is determined and SMA ports that are down are promptly reported.
- **Monitoring Juniper QFX Switch:** Juniper QFX Series Switches deliver industry-leading throughput and scalability, an extensive routing stack, the open programmability of the Junos OS, and a broad set of EVPN-VXLAN and IP fabric capabilities. Using eG Enterprise v7.2, you can monitor the CPU and memory usage of each hardware component of the switch to proactively spot resource contentions. The hardware components experiencing abnormal temperature fluctuations and the routing engines that are disabled, can be identified with ease. The firewall filters are monitored and the firewall filter sending abnormal packets and data is identified. The time taken to transmit the packets for each class is measured and the class on which packet loss is noticed is isolated. The count of active VPN connections initiated on the switch is periodically monitored and abnormalities if

any, in terms of connections are detected at the earliest.

- **Monitoring Cisco SD-WAN:** Cisco SD-WAN is a secure, cloud-scale architecture that is open, programmable, and scalable. Through the Cisco vManage console, administrators can quickly establish an SD-WAN overlay fabric to connect data centers, branches, campuses, and other facilities to improve network speed, security, and efficiency. eG Enterprise is capable of monitoring the Cisco SD-WAN in an agentless manner using REST API commands and reports a wide range of useful metrics. For each primary component within the Cisco SD-WAN, the resource utilization (CPU, memory, and disk) is monitored, and erratic resource utilization patterns are reported periodically. The number of times each primary component crashed helps in identifying the primary component that encountered frequent problems. The primary components that are in an abnormal state are proactively detected and problems are rectified at the earliest. Alerts are sent out if a connection is down for an unusually long time, so that the reason for the downtime can be investigated. The status, speed, data transmission rate and uptime of each network interface is reported. This way, data loss on the Cisco SD-WAN can be proactively detected and averted, which helps improve the overall user experience.
- **Monitoring Cisco ASR Router:** The Cisco ASR Router aggregates multiple WAN connections and network services including encryption and traffic management and forward across WAN connections at line speeds from 2.5 to 200 Gbps. They are ideal for high bandwidth applications, such as streaming audio or video, or video conferencing. eG Enterprise v7.2 monitors the Cisco ASR Router and reports a wealth of statistics, which includes capturing failures of the Field-Replaceable Units, and determining the utilization levels of each memory pool, cache pool and buffer pool in the router. The status, size and type of each flash file is monitored and flash files with 'invalid checksum' state are promptly captured. Inconsistencies in the CPU time of each processor and input discards from each queue are proactively detected and reported. Administrators can also keep a vigil on the requests made through the router to ascertain if there is any malicious activity over the router.
- **Monitoring Radware AppDirector:** Radware's AppDirector is an intelligent application delivery controller (ADC) that provides scalability and application-level security for service infrastructure optimization, fault tolerance and redundancy. Since application delivery delays, inefficiencies, and failures can cause prolonged service outages and cost an enterprise money and reputation, it is imperative to ensure the continuous operation and good health of the Radware AppDirector. By polling the Radware AppDirector proprietary SNMP MIB, eG Enterprise v7.2 monitors and reports the CPU usage, network usage and status of the application servers and server farms. In addition, the packet traffic and request processing ability of the application servers and server farms are periodically monitored and, in the process, the application servers and server farms that are slow in processing requests are identified.
- **Monitoring Cisco Intersight:** Cisco Intersight is a cloud operations platfortm that consists of optional, modular capabilities of advanced infrastructure, workload optimization, and Kubernetes services. eG Enterprise v7.2 offers deep insights into the performance and operations of Cisco Intersigh. The status and overall performance of each Chassis managed by Cisco Intersight and its core components such as fan modules, power supplies, blades, IO modules etc., are periodically monitored and abnormalities if any, are proactively detected and reported. This way, the core components can be replaced well in advance averting serious damages to the chassis. The status and overall performance of the blade servers are periodically monitored and failures are brought to administrator attention. Each hardware component of the blade server such as motherboard, processor, memory array, memory array unit is monitored and abnormalities if any are reported so that the problems can be resolved before they affect the functioning of the Cisco Intersight as a whole.
- **Monitoring Mellanox Switch:** Mellanox's family of switches is designed for performance, serviceability, energy efficiency and high availability. The switches are optimized for fitting into industry-standard racks and for scale-out computing solutions from industry leaders. With eG Enterprise v7.2, you can monitor the performance of the switch and be instantly alerted to

performance issues, so that problems can be rapidly resolved, and desired service levels can be maintained. This version tracks the QoS levels of the switch and warns you of potential QoS violations. The data traffic and pause packet traffic through each interface is monitored and the interface that is choked with pause packets is identified. The priority tags of each interface are monitored round the clock and the interface/priority tag combination through which maximum data traffic and pause packet traffic is flowing is determined with ease. The VPI ports are monitored periodically and the ports that are unavailable are isolated. The hardware components such as CPUs, fans, PSUs and temperature sensors are periodically monitored, and abnormalities are proactively captured and reported.

- **Monitoring PPC UPS:** The PPC UPS is a true online, continuous-duty, transformer free, double-conversion, solid-state, three-phase system, providing conditioned and uninterruptible AC power to protect the customer's load from power failures. eG Enterprise v7.2 monitors the PPC UPS and reports a host of metrics that help administrators keep constant vigil on the performance of the UPS. The input to the UPS is periodically monitored and input failures are detected and proactively reported. The status, load, output voltage of the UPS is monitored round the clock and discrepancies, if any are identified and rectified. The battery of the UPS is monitored, and voltage, temperature fluctuations experienced by the battery are promptly captured. Administrators are also alerted to dwindling battery capacity and the replacement date of the battery.
- **Identifying Disconnected Stack members of Juniper EX Switch:** Juniper EX Switch supports a flexible and scalable technology called Virtual Chassis using which you can connect individual member switches together to form one single unit. Virtual Chassis ports (VCPs) connect member switches together to form a Virtual Chassis and are responsible for passing all data and control traffic between member switches. When member switches are disconnected, data and control traffic may be disrupted, and the load may not be balanced across all the switches. To help administrators address such irregularities, starting with this version, the count of switch members disconnected from the virtual chassis and the count of switch members added to the virtual chassis are reported. The detailed diagnostics further reveals the MAC address, serial number, member role and member model of each switch member.
- **Monitoring the Health of VPN Tunnels:** eG Enterprise v7.2 reports the health of the VPN tunnels configured using FortiGate Firewall. The VPN tunnels that are unstable can be identified and the root cause of the instability can be ascertained with ease!
- **Performance SLA Link Monitoring on Fortigate Firewall is now Possible:** SLAs allow administrators to analyze IP service levels for IP applications and services by using active traffic monitoring - the generation of traffic in a continuous, reliable, and predictable manner - for measuring network performance. The Performance SLAs can perform network assessments and assist with network troubleshooting. Performance SLA link monitoring measures the health of links that are connected to SD-WAN member interfaces by sending probing signals through each link to a server. This also measures the link quality based on latency, jitter, and packet loss. With this integration, eG Enterprise has deeper network visibility.
- **Monitoring the Resource Utilization of VMWare Horizon Access Gateway via SNMP:** In previous versions, the eG agent collected metrics relating to the resource utilization (CPU, Disk and Memory) of the target VMware Horizon Access Gateway through SSH. However, in some high security environments, administrators did not want their appliance to be accessed via SSH, but still required metrics related to the resource utilization of the target appliance. To address this requirement, starting with this version, eG Enterprise is capable of collecting the resource utilization (CPU, Memory, and Disk) of the target VMware Horizon Unified Access Gateway by polling the SNMP MIB of the gateway.
- **Improved Monitoring of Network Elements Supporting SHA Algorithms:** In earlier versions, administrators were able to choose between MD5 and SHA authentication algorithms when SNMP v3 framework was chosen. However, with the advancement of technology, many of the network elements support a more secure Computer Security Cryptographic Algorithm called SHA-2 to ensure

security of their SNMP transactions. To keep pace with the recent advancements in the networking world, eG Enterprise v7.2 provides monitoring coverage to network elements that support SHA-2. To this effect, the A**uthType** parameter that appears when v3 option is chosen from the **SNMPVersion** list in the test configuration page now lists additional options – *SHA224*, *SHA256*, *SHA384* and *SHA512*.

- **Capturing the Battery Status of CryptoServer LAN:** Starting with this version, eG Enterprise captures the status of the battery operating in the CryptoServer LAN configured on the target CryptoServer HSM device. Administrators are alerted if the battery is low or absent so that they can replace/add the battery well in advance.
- **Enhancements to F5 Monitoring:** Starting with this version, if a F5 BIG-IP / F5 BIG-IP Traffic Manager is in a high availability setup, then, eG Enterprise will report the current status of the server. By closely monitoring the metrics reported, administrators can determine the servers that are currently offline.
- **Improved SNMP Validation for FortiGate and F5 Component Types:** If when configuring a test for any FortiGate or F5 component, the SNMP validation failed, then earlier, it was difficult to determine the reason for the failure and troubleshoot it. To enable administrators to diagnose why SNMP validation failed and how to fix it, eG Enterprise v7.2 pinpoints the exact validation step that failed and a recommendation to overcome such SNMP validation failures.

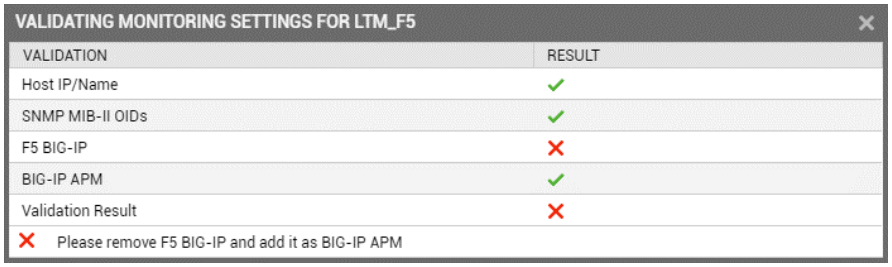


Figure 91: SNMP Validation Failures and Recommendations

- **Improved Trap Monitoring:** In previous versions, alerts were raised every time the eG trap receiver received a trap message. In order to triage the traps, administrators had to manually review the detailed diagnostics. This process was cumbersome in environments where hundreds of trap alerts were raised. To automate trap triaging and ease the troubleshooting process, eG Enterprise v7.2 allows administrators to custom-define priority for network traps. For this purpose, eG Enterprise v7.2 has introduced a brand-new **Trap Priority** page in the eG administrative interface using which administrators can configure alarm priorities to the traps based on their choice.

Figure 92: The Trap Priority page

To configure a new trap priority, administrators can choose a MIB, pick a trap from the list of traps and set a priority for the trap as shown in Figure 93.

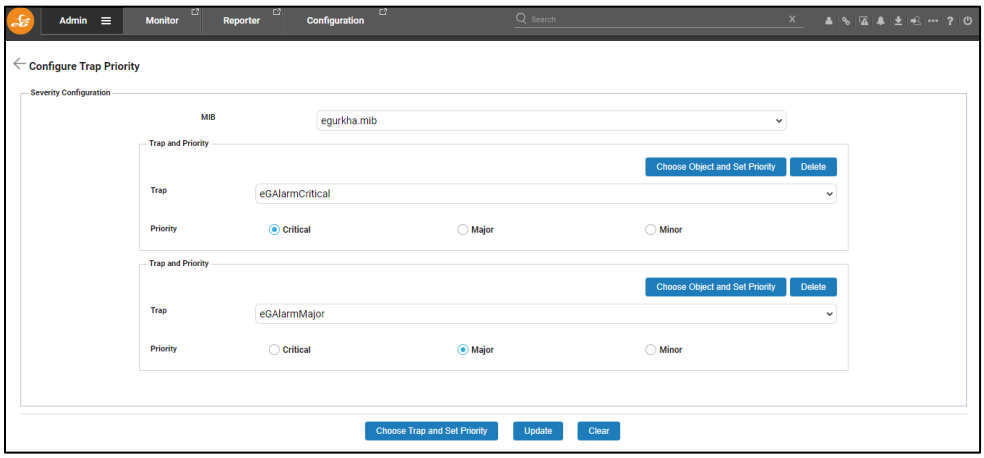


Figure 93: Configuring the priority for the traps of the chosen MIB

Once the alarm priorities are set for the traps, the **Network Trap Alerts** test of the target device will display the count of traps based on the configured alarm priorities (Critical/Major/Minor/Informational).

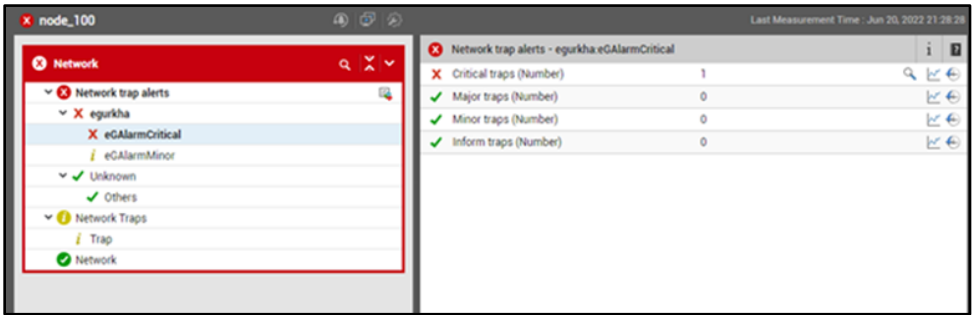


Figure 94: The Network Trap Alerts test

- **Traffic Analysis Dashboard Support Extended to Multiple Components:** In previous versions, the **Interfaces Dashboard** displayed the performance analytics for the network interfaces of only a select-few Network components (for e.g., Network Node, Cisco Router etc.). Starting with this version, this dashboard has been renamed to **Traffic Analysis Dashboard** and support for this dashboard has been extended to all the Network components monitored by eG Enterprise.
- **Enhancements to Network Traffic Monitoring:** Starting with this version, Network Traffic monitoring has been extended to Unix servers. By periodically monitoring the network interfaces on the target Unix servers, administrators can isolate error-prone network interfaces and those that are bandwidth-intensive.
- **Monitoring the Logical Disks in Cisco UCS Manager:** Starting with this version, the logical disks available in the target Cisco UCS Manager are auto discovered and for each logical disk, the overall health, operability, size and availability are revealed. In These metrics help administrators easily identify logical disks that are powered off, that failed to attach to the drive, and those that could not be configured.
- Starting with this version, eG Enterprise reports the network connectivity of each Meraki appliance i.e., switch, firewall, security camera etc., in the target environment. To this effect, a new Meraki

Device monitoring model has been included in this version.

16. Self-Monitoring Enhancements

- **Improvements to the Self-monitoring Capability of eG Manager:** By default, the eG manager alerts administrators regarding abnormalities that arise in their environment through emails and SMS messages. Any problem in the delivery of emails and SMS messages can delay problem identification and troubleshooting, prolong service outages, and thus adversely impact the business. In those environments where eG Enterprise monitors a multitude of servers, it is impossible for the administrators to manually track whether/not the emails/messages have been successfully delivered to the designated recipients. eG Enterprise v7.2 can now alert administrators if the eG manager fails to / slow in delivering emails. Additionally eG pinpoints the mail threads that were utilized for sending mails, and thus helps rapidly troubleshoot the delivery failures/delays. eG Enterprise v7.2 tracks the database partitions created for tests and diagnosis tables and identifies those tables for which partitions have not been created. The utilization of the thread pool from which threads are used to insert detailed diagnosis data into the eG backend database is periodically monitored and discrepancies if any, are reported.
- **Introduced Self-monitoring Capability for eG RUM Collector:** eG Enterprise v7.2 provides a specialized monitoring model for the eG RUM Collector component, and points to deficiencies in RUM Collector operations. Using this model, you can quickly detect breaks in eG RUM Collector-agent communication, be forewarned of overload conditions and spot inconsistencies in the request processing capability of the RUM Collector. The count of large datafiles and duplicate datafiles is also reported; these metrics are useful when troubleshooting space contentions on the RUM collector.

17. Enhancements for Increased Automation, Simplicity, Scalability and Security

17.1 Architecture Enhancements

- **Bandwidth optimization of eG Manager – Agent Communication:** In earlier versions, every configuration change that was effected on the eG manager – e.g., threshold change, alarm policy change, etc. – was automatically downloaded by all the eG agents reporting to that eG manager, even if that change was relevant to only a few agents. For instance, if the threshold values for an Oracle database server component was changed, then previously, these threshold changes were downloaded by even those agents that were not monitoring any Oracle database servers. This often increased the bandwidth consumed by eG agent-manager communications. In large environments where thousands of agents interact with a single manager, this unnecessary bandwidth usage directly translated into cost. To optimize bandwidth usage and to minimize the related costs, starting with this version, the eG agent has been re-engineered to intelligently download only those changes that are applicable to it. The eG agent sends a checksum of last updated configuration file to the eG manager periodically. If the checksum sent by the eG agent is different from that of the eG manager, the eG agent downloads the latest configuration file. In a high availability environment, when the primary eG manager is down, the eG agent will communicate with the secondary eG manager and

check for the checksum.

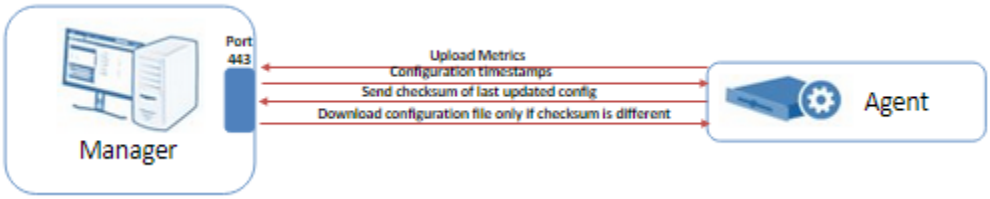


Figure 95: Manager - Agent communication optimized for downloading files based on checksum difference

Note that this logic will not apply to the eG VM Agent and for those eG agents of versions prior to v7.2.

- **Push Model of eG VM Agent is now more Flexible:** Traditionally, the eG VM Agent collects metrics from the virtual machines/virtual desktops. The eG remote agent monitoring these VMs/virtual desktops periodically polls the eG VM Agent and downloads the latest metrics from the VM agent. This methodology is called the **Pull** model. While monitoring cloud desktops on the other hand, the eG VM agent communicates with the eG manager, identifies the eG remote agent that is monitoring the cloud desktops, and transmits the collected metrics to that remote agent. This methodology is called the **Push** model. Though the Push model worked seamlessly for cloud desktops, sometimes, if the eG VM agent is unable to access the eG manager, it could not determine which remote agent it should talk to. As a result, metrics could not be sent to the remote agent, and or to the eG manager. This significantly delayed problem identification and state computation. To avoid this, eG Enterprise v7.2 imparts additional flexibility to the architecture of the eG VM agent. You can now configure the eG VM agent to send metrics to the eG remote agent directly, if it is not able to connect to the eG manager. This ensures uninterrupted transmission of metrics to the remote agent, rapid problem identification, and speedy resolution of desktop issues.
- **Wider platform support for the eG VM Agent:** Starting with this version, the eG VM agent can be installed on virtual machines/virtual desktops running Linux Operating Systems. In such environments, the eG VM agent runs as a Linux service. Installation procedure of the eG VM agent on Linux is similar to that of installing the eG agent on Linux environments.
- **eG Agent – eG Manager Communication is now Optimized:** In older versions, the eG agents transmitted performance data to the eG manager synchronously. In other words, the agents waited till the eG manager successfully inserted all the data it had already received from them into the eG database before resuming metrics transmission. Because of this synchronous approach, if the eG backend database was slow, the eG agents were forced to locally store large volumes of data pending transmission to the eG manager. Persistent database slowness sometimes resulted in loss of critical performance data. To reduce the strain on the eG agent under such circumstances and to prevent consequent data loss, starting with version 7.2, the eG manager inserts data into the eG database asynchronously. If the eG manager detects that the eG database is lazy, then it intelligently deploys additional threads asynchronously to insert data into the database. This way, the backlog on the eG agent can be minimized considerably. If database errors are noticed on the eG backend database, then the synchronous approach will be employed until such time the errors on the eG backend database are fixed.
- **Auto-Indexing is now Improved:** In previous versions, in environments where Database Partitioning was enabled on the eG backend database, slowness was noticed while accessing most pages of the eG monitor console. This was because, the automatic index rebuilding capability was disabled by default for trend tables and certain default tables (e.g., tables that maintained alert information, meta information about components being monitored, etc.) of the eG database. Due to this, issues were noticed in trend computation, and during updating/adding data to the default tables. If the issues persisted, it significantly increased the processing overheads of the eG backend database. To overcome this issue and to ensure that pages of the eG monitor console are loaded

quickly, starting with this version, indexes are rebuilt by default for the trend and default tables. This way, manual maintenance of the eG Enterprise system by the administrators can be minimized to a greater extent. **eG Enterprise recommends manual reindexing of those trend tables that store more than 50 GB of data.**

- **Performance of the JTDS Database Driver is now Optimized:** In previous versions, where the Microsoft SQL server was used as the eG backend, every time the eG manager attempted to connect to the backend, the jTDS driver had to find the local IP address and hardware address of the local NIC card to make the connection. This process caused significant delays in eG manager-database communications. In order to reduce the time taken to establish a database connection, starting with this version, the jTDS driver has been modified to cache the local IP address and the hardware address of the local NIC card for a day. This optimization helps in reducing the time taken to establish the database connection by atleast 50%.

- **MS JDBC Driver is now Supported for eG Manager-eG Backend Database Communication:** By default, eG Enterprise uses jTDS driver for communication between the eG manager and the eG backend database. jTDS driver is an 100% open-source pure Java (type 4) JDBC 3.0 driver for Microsoft SQL Server. In recent times, the jTDS driver has not released any new updates lately. Hence, driver issues have become more common, difficult to troubleshoot, and take longer to resolve. To eliminate such issues, starting with this version, eG Enterprise supports MS JDBC driver to connect the eG manager and the eG backend database. Administrators can switch over to the MS JDBC driver if the default jTDS driver bundled with the product encountered serious issues.

- **Improved eG VM Agent Version Tracking and Control:** eG Enterprise v7.2 offers a special **VM AGENT STATUS** page in the eG administrative interface. By merely glancing at this page, administrators can identify the Hypervisors/Hosts on which VMs are installed/not installed, the version of the eG VM agent installed on each VM and the upgrade package that was last installed on the eG VM agent. This saves administrators the time and trouble involved in manually checking each VM to determine whether/not an eG VM Agent is installed on it. The new interface also helps administrators quickly identify the VMs that are running obsolete VM agents. This way, they can rapidly make plans to upgrade those VM agents, so that they can avail of the benefits of critical bug fixes, optimizations, and enhancements that are part of the upgrade.

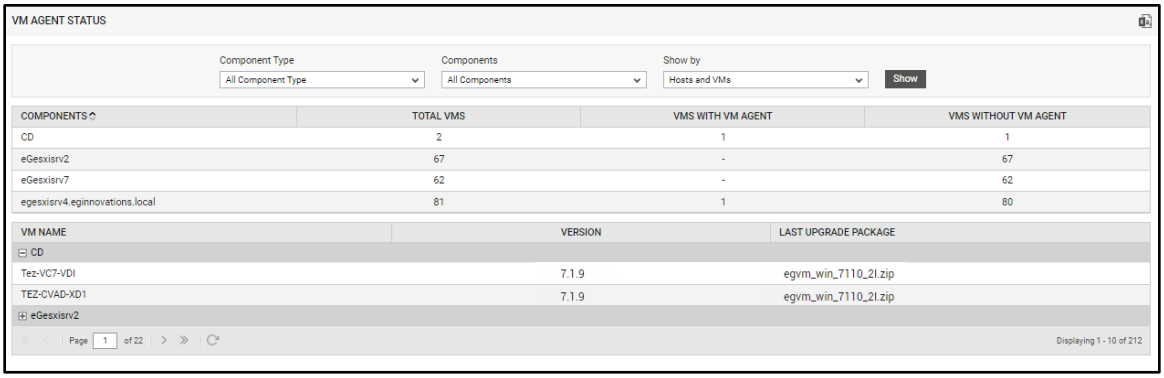


Figure 96: The VM Agent Status page

- **Greater Security in Agent Upgrade Process:** Previously, the eG agents downloaded the upgrade packages from the eG manager and applied the upgrade automatically. In recent times, many organizations are seriously affected due to malicious code being inserted by hackers into the deliverables, uploads/downloads etc. To ensure that the security of the target environment is not compromised and to ensure that the upgrade packages are safeguarded from manipulation during download, starting with this version, the eG agent compares the checksum of every file being extracted during upgrade with an expected value. The eG agent continues the upgrade process only if the checksum matches the expected value and if all the files that are extracted are valid. This way,

eG Enterprise assures to detect corrupt files or manipulated files during the upgrade process and prevents any malicious file from being installed on the eG agent system.

17.2 Auto-Discovery Improvements

- **Extending Discovery to Different Component Types:** In previous versions, discovery of components was limited to only a few Component Types only. Starting with this version, discovery has been extended to cover a lot of new Component Types.

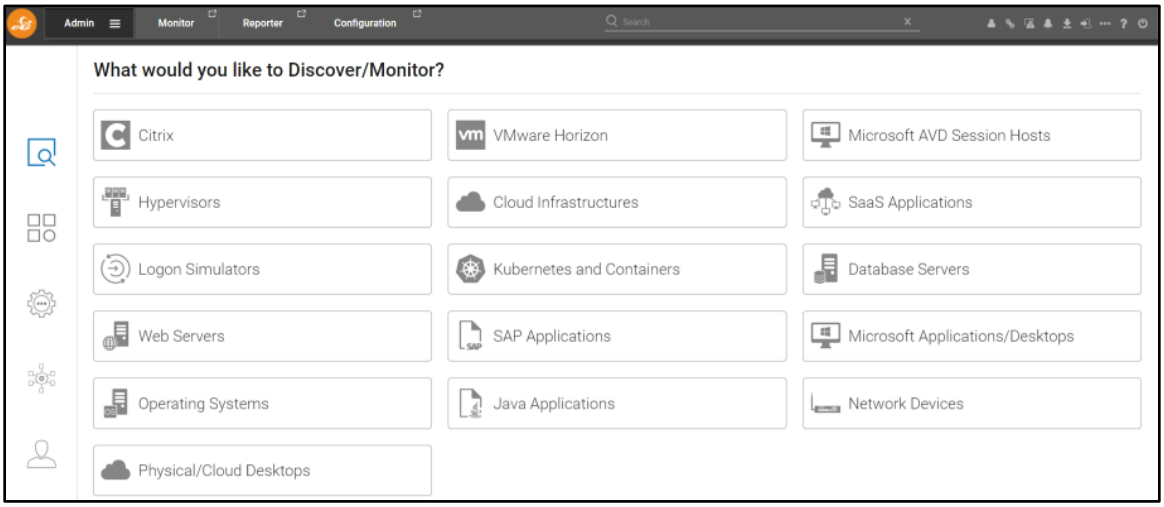


Figure 97: Discovery Extended to Newer Component Types

- **Improvements to Network Devices Discovery using eG Manager:** In previous versions, to discover the network devices in the target environment, the eG manager pinged each IP address in the discovery range, sequentially. This delayed auto-discovery of network devices via the eG manager. To speed up network device discovery, starting with this version, the IP addresses in the configured discovery range are pinged in parallel.

- **Auto-Discovery of Network Devices using External Agents:** In previous versions, network devices were discovered using the eG manager only. This discovery worked only in environments where the eG manager had access to all the network devices that are to be monitored in the target environment. In SaaS deployments of the eG manager, since the eG manager had no access to the target environment, discovery of the network devices could not be performed by the manager. To fill this void, starting with eG Enterprise v7.2, external agents can be used to auto-discover the network devices. Limited admins can choose to run this discovery from any external agent deployed

in the target environment.

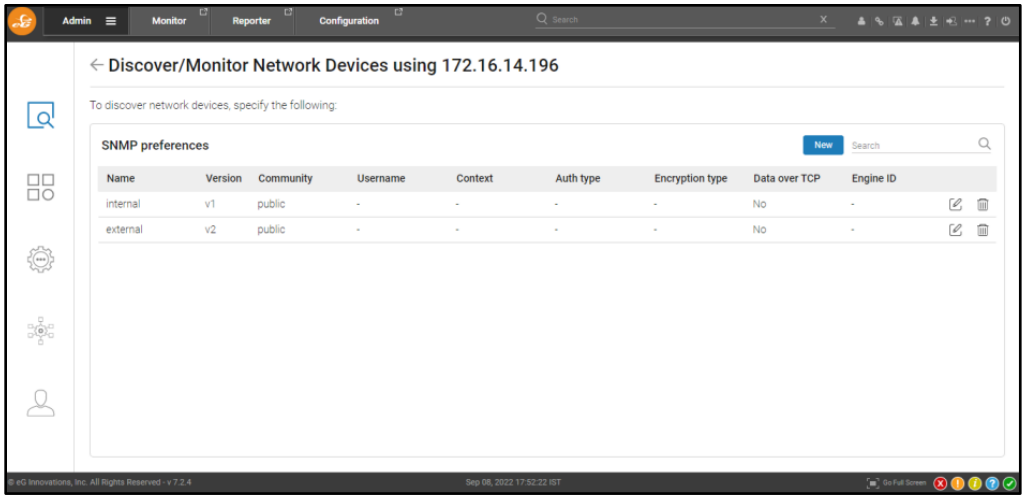


Figure 98: Discovering the Network devices using external agents

- **Enabled Discovery of Containerized Applications:** Starting with this version, the eG containerized agents are capable of automatically discovering the applications that run on containers (Kubernetes, OpenShift, Docker etc). Administrators are also allowed to automatically manage the discovered applications and automatically delete them too.

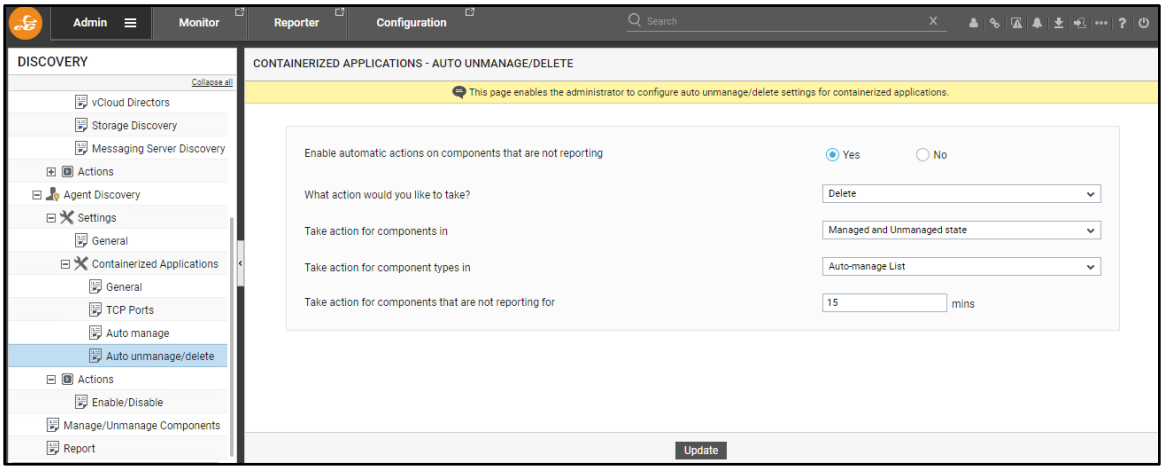


Figure 99: Discovering Containerized Applications

17.3 Usability Enhancements

- **Design Changes:** In eG Enterprise v7.2, the usability of the eG console has been enhanced, so that it is easier to navigate and operate the user interface. The older tile menu has been replaced with a sophisticated tree-view menu structure. Though the menu options are logically grouped as like the previous versions, the look and feel has been improved to ensure that browsing and selection is a

breeze.

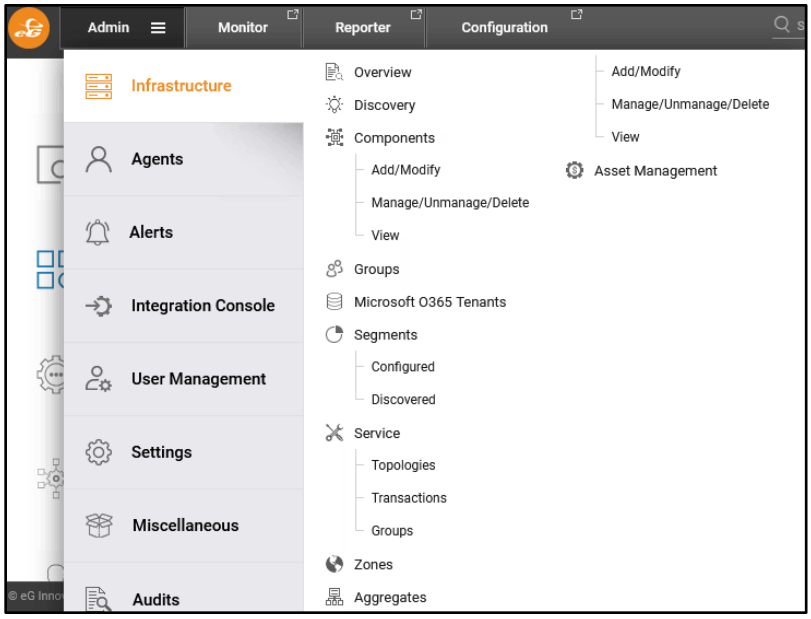


Figure 100: The revamped menu sequence in Admin module

17.3.1 Admin Interface

- **Improved Remote Control Actions:** In eG Enterprise v7.2, the scope of remote control actions has been significantly widened. Many domain-specific remote control commands have now been introduced. For e.g., remote control commands are now available for Citrix Delivery Controllers, Active Directory servers, virtual desktops, Citrix Hypervisors, Nutanix Acropolis, VMware Hypervisors etc. eG Enterprise v7.2 also offers remote control commands that can be executed on Azure sessions hosts available within a Microsoft AVD Host Pool. All the remote control actions for Citrix and VMware Horizon virtual desktops are also available to multi-session Azure virtual desktops.

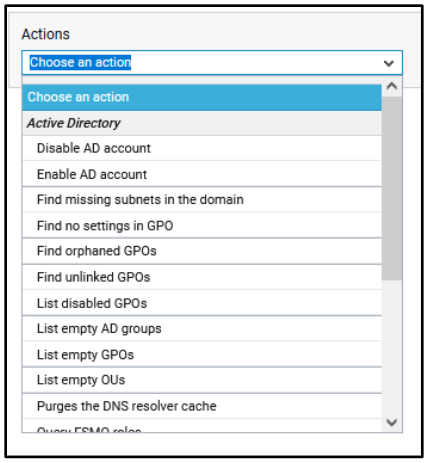


Figure 101: Remote Control Actions for Active Directory Servers

- **Audit Logs can now Capture Remote Control Actions Performed by Users:** Previously, remote control actions from the eG Monitor interface could not be audited. Starting with this version, audit logs for eG monitor console will capture and report the exact remote control action that was

executed, the user who executed the remote control action and the time at which the remote control action was executed. This way, unauthorized or incorrect remote operations can be rapidly captured and investigated.

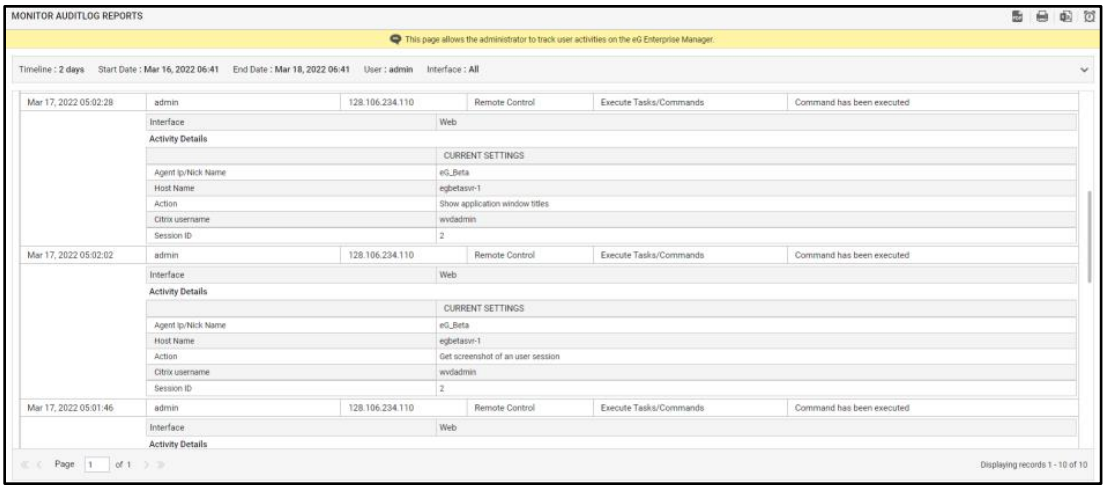


Figure 102: The Monitor Audit logs capturing Remote Control Actions

- **Selective, Role-based Activation of Remote Control Commands for eG Users :** In earlier versions, if an eG user's remote control capability was enabled via his/her user profile, then, all remote control actions were automatically enabled for that user, regardless of the roles and responsibilities of that user. This allowed users unnecessary remote control access to those components that were not even in their monitoring scope. To make sure that users can remotely control and execute commands on only those components that are in their monitoring radar, eG Enterprise v7.2 enables administrators to customize the remote control commands for each user. For this, administrators need to choose the **Customize actions** option against the **Remote control actions** flag from the **USER PREFERENCES** page that appears while adding a user in the eG administrative interface.

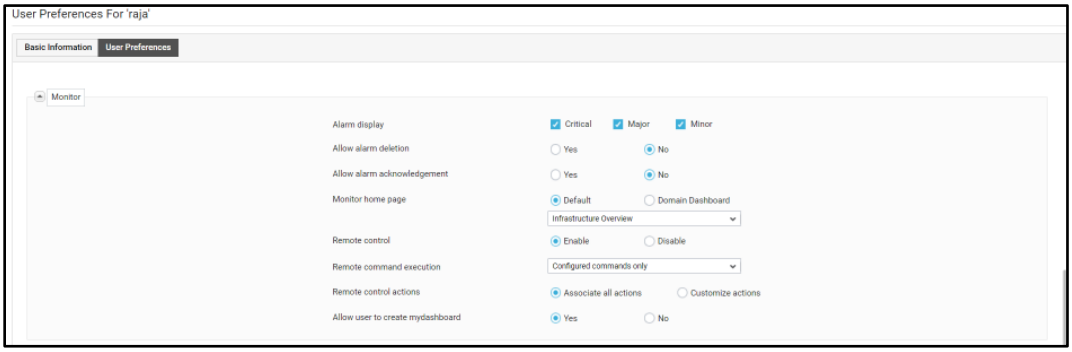


Figure 103: Customizing Remote Control Actions for a user

In the **Remote Control Actions** tab page that then appears, administrators can pick and choose the remote control actions that they deem applicable for that user.

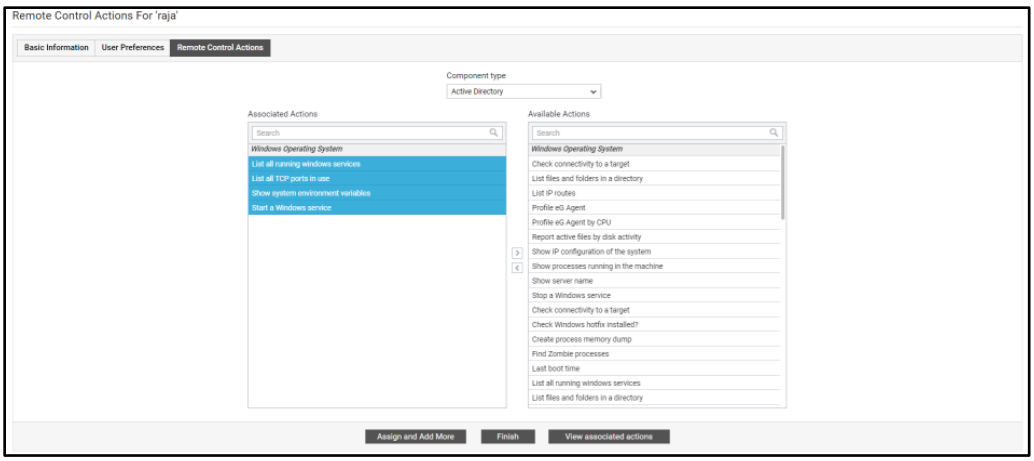


Figure 104: Choosing the Remote Control Actions applicable for the user

- **Role-based Access Enhancements for Users Accessing Monitor Interface:** In previous versions, when a new user role was created by the administrators, the user role was limited to access only a few pages of the eG Monitor interface. Many administrators felt that this restriction did not give them free hands in creating the user role of their own. To aid administrators in this regard, eG Enterprise v7.2 has introduced more pages (pertaining to the eG Monitor Interface) in the **MONITOR** section of the **USER ROLES** page (accessed by clicking the **Add New Role** button) that can be chosen when a new user role is being created.

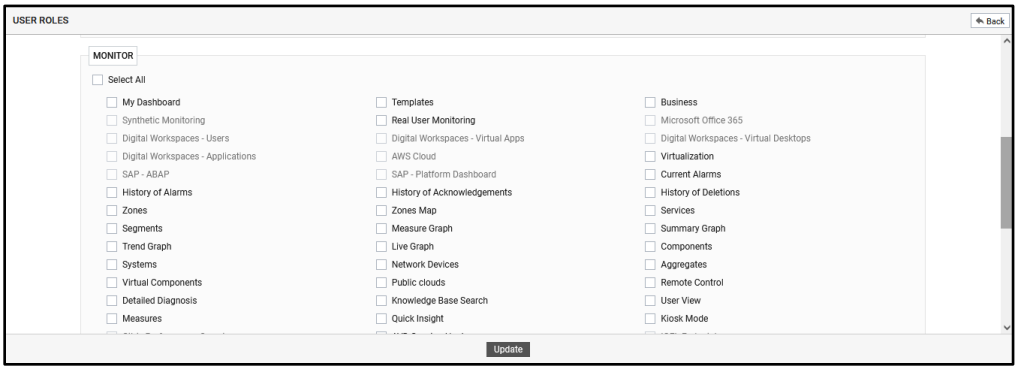


Figure 105: The USER ROLES page with support to additional pages in eG Monitor Interface

- **Support for Active Directory Integration with LDAP Channel Binding:** In previous versions, the eG manager integrated with an Active Directory server using Kerberos or LDAP authentication mechanisms. When LDAP authentication was used for integration, the eG manager used simple binding. The LDAP Authentication with simple binding was best suited for environments with not very high security concerns. However, in recent times, many environments using LDAP authentication with simple binding are prone to vulnerabilities such as replay attacks, man-in-the-middle attacks etc. since the communication between the Active Directory server and the eG manager was unencrypted. To address such vulnerabilities, eG Enterprise v7.2 allows users the flexibility to choose between simple and channel binding. When channel binding is used for LDAP authentication, communication between the eG manager and the Active Directory server remains encrypted thus increasing the security.

- **Ability to Block a User from Accessing the eG Console:** Sometimes, administrators of an environment may identify a user as a security threat to the environment due to reasons like the user encountering a recent malicious attack, non-compliance of the system that he/she is using to access the environment etc. If such a user has access to the eG console, administrators should be able to

temporarily restrict (block) the user from accessing the eG console. To enable administrator to restrict the monitoring access of such users, eG Enterprise v7.2 includes an unlock ( ) icon in the **USER INFORMATION** page of the eG administrative interface against all users registered with the eG monitoring system. By clicking this icon against a user, administrators can restrict the access of that user to the eG console. Note that the default users of eG console too (admin and supermonitor) can be temporarily blocked from accessing the eG console.

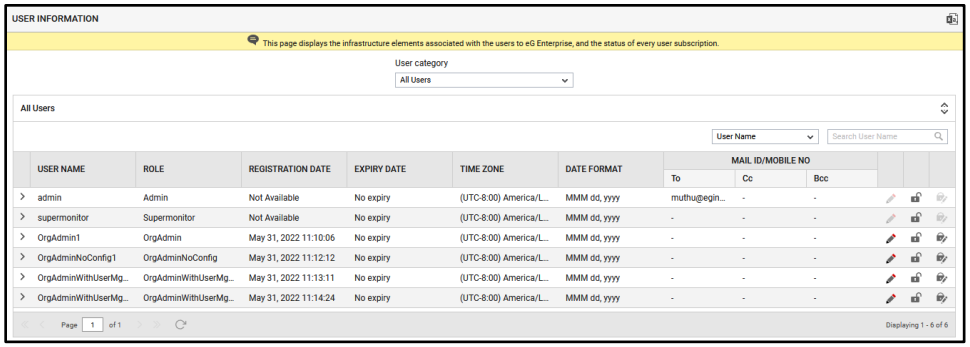


Figure 106: The USER INFORMATION page that lets you block a user of your choice

Administrators can even restrict the users (apart from the default users of eG Enterprise) from modifying their passwords from this page. To do so, they need to simply click the icon in the **USER INFORMATION** page.

- **Suppressing a User Login Authentication Mechanism:** By default, eG Enterprise allows users to login to the eG console using multiple login mechanisms. By default, **eG Enterprise** was chosen as the **Default Authentication Provider for Login**. However, in MSP environments, users logged into eG console using Active Directory and SAML authentication providers. Administrators of such environments felt that users needed a uniform login mechanism to login into eG console and hence wanted to choose one single authentication mechanism and disable the rest. For such administrators, eG Enterprise v7.2 had introduced a **Disable authentication providers** list in the **GENERAL SETTINGS** page. By choosing one/more options from this list, administrators can disable the authentication mechanisms from the **Login screen**.

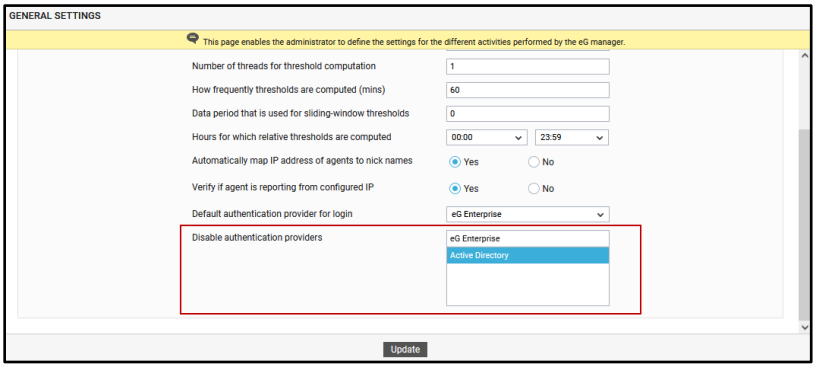


Figure 107: Disabling an authentication mechanism

17.3.1.1 Licensing Enhancements

- **Ability to View Distribution of Named/Concurrent User Licenses:** In previous versions, the **TOTAL NAMED USERS DAY WISE REPORT** and **TOTAL CONCURRENT USERS DAY WISE REPORT** popup windows showed a bar graph with the count of named/concurrent user licenses consumed per day. Though this bar graph helped administrators figure out the count of

named/concurrent user licenses consumed, it did not throw in-depth information on the distribution of licenses i.e., whether the licenses were consumed by users logged into virtual apps/virtual desktops etc. To help administrators with such distribution, eG Enterprise v7.2 has introduced a **Graph View** list box in the **TOTAL NAMED USERS DAY WISE REPORT** and **TOTAL CONCURRENT USERS DAY WISE REPORT** popup windows. Choosing the **Distribution** option from this list will display the bar graph with the distribution of named/concurrent user licenses in the target environment during the chosen time period.

Figure 108: Viewing the distribution of Concurrent user licenses

Also, administrators are allowed to choose either the **Distribution** or the **Total** option as the default License Graph View from the **LICENSE SETTINGS** page. By default, the **License graph view** flag is set to **Total** indicating that the graph displayed in the **TOTAL NAMED USERS DAY WISE REPORT** and **TOTAL CONCURRENT USERS DAY WISE REPORT** popup windows will be a simple bar graph with the total number of user licenses utilized in the target environment.

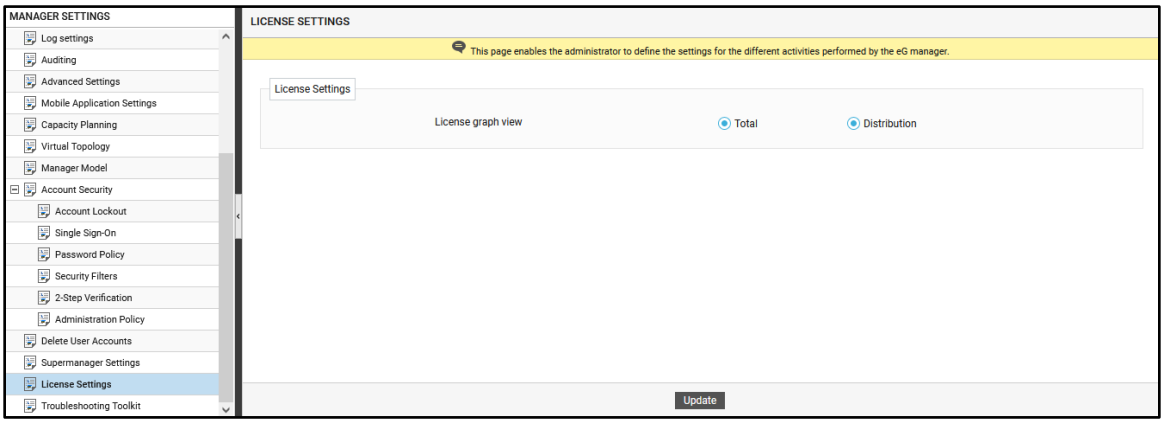


Figure 109: The LICENSE SETTINGS page

- **Ability to Upload License from the eG Administrative Interface:** Starting with this version, administrators can upload the eG license from the eG administrative interface using a single click. For this purpose, an **Upload License** button has been included in the **Total License Usage** tab of the **LICENSE INFORMATION** page. By specifying the full path to the license file, administrators can automatically upload the license in a single click. Once the license is uploaded successfully, the eG manager will be automatically restarted. This way, the license upload task is simplified and manual

errors during license upload is avoided.

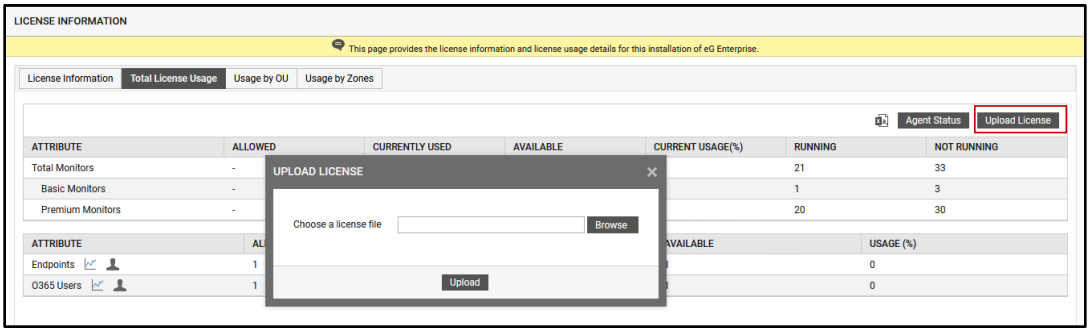


Figure 110: Uploading the License from eG admin interface

- **Improved Alerting Ability to Report License Violations:** In previous versions, whenever a named/concurrent user license violation was detected, users were unaware of such license violation until they navigated to the **LICENSE INFORMATION** page. In SaaS deployment of eG Enterprise, administrators took a long time to identify the users (belonging to Organization/Organizational Unit) with license violations. To ease the pain of such administrators, starting with this version, for every license violation that is detected for a user (named/concurrent, IGEL Endpoints or Office 365 users) belonging to an Organization/Organizational unit, a pop up message will be displayed as soon as that user logs into eG Enterprise.

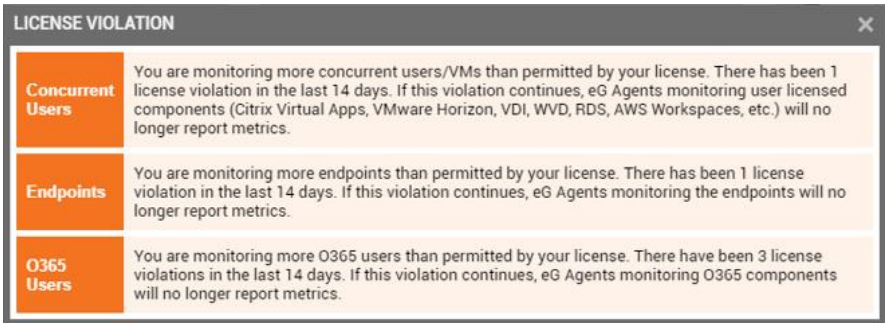


Figure 111: The pop up alert displaying license violation for a user

- Similarly, the **Manager Notification** window is also enhanced to display appropriate alerts when every license violation is detected for the users. For this, starting with this version, a **Show alert for subscription license violation for users** flag has been introduced in the **MANAGER NOTIFICATION** page of the eG administrative interface. Setting this flag to **Yes** will promptly

capture all the user license violations if any and display the same in the Manager Notification Window.

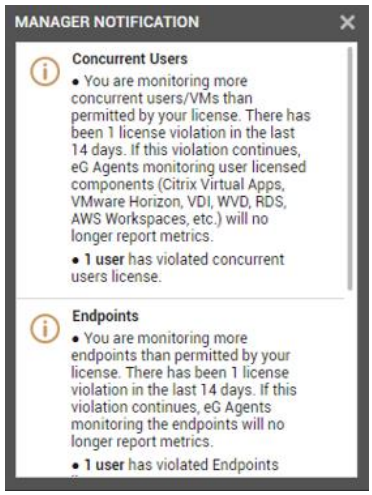


Figure 112: Manager Notification window displaying user license violation

In previous versions, eG Enterprise sent license violation alerts only to the user/administrator who has been configured with valid email ID to receive alerts. However, administrators of some environments wanted the license violation email alerts to be sent to a few users apart from the configured user/administrator. To aid administrators in this regard, starting with this version, eG Enterprise sends license violation mail alerts to a comma-separated list of email IDs specified against the **SendLicVioMailTo** flag in the **[MISC_ARGS]** section of the **eg_services.ini** file available in the **<EG_INSTALL_DIR>/manager/config** folder.

17.3.1.2 Integration Console Enhancements

- **Support to Display Component Type Associated with a Test:** In previous versions, when tests were added using the Integration Console capability, administrators could not identify the component types to which the tests were associated with from the **INTEGRATION CONSOLE – TEST** page. Administrators were forced to juggle across multiple pages to figure out the component types associated with the tests. To ease the pain of such administrators, starting with this version, the component types to which the test is associated will be displayed in the **INTEGRATION CONSOLE – TEST** page.
- **Multiple Authentication Methods Supported for Building REST API Test Type Using Integration Console Capability:** In previous versions, if a test based on REST API test type was created using the Integration Console capability, the eG agent could execute that test as any valid user with REST API access. However, to protect their critical servers and confidential data from malicious attacks, some high-security environments restricted REST API accessing multiple authentication methods such as API Keys, Bearer tokens, OAuth 2.0 protocols etc. To ensure that IC-based tests of type REST API execute without a glitch in such secure environments as well, eG Enterprise v7.2 also supports multiple authentication methods. By choosing any of the following options from the Authorization type list, administrators can build a REST API test type without compromising on the security of their environment.
    - **API Keys:** If this option is chosen, administrators will have to specify a valid API key. The eG agent will authenticate itself using this key in order to run API commands and pull relevant metrics.
    - **Bearer Token:** This option requires that the test be configured with a unique and valid security token. This token allows the test REST API access.

- **OAuth 2.0:** If this option is selected, administrators should create a custom App, which will be used to authenticate REST API requests. A client ID and secret should be assigned to the App, so that it can prove its identity when requesting a token for executing the test,

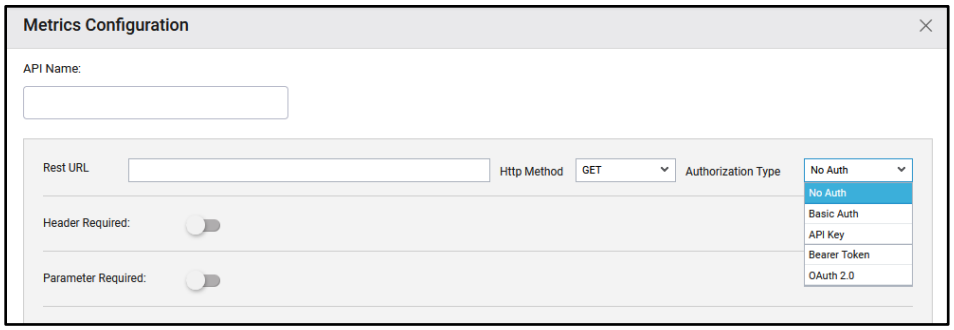


Figure 113: Modern Authentication Support for creating an IC based test of REST API test type

- **Enhancements to JMX Test Type:** Previously, it was noticed that some IC tests of JMX test type suddenly stopped reporting metrics for a couple of measurement periods, and switched to the *Unknown* state. It was later observed that this happened if the Java application being monitored stopped supporting one/more MBeans used by the test for metrics collection. To avoid displaying the IC based test in *Unknown* state in the eG layer model, starting with this version, a **Dynamic_Info_Test** parameter has been included as a default parameter. By default, this parameter is set to *true* indicating that the test will not be displayed in the layer model if it does not report metrics for 2 or more consecutive measurement periods.

17.3.1.3 Other Enhancements

- **REST API Client:** To perform critical configuration tasks on the eG manager without logging into the eG manager, eG Enterprise offers both eG CLI and eG REST API capabilities. From any third-party REST Client, administrators can access the URL of the eG manager using the HTTP POST method, connect to it and perform configuration tasks on it. However, to use the eG REST API capability, administrators had to install a REST Client of their choice in the target environment, painstakingly build the API commands with all the required parameters, import them into the REST Client and finally execute them. This process was time-consuming and sometimes, resulted in errors. To eliminate the dependency on a third-party REST client, and to save time, trouble, and errors in configuring that REST client, eG Enterprise offers a proprietary **REST API Client**. Using this capability, administrators can obtain the output of REST API commands, within minutes of choosing the API and executing the same from the eG administrative interface.

- **Modern Authentication Support for Email Alerting:** eG Enterprise supports automatic generation and transmission of email alerts to specified recipients. In earlier versions, to send email alerts, administrators had to configure a mail server that used basic authentication. However, in recent times, to ensure secure mail transmission/reception, many IT datacenters are employing modern authentication mechanisms like SAML, OAuth and WS-Federation. For secure email alerting, starting with eG Enterprise v7.2, administrators can use an Office 365 mail server that supports the OAuth 2.0 modern authentication protocol. OAuth is an authentication protocol that allows you to approve one application interacting with another on your behalf without giving away your password. Administrators can send email alerts to mailboxes managed by Office 365 by choosing **OAuth 2.0** as the **Mail authentication type** in the **MAIL SERVER SETTINGS** page of the eG administrative interface.

  Prior to selecting OAuth2.0 as the Authentication type, ensure that you do the following:

  - Create an App on Azure AD, which will be used to authenticate email alerts sent by eG

manager to Office 365;

- Assign a client ID and client secret to the App, so it can prove its identity when requesting a token from Office 365;
- Allow the App to read user profile and send emails to Office 365 as any user.

Once the above pre-requisites are fulfilled, specifying the Client ID, Client secret and Tenant ID in the **MAIL SERVER SETTINGS** page will ensure that the email alerts are sent seamlessly to user mailboxes.

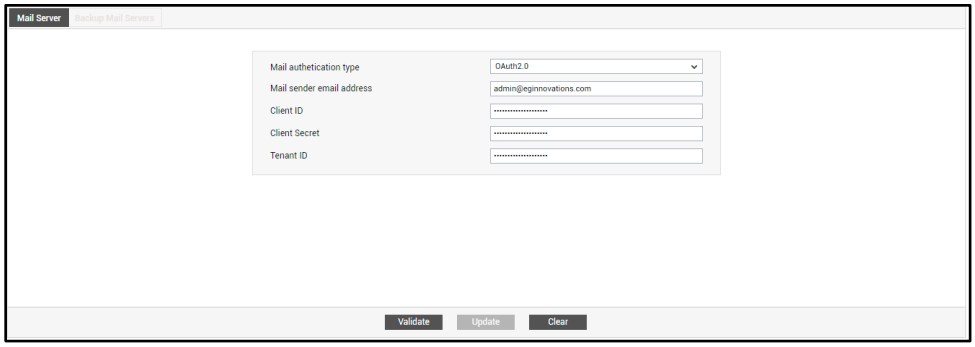


Figure 114: Choosing OAuth2.0 as the Mail authentication type for sending email alerts

Administrators can also opt to choose the Mail authentication type while installing the eG manager (from the Installation Wizard).

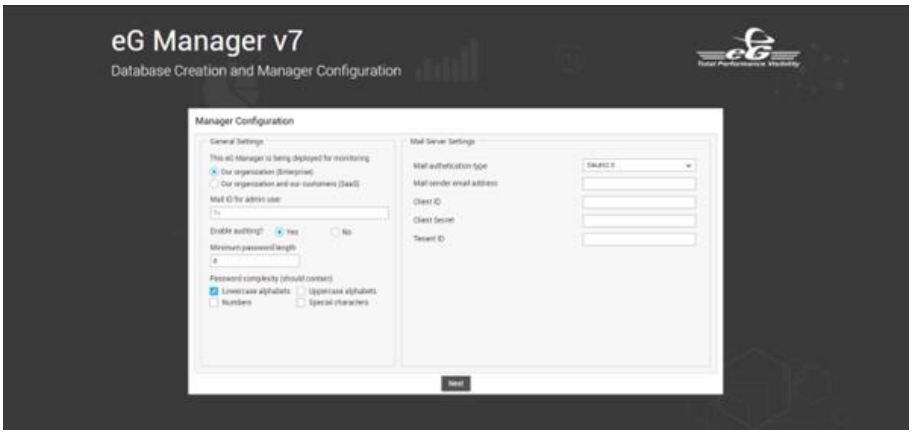


Figure 115: Choosing the Mail authentication type while installing the manager

- **Ability to Generate User – Zone/Service/Segment Assignment Report:** In SaaS installations of eG Enterprise typically, tenants log into the eG management console and use a 'self-service' dashboard to configure their infrastructure for monitoring, without any administrator intervention. A tenant can download and install agents, manage the components they want to monitor, and group them into segments / services / zones. In such eG installations, an administrator previously had no means of determining which tenant/user is associated with which zones / services / segments. To address this requirement, eG Enterprise v7.2 allows administrators to generate a detailed Assignments report. With the help of this report, the administrator can quickly oversee the configurations of tenants, and even identify those tenants who have not configured any component groupings.

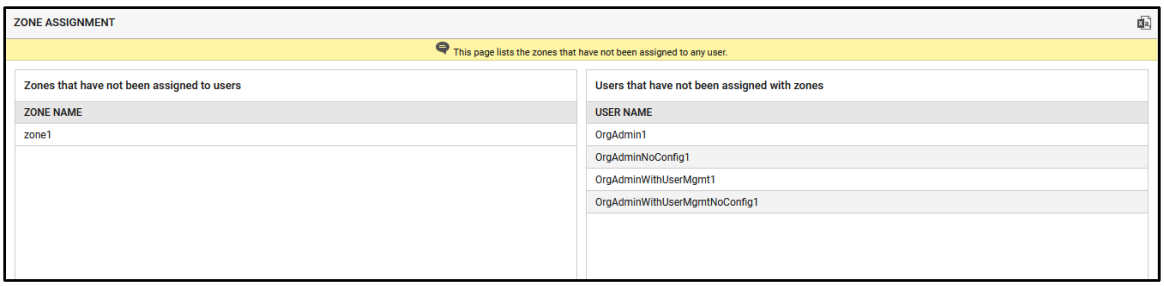


Figure 116: A sample Zone Assignment Report

17.3.2 Monitor Interface

- **Design Changes to Metrics View of a chosen Component Type:** The **Metrics View** page associated with a Component Type has been enhanced in v7.2. A brand-new **Overview** section has been included. This section reveals the count of managed components of the chosen type, aggregate health of the components, and the number alerts pertaining to the components. With the help of this section, you can determine, at-a-glance, how error-prone a component type silo is, and what type of issues (whether critical/major/minor) that silo is experiencing currently. Additionally, a **Performance Summary** section is also provided in this page, which rapidly alerts you to current/potential resource shortages in, and breaks in network availability of, the components of the chosen type

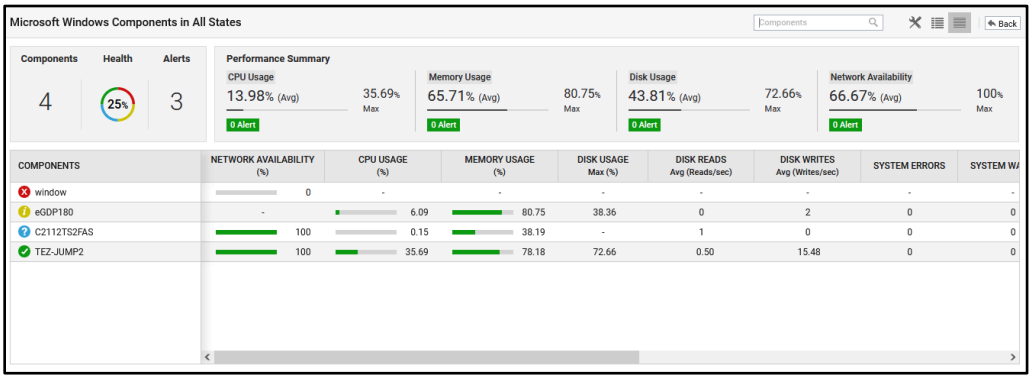


Figure 117: The Metrics View page for the components associated with Microsoft Windows

- **Improvements to Additional Alarm Details and Configuration Details in CURRENT ALARMS / UNKNOWNS Window:** In version 7.2, the icon that previously accompanied each 'clubbed' alarm in the **CURRENT ALARMS / UNKNOWNS** window has been replaced with a more intuitive 'down arrow' icon. Clicking on this icon reveals the individual alerts that are 'clubbed'. Also, you can now view the detailed diagnosis (if any) and generate graphs for each of the individual alerts

displayed here.

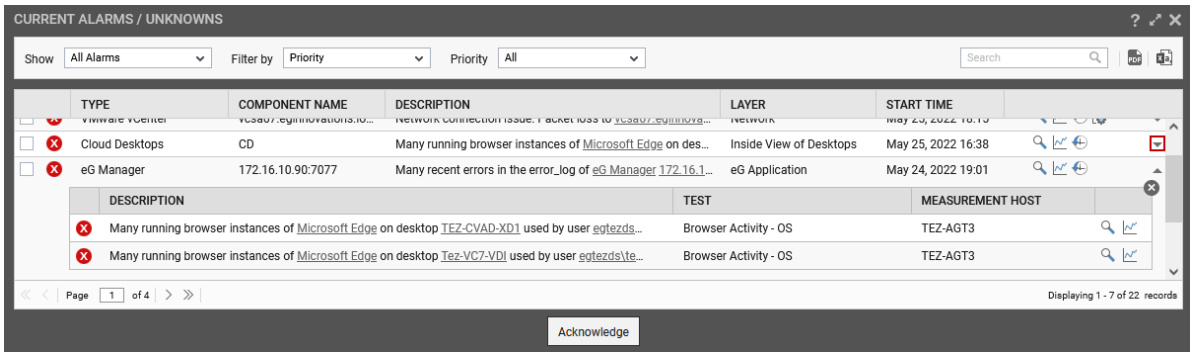


Figure 118: Improved Current Alarms / Unknowns page

Similarly, the 'look and feel' of the configuration changes captured and reported in the **CURRENT ALARMS / UNKNOWNS** page has also been improved. Starting with this version, intuitive colour codes have been used to help you rapidly differentiate between additions, changes, and removals. You no longer have to read the column headings/captions to understand the nature of a configuration change.

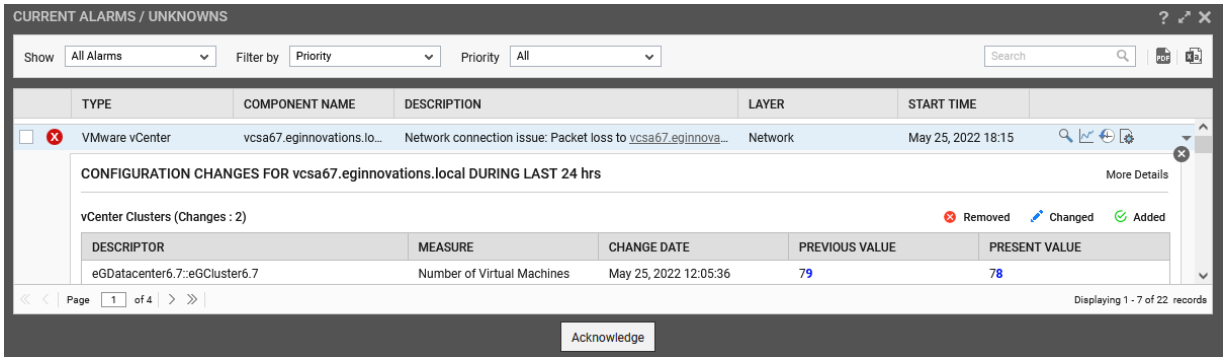


Figure 119: Viewing the Configuration changes with intuitive colors in the Current Alarms /Unknowns page

- **Incident Management Dashboard:** Often, administrators are required to keep track of their environment every other minute. In previous versions, administrators were forced to navigate through multiple pages across the eG monitor interface to view the list of current alarms, list of alarms that were acknowledged, history of unknowns etc. Also, administrators could not view the alarms that were correlated from a single interface. To ease the pain of administrators, eG Enterprise v7.2 offers a unified Incident Management dashboard that provides a single pane-of-glass view of

alarms, acknowledgements etc.

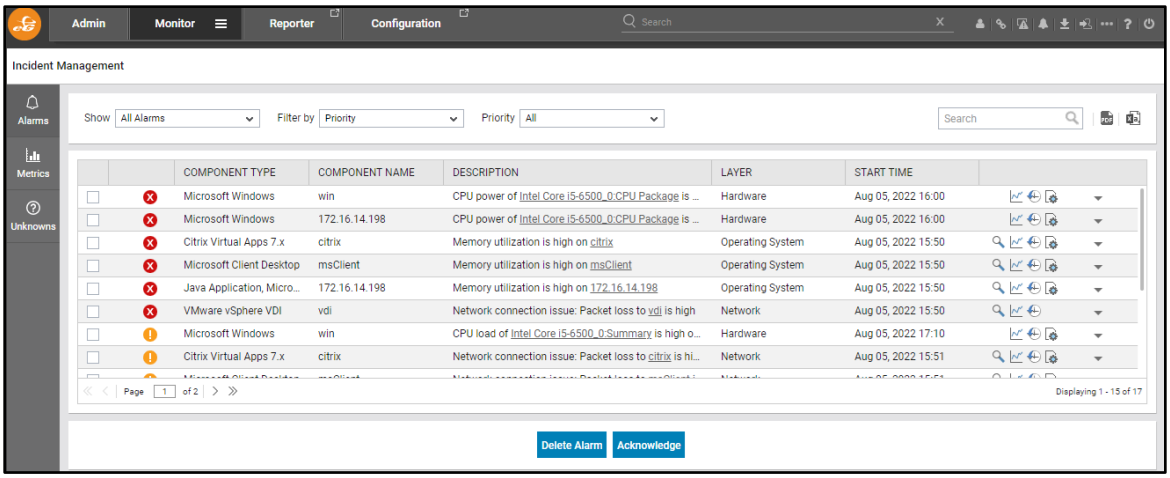


Figure 120: The Incident Management Dashboard

By default, eG Enterprise helps administrators detect and resolve performance issues by automatically correlating alerts across all tiers and pinpoints the root cause of those issues within a few minutes. To corroborate this functionality, eG Enterprise v7.2 displays all the alerts that are correlated in a single interface so that administrators can identify the alert that is the root cause of all other alerts that are correlated. This clear display of alarm correlation helps administrators in understanding the cause-effect relationship and perform better root cause analysis.

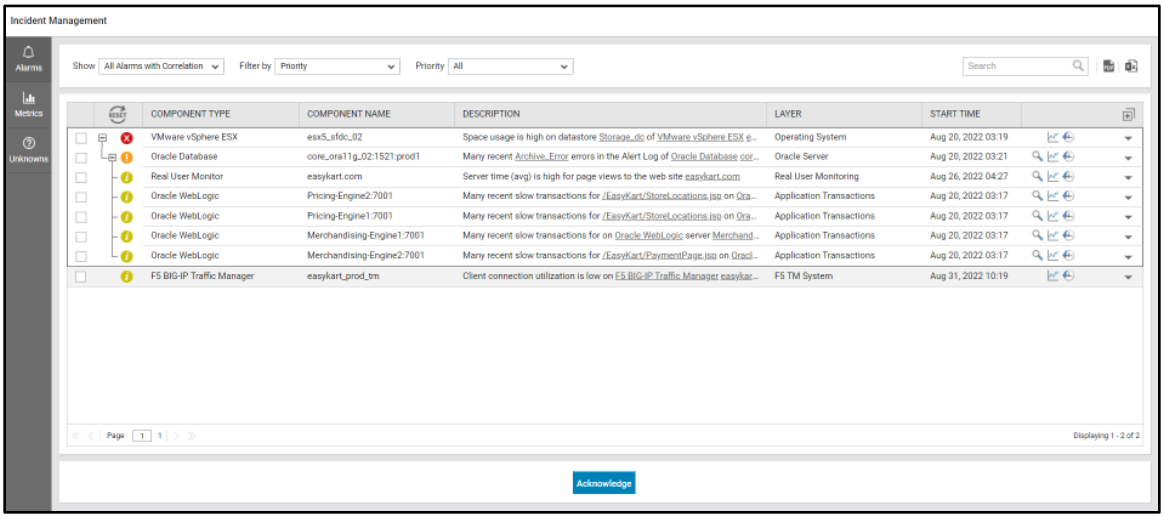


Figure 121: Displaying the alarms that are correlated

By navigating across the tabs of the Incident Management dashboard, administrators can view the list of alarms that were currently raised in the target environment, the alarms that were correlated, the alarms that were acknowledged/unacknowledged etc. This way, this dashboard helps administrators obtain an overview of what is happening in their environment, who acknowledged/deleted an alarm and how many alarms are correlated in the environment. Administrators can also obtain an overview of those tests/components that are in an 'Unknown' state.

- **Enhancements to My Dashboards:** Following are the enhancements made to My Dashboards in

eG Enterprise v7.2:

- **Ability to export My Dashboards as a PDF:** Starting with this version, administrators can export the dashboards created using My Dashboards as a PDF.
- **Ability to export My Dashboards as a Template:** Starting with this version, administrators can export the dashboards created using My Dashboards as a Template for future use.
- **Ability to Clone Widgets in My Dashboards:** Sometimes, administrators may be required to reuse a widget multiple times in the same My Dashboard but configure each widget for different components. If this is done manually, it can be a time consuming and laborious exercise. To save the time and effort that this redundant task entails, eG Enterprise v7.2 offers the Clone option. Administrators can use the Clone option to reproduce the same widget any number of times.
- **Ability to Include/Exclude Descriptors based on Wild Card Patterns:** In some environments, while building a My Dashboard template, administrators may be required to configure a widget only for a few descriptors and ignore a select few descriptors. To achieve this, in previous versions, administrators had to painstakingly select the descriptors of their choice for inclusion/exclusion. However, this process was tedious in environments where thousands of descriptors were available. To ease the pain of administrators in including/excluding the descriptors, starting with this version, administrators can include/exclude descriptors based on wildcard patterns. To this effect, a Filter By Wildcard slider has been introduced in the Widget Configuration window. By turning on this slider and specifying the wildcard pattern, administrators can quickly include/exclude the descriptors that match the specified wildcard pattern.
- **Introduced Multiple Pre-Built Templates:** eG Enterprise has included a host of pre-built dashboard templates for a variety of components based on which users can build **One-Click Dashboards** for the components of their choice. Figure 122 displays a list of pre-built templates for all the component types supported by eG Enterprise v7.2.

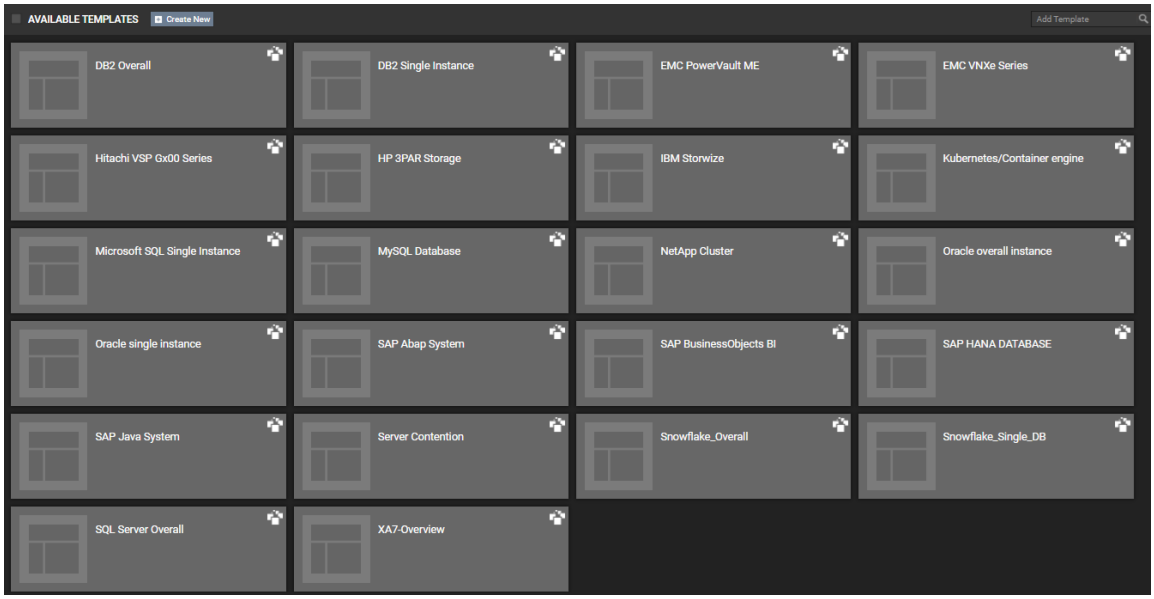


Figure 122: The newly introduced pre-built templates

- **Introduction of New Widgets:**
  - The **Web App Simulation** widget (available in the **Widgets Gallery** section) displays the transactions simulated using Web App Simulator, the status (whether it succeeded or failed)

of each transaction, and the time taken to successfully complete each transaction. Using this widget, administrators can identify the exact step at which a transaction failed or slowed down.

- The **Resource Consumption Analysis** widget (available in the **Widgets Gallery** section) tracks the resource (CPU/memory/disk) utilization of all the components managed in the target environment in the past 15 minutes by default.

  This widget consists of the following sections:

  - **Highest and Least <Resource> Utilization:** This section displays a bar graph revealing the top / least consumers of the chosen resource.
  - **Average <Resource> Utilization:** This section displays a time-of-day graph that reveals how the chosen resource was utilized during the past 15 minutes (by default). Using this graph, administrators can figure out when during the last 15 minutes (by default) resource usage peaked.
  - **Top 10 Servers by <Resource> Utilization:** This table displays the Top-10 components in the target environment in terms of their usage of the chosen resource. This table helps administrators identify the exact process executing on the chosen server that is consuming maximum resources.

    Administrators are even allowed to pick a different Timeline for this widget and are also allowed to pick and choose the components for which they want to perform resource usage analysis. By default, this widget will be plotted for CPU resource consumption.

- The **Up/Downtime Analysis** widget (available in the **Widgets Gallery** section) helps administrators identify the components that were down for the longest time during the given period.
- The **Citrix Receiver Analysis** widget (available in the **Widgets Gallery** section) displays a bar graph depicting the number of users connected to Citrix environments using Citrix Receivers of each type. This way, you can quickly figure out if any user is using an unsupported / obsolete Receiver. This widget also displays the count of users connecting from each client Operating System.
- The **User Experience** widget (available in the **Widgets Gallery** section) reports the level of satisfaction attained by users when working with web sites/web applications being monitored. The Apdex score is displayed along with a heat map chart that provides the distribution of users and the count of requests for which the user experience was measured as Satisfied, Tolerating and Frustrated.
- The **Geo User Experience – RUM** (available in the **Widgets Gallery** section) helps you measure the overall experience of users based on their geographies. At a single glance, administrators can determine which country/region's users are having a sub-par experience with a monitored web site/web application.
- The **Pie Chart** widget has been enhanced to display the chart as either a Pie or a Donut. Also, users are provided with the flexibility to display the labels (measure values) on the chart using the **Pie Labels** slider. They can also choose where exactly to place the legends (descriptors) in the chart i.e., they can place the legend at the top or bottom of the chart (using the **Legend Placement** list). The legends can also be displayed as a table or can be listed one below the other by choosing an appropriate option from the **Legend Mode** list.

➢ **Support for new Component Types in Application Dashboard:** Starting with this version, application dashboards are available for **Microsoft SQL on Cloud** and **Oracle Database on Cloud** component types.

- **Improvements to Kiosk Mode:** Starting with this version, administrators can play/view the User Experience dashboard and the Zones dashboard in Kiosk Mode. You can even play/view the Configuration dashboard (home page of the eG Configuration Management interface) and the Inventory dashboards of the eG Configuration Management interface.
- **Introduced Search Capability in Virtual Servers page:** In previous versions, where numerous hypervisors are monitored, an administrator had to scroll down the **Virtual Servers** page endlessly to locate a particular hypervisor. To help administrators quickly get to the virtual server they want without scrolling, a Search capability has been introduced in the **Virtual Servers** page. Clicking the **Search** icon after keying a specific search criterion will reveal the virtual servers that match their search.

17.3.3 Reporter Interface

- **Custom Report Templates can now be Cloned:** In earlier versions, if a user wanted to create a custom report template with similar specifications as an existing template, he/she had to painstakingly create a new template from scratch. This was both time-consuming and laborious, particularly where many such templates were to be created. To ease the pain of users, starting with this version, eG Enterprise supports cloning of report templates. Clicking the  icon against an existing report template in the **eG Custom Reports** page will enable you to create (clone) a new template based on that report template.
- **Health widget has been introduced in Custom Reports:** Starting with this version, to obtain a health report of the components of a particular type, administrators can use the **Health Executive** tab in the **Config Report Template (Template Name)** pop up window. By merely looking at the details displayed in this widget at runtime, administrators can identify the state of each component of the chosen component type. The count of currently unresolved issues for the component type is also reported in this widget, so you can tell if the component type silo is suffering many performance setbacks presently. The total count of problem events encountered by components of this type, and the average duration of these events are also displayed, so you can gauge how problem-prone the component type silo has been, and how efficient the administrative staff was in resolving the issues. This way, the widget paints a true picture of performance of the component
- **Automatically Zipping Large Report Attachments in Scheduled Emails:** In previous versions, where reports were scheduled to be emailed, eG failed to deliver a scheduled email if the size of the report attached to that email exceeded a certain limit (Default value is 5 MB). To make sure that emails are delivered as per schedule regardless of the size of the attachments, started with version, eG automatically zips report attachments that are of a size larger than the configured limit, and then sends the emails to the specified recipients. To this effect, a **MaxFileSizeForMail** option is available in the **[MISC]** section of the **<eG_INSTALL_DIR>/manager/config/eg_report.ini** file and is set to **5 (by default). Also,** the **SendMailAsZipFormat** flag has also been introduced, which is set to **Yes**, by default.
- **Scheduling Delivery of Reports via Email Every Hour:** In previous versions, reports/booklets can be scheduled to be emailed to one/more recipients once per day/week/month/weekend or on specific days of a week. However, administrators who rely entirely on the emailed reports to identify problems may want the reports delivered to them more frequently, so that problems do not go unnoticed or unattended for long periods of time. To help such administrators, eG Enterprise v7.2 now allows you to schedule the emailing of reports/booklets once every hour. To this effect, an **Hourly** option has been introduced in the **Mai**l drop down list available in the **Schedule this Report** pop up window.
- **eG Database Analysis Report:** One of the key challenges faced by administrators when using the eG monitoring system is making sure that the eG database is sized correctly and does not run out of space at any point in time. Some of the common causes for a space crunch in the eG database include poor capacity planning resulting in insufficient space allocation to the database, and abnormal

database growth owing to irregular cleanup and inefficient database maintenance. The shortage of space in the eG database often has serious repercussions:

- The eG database may not be able to store real-time performance measures collected by the agents. As a result, eG will not be able to alerts users to problem conditions; troubleshooting becomes a nightmare, support costs escalate, and infrastructure downtime increases;
- Without enough space to store even raw measures, trend computation and storage of trend data becomes impossible; hence, reports cannot be generated, performance cannot be historically analyzed, and potential problems cannot be predicted;
- Organizations may be forced to unnecessarily splurge money on additional hardware to quickly resolve the space crisis;

To prevent such eventualities, administrator should continuously keep track of the growth of the eG database to proactively detect and if possible, avert, abnormal growth in database size. For this purpose, eG Enterprise v7.2 offers the eG Database Analysis report.

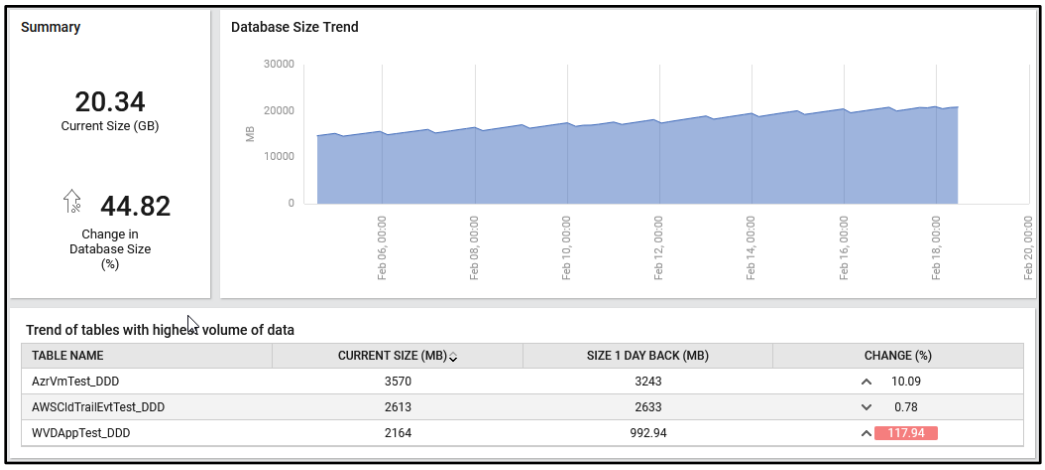


Figure 123: The eG Database Analysis Report

- **Top Tables by Space Used Report:** In environments where hundreds of components are monitored, there is a possibility that the eG backend database may run out of space. To conserve database space, it is essential to optimize the space used by database tables. For this purpose, eG Enterprise v7.2 offers the **Top Tables by Space Used** report. This report helps administrators identify those tables that are consuming the maximum amount of space in the eG backend database over a period of time, and isolate those tables that are growing at a rapid pace. The pointers provided by this report enable administrators to initiate remedial measures such as reducing the frequency of the test that is dumping data into the table, reducing the retention period of the detailed diagnosis

of the tests etc.

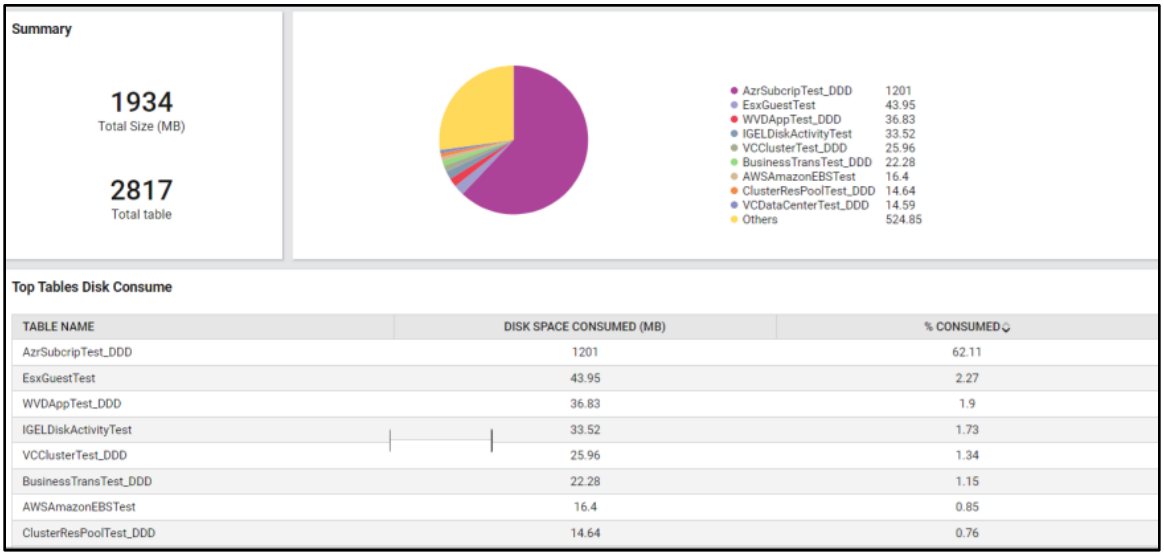


Figure 124: The Top Tables by Space Used report

- **Reports can now be generated for Previously Managed Components:** In previous versions, reports were generated by eG Enterprise only for those components that were currently managed in eG Enterprise. The historical data of a server was deleted once the server/component was deleted/unmanaged from eG Enterprise. This approach of eG Enterprise posed a big challenge in dynamic environments (Cloud infra, MSPs) where containers were created/deleted often, and servers were automatically scaled up/down. Also, in an on-premises environment where dynamic power management is supported by technologies such as Citrix, servers were powered off after office hours. Losing the historical data proved to be costly and detrimental to the health of such environments. This is why, eG Enterprise v7.2 supports generation of reports for even deleted/unmanaged components. To this effect, the **Components** list in the report generation criteria now lists all the components that were unmanaged/deleted in the recent past in the **Unmanaged Components** section. eG Enterprise maintains the historical statistics pertaining to a component, even after that component is no longer monitored, so that reports can be generated for that component. Also, all prior associations of that component – i.e., the service/segment that the component was a part of, the zone/component that component belonged to etc. This way, eG enables users to study how past issues with that component impacted the performance of the business services / segments / zones / groups it once belonged to. Historical reporting is supported even for server/application/device that is automatically removed from eG Enterprise by auto-discovery.

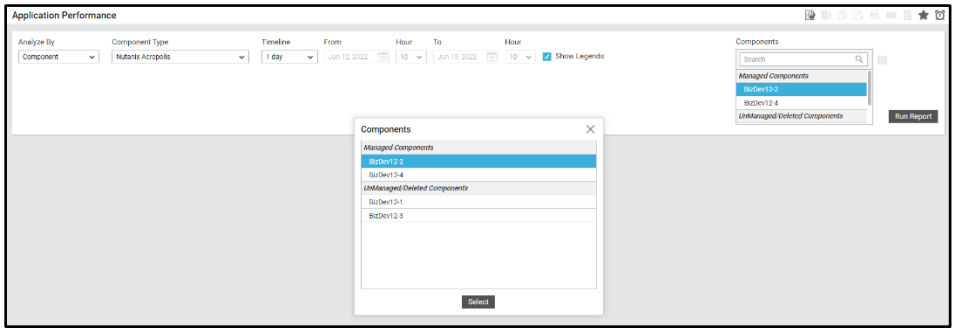


Figure 125: Listing the components that were previously managed/deleted

17.4 Installation Enhancements

- **Automatic Installation of eG Agents:** In previous versions, using the installers that eG Enterprise provided (i.e., exes and shell scripts), administrators installed an eG agent on a Windows/Linux host quickly and in a hassle-free manner. However, this traditional agent installation procedure was not fully automated. Administrators were required to manually provide certain inputs - for e.g., the IP address of the manager, nick name etc. Erroneous inputs often resulted in installation failures. Also, because of the need for manual intervention, it was tedious to install agents on hundreds of systems using this procedure. Alternatively, users could integrate with orchestration tools and gold images to install agents on numerous targets simultaneously. But these were atypical options, which were seldom used and difficult to implement. To enable faster, easier, and error-free installation of agents on multiple hosts, starting with this version, the eG manager supports automatic installation of agents.

  By automating the installation of agents, administrators can obtain the following benefits:

  - Super quick one-click installation process on hundreds of host systems;
  - Reduced manual work;
  - Reduced deployment time;
  - Error free deployment;
  - Centralized configuration and
  - Easy Troubleshooting with central logging.

  This feature is supported on both deployment models of eG Enterprise i.e., Enterprise and SaaS deployments.

- **In an Enterprise deployment of eG Enterprise**, the eG agents are pushed from the eG manager hosted on Windows operating system to the target systems (both Windows and Linux OS). If all the target systems are within a domain, then, administrators can push the eG agents using the **Agents Installation for Machines Attached With Domain** page in the eG administrative interface.

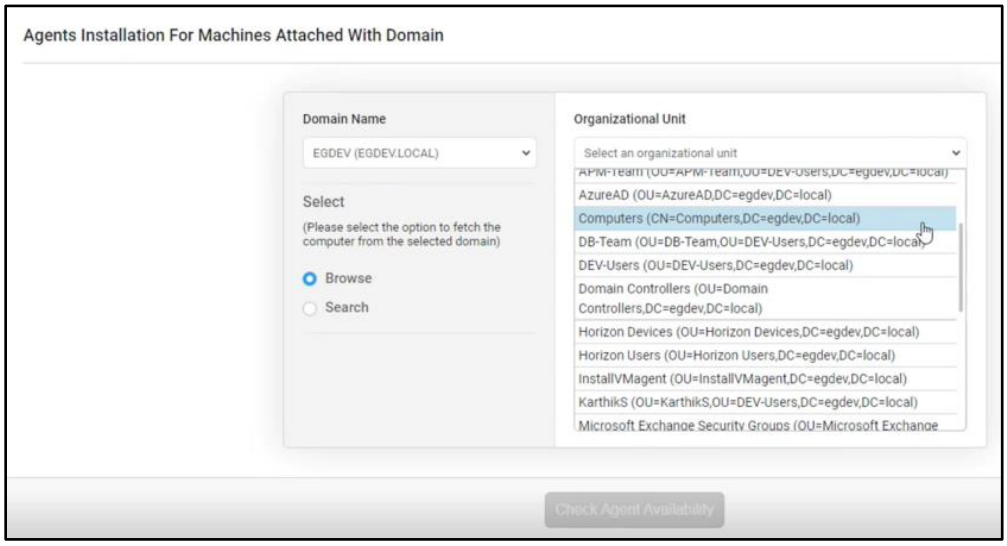


Figure 126: Automatically installing the agents on target systems within a Domain

If the target systems are not within a domain, then, administrators can push the eG agents by creating a Password Profile. Specifying a comma-separated list of IP addresses and the appropriate **Password Profile** from the eG manager will ensure that the eG agents are automatically installed

on the target systems.

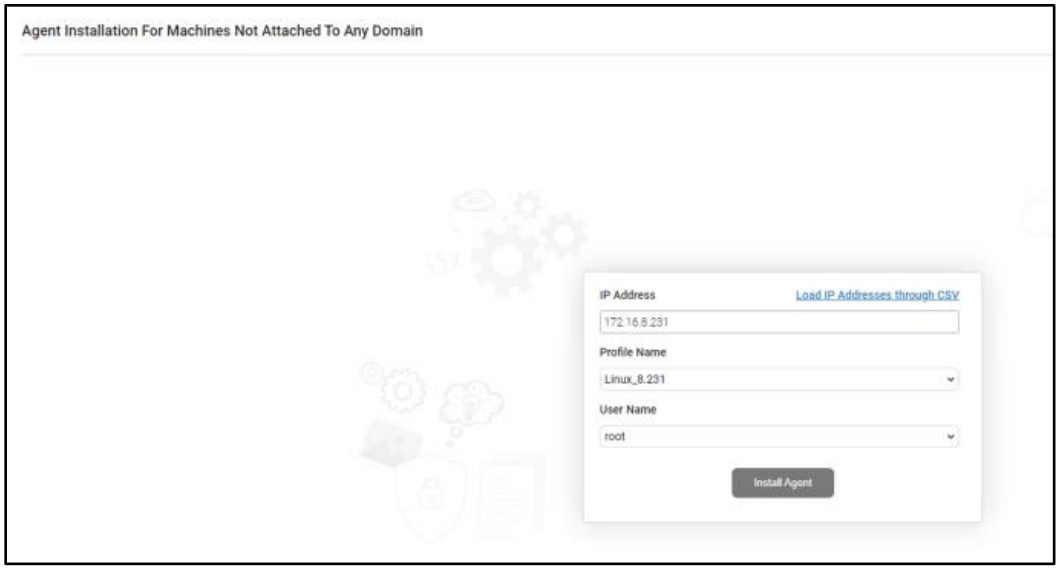


Figure 127: Automatically installing the agents on target systems that are not within a Domain

In a SaaS deployment of eG Enterprise, since the eG manager is hosted on cloud, the infrastructure/applications will not be accessible to the eG manager. Therefore, the eG manager will not be able to directly push the eG agents to the target systems. To automate agent installation, administrators need to download the agents and the installer from the eG manager to an on-premises system and use the eG Agent Installation Wizard to push agents to the target systems. In a SaaS deployment, the wizard can be used to automatically install agents on **Windows hosts only**.

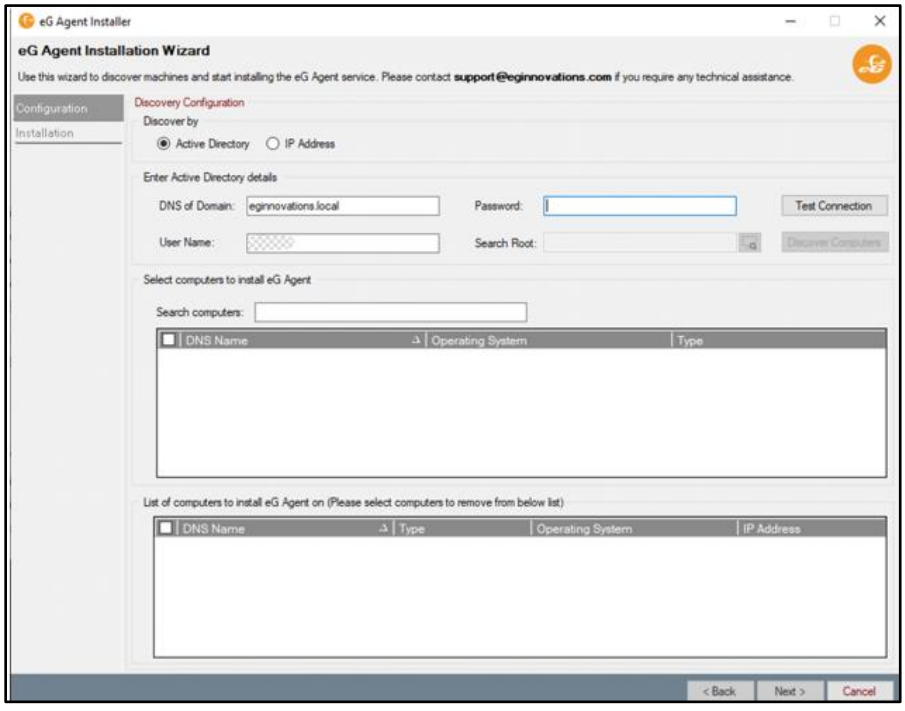


Figure 128: The eG Agent Installation Wizard

The **Installation Status** page in the eG administrative interface throws light on the status of agent

installation.

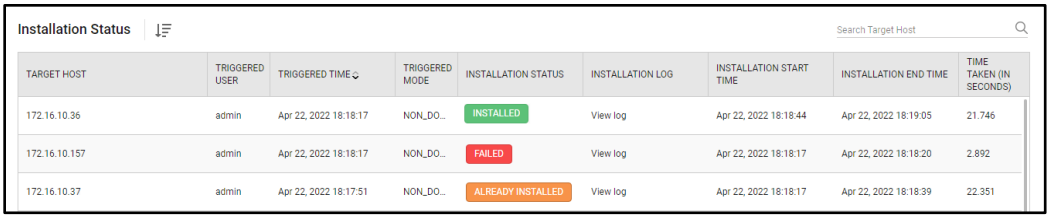


Figure 129: Viewing the status of agent installation on the target systems

- **Agent Installation is now Simplified:** In previous versions, administrators downloaded a ZIP/TAR package of the eG agent installation from the eG admin console and installed the eG agents. This process was tedious for administrators who had to install hundreds of agents in a target environment. To simplify this process and to ensure administrators install the agents in a hassle-free manner, eG Enterprise v7.2 offers a brand-new solution in the form of a one-line command which can be executed from the PowerShell command prompt of a Windows system/ shell prompt of a Linux system.

Figure 130: Installing the eG agents using a single command

Administrators can also integrate this one line command with orchestration tools for automated installation of eG agents.

- **Other Installation Changes:** Starting with this version, the eG manager is no longer supported on Windows 2008 and 32- bit Operating Systems. The eG manager is bundled with Tomcat v10.0.27 and Open JDK v17.0.5. The eG agent on Windows and Linux 64-bit systems are also bundled with Open JRE v17.0.4 starting with eG Enterprise v7.2. From this version, the eG agent cannot be installed on HPUX-PA-RISC systems while support has been provided to install the eG agent on Linux 64-bit PPCLE. In addition, starting with this version, the eG agent and the eG manager can be installed on Window 2022 operating systems.

17.5 eG Mobile Application Enhancements

In the latest update to the eG Mobile Application new mobile-optimized UI components, gestures, and tools have been added, making the application fast and interactive. Following are the enhancements:

- **Support Provided for Single Sign-on through SAML:** Starting with this version, if the eG manager is enabled with single sign-on, users are now allowed to login to the eG mobile application by choosing the SAML authentication provider and specifying their credentials.

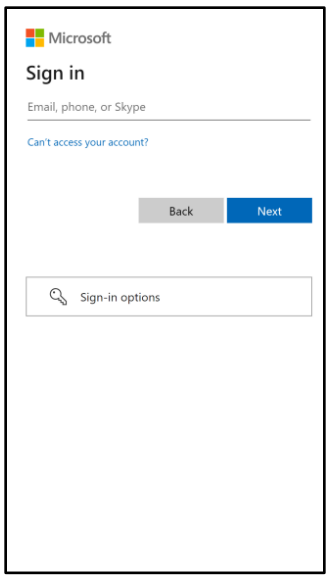


Figure 131: Logging into the eG mobile application using single sign-on capability

- **Improved Home Page:** Unlike previous versions of the eG mobile application, in the current version, the Home page does not only reveal the number and health of managed components. Additionally, the Home Page displays dough nut charts revealing the count and health of zones, segments, services, and aggregate components managed in the target environment. This way, the Home page provides an infrastructure-wide view of performance, and enables administrators to quickly isolate the problem areas.

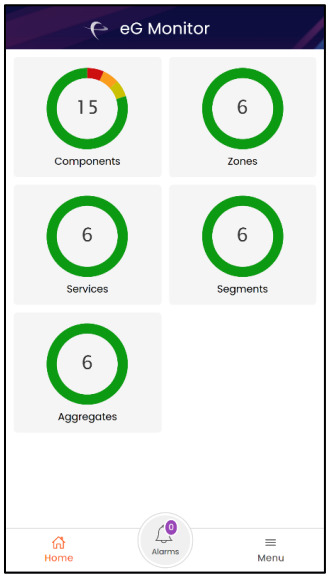


Figure 132: The eG mobile application Home Page

- **Tracking the Health of Individual Zones/Services/Segments/Aggregates:** In the new version, you can even click on a donut chart (representing the health of zones/services/segments/aggregates) in the Home page to know which elements are in what state

currently.

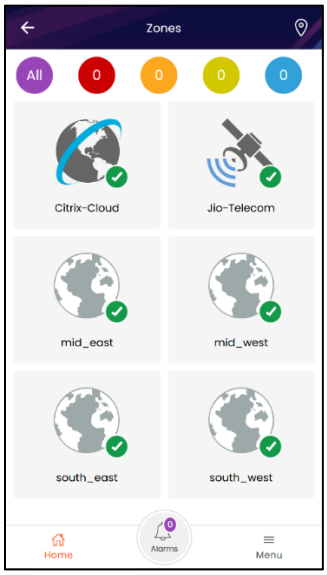


Figure 133: Viewing the Zones configured in eG Enterprise

- **Viewing Zone Maps:** Starting with this version, clicking the icon in the **Zones** window of the eG mobile application will invoke a Zone Map indicating the geographic location and state of each zone.

Figure 134: The Zone Map

You can drill down a problematic zone to view the performance issues that are affecting that zone's health.

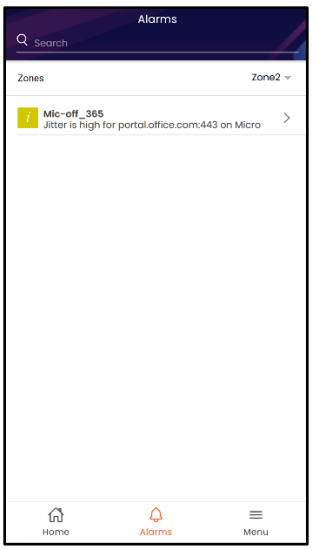


Figure 135: Viewing the alarms associated with a zone

- **Support Provided to view Dashboards:** Starting with this version, administrators can view a few key dashboards offered by eG Enterprise such as RUM Dashboard and User Experience Dashboard from the eG Mobile application.

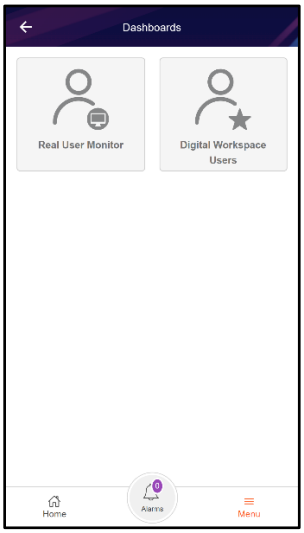


Figure 136: The Dashboards page

The RUM Dashboard, with the help of intuitive icons, graphs, geo maps etc helps administrators analyze the traffic to the managed web sites/web applications in the target environment, identify the devices through which traffic is coming from and figure out the user experience with the managed web sites/web applications. Where Real User Monitor components are managed, the eG mobile

application now displays the RUM Dashboard for each RUM component.

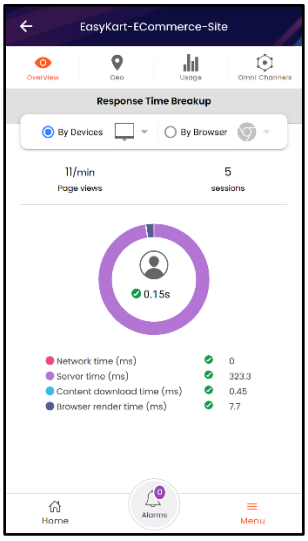


Figure 137: The RUM Dashboard

User Experience Dashboard helps end-users themselves to view the performance metrics related to their access to the Citrix/VDI infrastructure.

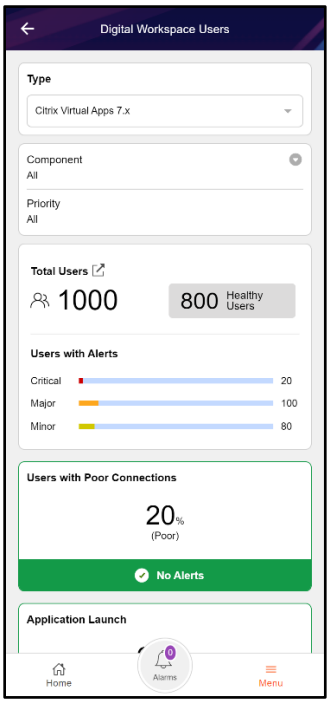


Figure 138: The Digital Workspace Users dashboard

Clicking the **Total Users** icon in Figure 138 will list all the users logged into the target Digital

Workspaces environment.

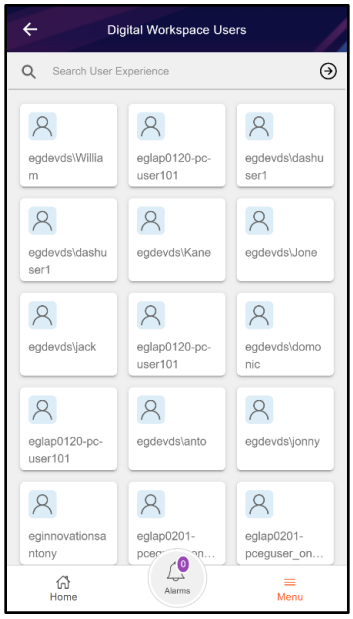


Figure 139: Users logged into the target environment

Drilling down each user will help administrators easily determine if the user had experienced slowdowns, experienced connectivity issues to the Citrix infrastructure, problems with application(s) that are being used in a Citrix session or a problem with the Citrix infrastructure itself.

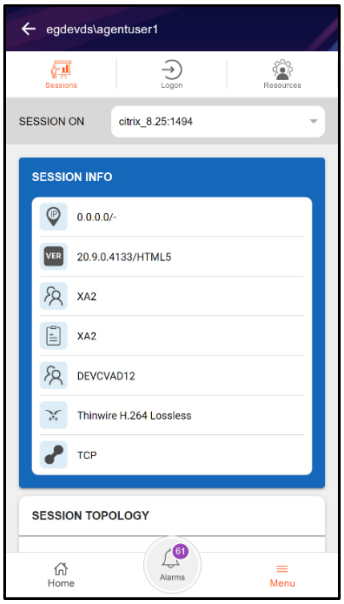


Figure 140: Dashboard showing the experience of an individual user

The Session, Logon and Resources tab provide in-depth insights into the sessions initiated by the user, the logon process of the user and the resources accessed/utilized by the user in the session.

- **Support to Initiate Remote Control Actions:** Starting with this version, administrators are allowed to perform remote control actions on a component from the eG mobile application.

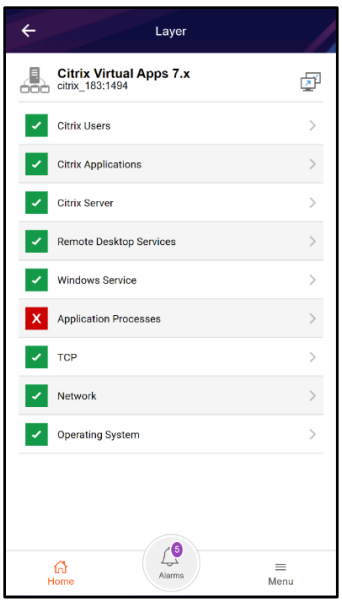


Figure 141: The remote control actions icon

Clicking the icon will help administrators pick an activity and initiate control action on the chosen component.

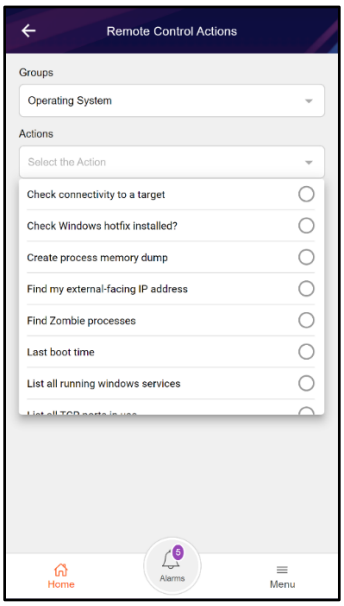


Figure 142: Initiating a remote control action

- **Quickly Switching to Another User's Monitoring View:** Sometimes, a help desk manager/administrator may want to know what issues have been assigned to a specific user / help desk executive, so they can understand why they are not resolved yet. Previously, to achieve this, the administrator had to log out of the eG mobile application and log back in as that user. This was tedious and time consuming. To avoid this, starting with this version, the eG mobile application enables an administrator to switch to another user's view, without having to log out. A **Switch User**

option has been introduced in the **User Profile** page of the eG mobile application to facilitate this.

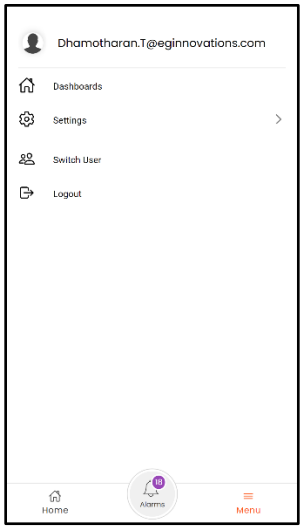


Figure 143: The Menu window

Clicking on the **Switch User** option will help administrators navigate to the **Users** page, where eG users who have accessed the mobile application at least once will be listed. The administrator will only have to pick a user and key in his/her credentials to see what that user sees in the eG console.

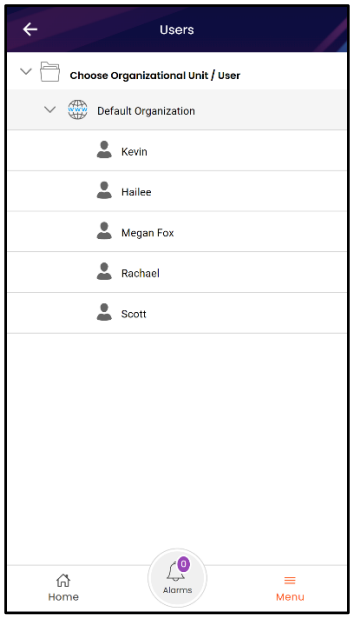


Figure 144: Listing the user profiles to switch login

- **Improved Push Notification:** Starting with this version, the eG mobile application uses the modern OneSignal Gateway, instead of the older Urban Airship messaging gateway, to send eG alerts as push notifications to the mobile device of users. With this transition, users accessing the eG mobile application can view push notifications that are more visually appealing and intuitive. For example, if a critical alert is sent as a push notification, the state of the alert will be highlighted in the

background of the eG logo.

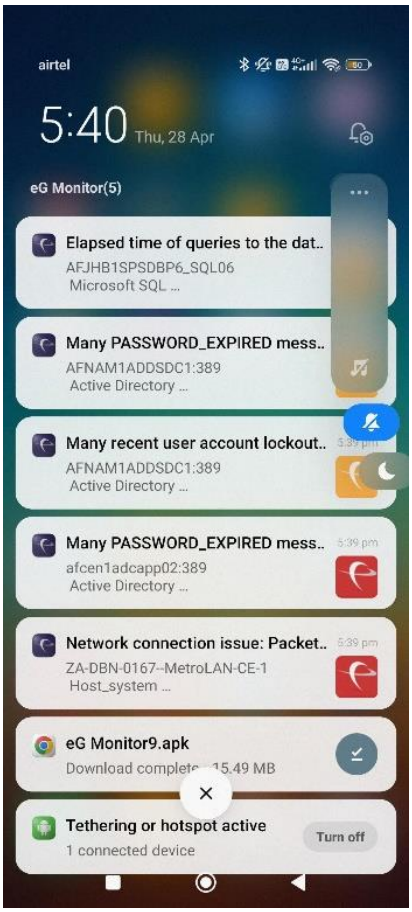


Figure 145: Improved push notification using OneSignal Gateway

17.6 Enhancements to eG CLI

In eG Enterprise v7.2, the eG CLI provides many additional capabilities. Using the eG CLI, you can perform the following operations:

- Associate one/more zone(s)/segment(s) to a user;
- Dissociate one/more zone(s)/segment(s) from a user;
- Add a user belonging to an Organization as well as an Organizational Unit;
- Modify a user belonging to an Organization or an Organizational Unit;

Also, starting with this version, a user with **Limited Admin** role is granted additional privileges to execute

the following CLI commands:

- Adding/Deleting External Agents
- Adding/Deleting Remote Agents
- Adding/Modifying/Deleing Components
- Managing/Unmanaging Components
- Adding/Modifying Quick Maintenance Policy
- Assigning Quick Maintenance Policy
- Deleting Quick Maintenance Policy
- Displaying External/Remote Agents
- Displaying Components
- Displaying Maintenance Policy names
- Displaying the details of Maintenance Policies
- Excluding/Including Components for Tests
- Excluding/Including Tests for Components
- Displaying the details of Tests
- Adding/Modifying/Renaming/Deleting Zones
- Displaying Managed Hosts
- Associating Components to Users
- Adding/Modifying/Renaming Groups

Enabling/Disabling eG CLI Capability: In previous versions, the eG CLI capability was enabled by default. In some highly secure environments, administrators wanted to disable the eG CLI capability for security reasons. To aid administrators in this regard, starting with this version, administrators are allowed to disable the eG CLI capability. For this, administrators should set the **RestrictEGCLIAccess** flag to **No** in the **eg_services.ini** file available in the **<eG_INSTALL_DIR>/manager/config** folder.

17.7 Enhancements to eG REST API

Following are the enhancements made to the eG REST API in eG Enterprise v7.2:

- Administrators can now retrieve the measure graph of a chosen measure. The graph can also be downloaded as an image in PNG format.
- Administrators can now retrieve the changes made to the configuration of a chosen component/zone/segment/service.
- The configuration changes made to the components of a chosen component type over a chosen time period can also be retrieved.
- Administrators can now retrieve the hourly/daily/monthly trend of a chosen measure.
- In previous versions, the eG REST APIs exposed raw metrics available in the database to third party tools on demand. Starting with this version, processed metrics are made available to third party tools. As a first step towards this, eG Enterprise v7.2 is now able to retrieve the uptime/downtime of servers and virtual machines managed in the target environment.
- The labels for all key values (both the input key values as well as key values obtained as output upon execution) of all the eG REST API commands have now been standardized. This way, administrators can maintain uniformity across all input values without having to remember separate input labels for each REST API command. Similarly, the Success/Failure responses obtained upon execution of the eG REST API commands too have been standardized so that the responses remain uniform across the API.

17.8 Integration Enhancements

eG Enterprise v7.2 can now be easily configured to route its alarms to a trouble ticketing system such as Sales

Force, TOPdesk, Fresh Service and BMC Remedy, via the web services framework.

- **Support for Multiple ITSM Integrations:** In previous versions, the eG manager can be integrated with only one trouble ticketing system. However, in SaaS and MSP deployments of the eG manager, each tenant would be using a different trouble ticketing system. In such cases, administrators found it difficult to route the alerts. To aid administrators route alerts to the respective trouble ticketing systems in SaaS and MSP deployments, starting with this version, the eG manager can be integrated with different trouble ticketing systems. To this effect, a **User name** list has been introduced in the **ITSM/COLLABORATION INTEGRATION** page. Administrators can route alerts to the respective trouble ticketing system corresponding to the entity type (Organizational Unit, Organization or user) assigned to the tenants. Alerts for those components that are associated with that entity type alone can be routed through the respective trouble ticketing system.
- **Detailed Diagnosis is now included with ITSM Integration:** In previous versions, where eG Enterprise integrated with a trouble ticketing (TT) system, only eG alerts were sent to the target TT system. For performing detailed analytics and troubleshooting, users had to log into the eG monitoring console. This process was tedious, and significantly delayed troubleshooting. To help administrators fix problems as soon as they are identified, eG Enterprise v7.2 sends detailed diagnostics along with the alert information to the trouble ticketing system.
- **OAuth 2.0 support for Service Now and SNOW ITOM:** In previous versions, to integrate with ServiceNow/SNOW ITOM via their web services framework, the eG manager connected to the configured web services URL using Basic Authentication method only. In some environments where OAuth 2.0 modern authentication protocol was enforced, eG Enterprise could not integrate with ServiceNow/SNOW ITOM. To address this issue, starting with this version, the eG manager can integrate with ServiceNow / SNOW ITOM even if they enforce the OAuth 2.0 modern authentication protocol. OAuth 2.0 lets an external client, like the eG manager, access resources on ServiceNow/SNOW ITOM and make required changes, without passing user credentials. Instead, this authentication technique requires the eG manager to obtain an access token. to create/modify trouble tickets in ServiceNow / SNOW ITOM. For this, the eG manager should first connect to the ServiceNow instance as a user who is authorized to request for an access token, and then submit web service requests as a valid 'Client'.
- **Enhancements to Integration with Moogsoft:** Earlier, eG Enterprise used Webhook integration to route eG alerts to Moogsoft. In some environments, this integration did not work as Moogsoft failed to authenticate access requests from the eG manager, even though valid credentials were provided. To ensure that the eG alerts are seamlessly routed to Moogsoft, starting with this version, eG Enterprise integrates with Moogsoft using its REST API. Via HTTP/S, eG alerts are POSTed to the REST endpoint URL of Moogsoft as JSON payloads containing problem information.

17.9 Security Enhancements

- **Improved Security upon Installation:** In earlier versions, eG Enterprise modules on Microsoft Windows were installed in the root folder. This not only compromised on security but also paved way for non-admin users to modify the files created in the folders of eG Enterprise's installation. For increased security and to avoid non-admin users from modifying the files, starting with this version, eG Enterprise's files are exclusively stored in the *Program Files* folder. This way, administrators can also avoid privilege escalation issues.
- **Enhanced Security to Prevent Vulnerabilities:** By default, eG Enterprise consists of a security filter option which automatically turns on to protect against vulnerabilities. These security filters are enhanced in v7.2 to prevent the following types of vulnerabilities:
  - **Cross-site Scripting:** Starting with this version, Cross-site Scripting vulnerability prevention has been enhanced by setting Content Security Policy, Referrer Policy, and Permissions Policy in the Response Headers of web pages associated with the eG manager.

- **Spell-Jacking:** Starting with this version, to address Spell-Jacking vulnerability, the spellcheck attribute of any text/text area of the eG manager interface is set to **false** by default.

17.10 Scalability Improvements

eG Enterprise v7.2 is now more scalable with certain improvements made towards state management, scalability of dashboards, and configuration file processing. Let us now have a more detailed discussion on these scalability improvements.

- **State management is More Efficient:** In previous versions, in environments where thousands of servers are monitored, state transition (Unknow to normal/abnormal) took a long time. Starting with this version, this process has been optimized, so that there is minimal-to-no time lag in state transitions.
- **Scalability of Dashboards in now Improved:** In previous versions, where a single dashboard displayed information pertaining to numerous components, the dashboard was found to load slowly. Starting with this version, the dashboards have been optimized, so that it can scale to handle any number of components.
- **Updating Configuration File Changes Made Faster:** By default, whenever a configuration file was changed in the eG manager, the eG agents downloaded the updated configuration file. In previous versions, in environments where the configuration files were modified frequently and where thousands of agents had to download the updated configuration file, the eG agents had to wait endlessly to update their configuration files and then proceed with their routine tasks. Due to this, the resource consumption of the eG manager increased, many blocked threads were noticed and hence slowness was noticed on the eG manager. To ensure that the update process of the configuration files is faster, eG Enterprise v7.2 has made significant improvements in processing the configuration files. The updates to the configuration files are cached in the JVM of the eG manager. The eG agents obtain the updated configuration files from the JVM as a background process while other data processing can be carried out in the foreground. This improvement to the configuration file processing greatly enhances the file processing speed and hence averts slowness of the eG manager.

18. Conclusion

As you can see, eG Enterprise v7.2 includes a wealth of new capabilities and improvements to existing monitoring capabilities. The goal of these enhancements is to provide customers with all the key capabilities they need as they look to modernize their IT infrastructures and IT operations.

It is easier than ever before to test drive eG Enterprise. To start a no hassle, quick trial, just connect to https://www.eginnovations.com/it-monitoring/free-trial