eG Innovations

Release Notes for eG Enterprise v7.2.8

Table of Contents

Release Notes for eG Enterprise v7.2.8

Version 7.2.8 is a minor release of eG Enterprise. While this release predominantly has bug fixes, 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.

The eG Manager and eG Agent upgrade packages are available for both Microsoft Windows and Linux operating systems. Note that you will need to install the eG Manager for v7.2.4 and then upgrade to v7.2.8 or you can directly upgrade your eG Manager from v7.2.4.1 to v7.2.8. Also, you can upgrade your eG Agent from v7.2.4/v7.2.6 to v7.2.8.

Before upgrading the eG manager to v7.2.8, make sure that the eG manager is of version 7.2.4. If the eG manager that is in use in your environment is of a version lower than eG 7.2.4, please contact support@eginnovations.com to obtain a prior upgrade.

Note:

To upgrade to v7.2.8, it would suffice if the eG manager is of v7.2.4. You do not have to upgrade to v7.2.4.1 or apply the 'April 2023' update patch on top of v7.2.4.

1.1 Monitoring Enhancements

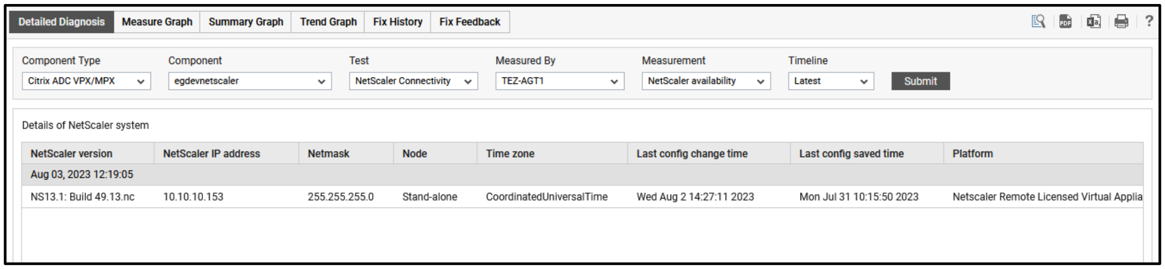
1.1.1 Citrix Monitoring Enhancements

- **Track User Logins to NetScaler appliance through RDP Connections:** Starting with this version, you can configure the **NetScaler Sessions** test (mapped to the NetScaler VPX/MPX appliance) to monitor the user sessions initiated using RDP connection, in addition to the user sessions initiated using ICA, DLTS ICA, VPN and AAA connections. To turn on this capability of the test, you should set the **Show RDP Session** flag of the test to **Yes**. By default, this flag is set to **No**. By enabling this capability, you will be able to capture the pattern with which user sessions were initiated through RDP connections to the target NetScaler appliance and identify deviations in those patterns, if any.

- **Citrix NetScaler events can now be Monitored:** NetScaler devices are capable of sending SNMP traps when abnormal conditions are encountered. eG Enterprise v7.2.8 includes a **NetScaler Traps** test using which remote agents can capture traps from NetScaler devices and report them in the eG Enterprise console.

- **Tracking Citrix NetScaler Configuration:** NetScaler vulnerabilities are common these days and IT admins often need to know what version of NetScaler they are running. Starting with this version, details such as the IP address of NetScaler, the NetScaler version, the last connection time etc., are made readily available to users in the detailed diagnosis of the *NetScaler availability* measure of the **NetScaler Connectivity** test. Earlier, this information was available only in the eG Configuration

Management module.



Component Type: Citrix ADC VPX/MPX
Component: egdevnetscaler
Test: NetScaler Connectivity
Measured By: TEZ-AGT1
Measurement: NetScaler availability
Timeline: Latest

Details of NetScaler system

NetScaler version	NetScaler IP address	Netmask	Node	Time zone	Last config change time	Last config saved time	Platform
Aug 03, 2023 12:19:05							
NS13.1: Build 49.13.nc	10.10.10.153	255.255.255.0	Stand-alone	CoordinatedUniversalTime	Wed Aug 2 14:27:11 2023	Mon Jul 31 10:15:50 2023	Netscaler Remote Licensed Virtual Applia

Figure 1: The detailed diagnosis of the NetScaler availability measure

- **Identifying FSLogix Profile Containers that are Configured with Cloud Cache:** In previous versions, in some environments, eG Enterprise raised false alerts stating that the FSLogix profile containers were not attached to the users. This issue was noticed only on the profile containers on which Cloud Cache was configured. To suppress such false alerts, eG Enterprise v7.2.8 offers the flexibility to identify the FSLogix profile containers on which the Cloud Cache is configured. This helps administrators identify those users who have logged on to the Citrix Virtual Apps/desktops or Microsoft Azure Virtual Desktops using an FSLogix profile container that is configured with Cloud Cache.

- **Ability to Track Citrix User Sessions Initiated using Rendezvous Protocol:** The Rendezvous protocol allows a VDA to bypass the Citrix Cloud Connectors to connect directly and securely with the Citrix Cloud control plane. While Rendezvous protocol version 1 supports bypassing the Citrix Cloud Connectors for HDX session traffic alone, the Rendezvous protocol version 2 supports bypassing the Citrix Cloud Connectors for both control plane traffic and HDX session traffic. eG Enterprise v7.2.8 is capable of capturing the user sessions initiated using Rendezvous protocol. To this effect, additional columns (Rendezvous protocol and Session Info) have been included in the detailed diagnosis of the Citrix Sessions and the HDX Channel from Desktop tests. The Session topology of the User Experience dashboard also reveals if the user had initiated his/her session through Rendezvous protocol.

1.1.2 Synthetic Monitoring Enhancements

- **OKTA Integration Support for AWS AppStream Logon Simulator**: In previous versions, AWS AppStream logon simulator did not support simulation in environments where the target Amazon AppStream was integrated with OKTA MFA mechanism (single sign-on system). Starting with this version, AWS AppStream logon simulator will perform simulation and report metrics if the target Amazon AppStream is integrated with OKTA authentication mechanism.

- **Microsoft AVD Logon Simulator updated for latest Azure portal changes:** Recent changes in the Azure web portal meant that the Microsoft AVD Logon Simulator did not work correctly. Starting with this version, the Microsoft AVD Logon Simulator has been modified to support the latest Azure portal changes.

- **AWS WorkSpaces Logon Simulator now supports the latest Amazon WorkSpaces portal changes:** Recent changes in the AWS web portal meant that the AWS WorkSpaces Logon Simulator did not work correctly. Starting with this version, the AWS WorkSpaces Logon Simulator has been modified to support the latest AWS portal changes.

- **Identifying Scripts that are not Running/Initiating during Web App Simulation:** Previously, in some environments where the Web App Simulation component simulated multiple scripts, eG Enterprise failed to capture those scripts that were not running during simulation and eventually did not generate alerts for the same. This issue was noticed only in environments where the Google Chrome browser failed to launch due to various reasons such as Chrome driver compatibility issues, failure of Chrome driver to create chrome process, etc. Starting with this version, eG Enterprise reports an additional *Is script running?* measure for the **Total** descriptor of the **Simulated Web Transactions** Test. This measure promptly alerts administrators whenever a script is not running/not initiated during simulation process.

1.1.3 Endpoints Monitoring Enhancements

- **Monitoring Microsoft Azure Intune:** Microsoft Intune is a cloud-based unified endpoint management platform that empowers IT to manage, assess, and protect apps and devices from one console. Intune provides a comprehensive set of features including device management, application management, information protection, and more. If the endpoint is non-compliant or is error-prone, it will affect the experience of the user accessing the infrastructure from the endpoint. At the same time, from an administrator's point of view, lack of visibility into such endpoints may hinder troubleshooting. Administrators often spend hours troubleshooting in the datacenter when the real issue is on the endpoint. Therefore, proactive monitoring of endpoints managed using Microsoft Intune can help IT administrators take preemptive action to improve user experience to a great extent. eG Enterprise v7.2.8 monitors Microsoft Azure Intune and reports its availability and responsiveness. The endpoints/devices managed by Microsoft Azure Intune are monitored and segregated based on their operating systems i.e., Android iOS, MacOS, Windows mobile etc. In the process, the devices/endpoints that are error-prone, non-compliant and are in grace period are identified. The devices/endpoints that are company owned and those that are personal devices can be isolated with ease. The Intune Certificate Connectors are closely monitored and the connectors that are inactive are identified. The Android device Enrollment profiles are monitored and the profile on which maximum android devices are enrolled is identified. The validity of each Intune Device certificate is periodically monitored and the certificates that had already expired and those that are about to expire are isolated.
- **Support for IGEL OS 12 and COSMOS** is now included in eG Enterprise. A new eG VM agent and deployment procedure is available for IGEL OS 12.

1.1.4 Database Monitoring Enhancements

- **Monitoring Redis OSS Cluster:** Redis Cluster is a distributed implementation of the Redis data store that allows data to be shared across multiple Redis nodes. In a Redis Cluster, data is partitioned across multiple Redis nodes, so that each node only holds a portion of the total data set. If any node is unavailable over the network or fails during the replication process, then it can affect the stability of the clustered environment, which in turn will lead to poor user experience. To ensure the operational efficiency of the nodes in the cluster, administrators need to keep a close watch on the health of the nodes in the cluster. eG Enterprise v7.2.8 monitors the Redis Cluster using an external agent and offers insights into its availability and responsiveness. In the process, the nodes added to and removed from the cluster can be determined with ease. Each node in the cluster is monitored and the availability and responsiveness of the node is reported. The role of each node is determined, and the replication status of each node is reported along with the count of slave nodes attached to the cluster. Administrators can also determine the amount of data that is yet to synced with the slave nodes and the time lag noticed in the transport of logs during replication. In the process, administrators can figure out if the data on the slave node is in sync with the primary/master at all times.
- **Enhanced Monitoring Visibility into MySQL/MongoDB Clusters:** Starting with this version, eG Enterprise offers a bird's eye view into the overall performance of the MySQL/MongoDB Clusters. By monitoring the MySQL/MongoDB Clusters, eG Enterprise provides in-depth insights into the availability and responsiveness of the clusters. The health of each node in the cluster is monitored and interconnectivity issues on the nodes are brought to light. The sessions/connections on each node are monitored and load balancing issues on the nodes are detected. The status of each node

is reported and the nodes that are error-prone/unreachable/offline are pinpointed. The health of the replication activity between the nodes is determined by analyzing the transaction errors on each node. Alerts are sent out if any time lag is noticed between the primary node and the replica node while the data is being synced. Using these monitoring models offered by eG Enterprise, administrators can easily traverse from the clusters to the individual nodes in the cluster to troubleshoot and perform root cause analysis of critical issues.

- **Improvements to SSL-enabled Oracle Cluster/MYSQL/MongoDB Database Server Monitoring:** In previous versions, eG Enterprise did not support monitoring the Oracle Cluster/MYSQL/MongoDB database servers if the servers were SSL enabled using valid signed certificates. Starting with this version, if the target Oracle Cluster/MongoDB/MySQL database servers are SSL-enabled using signed certificates from a valid certificate authority, the eG agent uses the certificate to establish an SSL connection with the target database servers and collects the required metrics. To this effect, additional parameters have been added to the tests pertaining to the Oracle Cluster/MongoDB/MYSQL database server components. Likewise, starting with this version, a custom test of **SQL Query** type can be created using **Integration Console** capability for **MYSQL** database servers that are SSL-enabled using valid signed certificates.

- **Enhancements to Oracle Cluster Monitoring:** eG Enterprise's Oracle Cluster monitoring has been significantly enhanced in v7.2.8. eG Enterprise now reveals the total number of database instances in an Oracle Cluster enabled with DataGuard feature and further reveals the count of database instances that are in primary, physical standby, logical standby and snapshot standby modes. Administrators are also promptly alerted to the mode using which maximum number of database instances/nodes were opened in the Oracle Cluster - is it the read write mode? or read only mode? or read only with apply mode? or mounted mode? The dead processes/sessions on each database node in the cluster are discovered and the time duration for which each process/session was dead is ascertained. Single block and Multi block I/O request processing to each file on each database node is closely monitored and the files that are experiencing I/O latencies are isolated. The query/request processing ability of each node in the cluster is monitored and the nodes that are experiencing processing bottlenecks are identified. The temporary files on each node are monitored and the temporary files that are experiencing read/write latencies are ascertained with ease. The nodes that are experiencing frequent rollbacks are swiftly ascertained and reported. User activity on each node is promptly monitored and the node with frequent user account lockouts and user session login failures is identified.

- **Enhancements to MySQL Monitoring:** With v7.2.8, eG Enterprise's MySQL Database server monitoring capabilities have been significantly enhanced to report a slew of metrics relating to I/O intensive tables, indexes and files. Each I/O intensive file/table/index is monitored and the file/index/table that is experiencing slowness due to read and write latencies are identified. The tables/Indexes that are experiencing high latencies while insert, delete, fetch, and update operations are also promptly identified and isolated. eG Enterprise v7.2.8 also clearly alerts administrators on whether/not the monitored MySQL Database server is deployed in a cluster setup.

- **Processes and Unix Services test associated with Oracle Database:** In older versions, the **Processes** and **Unix Services** tests were not associated to the Oracle Database servers installed on Linux operating systems but were associated with all other applications/servers that were installed on a Linux operating system. Starting with this version, the **Processes** and **Unix Services** tests on Linux are associated to the Oracle Database servers out of the box.

1.1.5 Enhancements to Monitoring Messaging Servers

- **Enhancements to Solace Message Broker Monitoring:** In previous versions, eG Enterprise monitored a Solace environment by integrating with a Solace PubSub+ Monitor Collector. A PubSub+ Monitor collector was a centralized collector for all events from individual Solace event brokers. Events aggregated by the Solace PubSub+ Monitor Collector are sent to an eG remote agent through one of the Solace brokers. A consolidated Solace Collector model in eG Enterprise then provided insights into the workloads of all the individual Solace event brokers. The challenges with this model included the large amount of event data exported to the eG remote agent, lack of availability insights about the individual brokers and several single points of failure.

To overcome these limitations, eG Enterprise now uses a pull-based monitoring approach, using SEMP API calls to track the performance of individual Solace PubSub+ Event Brokers and the Solace clusters.

- **Monitoring Solace PubSub+ Event Brokers:** Availability and responsiveness of Solace brokers is tracked, so any outage can be detected immediately. Using an agentless approach (SEMP APIs), 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 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 Primary Virtual Routers and Backup Virtual Routers in a redundant setup are periodically checked for issues in fail-over/load balancing abnormalities.
- **Monitoring Solace Cluster:** Now, eG Enterprise also monitors Solace Clusters. The count of nodes in the cluster is reported along with the count of nodes with TCP port connectivity, SEMP port connectivity and network connectivity. The primary and secondary node in the cluster is identified and the node with recent state change (from primary to mate and vice versa) is deduced. The configuration and redundancy status of each node is periodically monitored, the state change is captured and a slew of hardware and software component status such as Message spool status, Power module status, Disk status, database build status etc are reported.

1.1.6 Web Server Monitoring Enhancements

- **PHP Business Transactions Test associated with Nginx Servers:** In older versions, the **PHP Business Transactions** test was not associated with the Nginx Server. Starting with this version, this test is associated to the Nginx Server component out of the box.

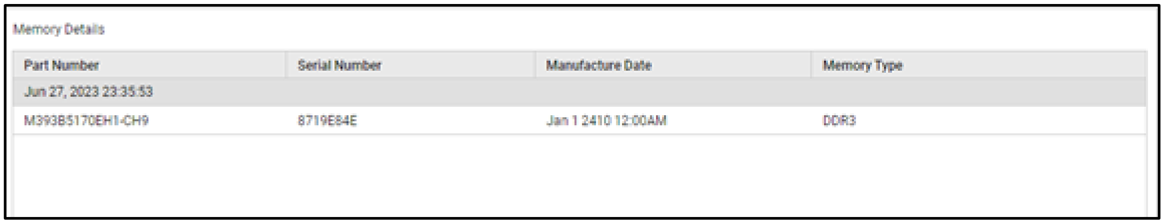
1.1.7 Network Monitoring Enhancements

- **Trap Tests are now associated with SNMP Generic Servers:** In previous versions, administrators could not associate the Network Traps and Application Traps tests with the SNMP Generic component. Starting with this version, out of the box support is provided to associate these tests to the SNMP Generic component.

1.1.8 Hardware Monitoring Enhancements

- **Improved Hardware Monitoring using Integrated Management Module:** Starting with this version, configuration metrics related to the memory module and power supply units of the target IBM Server such as Part number, FRU number, Manufacture date, Memory type, etc. are offered as part of detailed diagnostics. This would be helpful for administrators in environments where eG

Configuration Management capability is not enabled.



Memory Details

Part Number	Serial Number	Manufacture Date	Memory Type
Jun 27, 2023 23:35:53			
M393B5170EH1-CH9	8719E84E	Jan 1 2410 12:00AM	DDR3

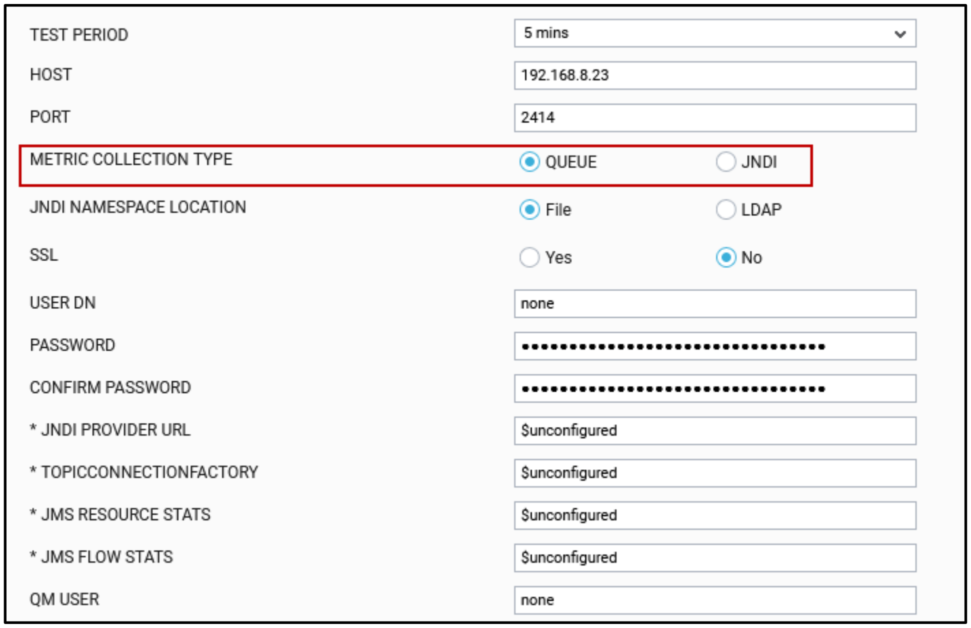
Figure 2: The detailed diagnosis of the Status measure of the IBM – IMM Memory Module test

1.1.9 Unified Communications Monitoring Enhancements

- **Ability to Identify Unresolved/Active Service Incidents on Zoom:** Often, service incidents affect the delivery of Zoom services. These incidents, when noticed at the right time, can be resolved within a short duration. However, a few incidents are more serious and may take a longer time to be resolved, leading to service outages. Administrators therefore wanted to proactively identify those incidents that are active on Zoom so that they can ascertain the time needed to resolve the incidents and alert users of any impending outage issues. To help administrators in this regard, eG Enterprise v7.2.8 reports the count of active incidents and resolved incidents on Zoom. The detailed diagnostics further points administrators to the exact incidents that were resolved and those incidents that are currently active on Zoom.

1.1.10 Application Middleware Monitoring Enhancements

- **Support to Monitor IBM Integration Bus Using Queue Manager:** In previous versions, to monitor the IBM Integration Bus, administrators used the JNDI approach wherein, they had to manually create a JMS Administered Object with a Connection factory and two JMS Destinations. The JMS Destinations stored the messages published by the IIB; the eG agent subscribed to those messages from the JMS Destinations and collected the required metrics for monitoring. In recent times, IBM Integration Bus has released multiple versions with higher security features. The traditional JNDI approach could not be used to collect metrics from such versions of IBM Integration Bus. To ensure that metrics are collected and reported for the IBM Integration Bus that supports enhanced security features, eG Enterprise offers to monitor the target IBM Integration Bus using IBM WebSphere MQ Queue Manager. In this approach, administrators are required to create a queue on the Queue Manager and a subscription. The eG agent uses the subscription to subscribe to the topic, collects the metrics/messages from the topic and adds them to the destination i.e., the created queue. To this effect, an additional **Metric Collection Type** flag has been included in the test configuration page where administrators can choose either the Queue method or the traditional JNDI approach using which they wish to collect the metrics from the target IBM Integration Bus.



TEST PERIOD	5 mins	
HOST	192.168.8.23	
PORT	2414	
METRIC COLLECTION TYPE	● QUEUE	○ JNDI
JNDI NAMESPACE LOCATION	● File	○ LDAP
SSL	○ Yes	● No
USER DN	none	
PASSWORD	••••••••••••••••••••••••••••••••	
CONFIRM PASSWORD	••••••••••••••••••••••••••••••••	
* JNDI PROVIDER URL	$unconfigured	
* TOPICCONNECTIONFACTORY	$unconfigured	
* JMS RESOURCE STATS	$unconfigured	
* JMS FLOW STATS	$unconfigured	
QM USER	none	

Figure 3: Choosing the Method based on which the eG agent collects metrics from IBM Integration Bus

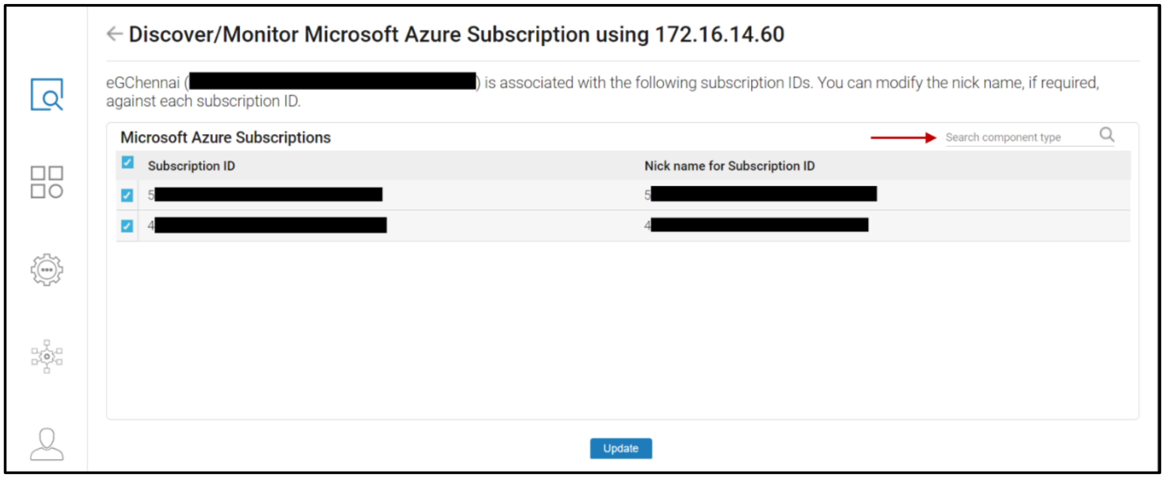
1.1.11 Storage Monitoring Enhancements

- **Monitoring HP MSA 2060 FC Storage system:** The HPE MSA 2060 Storage is a flash-ready hybrid storage system designed to deliver affordable application acceleration for small and remote office deployments. eG Enterprise v7.2.8 provides monitoring support to HP MSA 2060 FC Storage system using the existing *HP P2000 SAN* monitoring model. By default, eG Enterprise uses *MD5* authentication algorithm to monitor HP P2000 SAN Storage system. However, to monitor HP MSA 2060 FC Storage system, administrators are required to choose *SHA256* as the authentication algorithm from the **Authentication Type** list in the test configuration page while configuring the tests.

1.2 Usability Enhancements

1.2.1 Admin Interface

- **Ability to search for one/more Discovered Microsoft Azure Subscriptions:** In previous versions, in environments where hundreds of Microsoft Azure Subscriptions were discovered for a Tenant ID, administrators had to painstakingly scroll the entire page to locate an Azure subscription that they wish to manage. To ease the pain of such administrators, starting with this version, a **Search** option has been introduced in the **Discover/Monitor Microsoft Azure Subscriptions** page. Administrators can search for their desired subscription by specifying the whole/partial subscription in the **Search** text box.



← Discover/Monitor Microsoft Azure Subscription using 172.16.14.60

eGChennai ([redacted]) is associated with the following subscription IDs. You can modify the nick name, if required, against each subscription ID.

Microsoft Azure Subscriptions

Search component type

☑ Subscription ID	Nick name for Subscription ID
☑ [redacted]	[redacted]
☑ [redacted]	[redacted]

Figure 4: Searching a Microsoft Azure subscription from a list of discovered subscriptions

1.2.2 Monitor Interface

- **Improvements to AVD Infrastructure Dashboard:** In previous versions, the AVD Infrastructure dashboard helped administrators receive an overview of the performance of the Microsoft Azure virtual desktops in the AVD Infrastructure. Many administrators, however, wanted to view the performance of the Microsoft Azure virtual desktops that are associated with individual Microsoft AVD Brokers using the AVD Infrastructure dashboard. To aid the request of such administrators, starting with this version, a **Broker** list box has been included in the AVD Infrastructure Dashboard.

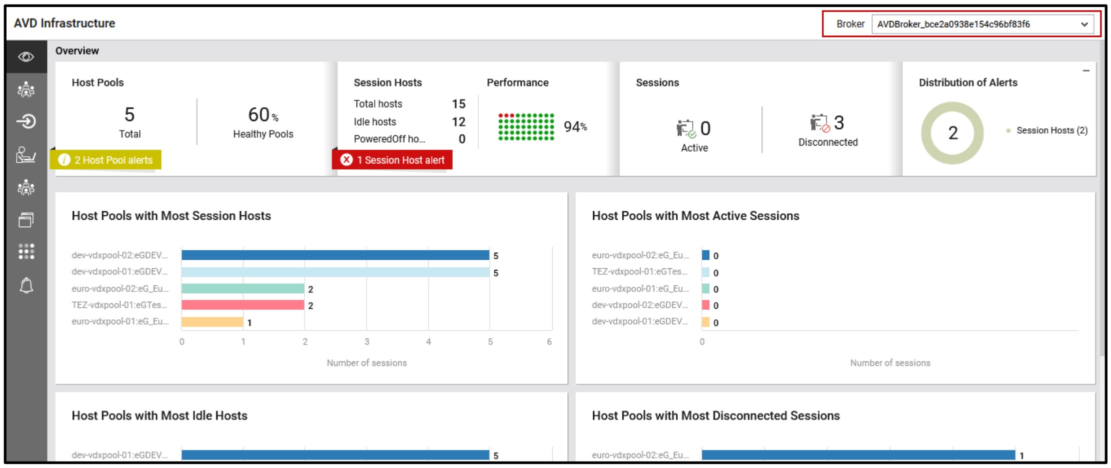

AVD Infrastructure
Broker
AVDBroker_bce2a0938e154c96bf83f6
Overview
Host Pools
5
Total
60%
Healthy Pools
2 Host Pool alerts
Session Hosts
Total hosts 15
Idle hosts 12
PoweredOff ho... 0
1 Session Host alert
Performance
94%
Sessions
0
Active
3
Disconnected
Distribution of Alerts
2
Session Hosts (2)
Host Pools with Most Session Hosts
dev-vdxpool-02:eGDEV... 5
dev-vdxpool-01:eGDEV... 5
euro-vdxpool-02:eG_Eu... 2
TEZ-vdxpool-01:eGTes... 2
euro-vdxpool-01:eG_Eu... 1
0 1 2 3 4 5 6
Number of sessions
Host Pools with Most Active Sessions
euro-vdxpool-02:eG_Eu... 0
TEZ-vdxpool-01:eGTes... 0
euro-vdxpool-01:eG_Eu... 0
dev-vdxpool-02:eGDEV... 0
dev-vdxpool-01:eGDEV... 0
0
Number of sessions
Host Pools with Most Idle Hosts
dev-vdxpool-01:eGDEV... 5
Host Pools with Most Disconnected Sessions
euro-vdxpool-02:eG_Eu... 1

Figure 5: The AVD Infrastructure dashboard for each Microsoft AVD Broker

1.3 Integration Enhancements

- **Last Measure Value is now included in WebHook Integration:** Starting with this version, the eG manager can be configured to send the last measure value in alerts routed to third-party trouble ticketing systems that accept incoming webhooks. To enable this capability, the **showLastMeasureValue** and **isEventBasedTroubleTicketingEnabled** flags under the **[TT_INTEGRATION]** section of the **eg_services.ini** file (available in the **<eG_INSTALL_DIR>/manager/config** folder) should be first set to **Yes**. Once this is done, you can configure the event payload to be fed into the Trouble Ticketing system with the last measure value.

- **Support to Include Host IP/Name with ServiceNow/SNOW ITOM Integration:** By default, alerts sent to ServiceNow/SNOW ITOM include the nick name of the problem component in the **Node** field. From this version however, administrators have the option of sending alerts with Host IP/Name of the problem component, instead of its nick name. This change will help IT staff quickly identify the problematic component. To override the default setting therefore, set the **node** parameter to **hostname** in the **[TT_INTEGRATION_SNOW_ITOM]** section of the **eg_services.ini** and **eg_ttconfig.ini** files that are available in the **<eG_INSTALL_DIR>/manager/config** folder.

1.4 Other Enhancements

- **Support to Integrate the eG Manager with an SMS Gateway that uses HTTP Post Method and is Behind a Proxy Server:** In previous versions, eG Enterprise offered the users the capability to configure the eG manager to send SMS alerts to mobile phones using a HTTP-based SMS Gateway. In some environments, however, the SMS alerts were not received by the users when,

  - the SMS Gateway was behind a Proxy server.
  - the SMS Gateway used the HTTP Post method.

  To support administrators of such environments in sending SMS alerts successfully, starting with this version, eG Enterprise offers to send SMS alerts from an SMS Gateway using HTTP Post method as well as from an SMS Gateway that is behind a proxy server. For this purpose, administrators should manually configure a set of entries that are available under the **[HTTP_POST_SMS_ALERTS]** section of the **eg_services.ini** file available in the **<eG_INSTALL_DIR>/manager/config** folder.

Bug Fixes/Optimizations for the eG Manager

2.1 Admin Interface

- Earlier, the **Last Restarted Time** for an agent was wrongly displayed in the **AGENT INFORMATION** page (that appears when you click the IP/nickname of the agent listed in the **AGENT - STATUS** page). This issue has been fixed now.
- In previous versions, in some environments, an aggregate component created by grouping the **Citrix Virtual Apps 7.x**, **Citrix StoreFront**, and **Citrix Delivery Controller 7.x** component types failed to report metrics. This issue has been fixed now.
- In previous versions, when **.NET BTM**, **.NETCOREBTM** options were chosen from the **Log File Directory** list of the **AGENT -LOGS** page, the logs were not displayed. This was because the logs were searched in the wrong directory path. Starting with this version, this page will display log entries correctly. If the **.NETBTM** option is chosen, then the page will display entries from the *eG_dotNetBTM* log file located in the **<OS_INSTALL_DIR>/ProgramData/eGurkha/agent/Logs** folder. Likewise, if the **.NETBTM** option is chosen, then the page will display entries from the **eG_dotNetCoreBTM** file located in the **<OS_INSTALL_DIR>/ProgramData/eGurkha/agent/Logs eG_dotNetCoreBTM** folder.
- Earlier, in a SaaS deployment of eG Enterprise, if the Host IP/Name of the discovered

server/component ended with a hyphen, then, eG Enterprise failed to automatically create an external or remote agent (as the case may be) corresponding to the Host IP/Name. To seamlessly monitor those discovered components whose Host IP/Name ended with a hyphen, starting with this version, eG Enterprise allows to create a corresponding external/remote agent that ends with a hyphen.

- Previously, in a SaaS deployment of eG Enterprise, sometimes, users were unable to add components of two different component types with same nick name. This issue has been fixed now.
- In older versions, in some environments, the eG manager failed to automatically delete components that did not report metrics for a configured duration, even if it was explicitly configured to do so. This issue has been fixed now.
- In prior versions, in environments where auto-discovery was enabled, remote agents added with the Host IP/Name of the auto-discovered containers (Docker, Podman and Container Engine) remained even after the corresponding container components were auto-deleted. This caused unnecessary license consumption. To avoid this, starting from this version, the remote agents automatically added will be automatically deleted when the corresponding components are deleted.
- Earlier, in environments where Concurrent/Named user licensing was enabled, the license consumption by the **Physical Desktop Group** component was not displayed in the **LICENSE INFORMATION** page. This issue has been fixed now.
- In older versions, the eG layer model page failed to display the measurement unit for the metrics reported by the tests that were added using the Integration Console (IC). This issue has been fixed now.
- In previous versions, the **NAMED USERS/MACHINES REPORT** and **CONCURRENT USERS REPORT** pages were empty even when concurrent/named user licenses were consumed in the target environment. This issue was noticed only in the environments where the eG manager was upgraded. This issue has now been fixed.
- Earlier, in environments where hundreds of SNMP traps were configured with priorities using the **Trap Priority** page (that appears upon selecting the **Trap Priority** option under the **SNMP Traps** node in the **Alerts** menu of the **Admin** interface), the **Trap Priority** page took long to load. This page has now been optimized to load quickly.
- In previous versions, users were unable to reconfigure the **AWS Service Usage by Region** test mapped to the **AWS Region** component type using the **Specific Test Configuration** page. This issue has been fixed now.
- Earlier, whenever a user was created by associating specific alarm priorities (i.e., by choosing one/more options against the **Alarm display** field in the **Monitor** section of the **User Preferences** page), the default settings of the **Alarm display** field could not be overridden. This is not the case any longer.
- In previous versions, in environments where users were auto associated with multiple component types (that contained hundreds of components), the **ADMIN AUDITLOG REPORTS** could not be generated for the **Element Association** activity of the **User Management** module. This issue was noticed whenever the eG manager was restarted in the target environment. This issue has been fixed now.
- Previously, administrators were unable to disassociate the components of a specific component type assigned to a particular user, using the **Elements Association** page. This was noticed only for those component types that were added to the **Auto associate component types** list of the said user. To resolve this issue, starting from this version, the **Component Type** list in the **Elements Association** page will not include those component types that are in the **Auto associate component types list** of a user.
- In previous versions, when a domain user attempted to login with the correct password soon after

entering an incorrect password, he/she was not allowed to login. This was because, eG Enterprise incorrectly locked the user account soon after the first failed attempt. This is not the case any longer.

- In older versions, in some environments where multiple VMware VDI components managed by one or more VMware vCenters were being monitored, applying a specific test configuration across VDI components using the **Apply to Other Components** button in the **Specific Test Configuration** page did not work as expected. This issue has been fixed now.
- In older versions, where eG manager integrated with **SNOW ITOM**, trouble tickets could not be automatically created in **SNOW ITOM** for certain alerts sent by the eG manager. This issue was noticed only in environments where the eG manager was in a redundant setup. Also, trouble tickets could not be created only for those components that were managed in eG using their FQDN. This issue has been fixed now.
- Previously, administrators faced issues while configuring the mail server for sending email alerts using the **MAIL SERVER SETTINGS** page. This happened because the validation check was not completed within the configured timeout period. To avoid this issue, timeout for validating the configuration settings has been increased in this release.
- Earlier, in environments where the eG manager and the users were in different time zones, email alerts were sent based on the time zone in which the eG manager was operating instead of users' time zone. This issue has been fixed now.
- In previous versions, sometimes, administrators could not create maintenance policies for those descriptors with names containing the equal to (=) symbol. This is not the case any longer.
- In previous versions, administrators could not modify the **Asset Management** settings if a chosen Component Type had outstanding alerts. However, administrators of some environments wanted to modify the settings even if the component was in critical/major/minor state. To enable this capability, starting from this release, a new flag **StateCheckNeededForAssetUpdate** has been introduced under the **[MISC_ARGS]** section of the **eg_services.ini** file (in the <EG_INSTALL_DIR>\manager\config directory). Setting this flag to **No** will enable the administrators to modify the **Asset Management** settings even if the component has outstanding alerts to be resolved.
- Earlier, in the eG manager redundant setup, the Asset Management configuration in the primary manager was not transferred to the secondary manager. This is not the case any longer.
- In previous versions, administrators were unable to configure the tests pertaining to the **Microsoft SQL Azure** component using the **Specific Test Configuration** page. This issue was noticed only when Fully Qualified Domain Name (FQDN) of a monitor user specified against the **USER** parameter contained a special character (@). This is not the case any longer.
- In older versions, administrators were unable to configure the **O365 Mail Sender** test mapped to the **O365 Mail Sender** component. This issue occurred only when the **Password Profile** was set for the O365 Mail Sender component. This issue has been fixed now.
- Previously, memory spikes were noticed on the eG manager when the auto-discovered components were being auto-deleted (this can be enabled by selecting **Delete** against the **What action you would like to take?** List in the **COMMON SETTINGS - AUTO UNMANAGE/DELETE** page). This led the eG manager to crash unexpectedly. Starting from this version, auto-delete process has been optimized to consume less memory while auto-deleting the discovered components.
- Prior to v7.2.8, if the security filter was enabled (the **Enable Security Filters** option was set to **Yes** in the **SECURITY FILTERS** page) for the eG manager, administrators were unable to generate **SQL Query** test using the **Integration Console**. This was because the SQL query contained special characters (braces). This is no longer the case.
- In previous versions, in environments where metric aggregation was enabled, aggregated metrics were not reported for the *Summary* descriptor of the **System Details – OS** test. Starting from this

version, eG Enterprise can report aggregated metrics for the *Summary* descriptor also.

- In previous versions, in environments where a user is not configured to receive Mail Alerts i.e., the Mail Server Settings were not configured for the user, the error log of the eG manager was unnecessarily dumped with messages stating that the Mail Manager was not running. This issue has been fixed now.
- In older versions, in environments where eG agent discovery was enabled, the eG agent failed to auto-discover the **Citrix Cloud Connectors** through the **Citrix Cloud Control Plane** component. This was because the file path specified against the **SECURE CLIENT FILE PATH** parameter contained space in it. This issue has been addressed now.
- Earlier, eG Enterprise could not discover the location of Citrix/VDI users whose logins were authenticated by an Active Directory server. This issue has been fixed now.
- Earlier, the test names listed under the **Tests excluded from the alerts** box in the **MAIL/SMS ALERTS FILTERING** page were duplicated. This issue has been fixed now.
- In older versions, in Linux environments where the eG manager was SSL-enabled, users were not able to retrieve zone details through eG CLI. This issue has been addressed in this version.
- Previously, users were unable to execute commands through eG CLI. This issue was noticed only when the user account used to create the manager profile was authenticated via LDAP. This issue has been fixed now.
- In prior versions, sometimes, when administrators tried to retrieve the detailed diagnostics for a specific test descriptor using eG REST API, the descriptors of the chosen test were not available for selection in the list box in the **REST API CLIENT** page. This issue was noticed only when the chosen component was added for monitoring without port configuration. This issue has been fixed in this release.
- By default, eG Enterprise does not store the password of the users belonging to a domain / domain group. In previous versions, if such users executed the REST API commands using the **REST API Client** capability, then, they failed to receive valid API responses. This was because, the users could not be validated against the domain / domain group to which they belonged to when the REST API commands were executed. Starting with this version, to validate such users and obtain valid API responses for the commands executed by such users, a Password text box has been introduced in the **REST API Client** page. Upon specifying the password, the users will be authenticated against the domain / domain group to which they belong, and then valid API responses will be returned.
- Earlier, API responses were not returned from the **REST API Client** for the users who used the Switch over functionality offered by eG Enterprise to login as a domain group (instead of a user belonging to a domain group) from the eG administrative interface. This was because, by default, eG Enterprise does not execute the API commands from the REST API Client without valid user credentials. Therefore, starting with this version, the REST API Client capability will be disabled for the users who use the **Switch over** functionality to login as a domain group.

2.2 Monitor Interface

- In older versions, in environments where the Physical Desktop Group component type was being monitored, the **Remote Control** icon (upon clicking this icon, users can execute certain commands and perform actions remotely) was wrongly displayed for a login user to whom the Remote Control feature was not enabled. This issue has been fixed now.
- In previous versions, the **Component Topology** page (that appears upon selecting the **Virtual Components** option from the Host/Applications menu in the Monitor interface) for the Docker Host component did not display the Docker containers available in the target Docker host. This issue has

been fixed now.

- In older versions, tests mapped to the **Amazon Cloud Desktop Group** component could not discover the names of AppStream users and display them as descriptors in the eG monitoring console. This issue was noticed in environments where PowerShell script execution / Command Prompt execution was blocked. To avoid this, the eG agent has been re-engineered in this version to discover AppStream usernames by reading registry variables, and not by executing PowerShell scripts.
- In versions prior to v7.2.8, though valid metrics were reported by the tests mapped to a **Citrix Virtual Apps 7.x** component, no measures were displayed in any of the widgets of the **At-A-Glance** tab page in the **Applications** dashboard of that component when the **Subsystem** was chosen as *Citrix Users*. This happened because inactive users were displayed in the Citrix Users tree. Starting from this version, to avoid this issue, this page has been optimized to list only the current and active Citrix users.
- Prior to v7.2.8, in VDI environments where thousands of applications were being monitored, all the applications were not displayed in the **Applications** dashboard. This occurred due to the pagination issues in the dashboard. In addition, the total number of applications was wrongly displayed in dashboard. This issue has been fixed now.
- In older versions, when the **Subsytem** was chosen as **Overview**, the **System** dashboard of the Physical Desktop Group component failed to load the **Top CPU Consuming Processes/Top Memory Consuming Processes/Top Processes By I/O Activity** widgets. This issue has been fixed now.
- Prior to v7.2.8, when the **Subsystem** was chosen as **Outside View of VMs** in the **Virtual** dashboard for VMware vSphere VDI component, a few widgets in that dashboard were empty. This occurred only when the tests associated with those widgets were not reporting metrics. Starting with this version, if the tests are not reporting metrics, the corresponding widgets will be automatically removed from the dashboard.
- Previously, in environments where **Physical Desktop Group** components were being monitored, the **Performance Metrics for Desktops/Users** dashboard did not feature the desktops without active users. Starting from this version, this dashboard has been optimized to display the details of the desktops without active users.
- In older versions, HTTP bad request error was reported when a user drilled down to view the component group from the **Topology** tab page of the **Service Dashboard**. This issue was noticed only when the user with **OrgAdmin** role logged into the eG manager. This issue has been fixed now.
- In prior versions, in environments where multiple tests that reported metrics for thousands of descriptors were mapped to a layer of target component, the eG layer model page took too long to load and also did not notify users that their request was being processed. Starting from this version, this page has now been optimized to indicate the users that their request to access the layer model page is being processed if the page is taking time to load the content.
- In older versions, the **Session Start-up Details** section in **LOGON DETAILS FOR USER** page (that appears upon clicking the **Logon Details** icon in the layer model page) failed to load for the **User Logon Performance - Cloud** test of the **Citrix Cloud Control Plane** component. This has been fixed now.
- In older versions, when administrators searched for a user using the **Global Search** capability, it took too long to render the results. This issue has been fixed.
- Earlier, in the eG layer model page, users did not have an option to view the name of the AVD Host Pool to which the target session host belonged to. Starting from this version, eG Enterprise displays the name of the host pool to which the session host belongs to in the layer model page.
- In earlier versions, when there were thousands of Amazon Cloud Desktops being monitored, the **User Experience Overview** dashboard was slow to load. Starting with this release, the dashboard

has been optimized to load faster.

- In previous versions, the **Session Topology** section of the **User Experience Dashboard**, failed to display the Citrix Cloud Control Plane and Citrix Cloud Connector components, even though these components were managed and were part of the target Citrix Cloud environment. This issue has been addressed in this version.
- In older versions, the **Browser Activity** widget in the **USER EXPERIENCE DASHBOARD** for an AVD user failed to display metrics related to browser activity, though the corresponding test was reporting valid metrics. This issue has been fixed now.
- Previously, the **Session Topology** section of the **USER EXPERIENCE DASHBOARD** failed to display the **Microsoft AVD Broker** thorough which the users accessed the Azure Virtual Desktop infrastructure. This issue has been fixed now.
- In older versions, where an **Amazon Cloud Desktop Group** component was monitored, the **Protocol Latency** section of the **USER EXPERIENCE DASHBOARD** did not display any metrics for the desktop group users. This issue was noticed only if the NICE DCV protocol was being used in the environment. This is not the case any longer.
- In prior versions, the **LOGON TIME BREAKDOWN** widget of the **USER EXPERIENCE DASHBOARD** showed incorrect logon time for a user. This issue was noticed only when the user logged into multiple desktops in the environment. This issue has been fixed in this release.
- In earlier versions, alignment issues were noticed in the **Session Topology** section of the **USER EXPERIENCE DASHBOARD**. This issue has been addressed in this release.
- Earlier, the **LOGON TIME BREAKDOWN** panel pf the **USER EXPERIENCE DASHBOARD** for an AVD user failed to load. This has been fixed now.
- In previous versions, the state of the Microsoft AVD Broker was wrongly displayed in the **Session Topology** of a user in the **USER EXPERIENCE DAHSBOARD**. This issue has been fixed now.
- Earlier, in Amazon Cloud Desktop environments, when a user viewed his/her user experience in the User Experience Dashboard, the **LOGON TIME BREAKDOWN** panel in the **USER EXPERIENCE DASHBOARD** reported metrics in an inconsistent manner. This issue has been resolved now.
- In previous versions, in the Amazon Cloud Desktop environments, the **User Experience Overview** dashboard failed to display the logon duration for desktop users. This has been addressed in this release.
- In earlier versions, when there were there were many Citrix users being monitored, the **USER EXPERIENCE DASHBOARD** took too long to load. Starting with this release, the dashboard has been optimized to load faster.
- Earlier, when users drilled down to the eG layer model page of the Citrix Cloud Control Plane component from the **SESSION INFO** section of the **USER EXPERIENCE DASHBOARD**, users directed to the layer model page of incorrect component instead of the chosen component. This happened in environments where the Citrix Cloud Control Plane was monitored using its Fully Qualified Domain Name (FQDN). This issue has been fixed now.
- In earlier versions, the **APPLICATION PERFORMANCE STATISTICS** window (that appears upon clicking the icon provided adjacent to **Applications** in the **Session Topology** page of the **USER EXPERIENCE DASHBOARD**) wrongly displayed the measurement unit of the **MEMORY USAGE** column in the **Application Usage - Memory** widget. This issue has been fixed now.
- In prior versions, users were unable to sort the Session Hosts and Unique Users columns of the Performance dashboard of AVD Host Pool dashboard. This issue has been fixed now.
- Earlier, when a user downloaded the Performance dashboard of AVD Session Hosts in Host as a PDF file, the Downloading prompt (showing the file downloading progress) did not disappear soon after

PDF download was completed. This issue has been fixed now.

- Prior to v7.2.8, users were unable to drill down by clicking the **Servers in Unknown state** legend from the **Virtual App Server Health** widget of the **Virtual Apps** dashboard. This issue has been resolved now.
- In older versions, when the **Web App Simulation** option was chosen from the **Simulations** drop-down, the **SYNTHETIC MONITORING** dashboard was empty even though valid data was available in the eG backend database. This issue has been fixed now.
- In older versions, the hyphens were displayed for the **Client Session Simulation** components in *Unknown* state in the **Synthetic Monitoring** dashboard. This issue was noticed when the user drilled down from the Home page of the Monitor interface. This issue has been fixed now.
- In prior versions, inconsistencies were noticed in displaying the component name in the Performance Metrics view for the IGEL Endpoint components. This issue was noticed when users drilled down from the Home page of the Monitor interface. This issue has been fixed now.
- Previously, the measures displayed in the widgets of the **My Dashboard** disappeared when the measures turned to "*Unknown*" state. Starting with this version, you can make sure that measures continue to appear in the **My Dashboard**, even after the state of the measures turns to *Unknown*. For this, you have to set the **DisplayUnknownMeasures** flag in the **[DASHBOARD_SETTINGS]** section of the **eg_customdashboard.ini** file ((in the <EG_INSTALL_DIR>\manager\config directory)) to *Yes*.
- In previous versions, in the **NetFlow** dashboard for the **Fortigate Firewall/WiFi Controller** (that was NetFlow-enabled), the graphs failed to load in the **Protocols**, **Top Sources**, **Top Destinations** and **Top Conversations** tab pages. Starting from this version, this dashboard has been optimized to address this issue.
- Earlier, the **Incident Management** dashboard did not display the event IDs of alarms raised in the target environment. However, administrators of some environments wanted to know the event IDs for which the alarms were raised. To cater to the needs of such administrators, starting with this version, a new flag **eventIdEnabled** has been introduced in the **[MISC_ARGS]** section of the **eg_services.ini** file (in the <EG_INSTALL_DIR>\manager\config directory). The administrators need to set this flag to **yes** to view the event IDs in the **Incident Management** dashboard.
- In older versions, it was noticed that the **Incident Management** dashboard was not auto refreshed at regular intervals. Starting from this version, this dashboard will automatically refresh at configured intervals.
- Prior to v7.2.8, by default, options to acknowledge and delete alarms were provided in the **Metrics** tab page of the **Incident Management** dashboard even if the privileges for acknowledging and deleting the alarms were not configured for a user. Starting from this version, the Acknowledge and Delete options will be provided in the **Metrics** tab page while displaying the current alarms only if the user has privileges to do so.
- In older versions, when the **All Alarms with Correlation** option was chosen from the **Show** drop down, the **Alarms** tab page of the **Incident Management** dashboard failed to load search results. This happened only when the users searched the alarms using the details of child alarms such as alarm ID, component type, component name, description, and start time. Starting from this version, the search capability of the **Alarms** page has now been optimized to render a result set even if the users use details of child alarms.
- In earlier versions, when a user deleted an alert raised for an event listed in the **Metrics** tab page of the **Incident Management** dashboard, other alerts associated for the same event were also deleted in the process. This issue has now been fixed.
- Previously, if an alarm was acknowledged, the **CURRENT ALARMS / UNKNOWNS** window did not feature the information on alarm acknowledgment such as user who acknowledged the alarm, time

and details of alarm acknowledgment and zones to which the components for which the alarms were raised. Starting with this version, **CURRENT ALARMS / UNKNOWNS** is optimized to show the above-mentioned details.

- In previous versions, when a user tried to view all the alarms by clicking the **Show Alarms** button, the **History of Alarms** page wrongly showed a result set obtained for a keyword searched using the **Description Search** box. This issue has been fixed now.
- In older versions, Normal email alerts sent after an issue was resolved were not sent to all the users who were configured to receive them. This issue was noticed only when a few descriptors were excluded from the email alerts. This issue has been fixed now.
- Prior to v7.2.8, a few OIDs associated with the received traps were not translated properly and displayed in the detailed diagnostics reported for the **Network Traps** test. This issue was noticed when the uploaded MIB file was invalid. This issue has been fixed now.
- Earlier, the **More Infos** window (that appears upon clicking the encircled plus icon adjacent to a test in the layer model page) wrongly displayed the state of a descriptor. This issue has been fixed now.
- Previously, when a test in the eG layer model contained thousands of descriptors, then the **More Infos** pop up window took too long to load to all the descriptors of a test. Starting from this release, pagination has been introduced to optimize load time of the **More Infos** window.
- In older versions, the detailed diagnostics reported for the Root blockers measure of the SQL Blocker Processes test mapped to the Microsoft SQL component failed to display the details of queries being issued by the root blocker processes to block other processes running in the target component. This issue has been fixed in this version.
- Earlier, JVM CPU spikes were noticed on the eG manager when a user accessed the **Measures** page upon selecting the **Measures** option from the **Miscellaneous** tile. This page has now been optimized to minimize CPU usage.
- In older versions, the email alerts were not sent to the users who were configured to receive them. This was noticed only in environments where the **Show last measure value in the mail alerts** flag in the **MAIL/SMS ALERT CONFIGURATION** section of the **MAIL/SMS ALERT PREFERENCES** page (that appears when you follow Admin->Alerts->Mail Settings->Alert Settings menu sequence) was set to **Yes**. This issue has been fixed now.
- In prior versions, it was noticed that a bar representing first month data was always empty when the **Summary** graph was plotted to show month-wise trend. This issue has been fixed now.
- Prior to v7.2.8, the *Trap details* column of the detailed diagnosis reported for the **Number of messages** measure of the **Network Traps** test was in unreadable format. This column has now been optimized to show trap details in a tabular format.
- Earlier, false alerts were generated for a few descriptors of the **WebSphere MQ Queue Details** test. Such false alerts were generated only in environments where global threshold was applied for the test and default threshold settings were applied for a descriptor pattern of the test. Also, the name of the descriptors matched either exactly or partially with the descriptor pattern. Starting with this version, in such environments, the thresholds set for the descriptors will take precedence over the thresholds set for the descriptor and hence, such false alerts will be suppressed.

2.3 Reporter Interface

- Earlier, the **Virtualization Manager - Cluster Details** report could not be generated for the **Nutanix Prism Central** component type. This is no longer the case.
- In older versions, when building a custom report for the eG Manager component using the **Config**

Report Template window, users were unable to add a widget to display the detailed diagnosis reported by the **eG Registered Users** test of that component. This issue has been fixed now.

- In previous versions, when administrators drilled down to a session initiated by a user in the generated **Cloud Desktops - Sessions by Users** report, a few graphs wrongly displayed the protocol using which the user initiated the session to the Cloud Desktops brokered by VMware Horizon/Nutanix AHV. This issue has been fixed now.
- Previously, in environments where NTLMv2-enabled Microsoft SQL server was used as the eG backend database, the **Applications - Users by Application** report for the **Citrix Virtual Apps** component type could not be generated even though valid metrics were available in the backend database. This issue has been fixed now.
- By default, the **Virtual Applications and Desktops – Overview** report can be generated for the virtual applications/desktops based on the hypervisor that was used to provision those virtual applications/desktops. In previous versions, in some environments where Citrix Hypervisors alone were used to provision the virtual applications/desktops, the **Brokered by** list in the More Options window wrongly displayed an **Others** option too. If administrators chose to generate the report by choosing the **Others** option, empty reports were generated. Starting with this version, the Brokered by list will be visible only in environments where different hypervisors (Citrix/VMware Horizon/Nutanix AHV) are used to provision the virtual applications/desktops.
- Previously, in environments where hundreds of virtual components were monitored, slowness was observed while generating the **Virtua**l **Machines – VM Sprawl** report when all the components were chosen for generating the report from the **Component** list. This report has now been optimized to load faster.
- In prior versions, in double-byte enabled virtual environments, when the **Users – Slow Logons** report was generated for Microsoft AVD Host Pools, the **Pool Name** column in the generated report displayed junk/unwanted characters instead of displaying valid pool names. This issue has been fixed now.
- Earlier, in environments where Microsoft Azure Virtual Desktops were monitored, incorrect values were reported in the **% TIME IN USE** column of the generated **Applications - Top Applications** report. This issue has been fixed now.
- Prior to v7.2.8, in environments where Amazon Cloud Desktops were monitored, the **Sessions by Users** report could not be generated when *Inside view* option was chosen from the **Resource Details from** list box. This issue has been fixed view.
- In older versions, administrators could not drill down to view the user logon duration, session duration, logon time breakdown, etc. from the generated **Sessions - Sessions by Users** report if the report was generated for Amazon Cloud Desktop Group component. This was because, the **Details** icon that was used to drill down was not included in the generated report. This issue has been fixed now.
- Earlier, when an **Uptime / Downtime Analysis** report was generated for a Linux server, the **DOWNTIME** and **%DOWNTIME** columns in the generated report displayed hyphens (-) instead of valid downtime. This issue has been fixed now.
- In prior versions, in environments where Microsoft Azure Virtual Desktops were monitored, clicking the graph icon against a user from the generated **Applications – Billing** report resulted in an empty page. This issue has been fixed now.
- In previous versions, in environments where hundreds of Microsoft Azure Virtual Desktops were monitored, the following bugs were noticed when the **Host Performance** report (Azure Virtual

Desktop -> By Session Host -> Host Performance) was generated:

- the title of the generated report was wrongly displayed as **Application Performance** report.
- A few graphs in the generated report displayed "No measures available" message. However, users were able to view the graphs by expanding the graphs. This issue was noticed only when the report was generated when multiple sessions hosts were chosen from the **Session Host** list. Also, the report was slow to load.

These issues have been fixed now.

- In older versions, when a **Service Level Analysis - By Component** report was generated, if an administrator drilled down to the **Event History** page by clicking the layers from the **Top 5 Events** or **Event Summary** sections, he/she was unable to view the entire description of an event provided in the **DESCRIPTION** column. Starting with this version, administrators can hover over the description to view entire description.
- In older versions, the **Applications – Billing** report could not be generated for virtual desktop infrastructure component types. This is not the case any longer.
- Previously, in a SaaS deployment of eG Enterprise where Microsoft Azure Virtual Desktops were monitored, the **SESSION HOST** column in the generated **Sessions by Hosts** report wrongly displayed the session host to which the user belonged to. This issue has been fixed now.
- In earlier versions, in environments where Microsoft Azure Virtual Desktops were monitored, empty pages were returned when administrators drilled down a few columns such as **CPU UTIL**, **MEMORY UTIL**, **IO READS** and **IO WRITES** columns from the generated **Session by Users** report (Azure Virtual Desktop -> By Session Host - > Sessions). This issue was noticed only when the duration of the user session was less than 5 minutes. This issue has been fixed now.
- Previously, when the **Sessions by Users** report was generated for Cloud Desktops, hyphens were noticed in the **PHYSICAL CPU UTILIZATION** and **MEMORY UTILIZED** columns of the generated report. This issue has been fixed now.

2.4 Manager Operations

- Earlier, frequent eG manager restarts were noticed in the environment. This was because the eG manager tried to fetch new connections from the database connection pool instead of reusing the available connections to process the requests. The eG manager has now been optimized to avoid such issues.
- In prior versions, email alerts for all open alarms were not sent to users who were configured to receive them even when the **Type of Notification** flag in the **USER PROFILE** page was set to **Complete** and the **Send separate mails for each alert** flag in the **MAIL/SMS ALERT PREFERENCES** page was set to **No**. This issue has been fixed now.
- In previous versions, in redundant eG manager configurations, sometimes, file transfer between the primary and secondary managers stuck abruptly. This issue was noticed only when the primary manager tried to transfer the unused/empty files to the secondary manager. As a result, the managers were not synchronized with each other. To avoid this, starting with this version, data transfer between the managers in a redundant setup has been optimized to ignore the unused/empty file during data transfer.
- In older versions, sometimes, slowness was noticed on the eG manager/agent host. This happened when command/script execution on the eG manager/agent stuck or did not complete within timeout

period. This has been fixed in this release.

Bug Fixes/Optimizations to the eG Agent

3.1 Citrix Monitoring

- In older versions, the **Citrix Teams Status** test mapped to the **Citrix Virtual Apps 7.x** component reported incorrect value for the *Microsoft Teams optimization* status measure. This is not the case any longer.
- In previous versions, the **Sever OS Machines** test mapped to the **Citrix Virtual App/Desktop Site 7.x** component wrongly reported the registration state for the server OS machines even when the machines were powered off. Starting from this version, the **Server OS Machines** test is optimized to report the registration state only for the machines that are powered on.
- In older versions, sometimes, the **User Logon Performance** test mapped to the Citrix Cloud Control Plane component failed to report metrics. This issue was noticed in environments where thousands of users tried to access the Citrix Cloud. This issue has been fixed now.
- Prior to v7.2.8, the **CVAD License Usage - Cloud** test mapped to the Citrix Cloud Control Plane component reported incorrect values/zero for the metrics. This issue has been fixed now.
- Earlier, the **PVS Availability** test mapped to the Citrix Provisioning Server component reported an incorrect value for the *Response time* measure. This is not the case any longer.
- Previously, in some environments, the tests mapped to the **Citrix Cloud Connector** and **Citrix Cloud Control Plane** components failed to report metrics. This was because the valid SSL certificates of Citrix Cloud were not downloaded to the <EG_INSTALL_DIR>/jre/lib/security folder. Starting from this version, eG Enterprise can automatically download the valid certificates to the specified folder when an exception is thrown due to unavailability of the certificates.

3.2 Virtual Desktop Monitoring

- In older versions, the presence of multiple blocked threads caused the eG remote agent monitoring **VMware vSphere VDI** component to consume the JVM's CPU resources abnormally. This issue has been fixed now.

3.3 Virtualization Monitoring

- In previous versions, issues were noticed where eG agents used VMware vCenter to automatically discover vSphere servers. In some environments, discovery failed because the vSphere API was unable to retrieve the IP address of the vSphere servers. In some other environments, the eG agents could not auto-discover the correct host names of the vSphere servers, owing to improper DNS server configuration. To avoid these issues, going forward, the eG agent will, by default, auto-discover vSphere servers using the server names configured in vCenter, and not using host names as was done previously.
- Previously, in large environments where the target VMware vCenter was managing hundreds of VMware vSphere ESX servers, the **ESX Servers** test failed to report metrics. This test has now been

optimized to collect and report performance metrics rapidly, even in large environments.

- Earlier, false alerts were generated for the **Replication Details** test mapped to the **VMware Horizon Connection Server** component that was a part of the VMware Horizon Cluster/Pod. This issue has been fixed now.

3.4 Endpoints Monitoring

- In older versions, the false alerts were generated for the *ISP packet loss* measure of the **Client Network Performance** test mapped to the **Physical Desktop Group** component. This issue has been fixed now.
- Previously, the **Client Network Performance** test associated with the **Physical Desktop Group**, **IGEL Endpoints** and **Client Desktop** displayed incorrect values for the *Wi-Fi signal strength* and *Wi-Fi signal quality* measures when the target component was connected to the LAN network. This issue has been fixed.
- Earlier, the **Endpoint Performance – IGEL** test mapped to the **IGEL Endpoints** component failed to report metrics. This has been fixed now.
- In previous versions, the **System Details - IGEL** test mapped to the IGEL Endpoints component wrongly reported CPU and memory usage of every processor supported by each IGEL Endpoint. Due to which large volume of space consumption was noticed on the eG backend database. To avoid this, starting from this version, this test is optimized to report metrics only for *Summary* descriptor.
- Earlier, in some environments, detailed diagnostics was not reported for the tests mapped to the **IGEL Endpoints** component. This issue has now been fixed.

3.5 Cloud Monitoring

Microsoft Azure Subscription

- Previously, in environments where Microsoft Azure components such as **Microsoft Azure Subscription** and **Microsoft AD Connect** were monitored, sudden spikes were noticed in the CPU usage of the eG remote agent monitoring these components. This led to a lot of threads being blocked, causing the remote agent to stop metrics collection. This issue has been fixed now.
- In previous versions, the **Azure Billing By Services - Current Month** and the **Azure Billing Details - Current Month** tests mapped to the **Microsoft Azure Subscription** component failed to report metrics. This issue has been fixed now.
- In older versions, sometimes, the tests mapped to the **Microsoft Azure Subscription** component did not report metrics. This was because the eG agent failed to properly handle Azure access token it used to connect to the target subscription. This issue has been fixed now.
- In older versions, CPU spikes were noticed on the target **Microsoft Azure Subscription** when the **Azure Storage Details** test was executed. The test has now been optimized to consume minimal CPU while execution.
- Previously, false alerts were generated for the *Storage account service availability* measure reported by the **Azure Storage Details** test mapped to the **Microsoft Azure Subscription** component. Such alerts are no longer issued.

Microsoft Azure Active Directory

- In prior versions, sometimes, the **Azure Non Interactive Sign-ins** test mapped to the **Microsoft**

Azure Active Directory component failed to report metrics. This issue has been fixed now.

AWS Cloud

- Earlier, the **AWS WorkSpaces - Directory** test pertaining to the **AWS Cloud** component reported an incorrect value for the *Session latency*. This issue has been fixed now.
- In older versions, the **AWS WorkSpaces Details** test mapped to the **AWS Cloud** component failed to report values for the *Sessions with high latency* measure. This was because of incorrect calculation. This is not the case any longer.
- Prior to v7.2.8, the **AWS Simple Email Service (SES)** test mapped to the **AWS Cloud** component failed to report metrics for a few descriptors (regions). This issue has been fixed now.
- In previous versions, the detailed diagnostics reported for the *Estimated monthly savings* measure of the **AWS Trusted Advisor** test mapped to the **AWS Cloud** component was incomplete. This issue has been fixed now.

Cisco Intersight

- Earlier, the tests mapped to the Cisco Intersight component did not report metrics when the eG agent communicated with the Cisco Intersight via a Proxy server. This is not the case any longer.

3.6 Business Transactions Monitoring and Real User Monitoring

- In older versions, sometimes, the **Resource Details** page failed to display the details of resources downloaded while processing a request. This happened if the request's URL contained disallowed special characters (for example, white space and hash (#)). This issue has been fixed now.
- Earlier, wrong timestamps (date/time) were displayed in the detailed diagnostics reported by the tests mapped to the **Real User Monitor** component. This issue has been fixed now.
- In previous versions, the **Error Details** page of the **RUM Topology** reported an empty page. This issue has now been fixed.
- In previous versions, in RUM-enabled environments where Googlebot was enabled on the browser, sudden spikes were noticed in the value of the *Recent messages* measure of the **eG Manager Error Log** test mapped to the **eG Manager** component. This issue was noticed only for the error descriptor where Googlebot included the same information such as browser activity, as part of Google Analytics for same error for every measure period resulting in the accumulation of messages. This issue has been fixed now.
- In prior versions, the transaction URLs (descriptors) were wrongly displayed with all segments without considering the value specified against the **MAX URL SEGMENTS** parameter. This was noticed only when the **Java Business Transactions** test reported values for the metrics related to stalled transactions. This is not the case any longer.
- In prior versions, high CPU spikes were noticed on the eG agent host when the **Java Business Transactions** test was executed. This was because a large volume of data was processed in the background to report detailed diagnostics. This issue has been resolved in this version.
- In older versions, the **Cross-Application Transaction Flow** of the **eG Java Business Transaction Monitor** failed to capture the database to which the database queries were sent. This issue was noticed only in environments where the target application used a combination of ColdFusion and JDBC driver to initiate SQL calls to the database. This issue has been fixed now.
- Earlier, in a SaaS deployment of eG Enterprise, administrators were wrongly allowed to add a Real

User Monitor component without a valid RUM collector. This issue has been fixed now.

- Previously, in environments where the Microsoft SQL database was used as the eG backend database, performance metrics were not reported for BTM-enabled servers (e.g., Oracle WebLogic server). The queries executed to fetch the metrics have been optimized to avoid such issues.

3.7 PHP Transaction Monitoring

- In earlier versions, the detailed diagnosis of the *Healthy transactions* measure of the **PHP Business Transactions** test was reported even if the detailed diagnosis capability was disabled by default. This issue has been fixed now.

3.8 Synthetic Monitoring

- Earlier, in some environments where logon simulation/web app simulation was performed, cache files created by the Chrome driver while initiating the simulation were not cleared by the Chrome driver when the simulation was complete. As a result, the storage space depleted drastically on the host where the logon simulator/web app simulator agent was installed. To ensure that the storage space is not hogged by such cache files, starting with this version, the logon/web app simulator agent is directed to clear the cache files soon after a simulation is complete.

3.9 Java Monitoring

- In older versions, sometimes, the **JVM Threads** test mapped to the **Tomcat** component failed to report metrics. This issue was noticed only when the target component was being monitored by a user with '*monitorRole'* privileges. This issue has been fixed now.

3.10 Web Server Monitoring

- Earlier, the *SSL Certificate Validity* measure of the **SSL Certificate** test mapped to a web server component type reported the number of days in decimal values. Starting with this version, you can configure this test to report values for this measure in whole numbers and not decimal values. For this purpose, a new **REPORT DECIMAL** flag has been introduced for this test. By default, this flag is set to *Yes. To display values in whole numbers, set this flag to No.*

3.11 Unified Communications Monitoring

Microsoft Teams

- In prior versions, in some Microsoft O365 environments where Modern Authentication was enabled, the **Audio Streams**, **Call Summary**, **Feedback Summary**, **Network Quality Summary**, **VBSS Streams** and **Video Streams** tests mapped to the **Microsoft Teams** component failed to report metrics for a few tenants. This issue was reported only when a trial tenant was used to monitor the target environment. This issue has been fixed now.

Microsoft Exchange Online

- Earlier, high CPU spikes were noticed when the **Transport Rule Hits** test mapped to the Microsoft Exchange Online component was executed. This test has now been optimized to consume less CPU.

Zoom

- Earlier, the **End Time** column reported as part of the detailed diagnostics of the *Scheduled Maintenance* measure reported by the **Service Status** test (pertaining to **Zoom** component type) displayed the date in a wrong format i.e., instead of DD/MM/YYYY, the date was displayed as

MM/DD/YYYY. This issue has been fixed now.

3.12 DevOps

- Earlier, in some environments, the tests mapped to the **Jenkins** component did not report metrics. This issue was noticed only when the target Jenkins component was deployed in the Linux environment. This issue has been fixed now.

3.13 Microsoft Windows and Unix Server Monitoring

- In previous versions, when the **File/Folder Modification Checks** test mapped to **the Microsoft Windows** component was executed with the **FILES TO BE MONITORED** parameter set to *none*, then the test continuously reported that zero files/folders were modified. Starting with this version, this test will not report metrics if the **Files to be Monitored** parameter is set to *none*.

- In older versions, the **Root/System Folders Checks** test (of the **Microsoft Windows** component) generated multiple alerts on the *New files added to root/system folders* measure, if the eG agent executing the test was installed within a root/system folder. To suppress such alerts, starting with this version, the test will automatically ignore the eG agent install directory, if it is within the root/system folder.

- In prior versions, in some environments, the **Application Event Log** test failed to report metrics. This issue has been fixed now.

- Earlier, the **Windows Security Center Status** test mapped to the **Microsoft Windows** component wrongly reported product status as the real-time protection status for all descriptors. Starting with this version, the real-time protection status will be reported only for the Windows Defender (descriptor), whereas the product status will be reported for other descriptors.

- Previously, the **Failover Cluster Services/Applications** test mapped to **the Microsoft Windows Cluster Node** component failed to report metrics. This issue was noticed only in environments where more than one external agent was used to monitor the target component. This issue has been fixed now.

3.14 SAP Monitoring

- Earlier, the tests mapped to the **SAP Basis** layer of the **SAP ABAP Instance** component failed to report metrics. This issue has been fixed now.

3.15 Database Monitoring

- In previous versions, the **PostgreSQL Locks** and **PostgreSQL Connections** tests of the **PostgreSQL** component type did not report metrics. This happened only if the target PostgreSQL component was upgraded to its latest version. This issue has been fixed now.

- In earlier versions, the **Oracle RAC Temp Tablespaces** test mapped to the **Oracle Cluster** component reported an incorrect value for the *Free percentage* measure. This issue has been fixed now.

- Prior to version 7.2.8, connection leaks were observed in environments where the **MongoDB** component was being monitored. In this version, the connection leak is no longer observed.

- In older versions, the eG agent that monitored the **Microsoft SQL** component ran the query used to obtain execution plans (to be displayed in the detailed diagnostics of the **SQL Blocker Processes** test) for a long time. This was because the query attempted to obtain execution plans of all processes running on the target component instead of processes that were identified as root blocker processes.

This was leading to unnecessary resource consumption. Starting from this version, the query executed to obtain execution plans is optimized to obtain the execution plans of root blocking processes alone.

3.16 Storage Monitoring

- Earlier, the tests pertaining to the **HPE StoreOnce Backup** component did not report metrics, if the eG agent monitoring that component was deployed on a remote Linux host. This issue has been fixed now.
- In previous versions, if an eG remote agent monitoring **EMC Unity** was monitored, the detailed diagnostics of the **System Details** test (mapped to the eG Agent component) reported the credentials of the user that the eG agent used to execute the *UEMcli* on **EMC Unity** to collect the required metrics. This was considered as a security violation by administrators of some environments. To avoid displaying the credentials of the user when *UEMcli* was executed, starting with this version, administrators have an option to save the credentials of the user who has privilege to access the EMC Unity storage system on the remote host on which the eG agent monitoring the **EMC Unity** is installed. To this effect, a **USE SAVEUSER OPTION** flag has been introduced in the test configuration page of EMC Unity. Administrators can set this flag to *Yes* if they wish to save the credentials of the user on the remote host where the eG agent is installed rather than providing the same in the test configuration page. In this case, administrators need to specify the **USER**, **PASSWORD** and **CONFIRM PASSWORD** parameters as *none* in the test configuration page. By default, this flag is set to *No*.

3.17 Network Elements Monitoring

- In prior versions, the **Solace Queues** test mapped to the **Solace Collector** component type did not report values for the *Time since the earliest message has been queued* measure. This issue has been fixed now.
- Earlier, in some environments, false alerts were generated for the *Packet loss* measure reported by the **Network** test mapped to the **Cisco Router** component. This issue has been fixed now.

3.18 Self-Monitoring of eG Agent/eG Manager

- Previously, the tests mapped to the **JVM** layer of the **eG Agent** component stopped reporting metrics after the target eG Agent was upgraded. This issue has been fixed now.
- Earlier, the **eG Database Cleanup** test mapped to the eG Manager component reported wrong value for the *Cleanup status* measure. This issue was noticed even when the cleanup process was running without any issues. This issue has been fixed now.
- In older versions, the **Email/SMS Alerting** test mapped to the eG Manager component reported incorrect values for the *SMS messages sent* measure. This issue has been fixed now.
- Previously, the **eG Cluster** test mapped to the eG Manager component wrongly reported zero values for the **Files stored for the other manager** and **Data stored for the other manager** measures. This happened even when the files to be transferred to the secondary manager from the primary manager were empty. This issue has been fixed now.

Bug Fixes/Optimizations Made to the

eG VM Agent

The following issues noticed on the eG VM agent on the Linux host have been fixed in this release:

- In older versions, the eG VM agent on a Linux host consumed 100 percent of CPU resources whenever metrics were collected from the target component. This issue has been fixed now.
- Previously, high CPU spikes were noticed on the Linux host on which the eG VM agent was installed. This is not the case any longer.
- Earlier, the *In connection rate* and *Out connection rate* metrics reported by the **TCP – OS** test frequently turned to "*Unknown*" state. This issue was noticed only in environments where the eG VM agent on the Linux host was used to monitor a target component. This is no longer the case.

  In prior versions, in environments where the eG VM agent on the Linux host was used to monitor a target component, the **TCP Traffic - OS** test failed to report metrics consistently. This issue has been fixed now.

Other Big Fixes/Optimizations

5.1 eG Super Manager

- In previous versions, administrators were unable to restrict certain users from accessing the SuperManager. However, administrators of some environments wanted to restrict user access to the eG SuperManager. To achieve this, administrators need to specify a comma-separated list of users against the **Usernames** parameter available in the **[<ManagerID>]** of the **eg_smusers.ini** file in the **<SuperManager_Installed_Dir>/manager/config** folder. Here, **ManagerID** is the IP address of the manager that is configured in the SuperManager.
- In prior versions, in some environments, when the eG SuperManager was upgraded to the latest version, users were unable to access the eG SuperManager using the eG Mobile application. This is not the case any longer.

5.2 eG Mobile Application

- Earlier, when tests contained multiple descriptors, the eG Mobile Application displayed an empty page instead of showing the complete list of descriptors. This issue was noticed even when the descriptors were displayed in the layer model page of the eG manager. This issue has been fixed now.

5.3 Database Optimization

- In previous versions, in environments where database partitioning was enabled for the eG backend database, the cleanup process failed. This happened only when multiple schemas were used for the eG backend database. This issue has been fixed now.
- In older versions, connections between the eG manager and the backend database became invalid frequently. To avoid this, starting from this version, eG Enterprise offers a capability (if enabled) that validates every database connection maintained in the connection pool before giving them to the manager. This capability can be enabled by setting the **Connection_ValidCheck** flag in the **[DB_PROPERTIES]** section of the **eG_DB.ini** (in the <EG_INSTALL_DIR>\manager\config

directory) to yes.

- Earlier, sometimes, the cleanup operation performed on the eG backend database failed. This occurred because the query procedure used to perform cleanup operation was not handled properly. The query procedure has now been optimized to avoid cleanup failures.

5.4 eG SCOM

- In previous versions, in environments where the eG manager was integrated with Microsoft SCOM, when a user tried to launch the eG manager console from the Microsoft SCOM console, the eG login page appeared instead of the eG layer model page. This issue has been fixed now.
- Earlier, in environments where the eG manager was integrated with Microsoft SCOM, the alarms that were acknowledged/removed in the Microsoft SCOM console did not reflect in the eG manager console. This was because the eG manager failed to validate the password of the user. This issue has been fixed now.

5.5 Security

- Earlier, users were allowed to upload files in the file format that were not relevant to the pages that supported file upload. For example, users were allowed to upload a file of MP3 format while uploading bulk component data. Starting with this version, the security of the eG manager has been tightened while unauthorized file uploads have been prevented.
- Starting from this version, in order to tighten the security of the manager and prevent malicious attacks from unauthorized sources, JavaScript library (jQuery) files used by the eG manager have been updated to the latest version.
- Earlier, in some environments, HTTP Header security vulnerabilities were noticed in the eG RUM Collector. Starting with this version, the **eG RUM Collector** has been optimized to prevent such vulnerabilities.
- Previously, deserialization vulnerability was detected during eG manager agent communication when basic validation of the eG agent was performed. This issue has been fixed now.