



Release Notes for eG Enterprise v7

TABLE OF CONTENTS

| | |
|--|-----------|
| INTRODUCING EG ENTERPRISE V7 | 1 |
| 1. EG ENTERPRISE V7: THE TOTAL USER EXPERIENCE MONITORING AND MANAGEMENT SOLUTION | 1 |
| 2. SUMMARY OF NEW CAPABILITIES IN EG ENTERPRISE V7 | 2 |
| 3. DIGITAL WORKSPACE MONITORING | 3 |
| 3.1 Citrix Workspace Monitoring Enhancements | 3 |
| 3.1.1 Citrix Logon Simulator | 3 |
| 3.1.2 Client Session Simulation | 6 |
| 3.1.3 Citrix Delivery Controllers..... | 7 |
| 3.1.4 Enhancements to Citrix Cloud Site Monitoring | 8 |
| 3.1.5 Enhancements to Citrix XenApp Servers Monitoring | 9 |
| 3.1.6 Enhancements to Monitoring the Citrix StoreFront | 9 |
| 3.1.7 Enhancements to Citrix NetScaler Monitoring..... | 10 |
| 3.1.8 Enhancements to Citrix License Server Monitoring..... | 11 |
| 3.1.9 Other Citrix Monitoring Enhancements | 11 |
| 3.1.10 Citrix Reporting Enhancements | 17 |
| 3.1.11 Reports pertaining to Citrix Delivery Controllers: | 19 |
| 3.2 VMware Horizon Monitoring Enhancements | 27 |
| 3.2.1 VMware Horizon Logon Simulator..... | 27 |
| 3.2.2 VMware Horizon Monitoring Enhancements | 28 |
| 3.2.3 Enhancements to VMware Identity Manager Monitoring | 30 |
| 3.2.4 VMware Reporting Enhancements..... | 30 |
| 4. WEB APPLICATION PERFORMANCE MONITORING | 36 |
| 4.1 Synthetic Monitoring Capability for Web Applications..... | 36 |
| 4.2 Real User Monitoring Enhancements..... | 40 |
| 4.3 Enhancements to Business Transaction Monitor..... | 48 |
| 4.4 Deeper Visibility of the JAVA Virtual Machine (JVM) | 54 |
| 5. ENTERPRISE APPLICATION MONITORING | 60 |
| 5.1 Enhancements for SAP Monitoring | 60 |
| 5.2 Enhancements to Office 365 Monitoring | 64 |
| 5.3 Reporter Enhancements for Exchange Online..... | 69 |
| 5.4 Reporter Enhancements for Microsoft Office 365 | 74 |
| 5.5 Reporter Enhancements for Microsoft SharePoint Online | 77 |
| 5.6 Additional Monitoring Support for SaaS Applications | 82 |

| | |
|---|------------|
| 6. EXTENDED MONITORING REACH TO SUPPORT NEW IT INFRASTRUCTURE COMPONENTS .. | 82 |
| 6.1 Network Monitoring Enhancements | 83 |
| 6.2 Database Monitoring Enhancements | 86 |
| 6.3 Storage Monitoring Enhancements | 90 |
| 6.4 Cloud Monitoring Enhancements | 91 |
| 6.5 DevOps Monitoring Enhancements | 92 |
| 6.6 Other Monitoring Enhancements | 93 |
| 6.7 Monitoring Container Environments | 97 |
| 7. ENHANCEMENTS FOR INCREASED AUTOMATION, SIMPLICITY, SCALABILITY AND SECURITY | 98 |
| 7.1 SaaS Enhancements | 98 |
| 7.2 Architecture Enhancements | 103 |
| 7.2.1 Installation Enhancements | 103 |
| 7.2.2 Administration Enhancements | 105 |
| 7.2.3 Improved Alerting | 109 |
| 7.2.4 Enhanced Display | 115 |
| 7.2.5 Reporter Enhancements | 120 |
| 7.2.6 Configuration Management Enhancements | 121 |
| 7.3 eG CLI Enhancements | 123 |
| 7.4 Support for REST API for Administering the eG Manager and Retrieving Analytics | 123 |
| 7.5 Security Enhancements | 123 |
| 7.6 eG Mobile Application Enhancements | 127 |
| 7.7 Integration Enhancements | 128 |
| 7.8 Scalability Improvements | 128 |
| 8. CONCLUSION | 130 |

Introducing eG Enterprise v7

User experience is top of mind for IT executives in today's application-centric world. Monitoring just the resource usage of applications and utilization levels of infrastructure elements is not enough any longer. In today's digital era, organizations must take a holistic perspective of user experience:

- Clearly, the availability of an organization's key IT services and their response times to end users is a key measure of user experience. At the same time, these two metrics alone are not sufficient.
- The degree of proactiveness of an organization also contributes to user experience. The more proactive an organization is, the fewer problems that users notice and hence, better the user experience.
- The reliability of IT services is another key metric. When a service goes down, how long does it take for the organization to bring it back up to normalcy? The mean time to repair and frequency of such outages also contribute to user experience. The more accurate the diagnosis and faster the resolution, the better is the user experience.
- As the workload of a service changes, the IT organization must make sure that the user perceived quality of service remains good. Proactive capacity planning plays a key role in this.

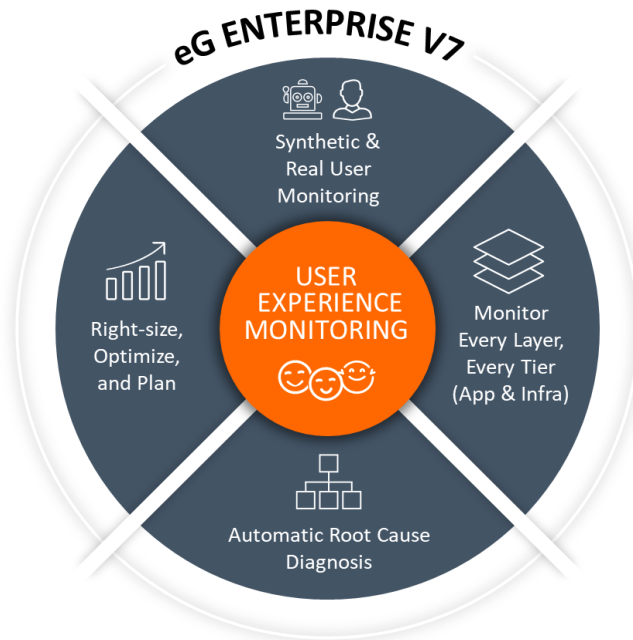
Therefore, **organizations need to take a 360° view of user experience and make it a central component of their IT monitoring strategy.** This is true irrespective of the type of applications being used by the business – whether digital workspaces (Citrix, VMware Horizon), web applications (Java, .NET, etc.), packaged enterprise apps (SharePoint, SAP, etc.), or SaaS applications (Office 365, Salesforce, etc.).

eG Innovations is proud to announce the general availability of the latest version of its flagship performance monitoring software – eG Enterprise Version 7. This release introduces a number of new monitoring capabilities, detailed diagnosis features, new reports and analytics that help IT organizations deliver the best experience to their business/IT users.

1. eG Enterprise v7: The Total User Experience Monitoring and Management Solution

eG Enterprise v7 makes user experience the centerpiece of your IT monitoring and management strategy.

- Using a combination of synthetic and real user experience monitoring, eG Enterprise enables IT organizations to quantify the quality of service being delivered to users, and proactively notifies IT operations teams of impending problems.
- From a central web console, IT teams have insights into the performance of every layer and every tier of the application stack and the underlying infrastructure.
- Correlated topology views and an embedded root cause diagnosis engine help pinpoint the root cause of user experience issues quickly, thereby helping IT teams reduce mean time to repair and enhance service uptime and performance.
- Lastly, advanced analytics embedded in the solution helps IT teams make the right decisions – from determining how to balance load in the infrastructure, estimating where to add additional resources, and planning for additional capacity in the future.



The result: happy users, enhanced productivity, and tangible business ROI.

2. Summary of New Capabilities in eG Enterprise v7

In the following sections, we present the new capabilities in eG Enterprise v7, grouped by use cases that these capabilities apply to. Enhancements to make the platform more scalable, secure and performant are also included in this release.

Digital Workspace Monitoring

- Enhancements for Citrix Workspace monitoring
- Enhancements for VMware Horizon VDI monitoring

Web Application Performance Monitoring (APM)

- New synthetic monitoring capability for web applications
- Enhancements to Real User Monitoring
- Expanded coverage for distributed transaction tracing

Enterprise Application Monitoring

- Enhancements for SAP monitoring
- Enhancements for Office 365 monitoring
- Monitoring support for more packaged enterprise applications

Extended Unified Monitoring Capability

- Monitoring support for new devices, platforms and applications
- Greater visibility into the public cloud
- Monitoring support for DevOps tools
- Monitoring extended for container environments

Platform Enhancements for Increased Automation, Simplicity, Scalability and Security

- Platform upgrade and other product enhancements
- Increased security to protect against vulnerabilities and threats
- One-Click Dashboards: Pre-built templates for creating custom dashboards
- Report Builder: New interface to easily build custom reports
- SaaS deployment made simpler, more automated and truly self-provisioned

The following sections cover the enhancements in each of the above areas.


3. Digital Workspace Monitoring

3.1 Citrix Workspace Monitoring Enhancements

3.1.1 Citrix Logon Simulator

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

- **Troubleshooting logon failures made easy:** The eG Logon Simulator for Citrix XenApp and XenDesktop presents a graphical view of the logon process, which helps administrators quickly and accurately identify the exact step of the logon process that caused slowness. This graphical representation has been enhanced in v7, so that it not only points administrators to where the bottleneck is, but also reveals in a single click, what caused the bottleneck!

In this version, the simulator automatically takes screenshots of failure conditions and displays them in the graphical view. To this effect, an  icon is introduced against the step that has failed or is sluggish. Clicking on this icon reveals the screenshot that was taken at the time of the failure, so administrators can instantly determine what error caused the failure and easily figure out how to fix

it.

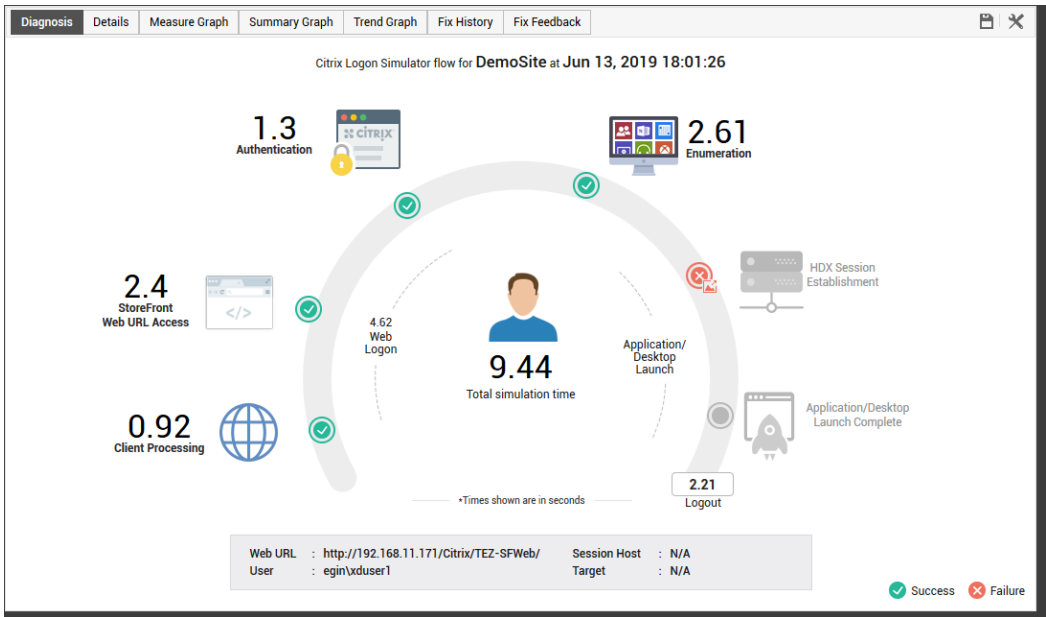



Figure 1: The icon that is used to trace the transaction failures

These screenshots can also be accessed from the layer model view. The measure reporting a failure is accompanied by a  icon, which will lead administrators to the screenshot that was captured during failure.

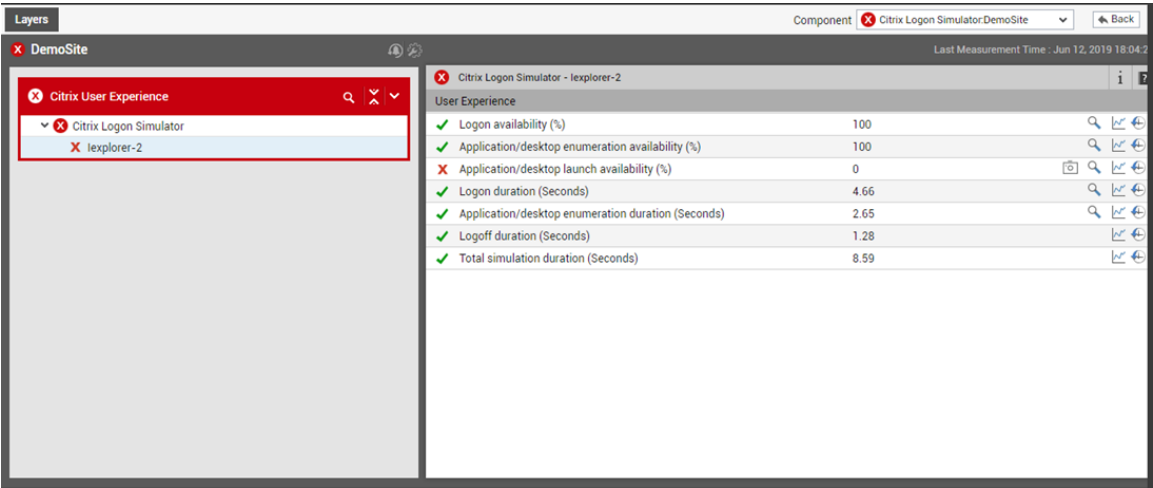


Figure 2: The screenshot icon that appears in the layer model

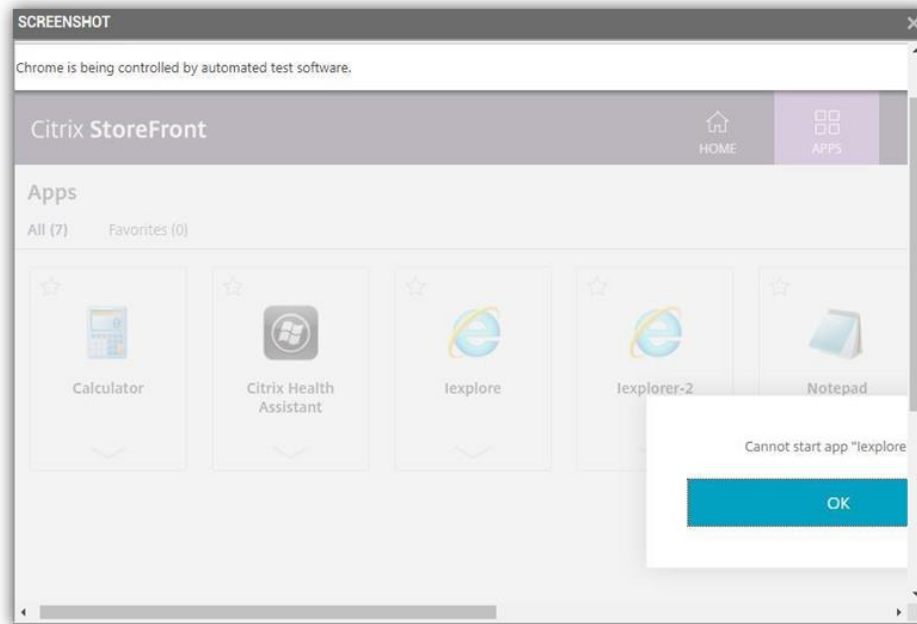


Figure 3: The screenshot captured during transaction failure

- **Support for additional authentication mechanisms:** Users can access their Citrix environments through different means. Users within the Citrix environment use the Citrix StoreFront to access the Citrix hypervisors and applications whereas users accessing the Citrix environment from remote/external locations use the Citrix NetScaler. Some Citrix environments may also use F5 load balancers through which the users can access their environments. Citrix NetScaler can be integrated with additional authentication mechanisms (single sign-on systems) such as OKTA, Azure AD, AD FS. In previous versions, the Citrix Logon Simulator failed to simulate the transactions when the Citrix NetScaler was integrated with authentication mechanisms such as Microsoft Azure AD and AD FS. This has been supported in eG Enterprise v7. Citrix Logon Simulator also works with the latest Citrix Cloud Access.
- **Capturing HDX Channel details in Citrix Logon Simulator:** Where simulations are performed through HDX virtual channels, the eG agent v7 uses Citrix APIs to collect and report additional metrics revealing the HDX experience. The average screen refresh latency, the amount of data sent/received, and the count of frames sent/received are reported for each simulation. These metrics are collected

without needing any software to be deployed on the servers / virtual desktops being accessed.

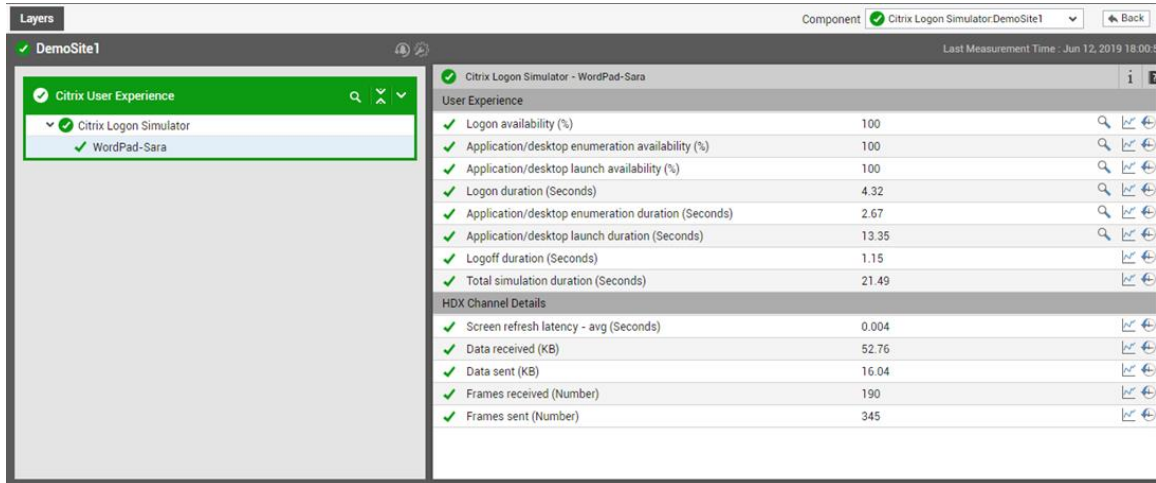


Figure 4: Additional metrics revealing the HDX user experience

3.1.2 Client Session Simulation

Client session simulation allows organizations to simulate entire Citrix sessions, going beyond just logon. A simulation script can be recorded to open an application inside a Citrix session, login to the application, perform actions within the application and then logout of the Citrix session.

eG Enterprise v7 provides a new visualization of the results of Citrix session simulation. A new transaction flow graph shown in Figure 5 below depicts the sequence of steps involved in the simulation. For each step, the success/failure of the step and time taken are shown, so it is easy for administrators to see where the performance bottlenecks are.

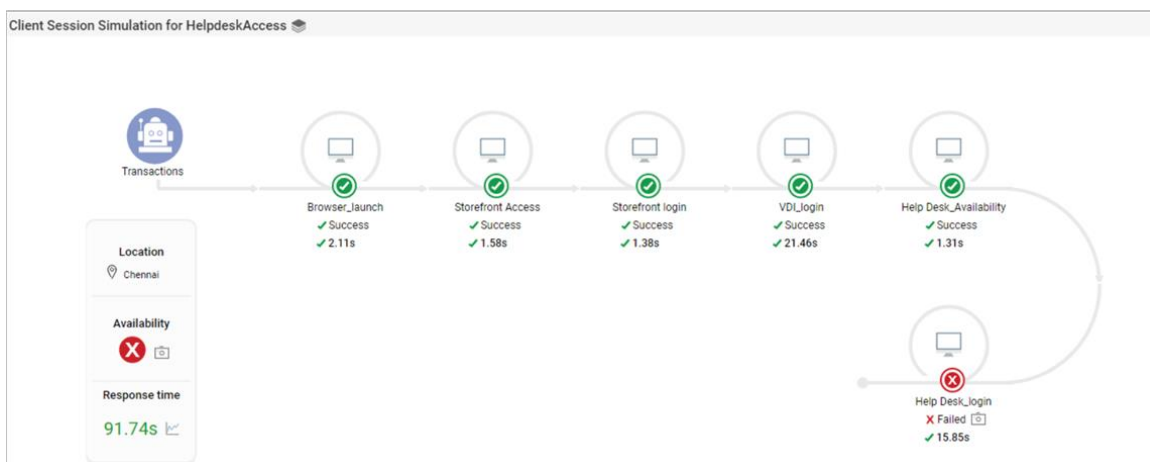



Figure 5: The step by step transaction flow performed by a user

The transactions that failed are marked with a red colour and clicking the  icon against the failed transaction will lead you to the screenshot that was captured when the transaction failed. In the example below, the screenshot indicates a failure within the application being accessed (i.e., not an error in the Citrix

infrastructure itself).



Figure 6: The screenshot captured for failure transaction

3.1.3 Citrix Delivery Controllers

Citrix Delivery Controllers coordinate all user accesses to a Citrix infrastructure. Following are the enhancements that have been made in eG Enterprise v7 for monitoring Citrix Delivery Controllers:

- **In depth visibility into logon performance of users:** To provide a 360 degree view of Citrix logon performance, eG Enterprise tracks logon performance from two perspectives: from the Citrix Delivery Controller and from the Citrix XenApp servers or virtual desktops (for VDI). To measure the logon performance of the users from a Delivery Controller perspective, eG Enterprise uses Citrix APIs. eG Enterprise v7 integrates with the latest Citrix APIs to provide more granular details of the logon performance of the users. New metrics provided for each user logon include:
 - Pre-user initialization duration
 - User initialization duration
 - Shell duration
 - Delay duration

In-depth visibility is now provided into the interactive session experience for each user, thus enabling administrators to quickly identify where exactly delays were noticed - before user initialization (due to improper configuration of group policy objects and logon scripts), during user initialization (due to network issues, corrupt logon scripts, etc) or after user initialization (due to VDA being loaded with too many applications, desktop containing too many icons) or during transition from one initialization phase to another. These metrics are for on-premise Citrix deployments as well as for deployments using the Citrix Cloud service deployments.

- **Monitoring Tags and Tag restrictions in a Citrix Delivery Controller:** Tags are strings that identify items such as machines, applications, desktops, Delivery Groups, Application Groups, and policies. After creating a tag and adding it to an item, you can tailor certain operations to apply to

only items that have a specified tag. A tag restriction, similar to the Worker groups concept in Citrix XenApp servers can be thought of as subdividing (or partitioning) the machines in a Delivery Group. With tag restrictions, you can use your existing machines for more than one publishing task, saving the costs associated with deploying and managing additional machines. eG Enterprise v7 monitors the tags and reveals the count of applications, application groups, machines, desktop groups, objects and unknown objects that have been tagged. Tag restrictions are also monitored, and the applications, objects, unknown objects, and actions with tag restrictions are revealed. Tag usage is also monitored for each VM.

- **Monitoring Local Host Cache in a Citrix Delivery Controller:** Sometimes, the connection between a Delivery Controller and the Citrix site database may fail, resulting in an outage. If the outage persists for over 90 seconds – i.e., if the site database remains inaccessible for over 90 seconds – then the Local Host Cache takes over and allows connection brokering operations in a Citrix site to continue. If the Local Host Cache is active in an environment, it is a sign that network disturbances or site database issues exist in that environment. This is why, Citrix administrators often want to check whether the Local Host Cache is in use, and if so, for how long. With version 7, this check is now possible! In this version, the eG agent periodically checks whether/not the local host cache is active. If it is, then the agent additionally reports the duration for which the local host cache was active, so that administrators can quickly figure out how long the site database in their Citrix environment has been inaccessible.
- **Monitoring the power state of machines in delivery groups of the Citrix Delivery Controller:** Power management of virtual desktops/VMs allows automatic changes to the power states (shut down, suspend, etc.) to be made based on pre-defined conditions set by the Citrix administrator. When a session has been disconnected for a long time, power management can be used to suspend or shut down the desktop. eG Enterprise v7 provides additional insights into the power state of machines in delivery groups. The count of powered on machines, the machines that are in unknown power state, the powered off machines, the machines with unmanaged power state, and the machines with suspended power state are now reported per delivery group.
- **Monitoring the registration state for the High Availability service of the Citrix Delivery Controller:** In older versions, the high availability of the Citrix Broker Service was constantly monitored by periodically checking the availability of the SQL database and the effectiveness of the Connection Leasing feature. Though these checks helped administrators to a large extent, administrators still found it hard to figure out the registration of the virtual desktop agents with the Citrix Delivery Controllers on the site. If the registration between VDAs and the delivery controller fails or is not accurate, then the VDAs may reject the session launches brokered by the delivery controllers. eG Enterprise v7 offers greater visibility into the registration of the VDAs with the delivery controllers. The measures such as soft registrations, hard registrations, registration requests, expired registrations are revealed by monitoring the Citrix Broker Service of the Citrix delivery controller. Using these metrics, administrators can figure out if forceful registrations are happening too often and realize the pattern of forceful registrations.

3.1.4 Enhancements to Citrix Cloud Site Monitoring

- **Citrix Cloud Service visibility is now improved:** Starting with this version, eG Enterprise auto-discovers the Citrix cloud services and for each cloud service, reports the number of licenses assigned and tracks the number of days to license expiry. This helps administrators determine the most sought cloud service and the cloud service on which license is about to expire. The overall license utilization of the Citrix Cloud Services is also monitored, and alerts are raised when license utilization peaks. The count of service tickets that are open for various Citrix products are also reported. Drilling down the detailed diagnostics reveals the status of each open ticket, the date and the Citrix product on

which the ticket was raised and the email ID of the user who raised the ticket.

3.1.5 Enhancements to Citrix XenApp Servers Monitoring

- **Monitoring User Input delay for Citrix sessions:** On Citrix XenApp servers running on Windows 2019 or higher and Citrix virtual desktops running Windows 10 (1809) or higher, eG agents now report a new metric – User Input Delay. The user input delay measures how long any user input (such as mouse or keyboard usage) stays in the kernel queue before it is picked up by a process. User input delay is measured and reported for an application process, for a user's session, and for a machine. When the user input delay is high, it means the slowness has been introduced on the server machine or the virtual desktop (and is not due to the network). Tracking this metric allow administrators to differentiate server/desktop-side issues from network issues.
- **Identifying resource intensive browsers/URLs in a Citrix XenApp user session:** Previously, the **Citrix Users** test (mapped to a Citrix XenApp server) reported the aggregate CPU and memory usage of each user, across all that user's sessions. This enabled administrators to precisely identify the user engaged in resource-intensive activity, and the resource-hungry application/process they were accessing. However, when browser-based applications - e.g., Salesforce - are accessed by users, it may not suffice for administrators to know just which application is draining the server resources; for effective troubleshooting, they will also want to know the exact browser URL that is hogging the resources. This is why, in version 7, the detailed diagnostics of the **CPU time used by user's sessions** measure has been enhanced to include the URLs accessed by a user through published IE/Edge browser, and the resource consumption of each URL. This will lead administrators to the resource-intensive URL. In the process, administrators can also figure out the exact reason behind the high CPU/memory consumption - i.e., whether the user was accessing video content, games etc.
- **Identifying user sessions on a Citrix XenApp server initiated through mobile devices:** In today's fast paced world, users in a Citrix environment can either be physically present to login to their environment or access the environment from remote locations through their mobile devices. To keep tab of Citrix users accessing the Citrix XenApp servers via mobile devices and desktops, eG Enterprise v7 monitors and reports the count of user sessions initiated through mobile devices and via desktops.
- **Monitoring the performance of the client printers on the Citrix XenApp servers:** Often, Citrix administrators get bombarded with complaints relating to print jobs. The print jobs in the environment may either be slow or get disconnected or may fail inadvertently. For an administrator, the first step towards troubleshoot any printer related issue is to figure out how many print jobs have failed. Administrators may also want to figure out the type of print jobs (EMF jobs, RAW jobs, Microsoft XPS) that failed too often and whether the entire data for printing was transferred from the user terminal to the printer. To aid administrators in this step of troubleshooting, eG Enterprise v7 monitors the printers configured on the Citrix XenApp servers. For each configured printer, eG Enterprise v7 reports the print jobs that were created and completed and the print jobs that failed. The amount of data that was transferred between the user terminal and the printer is also reported. By comparing the metrics reported, administrators can figure out the type of print job that failed often.

3.1.6 Enhancements to Monitoring the Citrix StoreFront

- **Synthetic monitoring to test Citrix StoreFront Application Availability:** In version 7, eG's ability to measure the logon experience of users connecting via Citrix StoreFront has been enhanced. The eG agent on Citrix StoreFront can now be easily configured to emulate accesses to specific applications/desktops published on StoreFront. In the process, the availability, authentication, and

enumeration of each application and/or desktop is reported. These metrics offer insights into certain key factors that may influence a StoreFront user's logon experience. This includes the availability and responsiveness of the StoreFront home configuration, the authentication method, the availability of the ICA file and the time taken to download it, and more! These granular metrics, coupled with the deep-dive diagnostics already offered by the eG Citrix Logon Simulator, enable Citrix administrators to track the complete journey of a Citrix StoreFront user through the Citrix application/desktop delivery landscape and accurately isolate logon bottlenecks. This functionality is similar to the App Probing feature of the Citrix Director.

- **Enhanced StoreFront authentication monitoring capabilities:** In previous versions, user information authenticated through Citrix Wallet Service, language preferences settings and explicit user credentials were monitored and reported. To be upto date with the support for monitoring the Citrix StoreFront authentication mechanisms, starting with eG Enterprise v7, the users who enter the Citrix Receiver for accessing the applications/virtual machines through SAML authentication and domain pass through authentication are monitored and reported. By continuously monitoring the average time taken for Serialization calls and Deserialization calls help administrators in figuring out whether/not the users were authenticated at a faster pace.

3.1.7 Enhancements to Citrix NetScaler Monitoring

- **Capturing TCP errors encountered during sessions accessed via Citrix NetScaler:** By default, TCP communication is set up between a source-port on the requesting end and a destination-port on the receiving end. The client/ user initiates a request through the Citrix NetScaler to access a backend server. The Citrix NetScaler in turn opens a TCP connection to the backend server based on the request received. For each virtual IP address or a Subnet IP, the Citrix NetScaler cannot open more than 65,536 TCP connections. TCP port exhaustion is just one of the TCP abnormalities that needs to be monitored on a Citrix NetScaler. In addition to monitoring TCP port exhaustion, eG Enterprise v7 also tracks bad checksum errors, incorrect SYN/ACK packets received, reset packets dropped due to threshold violation and so on.
- **NetScaler Request Flow Dashboard:** Typically, when monitoring a Citrix NetScaler VPX/VPX appliance, eG Enterprise tracks the request traffic to the appliance and automatically discovers how the traffic flows within the NetScaler ecosystem. In other words, eG intelligently auto-discovers the virtual servers, services/service groups, and nodes (in a server farm), using which the appliance load-balances the traffic, and also reports the health of these virtual entities. Previously however, to obtain this information, administrators had to click through many layers of eG's layer model for the NetScaler appliance, or pour over rows of detailed diagnostics. To provide administrators with a holistic, at-a-glance view of the request flow on demand, eG Enterprise v7 offers a useful NetScaler Request Flow Dashboard. For a chosen NetScaler appliance, this dashboard quickly reveals which virtual servers front-ended client requests, which services/service groups were being requested, and which nodes (in the server farm) fielded the requests. The health of each of these virtual entities can also be instantly determined using this dashboard.

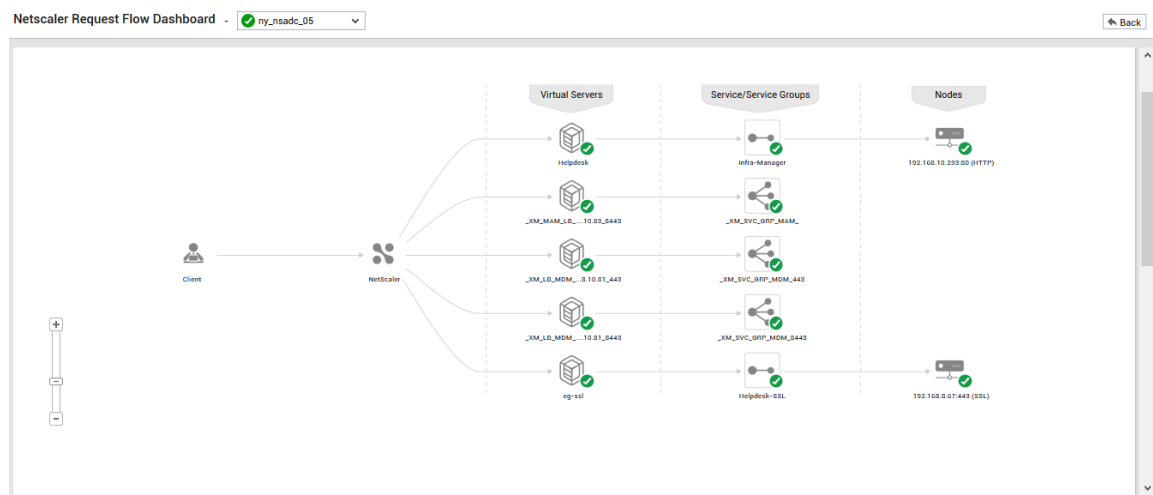


Figure 7: The NetScaler Request Flow Dashboard

3.1.8 Enhancements to Citrix License Server Monitoring

Tracking the utilization of Citrix licenses offered as 'overdraft': By default, Citrix includes License Overdraft as a feature in all user/device, per user and per device licenses. Citrix provides 10% of the purchased licenses as overdraft. For example, if you purchase 1000 licenses, you will be offered 100 licenses as overdraft. The total licenses installed in the environment will therefore be 1100. In previous versions, eG Enterprise calculated the 'Licenses available' and 'License utilization' measures inclusive of the overdraft licenses. A few Citrix administrators wanted to calculate these measures by excluding the overdraft licenses i.e., they wanted to take the actual purchased licenses alone in consideration. When overdraft licenses were also included for calculating the licenses available, administrators were not able to proactively figure out if they needed additional licenses. eG Enterprise raised an alert only after the exhaustion of the purchased licenses which provided a very little time to purchase additional licenses. For the convenience of such administrators in proactively figuring out the necessity of additional licenses, eG Enterprise v7 includes an additional "REPORT UTIL BY OVERDRAFT" flag in the Citrix Licenses test configuration page. Setting this flag to No will excluded the overdraft licenses while calculating the Licenses available and License utilization measures. Starting with this version, the total number of licenses installed (including the overdraft licenses) is reported. Administrators are also provided insights into whether/not the licenses have expired and whether/not overdraft licenses are currently in use. The number of users and devices using each type of license is also reported.

3.1.9 Other Citrix Monitoring Enhancements

Following are some of the significant Citrix monitoring and display enhancements that have been included in eG Enterprise v7:

- **User specific Session Topology:** In previous versions, when administrators drilled down the USER EXPERIENCE DASHBOARD to view the user experience of a chosen Citrix user, the session login details of the user alone were displayed. Though this helped administrators figure out the exact time during which the user logged in, administrators were not able to use the dashboard to troubleshoot user experience issues. To fill this void, the User Experience Dashboard of v7 provides an end-to-end topology view of the complete user session, revealing every component engaged in the user access and the health of each component. A quick look at this topology will help administrators instantly figure out which StoreFront server / NetScaler appliance front-ended the user session, which delivery controller brokered the connection, which XenApp server / virtual desktop the user logged into, and on which hypervisor the virtual desktop is operating (available only for virtual desktops hosted by Citrix XenServers). Using conventional color-codes as health indicators, the dashboard also

quickly and accurately pinpoints which component of the session topology is adversely impacting user experience with Citrix. 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.

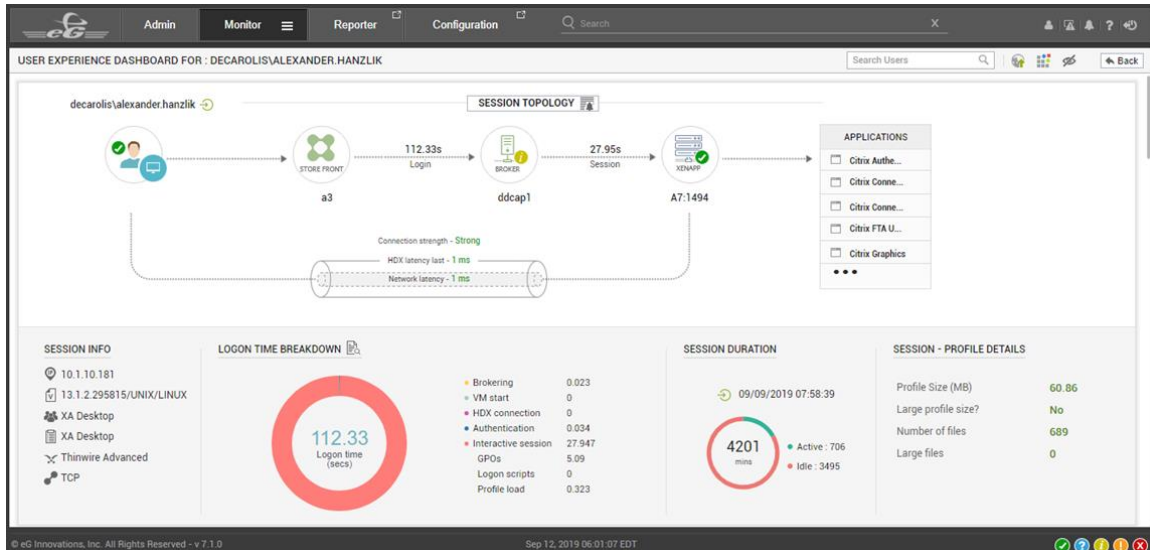


Figure 8: Viewing the Session topology for the user

- **Citrix Overview Dashboard/Virtual Apps Dashboard:** To receive quick insights into the performance of a single Citrix XenApp server, administrators can use the Application dashboard that eG provides for Citrix XenApp. To receive an overview of the performance of a Citrix XenApp farm that spans geographies and to quickly spot 'grey areas', administrators can use the new Citrix Overview Dashboard that eG Enterprise v7 provides. Using this dashboard, administrators can:

- View the overall health and aggregate resource utilization of the Citrix XenApp servers in a farm, so problematic XenApp servers in the farm and potential resource contentions at the farm-level can be promptly detected;
- Track the state of Citrix performance KPIs across geographies and spot issues affecting user experience in real-time;
- Assess the session load on the farm, and identify the precise geographies and devices contributing to the load;
- Identify the applications, servers, and users who are draining the resources of the farm.

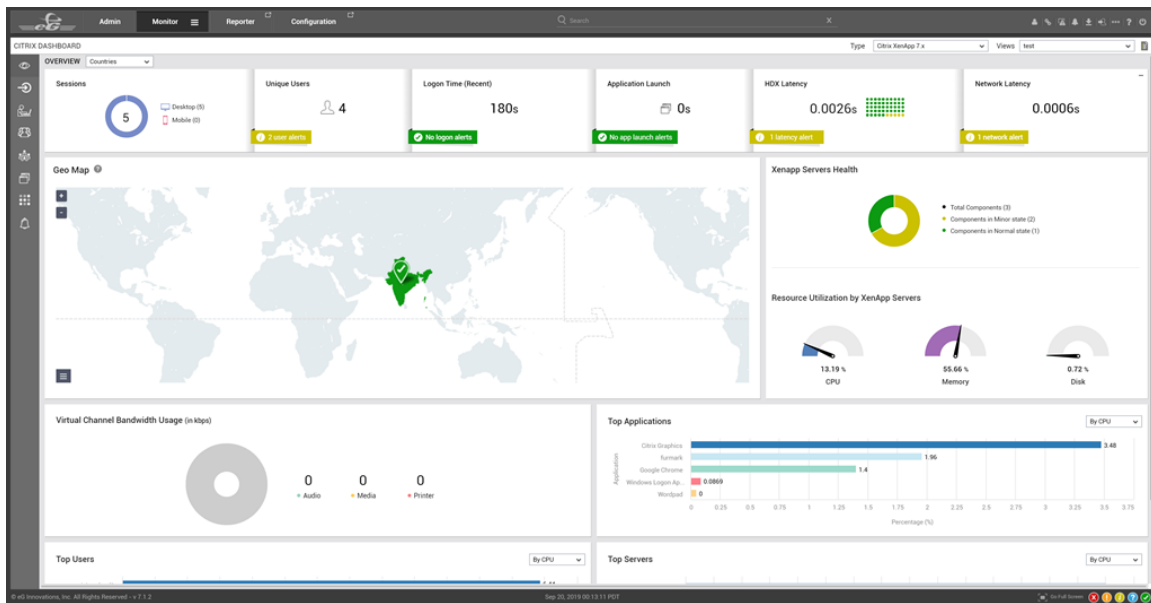


Figure 9: The Citrix Overview dashboard

For further insights into the logon experience, user sessions, applications, resource usage, delivery groups and alerts, administrators can use the dashboards that appear upon clicking the icons available in the left pane as shown in Figure 9.

Option to manually configure geo locations: eG Enterprise has an in-built capability to auto-discover the geographic locations (Country/City/Region) of the users logged into Citrix XenApp servers/Citrix XenDesktop VMs. Geo location information of a user is determined by mapping the IP address of the client reported in Citrix NetScaler to a geo location. In case the user connects directly using Citrix StoreFront (i.e., without connecting through NetScaler), the client IP address on the XenApp server is used to determine the geo location (this capability is not supported for Citrix virtual desktops). In the event that eG Enterprise is not able to automatically determine a user's geo location, administrators can provide a custom mapping of IP address ranges to geo location using the **Geo Locations** page in the eG administrative interface.

Using the Geo Locations page, administrators need to configure a Network location. For this location, an XML file has to be provided mapping IP address ranges to a country, region and city. The XML file should be populated in the format mentioned below:

```
<location start-ip-address="<First IP address in a range>" end-ip-address="<Last IP address in a range>">
  <country><name of the country></country>
  <region><name of the region></region>
  <city><name of the city></city>
  <country-code><code of the country></country-code>
  <latitude><latitude of the user location></latitude>
  <longitude><longitude of the user location></longitude>
</location>
```

A sample XML file is as follows:

```
<location start-ip-address="192.168.8.1" end-ip-address="192.168.8.100">
  <country>India</country>
  <region>Tamil Nadu</region>
  <city>Chennai</city>
  <country-code>IN</country-code>
  <latitude>13.0827</latitude>
```

```
<longitude>80.2707</longitude>
</location>
```

The country code has to be the same as the value provided for the corresponding country name in the **eg_geodetails.ini** file available in the **<EG_INSTALL_DIR>\manager\config** directory. Once the XML file is populated and uploaded, the exact geographic location of the users will be plotted in the Geo Map. Note that Geo Map is not yet supported for VMware Horizon infrastructures.

- **VDI Resource Usage Analysis dashboard for Hypervisors:** In older versions, administrators found it difficult to figure out the resource consumption of the VMs/virtual desktops and compare the results so that they can understand the resource utilization better. For such comparison, eG Enterprise 7 has introduced a new dashboard using which administrators can easily track and compare the resource utilization of the VMs/virtual desktops with the resource utilization of the host.

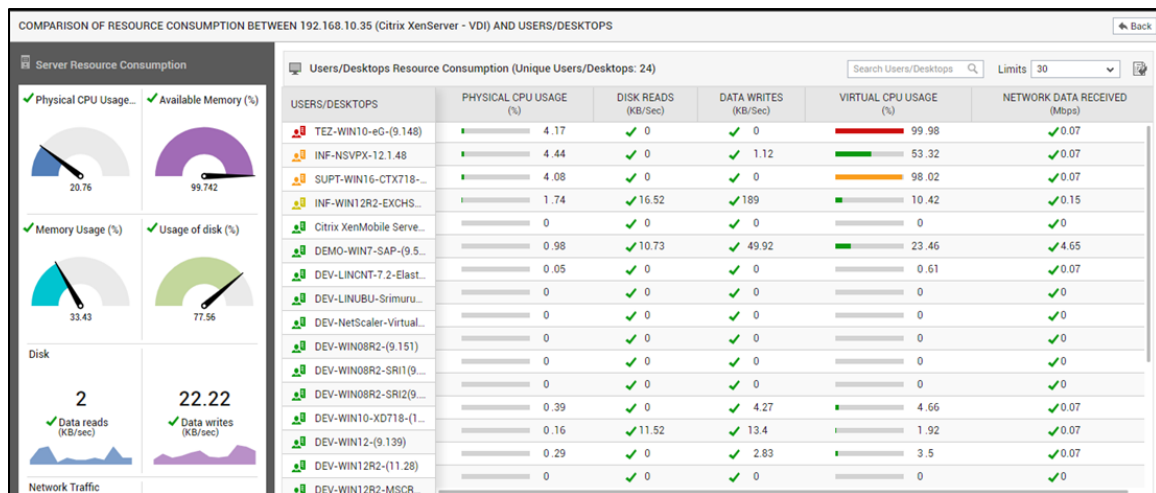



Figure 10: The resource utilization of VMs/virtual desktops compared with that of the hypervisor

- **New shortcut introduced to access Remote Control Actions from layer model:** Citrix administrators often have to run a number of actions to control user sessions – for example, to shadow a session, to take a screenshot of a session, to logoff/disconnect a user from a session, kill user GPO policies, etc. With eG Enterprise v7, these control actions can be remotely initiated by administrators from their web browsers themselves. While control actions were supported in earlier versions, they were initiated at the server level only. In eG Enterprise v7, administrators can initiate these actions for specific user sessions. These actions are made easily accessible to admins, from the layer model view of a component itself. To this effect an  icon has been introduced on top of the layer model. The actions that are available will change automatically based on the component type being analyzed. As soon as an alert is detected on the layer model of a component, the admin can initiate a control action and begin troubleshooting.

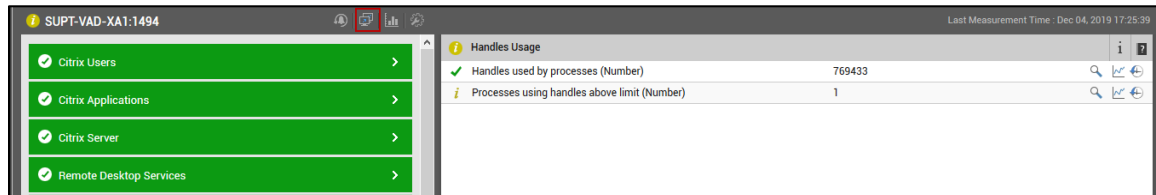


Figure 11: The Remote Control Actions icon in the layer model

- **Tracking the Citrix XenServer VMs in Dead Beef state:** When trying to shut down a VM hosted

through Citrix XenServer 6.5 SP1 and above, sometimes, the VM may stay in an amber state for a long time. These VMs cannot be accessed unless and until they are rebooted. Such VMs are called dead-beef VMs. Too many dead-beef VMs in a Citrix environment will result in unavailability of the VMs and eventually create a shortage of VMs. This will affect the experience of the users logged in the Citrix XenServer environment. To improve the user experience, it is necessary for the administrators to provision the VMs instantly. For this, administrators need to proactively detect the dead-beef VMs and reboot them now and then so that the VMs remain available to the users when necessary. eG Enterprise v7 helps administrators in identifying the dead-beef VMs.

- **Monitoring Citrix App Layering:** Citrix App Layering is a software that separates virtual applications from their underlying virtual desktop in a way that enables them to take advantage of the host operating system's native functions and can interact with other applications. For example, in a Citrix environment where Citrix App Layering software is installed, Citrix administrators can apply patch/update to all the applications in the environment in a single shot through a VM/Golden Image. Since the applications are separated from the operating system, they can be delivered and updated without installing them on the operating system. User experience may suffer when the layered app delivery is slow. To identify slowness, administrators should periodically check if the vDisk attachment is successful, the time taken for the layered app to get attached to a user session and the vDisks attached to the user session. eG Enterprise v7, performs all these checks by monitoring the Citrix App layering. Additionally, eG Enterprise is also capable of monitoring the App Layering attachment in the virtual desktops that are brokered by Citrix XenServer hypervisors.
- **Monitoring Citrix Workspace Environment Management (WEM):** eG Enterprise v7 helps administrators in analyzing the impact of CPU management features of WEM on XenApp / XenDesktop VM performance. CPU-intensive processes that have been throttled owing to CPU clamping are captured and reported. An alert is also sent out if the priority of any process has been reduced because of CPU Spikes Protection.

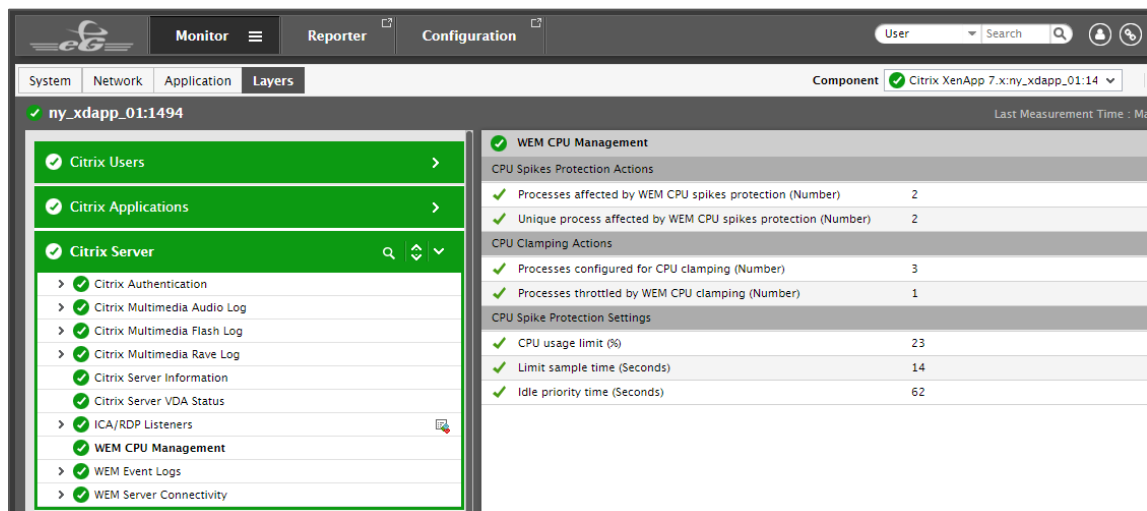


Figure 12: Monitoring CPU clamping and CPU Spike Protection on WEM-enabled XenApp servers

- **Monitoring Citrix SD-WAN:** Citrix SD-WAN is a WAN Edge appliance that provides application control deep packet inspection, dynamic routing, virtualized WAN, built-in application-aware stateful firewall and WAN optimization capabilities. eG Enterprise v7 is capable of monitoring the Citrix SD-WAN in an agentless manner and reporting a host of useful metrics. For every observed protocol and configured site, the LAN to WAN and WAN to LAN data transmission is monitored to check for abnormalities. The QoS of applications accessed through the Citrix SD-WAN is reported periodically. The congestion, jitter or packet loss can be easily identified by monitoring the virtual paths. The route type, reachability, eligibility, hits, cost, Virtual path service state latency, jitter, data received

of the WAN connections are monitored and reported frequently. This way, any data loss on the Citrix SD-WAN can be proactively identified and averted and the user experience can be improved considerably.

- **Citrix Session Recording Server:** Session Recording enables recording the on-screen activity of any user session hosted from a VDA for Server OS or Desktop OS, over any type of connection, subject to corporate policy and regulatory compliance. Session Recording records, catalogs, and archives sessions for retrieval and playback. eG Enterprise v7 is capable of monitoring the Citrix Session Recording Server which runs on IIS and .Net Framework. The eG agent is installed on the Citrix Session Recording server to pull out useful metrics.

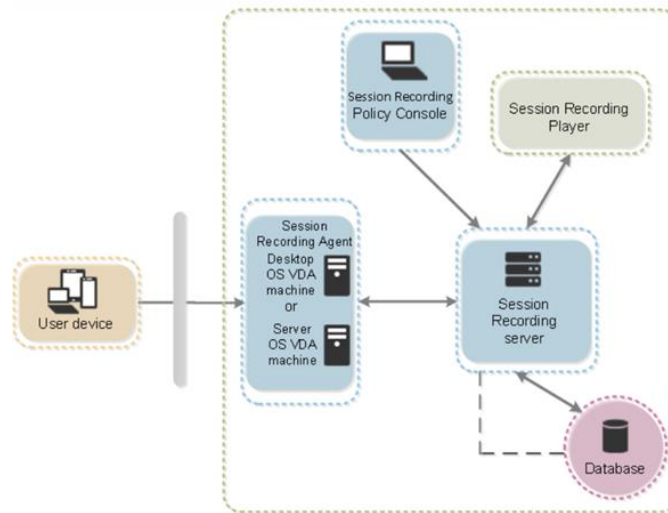


Figure 13: The architecture of the Citrix Session Recording Server

The Citrix Session Recording Storage stores the recordings received from the Session Recording Agent on the Citrix XenApp/XenDesktop server. These recordings help technical support executives resolve issues faster. The number of files in the storage and the file size is constantly monitored so that administrators can keep tab on the capacity of the drive on which the recording folder of the Citrix Session Recording storage exists. This check helps administrators determine if they need to can either clear up older recordings or add extra space for new recordings. Message processing delays recorded by the Citrix Session Recording Manager helps administrators figure out processing bottlenecks. By default, the eG agent communicates with the Citrix Session Recording Server to collect metrics via MSMQ. The MSMQ message queues and growth rate needs to be frequently monitored to ensure healthy communication between the eG agent and the Citrix Session Recording Server.

- **Monitoring Citrix Federated Authentication Service:** CFAS integrates with Active Directory Certificate Services and dynamically issues certificates for users, allowing them to log on to an AD environment instantly. CFAS allows Citrix StoreFront to use a broader range of authentication options, such as SAML assertions (alternate to traditional Windows user accounts). The Citrix StoreFront server contacts the CFAS whenever user requests access to the virtual desktop application (VDA).

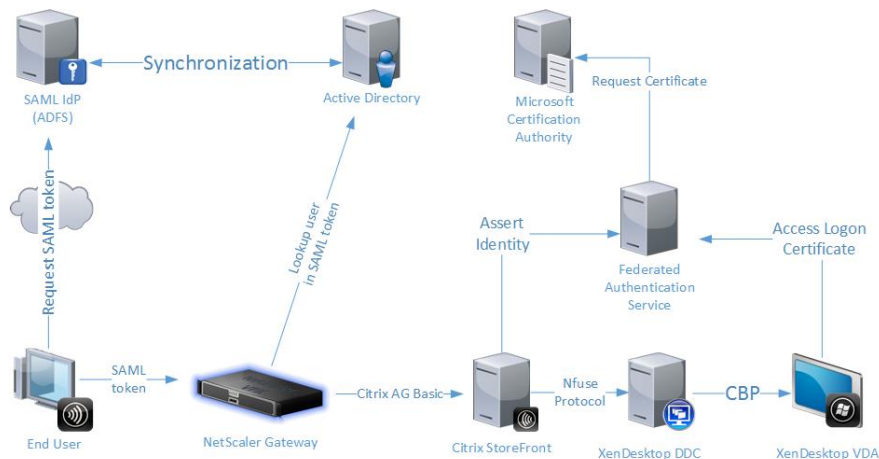


Figure 14: The architecture of the Federated Authentication Services

eG Enterprise v7 is capable of monitoring the Citrix Federated Authentication Service. The status of each CPAF authorization certificate is monitored and their details are reported. Administrators can check whether/not the CFAS definitions are in session and view the definition details. The active sessions, request time, certificate count are revealed by monitoring the CFAS. The users authenticated through CFAS are tracked and the number of users, unique users, expired users and their respective certificate details and thumbprint details are reported.

- **Monitoring Active Directory Federated Service on Citrix deployments:** AD FS is a feature of the Windows Server that extends end users' single sign-on (SSO) access to applications and systems outside the corporate firewall. AD FS authenticates users to SaaS apps and web apps during a single online session. Once a user logs in with his or her Windows credentials, AD FS authenticates access to all approved third-party systems i.e., ties different applications' usernames and passwords to existing identities. AD FS can provide sign-on and access control based on a unified set of credentials. AD FS is an important part of CFAS deployment and therefore, it is critical to monitor AD FS for Citrix deployments. eG Enterprise v7 monitors AD FS and promptly alerts administrators to authentication failures and SSO authentication failures. Device authentications, external authentications, OAuth authentication, and FAS requests are monitored, and issues if any brought to light. Account lockout conditions are also promptly captured and brought to the attention of administrators, so that remedial measures can be initiated before end users start complaining.

3.1.10 Citrix Reporting Enhancements

Reports offered by eG Enterprise v7 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 Citrix environments:

- **Citrix XenApp Overview Report:** eG Enterprise includes 20+ key reports that every Citrix administrator needs. However, determining which report to use in what scenario can be a bit of a challenge for the admin and generating all the reports may be time consuming too. eG Enterprise v7 now includes a Citrix XenApp 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.

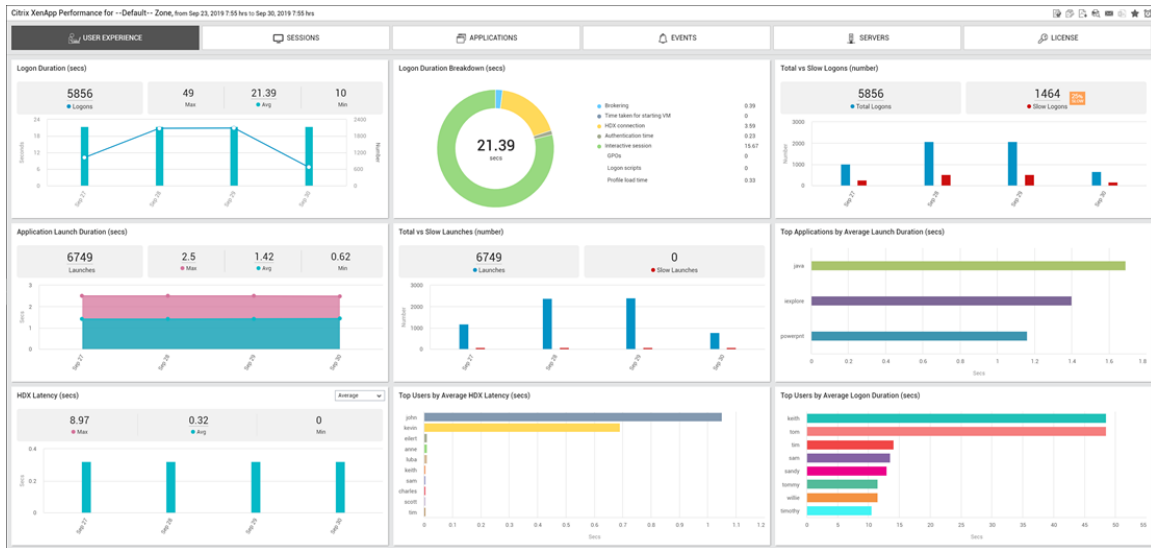


Figure 15: The Citrix XenApp Overview report

➤ **Capacity Planning report for Citrix XenApp Servers:** Load balancing and capacity planning are critical requirements for Citrix administrators. The main challenge of the Citrix administrators lies in supporting more users per Citrix XenApp server with minimal server resources. The Citrix XenApp capacity planning report answers many key questions:

- Based on the average resource consumption per session, how many more concurrent sessions are possible?
- How are sessions load-balanced across servers?
- Is the server capacity bottlenecked by resource usage?
- How many more sessions can be supported after increasing resource capacity?



Figure 16: The Citrix Capacity Planning report

- **Citrix XenApp Server Capacity Prediction Report:** Perform what-if analysis with Capacity Prediction for Virtual Applications report. Administrators can increase the user load on Citrix XenApp servers and they themselves can predict the resource utilization. Also, administrators can figure out how many more servers will be needed to support an increase in user workload. This report is more helpful in environments where administrators have to perform VDI roll outs, add more resources to their infrastructure, include an additional deployment for provisioning resources to new employees in the organization.

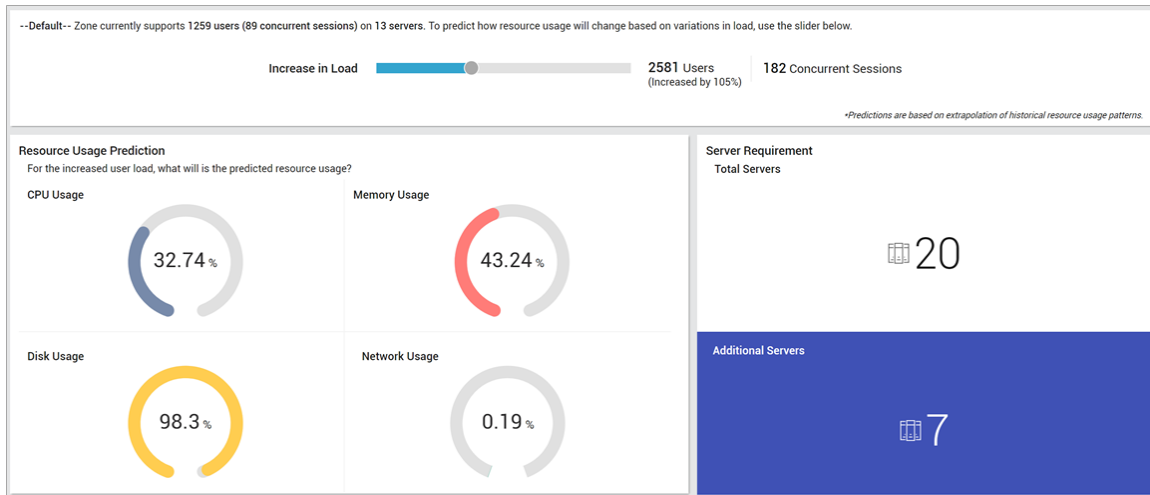


Figure 17: The Citrix XenApp Server Capacity Prediction report

3.1.11 Reports pertaining to Citrix Delivery Controllers:

Following are the reports that are introduced in eG Enterprise v7 with respect to Citrix Delivery Controllers:

- **User Connection Failures Report:** Connection failures to a desktop/application impact user experience with Citrix. Administrators should promptly identify such failures and rectify them at the earliest, so that Citrix users can be assured of a top-notch experience! For this purpose, administrators should look back at the connection failures that have occurred in the past and identify the common causes for such failures. The User Connection Failures report helps with this! This report enables administrators to historically analyze connection failures and accurately identify what has most often caused connections to fail – client-side issues? machine failures? configuration errors? exhaustion of delivery group capacity? absence of a license? Additionally, the report also enables a detailed analysis of connection failures by delivery group, thus pointing administrators to those delivery groups with the highest number of connection failures, along with the reasons for the same. The report also provides useful information related to each connection attempt that failed per delivery group – this includes the user who initiated the connection, the IP and operating system of the client from which the connection was initiated, and the reason for the failure. This way, the test enables quick and accurate diagnosis of the root-cause of connection failures, sheds light on the delivery groups and users impacted by the same, and thus hastens an effective and appropriate resolution.

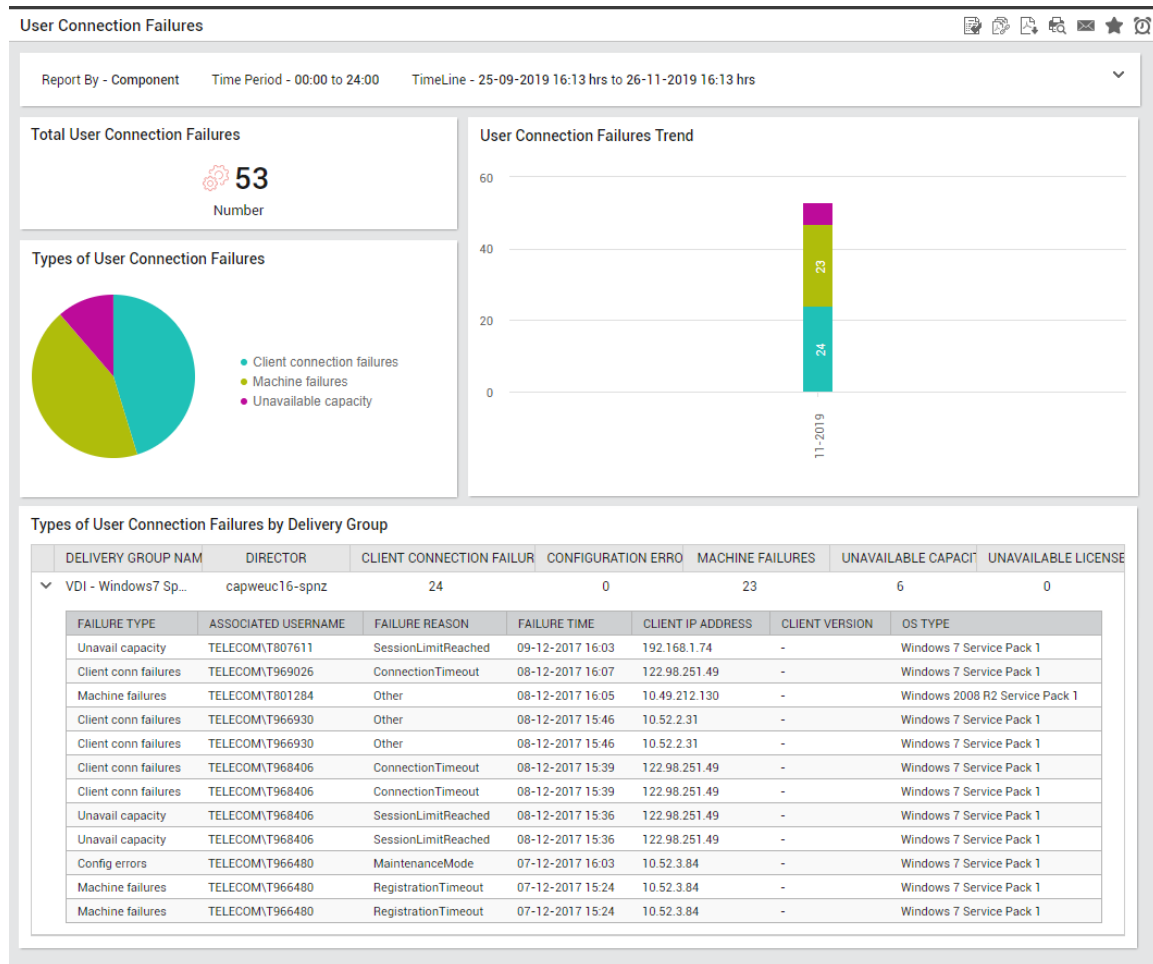


Figure 18: User Connection Failures report

- **Machine Failures Report:** One of the key causes for poor user experience in a Citrix environment is the failure of virtual machines/virtual desktops. Typically, such failures can occur if virtual machines/virtual desktops are unable to start or are not able to boot, or because of the loss of network connectivity between the Citrix broker and the virtual machine/virtual desktop. In such failure situations, delivery groups will not be able to provision virtual machines/virtual desktops to users, thus denying users on-demand access to their critical virtual resources. To make sure that Citrix user experience remains above-par at all times, administrators must take a closer look at machine/desktop failures, identify where they occurred most often (i.e., in which delivery group), and isolate what caused them. This is where the **Machine Failures report** helps. This report enables Citrix administrators to analyze the historical trends in machine/virtual desktop failures, so they can quickly tell when the failure trends were most disturbing. A single glance at this report also enables a quick analysis of failures by delivery group and failure type (i.e., cause of failure), so they can rapidly identify where these failures were most prevalent and why. This information aids administrators in easily and effectively troubleshooting the failures and improving user experience.

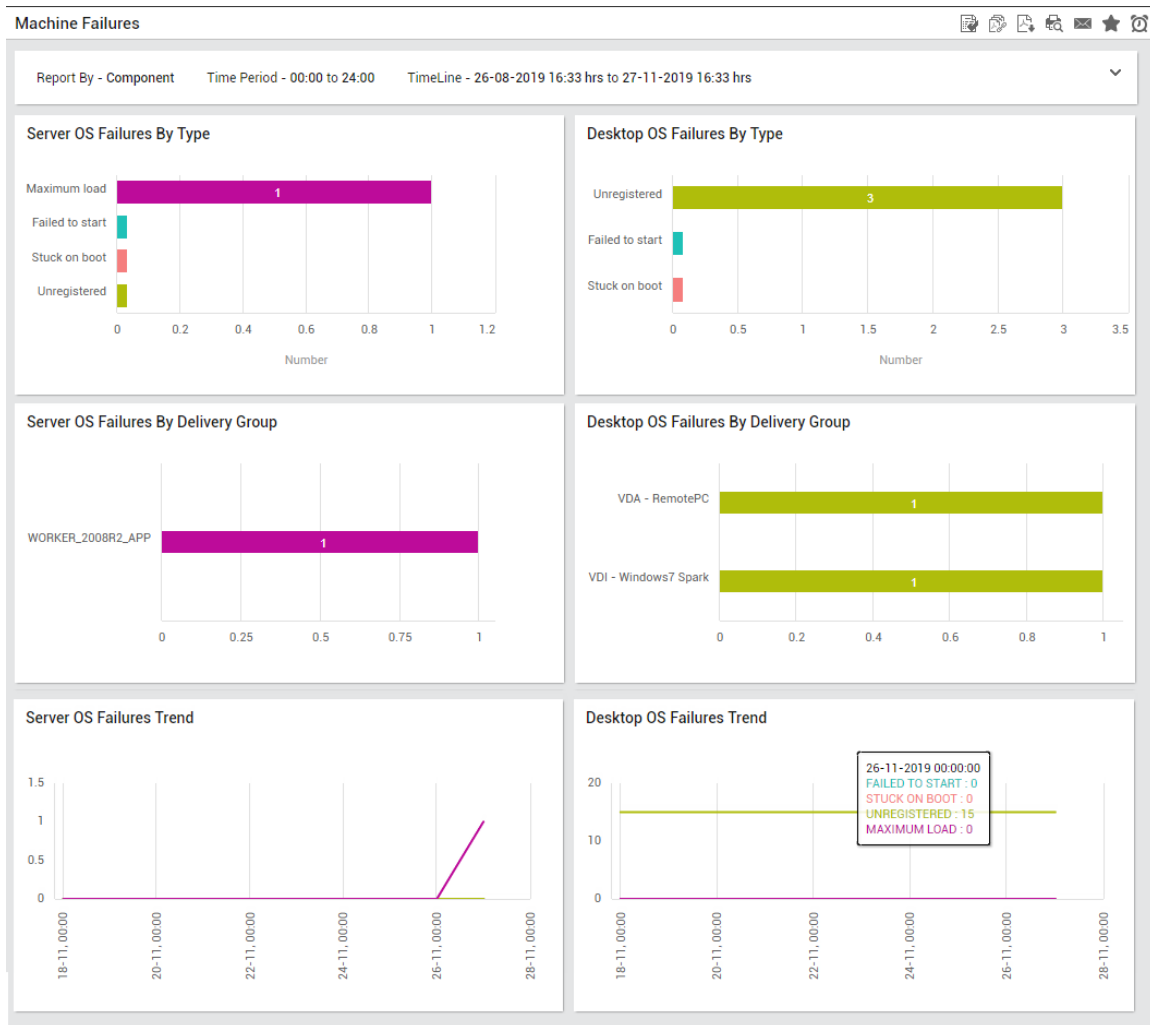


Figure 19: The Machine Failures report

- **Machine Failures by Reason Report:** For more granular analytics on machine/desktop failures in Citrix environments, Citrix administrators can use the **Machine Failures by Reason** report. While the Machine Failures report offers a quick summary of the past failures and points to the broad areas of concern, the Machine Failures by Reason report offers deep-dive analytics related to the failures. Using this report, administrators can swiftly figure out which precise machines/desktops failed, when the failure occurred, and what caused the failure. With the insights provided by this report, administrators can identify the exact machines/desktops that failed often and why.

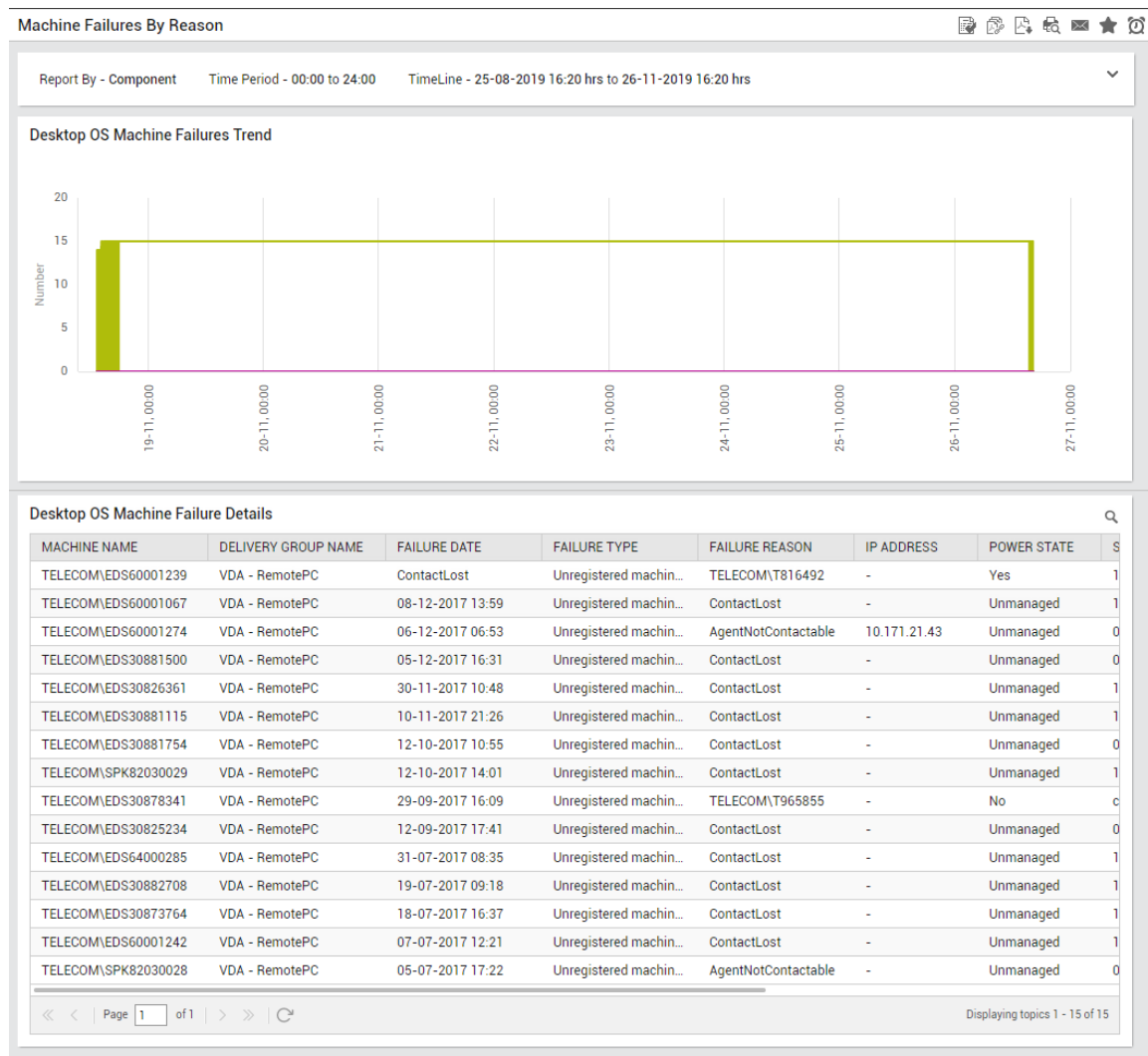


Figure 20: The Machine Failures by Reason report

- **Machine Utilization Report:** This report offered by eG Enterprise v7 provides the administrators with an overview of the status of virtual machines/virtual desktops in each Citrix delivery group. Using this report, administrators can identify the delivery groups where many machines/virtual desktops are in an abnormal state – for e.g., unregistered, unavailable, disconnected etc. – and are hence not ready to be assigned to users. The usage of machines/desktops can also be analyzed per delivery group, so that over-utilized groups and least-used groups can be accurately isolated.

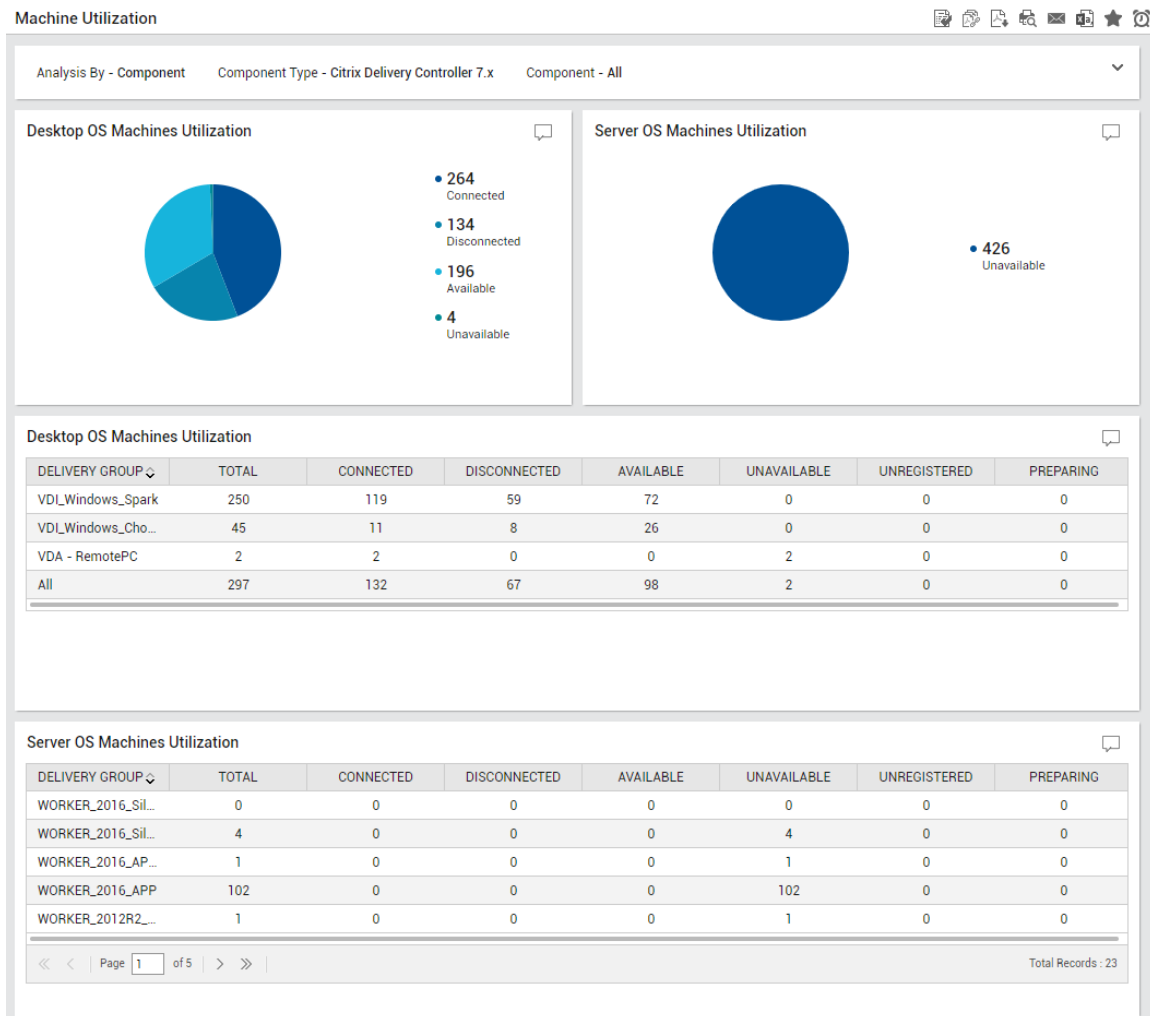


Figure 21: The Machine Utilization report

➤ **Load Evaluator Index Analytics:** A server's load index may be the aggregate of:

- Various computer performance counter related metrics, namely CPU, Memory and Disk Usage
- Session Count

The Citrix Delivery Controller computes the load evaluator index for each XenApp server it manages and uses this index to determine how suitable a Citrix XenApp worker is to receive a new user session. It is the Citrix Delivery Controller's responsibility to calculate the load index based on the aggregate of the normalized load rule indexes generated by the various load rules. As only the Delivery Controller can determine the session load, a server's overall load index is calculated on the Delivery Controller. Citrix administrators need to periodically evaluate the load on the servers managed by a Citrix Delivery group. Also, they need a historical analysis of the load on the servers to ensure that the load is uniformly balanced across all the servers. Using the Load Evaluator Index Analytics report, administrators not only obtain the historical analysis of the load but are also pointed to the server that is overloaded and the exact resource that is a constraint.

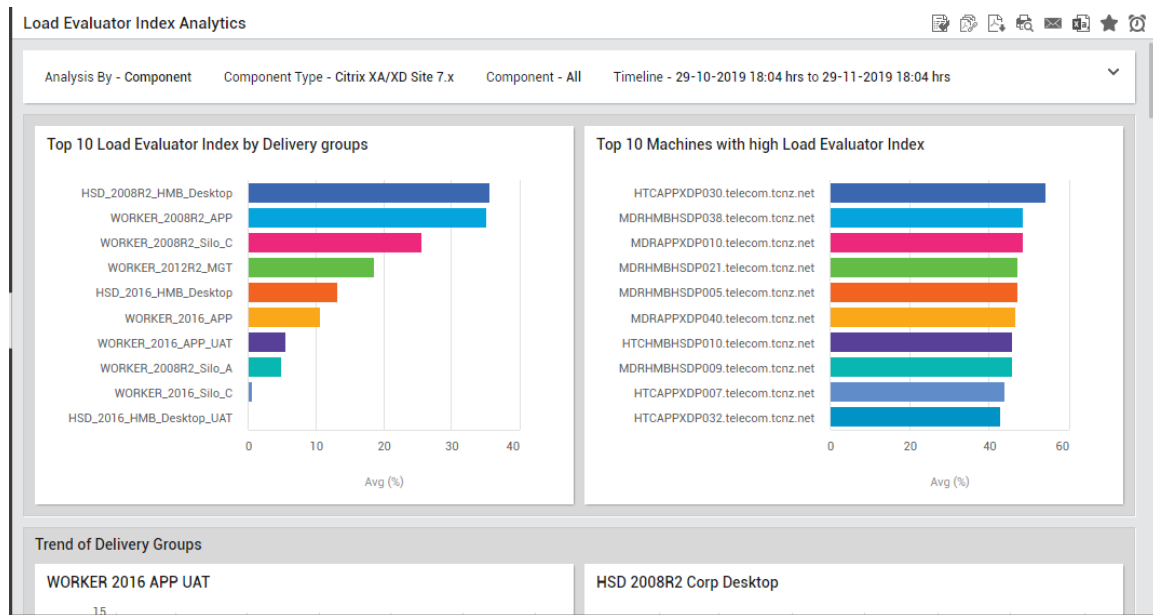


Figure 22: The Load Evaluator Index Analytics report

- **Unregistered Machines Report:** Citrix administrators often need a historical analysis of the virtual desktops that are not registered with the Citrix Delivery Controller. This historical analysis will help them in identifying the reason for this condition, the pattern of registration failure and the virtual desktops that are frequently failing. This analysis eventually helps administrators in quickly fixing the problem conditions. The Unregistered Machines report helps administrators with these details.

Details of Unregistered Machines

Report By - Component Time Period - 00:00 to 24:00 TimeLine - 26-11-2019 15:58 hrs to 26-11-2019 16:58 hrs

Unregister Machine Details

| SUMMARY | | |
|------------------------------|----|--|
| Total Unregistered Machines | 15 | |
| Total Unique Delivery Groups | 1 | |

| SERVER NAME | MACHINE NAME | DELIVERY GROUP |
|----------------|---------------------|----------------|
| capweuc16-spnz | TELECOM\EDS30825234 | VDA - RemotePC |
| capweuc16-spnz | TELECOM\EDS30826361 | VDA - RemotePC |
| capweuc16-spnz | TELECOM\EDS30873764 | VDA - RemotePC |
| capweuc16-spnz | TELECOM\EDS30878341 | VDA - RemotePC |
| capweuc16-spnz | TELECOM\EDS30881115 | VDA - RemotePC |
| capweuc16-spnz | TELECOM\EDS30881500 | VDA - RemotePC |
| capweuc16-spnz | TELECOM\EDS30881754 | VDA - RemotePC |
| capweuc16-spnz | TELECOM\EDS30882708 | VDA - RemotePC |
| capweuc16-spnz | TELECOM\EDS60001067 | VDA - RemotePC |
| capweuc16-spnz | TELECOM\EDS60001239 | VDA - RemotePC |
| capweuc16-spnz | TELECOM\EDS60001242 | VDA - RemotePC |
| capweuc16-spnz | TELECOM\EDS60001274 | VDA - RemotePC |
| capweuc16-spnz | TELECOM\EDS64000285 | VDA - RemotePC |
| capweuc16-spnz | TELECOM\SPK82030028 | VDA - RemotePC |
| capweuc16-spnz | TELECOM\SPK82030029 | VDA - RemotePC |

Page 1 of 1 Displaying topics 1 - 15 of 15

Figure 23: Unregistered Machines report

- **Machines Under Maintenance Report:** Administrators can use this report offered by eG Enterprise v7 to figure out the virtual machines /virtual desktops (belonging to a Citrix Delivery group) that were put under maintenance. This report helps administrators in identifying the Citrix Delivery group to which the virtual machine/desktop belongs to, the date on which the virtual machine/virtual desktop was put under maintenance. This report helps administrators in figuring out the delivery groups from which the virtual machines/desktops were more frequently put under maintenance.

| Machines Under Maintenance | | | |
|--|---------------------------------|----------------------------|------------|
| Report By - Component Time Period - 00:00 to 24:00 TimeLine - 26-09-2019 17:24 hrs to 27-11-2019 17:24 hrs | | | |
| Details of Maintenance Mode Machines | | | |
| SUMMARY | | | |
| Total Machines in Maintenance Mode | | 7 | |
| Total Unique Delivery Groups | | 7 | |
| SERVER NAME | MACHINE NAME | DELIVERY GROUP | EVENT DATE |
| capweuc16-spnz | XDSLWORKER02.telecom.tcnz.net | WORKER_2016_Silo_C | 27-01-2019 |
| capweuc16-spnz | XDAPPWORKER02.telecom.tcnz.net | WORKER_2016_APP_UAT | 27-01-2019 |
| capweuc16-spnz | XDMGTWORKER02.telecom.tcnz.net | WORKER_2012R2_MGT_UAT | 27-01-2019 |
| capweuc16-spnz | HTCSLCXDP006.telecom.tcnz.net | WORKER_2008R2_Silo_C | 27-01-2019 |
| capweuc16-spnz | HTCAPXPDP047.telecom.tcnz.net | WORKER_2008R2_APP | 27-01-2019 |
| capweuc16-spnz | XDHMBDESKTOP02.telecom.tcnz.net | HSD_2016_HMB_Desktop_UAT | 27-01-2019 |
| capweuc16-spnz | MDRHMBHSDT002.telecom.tcnz.net | HSD_2008R2_HMB_Desktop_UAT | 27-01-2019 |
| capweuc16-spnz | MDRHMBHSDT002.telecom.tcnz.net | HSD_2008R2_HMB_Desktop_UAT | 26-01-2019 |
| capweuc16-spnz | XDHMBDESKTOP02.telecom.tcnz.net | HSD_2016_HMB_Desktop_UAT | 26-01-2019 |
| capweuc16-spnz | HTCAPXPDP047.telecom.tcnz.net | WORKER_2008R2_APP | 26-01-2019 |
| capweuc16-spnz | HTCSLCXDP006.telecom.tcnz.net | WORKER_2008R2_Silo_C | 26-01-2019 |
| capweuc16-spnz | XDMGTWORKER02.telecom.tcnz.net | WORKER_2012R2_MGT_UAT | 26-01-2019 |
| capweuc16-spnz | XDAPPWORKER02.telecom.tcnz.net | WORKER_2016_APP_UAT | 26-01-2019 |
| capweuc16-spnz | XDSLWORKER02.telecom.tcnz.net | WORKER_2016_Silo_C | 26-01-2019 |
| capweuc16-spnz | XDSLWORKER02.telecom.tcnz.net | WORKER_2016_Silo_C | 18-01-2019 |

Figure 24: Machines under Maintenance report

- **Sessions by Delivery Groups report:** Use this report to historically analyze the session load on delivery groups, so you can quickly identify the delivery group that is the busiest in terms of the count of sessions it handles. The report also provides session-by-session details, with the help of which you can identify:
 - the user who has initiated the maximum number of sessions;
 - the machines that were accessed most frequently during the given period, the delivery group to which the machines belong, and the server hosting each machine;
 - the user responsible for the longest session, the machine to which that user connected, and the client from which that connection was established;

The report also graphically represents the usage of delivery groups by the start time of sessions. Using this representation, you can easily figure out if an unusual/abnormal number of sessions was suddenly initiated on delivery groups during the chosen period, and if so, at what time exactly this anomaly occurred. This sheds light on suspicious user accesses.

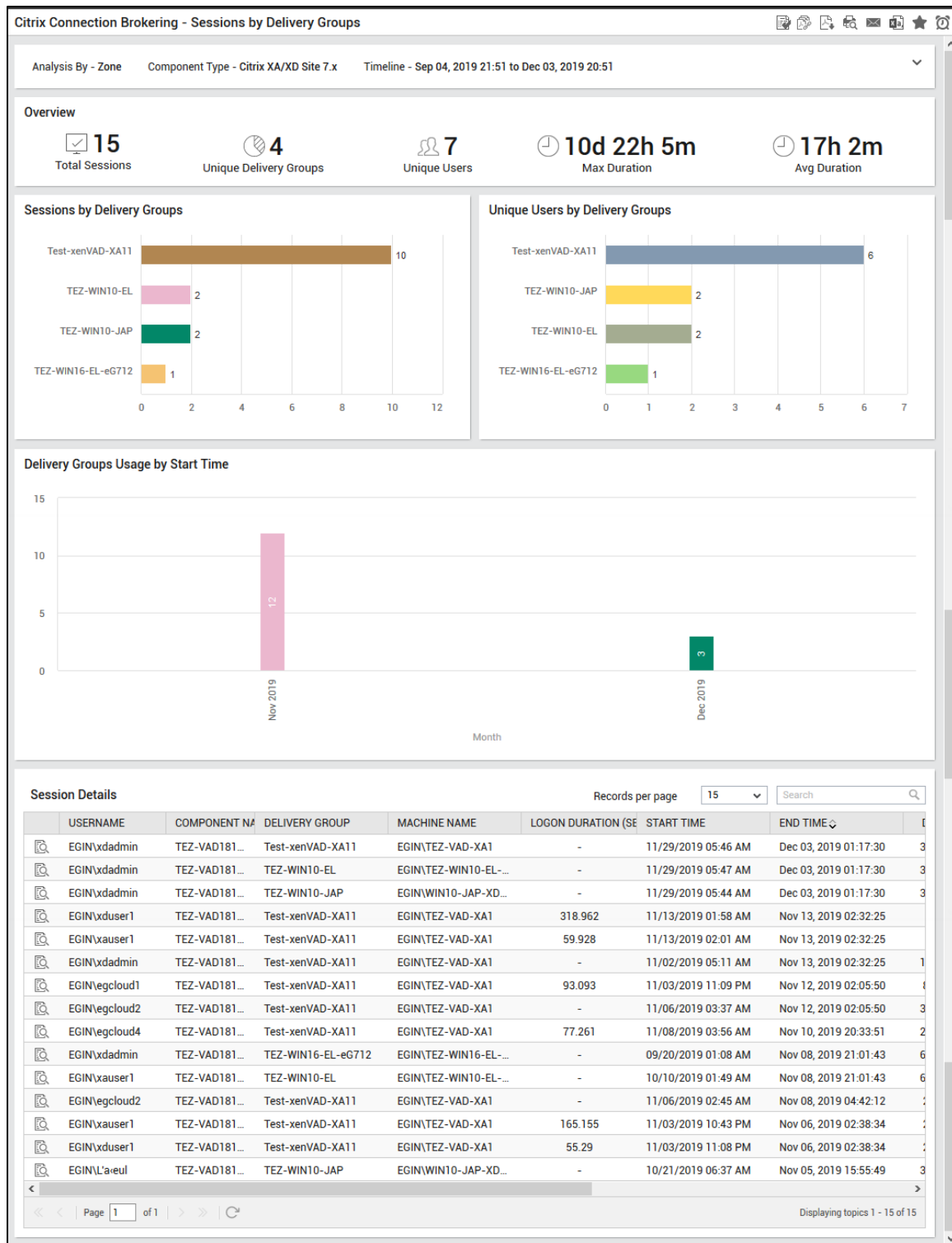


Figure 25: The Sessions by Delivery Groups report

- **Optimization of Sessions by Users Report:** In previous versions, the Sessions by Users Report (formerly, User Sessions Details Report) used to pull out the Citrix user logon and logoff details directly from the eG backend database. In Citrix environments where user sessions were always high, the report generation took longer than usual since the data was stored in the database across


multiple tables. To optimize the time taken for report generation, starting with eG Enterprise 7, the Citrix user logon and logoff details pertaining to this report are stored in a separate table in the eG backend database. The report when generated uses the data from the table and hence the report is generated at a faster pace.

3.2 VMware Horizon Monitoring Enhancements

3.2.1 VMware Horizon Logon Simulator

Following are the enhancements that have been made to the VMware Horizon Logon Simulator:

- **Troubleshooting logon failures made easy:** The eG Logon Simulator for VMware Horizon presents a graphical view of the logon process, which helps administrators quickly and accurately identify the exact step of the logon process that caused slowness. This graphical representation has been enhanced in v7, so that it not only points administrators to where the bottleneck is, but also reveals in a single click, what caused the bottleneck!

In this version, the simulator automatically takes screenshots of failure conditions and displays them in the graphical view. To this effect, an  icon is introduced against the step that has failed or is sluggish. Clicking on this icon reveals the screenshot that was taken at the time of the failure, so administrators can instantly determine what error caused the failure and easily figure out how to fix it.

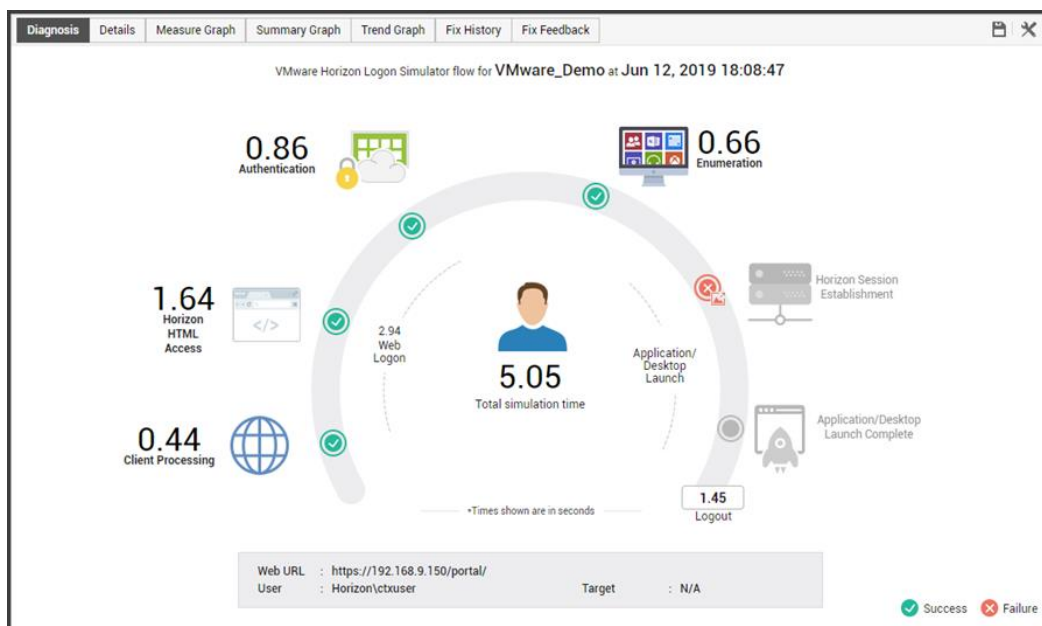



Figure 26: The icon that is used to trace the transaction failures

These screenshots can also be accessed from the layer model view. The measure reporting a failure is accompanied by a  icon, which will lead administrators to the screenshot that was captured

during failure.

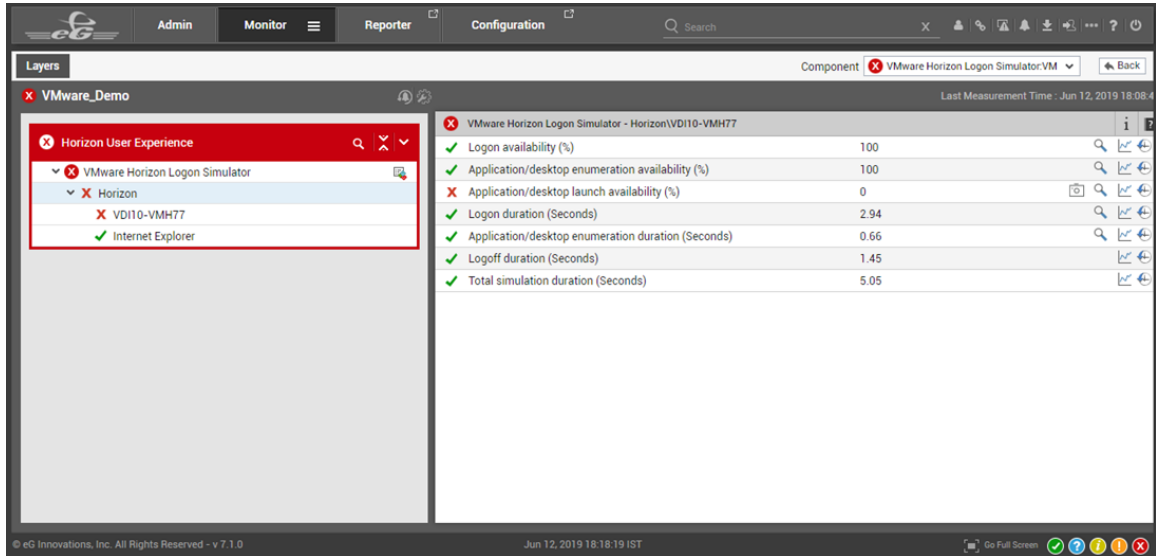


Figure 27: The screenshot icon that appears in the layer model

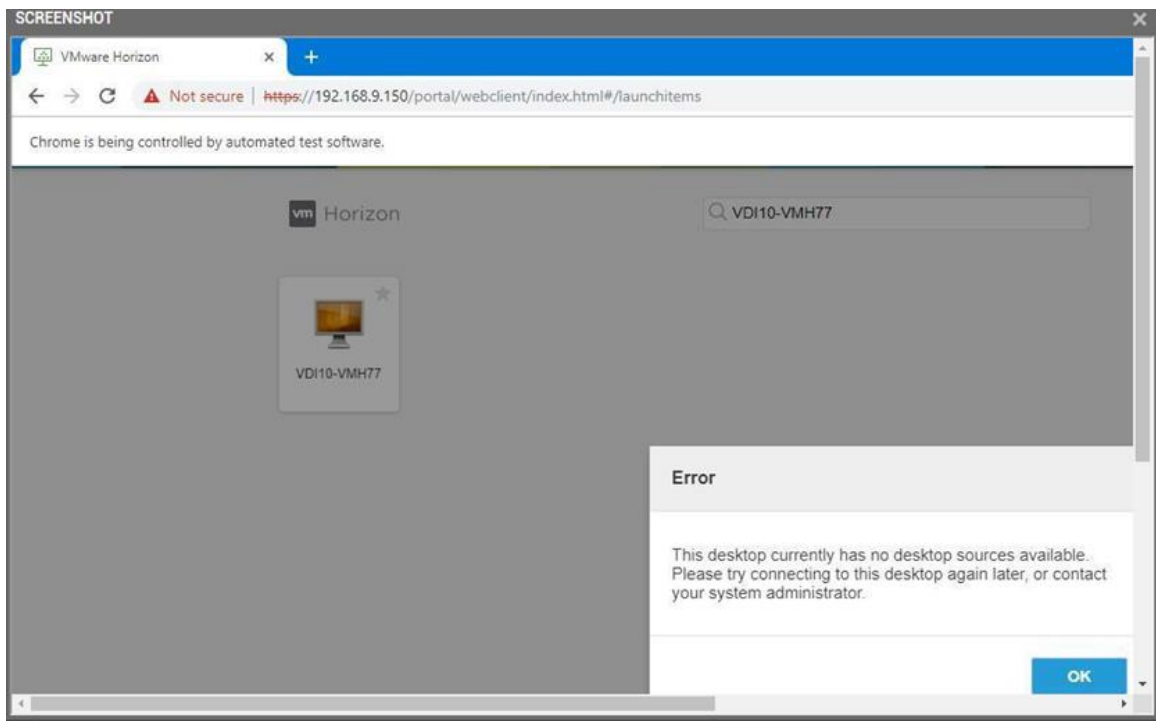


Figure 28: The screenshot captured during transaction failure

3.2.2 VMware Horizon Monitoring Enhancements

eG Enterprise v7 adds several enhancements for VMware Horizon monitoring:

- **Identifying desktops created using Instant Clone Technology:** Instant Clone Technology is all about facilitating faster delivery of desktops by allowing administrators to rapidly clone and deploy

a virtual machine. eG Enterprise v7 is capable of reporting if the desktop provisioned by the VMware Horizon Connection server is created using Instant Clone or a Linked Clone.

- **Deprecating session related metrics for VMware Horizon Connection Server when the server is in high availability mode:** By default, eG Enterprise monitors the VMware Horizon Connection Server that was installed with the roles of Standard Server, Replica Server and Security Server. In environments where multiple VMware Horizon Connection Servers are installed in a cluster setup, for the very purpose of load balancing, there will be multiple Replica Servers connected to the Standard Server. One of the Replica Server will automatically act as a Standard Server whenever the Standard Server is down. During such change over, session related metrics could not be captured and reported based on the changed server in versions prior to eG Enterprise 7. In order to report accurate session related metrics in high availability installations, starting with eG Enterprise v7, session related metrics are captured and reported only for the VMware Horizon Connection Server that takes up the role of a Standard Server. If administrators wish to view the session related metrics for all the other servers in the high availability setup, then, administrators can use the VMware Horizon Pod component offered by eG Enterprise.
- **Monitoring VMware App Volumes Manager:** VMware App Volumes is a real-time application delivery system that enterprises use to dynamically deliver and manage applications. Applications are bundled in AppStacks and delivered by attaching a standard VMDK file to a virtual machine. Where VMware App Volumes is used, any issue in the health of App Volumes or AppStacks can deny users access to business-critical applications. To avoid this, eG Enterprise 7 closely monitors the VMware App Volumes Manager - a Web-based interface used for centrally managing the applications delivered via VMware App Volumes. Using this eG Monitor, administrators can accurately isolate problematic AppStacks, Writable Volumes and the App Volumes. eG Enterprise also provides the availability and response time of the VMware App Volumes Manager round the clock so that administrators can detect the non-availability of the VMware App Volumes Manager before end users notice and initiate corrective measures. The license validity of the VMware App Volumes Manager is also monitored and the users who are currently using the licenses are enumerated. Each datastore of the VMware App Volumes Manager is also monitored and the datastore that is running out of space is pinpointed.
- **Monitoring of VMware Horizon Pods:** A VMware Horizon Pod is a collection of View Connection Server instances. A pod also consists of shared storage, a database server, and the vSphere and network infrastructures that host desktop and application pools. The primary goal of a pod is to load-balance connections to a site/datacenter and to ensure the high availability of the VDI infrastructure through fail-over capabilities. This means that performance issues in a pod can deny/delay users access to their desktops. To prevent this, 7 provides deep dive visibility into the performance of a pod. The eG Monitor for the VMware Horizon Pod reports the status of each connection server instance in a pod, pointing you to unavailable/disabled instances. The status and usage of desktop/application pools managed by a pod are also reported, so that over-utilized pools and those that are in an abnormal state are highlighted. The session load on each pool is monitored, and load-balancing irregularities are brought to light.
- **Simplified presentation of inside view metrics for VMs and virtual desktops:** In previous versions, administrators had to endlessly scroll the Measures tab page to view the inside view metrics of a VM or a virtual desktop. Though necessary information was available, it was tedious for the administrators to instantly obtain the required information. To ease the pain of the administrators and simplify the data presentation in the user interface, starting with eG Enterprise v7, all the inside view metrics are grouped and displayed in separate tabs. Clicking on the tabs enables administrators to view the metrics of their interest with ease. Administrators are also provided the capability to view the inside view metrics of any virtual desktop user from the Measures tab page.

3.2.3 Enhancements to VMware Identity Manager Monitoring

VMware Identity Manager is a service that extends your on-premises directory infrastructure to provide a seamless Single Sign-On (SSO) experience to Web, Mobile, SaaS, and legacy applications that may be consumed as a service or downloaded and installed on premises. With VMware Identity Manager, administrators give users a way to access a "self-service catalog" of approved applications and desktops in a secure manner from a variety of devices. It eliminates the possibility for users to sign on from unsecure devices and accessing important and possibly confidential documents and information.

eG Enterprise already had monitoring support for VMware Identity Manager. This monitoring capability has been enhanced to report the count of users and groups created on the VMware Identity Manager. The count of applications and devices accessed by the users via the VMware Identity Manager are also reported. Administrators can identify the applications/desktops that were launched by the users through the VMware Identity Manager. Administrators can also determine which application/desktop failed to launch frequently and start probing the reasons behind frequent launch failures. Administrators are also alerted to different types of failure events (login failures, launch failures, directory sync failures, password resets etc.) that arise when applications/desktops are accessed through the VMware Identity Manager.

3.2.4 VMware Reporting Enhancements

Following are the reports that have been included in eG Enterprise v7 for in-depth analysis in environments where VMware App Volumes Manager is used to provision desktops/servers:

- **VMware App Volumes - License Utilization Report:** In virtual environments where the VMware App Volumes Manager is used to deliver applications to the users, application delivery mainly depends on the license type of the VMware App Volumes Manager. The App Volumes are licensed based on named users or concurrent users in the target environment. Often, administrators have to track the utilization of the licenses in the environment, figure out if there are adequate licenses and check the validity period of the license so that license issues will not hamper the functioning of the server in the target environment. To keep tab on the license utilization of the VMware App Volumes Manager, eG Enterprise v7 offers a License Utilization Report. This report will help administrators in figuring out the validity of the license, the count of licenses utilized by the users, terminal users, desktops and the servers accessing the VMware App Volumes Manager. The user utilization and computer utilization trend over time is analyzed and any spurt in users and desktops are identified. The AppStacks available in the App Volumes Manager analyzed over a period of time and the trend noticed in users accessing the AppStacks is determined.



Figure 29: The VMware App Volumes – License Utilization report

- **AppStack Details Report:** Administrators can use this report offered by eG Enterprise v7 to analyze the trend/behavior noticed in the access of AppStacks, determine which users are accessing the AppStacks and which applications are attached to the AppStacks. This report helps administrators in understanding the applications that are frequently used by the users by accessing the AppStacks. Additionally, this report is more useful to figure out the users who are accessing the AppStacks and helps in determining which users will be impacted the most if the frequently accessed AppStacks encountered problems.

VMware App Volumes - AppStack Details

Report By - Zone

Zone - --Default--

Component Type - VMware App Volumes Manager

Components - All

AppStacks Details

| APPSTACKS NAME ^ | STATUS | NUMBER OF APPLICATIONS | ASSIGNMENTS TO USER (NUMBER) | ATTACHMENTS (NUMBER) | SIZE (MB) | DATASTORE NAME | MOUNT COUNT | LAST MOUNTED DATE | CREATED DATE |
|------------------|---------|------------------------|------------------------------|----------------------|-----------|----------------|-------------|-------------------|--------------|
| Browsers | - | - | - | - | 142 | eGVNXE-Lun22 | 30 | Dec 02 2019 | Nov 24 2019 |
| Browsers | Enabled | 2 | 1 | 1 | - | - | - | - | - |
| APPLICATION NAME | | VERSION | | PUBLISHERS | | ASSIGNABLE | | ATTACHED DATE | |
| FireFox 60 | | 60.1 | | - | | false | | Dec 02 2019 | |
| Google Chrome | | 72.0.3626 | | - | | false | | Dec 02 2019 | |
| USER | | | | | | | | | |
| chn\keith | | | | | | | | | |
| Editors | Enabled | 2 | 2 | 2 | 123 | eGVNXE-Lun24 | 57 | Dec 02 2019 | Nov 22 2019 |

Figure 30: The VMware App Volumes – AppStack Details report

- **VMware App Volumes User Details Report:** Use the App Volumes User Details report offered by eG Enterprise v7 to analyze the space consumed by each user from the assigned Writable volumes, detect the variations in the volume mount count periodically and determine the state of the writable volumes over a period of time. This report will help administrators in identifying the times during which the writable volumes were detached from the user.

| USER | FULL NAME | VOLUME TOTAL STORAGE SPACE (MB) | USED SPACE (MB) | FREE SPACE (MB) | VOLUME MOUNT COUNT | TOTAL USER LOGIN COUNT | ATTACHMENTS | USER LAST LOGIN TIME | WRITABLE VOLUME STATE |
|------|-----------|---------------------------------|-----------------|-----------------|--------------------|------------------------|-------------|----------------------|-----------------------|
| Jeff | Johanson | 10236 | 1213 | 9023 | 43 | - | - | - | Attached |

Figure 31: The VMware App Volumes User Details Report

- **AppStacks Assigned to Users Report:** To periodically check which AppStacks are assigned to which users and which VMware App Volumes Manager is being used for the assignment, administrators can use the AppStack and User Attachment report offered by eG Enterprise v7. This way, administrators can instantly identify which users and AppStacks will be impacted if an App Volumes Manager fails.

VMware App Volumes - AppStacks Assigned to Users

Analysis By - Zone

Component Type - VMware App Volumes Manager

Timeline - Nov 25, 2019 06:21 to Dec 02, 2019 06:21

User AppStacks Details

| USERNAME | NUMBER OF APPSTACKS ASSIGNED | | | | | | | | | |
|--|------------------------------|---------------------|---------------|-------------------|----------|---------------------|-------------------|---------|---------------------|--|
| chn\keith | 2 | | | | | | | | | |
| <table><thead><tr><th>APP VOLUME MANAGER</th><th>APPSTACKS</th><th>ASSIGNED TIME</th></tr></thead><tbody><tr><td>ny_app_vol_mgr_01</td><td>Browsers</td><td>Dec 02 2019 06:19AM</td></tr><tr><td>ny_app_vol_mgr_01</td><td>Editors</td><td>Dec 02 2019 05:31AM</td></tr></tbody></table> | APP VOLUME MANAGER | APPSTACKS | ASSIGNED TIME | ny_app_vol_mgr_01 | Browsers | Dec 02 2019 06:19AM | ny_app_vol_mgr_01 | Editors | Dec 02 2019 05:31AM | |
| APP VOLUME MANAGER | APPSTACKS | ASSIGNED TIME | | | | | | | | |
| ny_app_vol_mgr_01 | Browsers | Dec 02 2019 06:19AM | | | | | | | | |
| ny_app_vol_mgr_01 | Editors | Dec 02 2019 05:31AM | | | | | | | | |
| chn\sandy | 1 | | | | | | | | | |
| <table><thead><tr><th>APP VOLUME MANAGER</th><th>APPSTACKS</th><th>ASSIGNED TIME</th></tr></thead><tbody><tr><td>ny_app_vol_mgr_01</td><td>Editors</td><td>Dec 02 2019 11:37AM</td></tr></tbody></table> | APP VOLUME MANAGER | APPSTACKS | ASSIGNED TIME | ny_app_vol_mgr_01 | Editors | Dec 02 2019 11:37AM | | | | |
| APP VOLUME MANAGER | APPSTACKS | ASSIGNED TIME | | | | | | | | |
| ny_app_vol_mgr_01 | Editors | Dec 02 2019 11:37AM | | | | | | | | |

Figure 32: The VMware App Volumes – AppStacks Assigned to Users Report

Following are the reports that have been included in eG Enterprise v7 for in-depth analysis of VMware Horizon environments:

- **User Connection Failures Report:** Failures when connecting to virtual desktops have a very adverse effect on user experience. Administrators should promptly identify such failures and rectify them at the earliest so that the user experience does not suffer. By knowing why a failure happened, administrators can determine quickly how to rectify the failure. The User Connection Failures report helps administrators in this regard. Using this report, administrators can historically analyze the user connection failures by event type or by desktop pool. They can see the failure count for each event type, and also determine the details of when exactly the desktop failed, the event message, node name, desktop ID, etc. for each failure. For instance, if a large number of bad password related failures have happened, this could indicate that some form of attack has been attempted. On the other hand, failures because of pool overload may indicate that the desktop pool is being heavily used and additional desktops may be needed in the pool to handle the workload it is receiving.

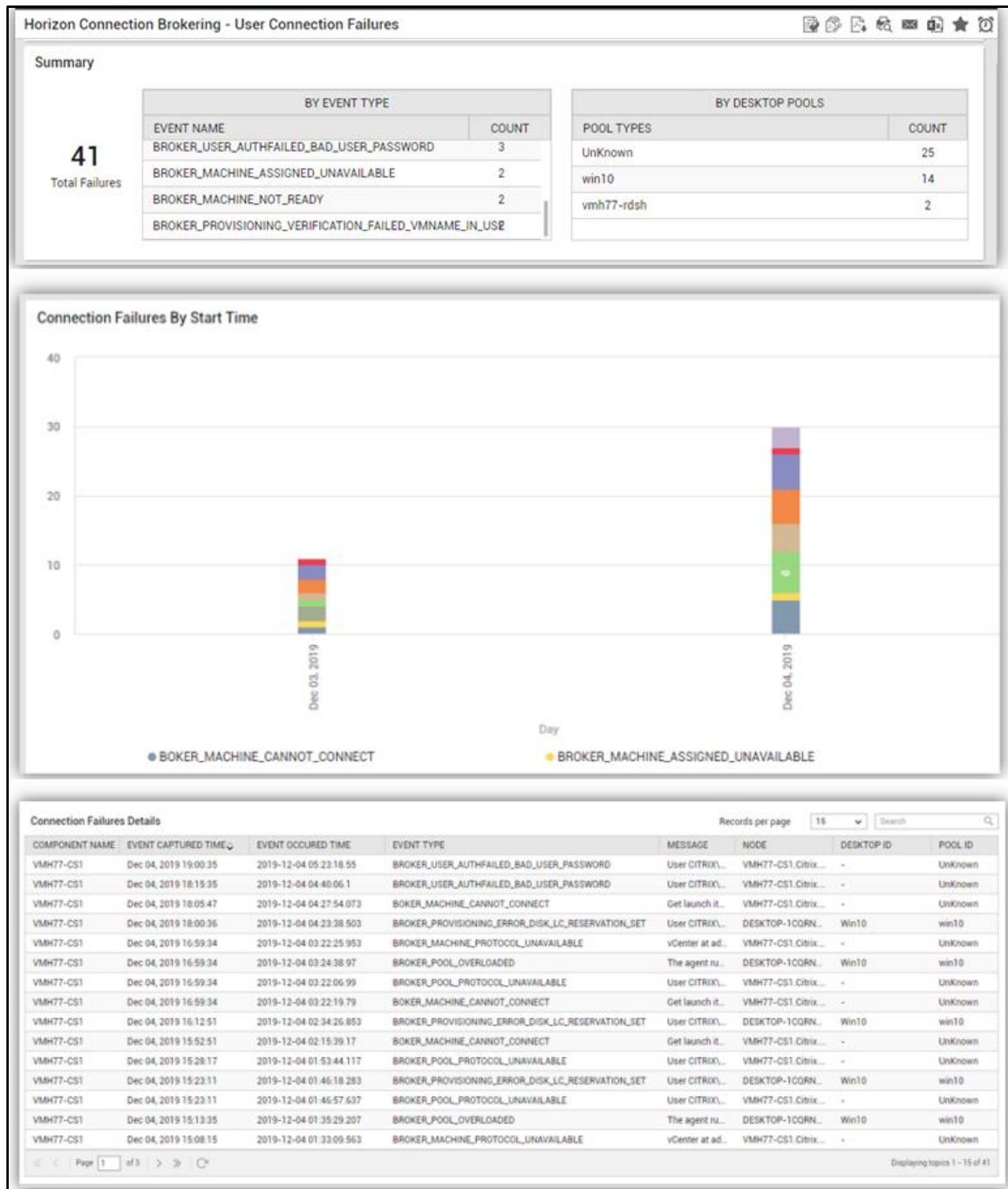


Figure 33: The Horizon Connection Brokering – User Connection Failures Report

- **Long-Running Sessions Report:** In virtual desktop environments where effective management of the resources is vital, the users logging into the virtual desktops are expected to utilize the sessions optimally. When more user sessions are initiated with the available resources, users may feel a lag in their sessions. This is due to minimal resources available to them for accessing the applications. Administrators of such environments must identify the users who have initiated the sessions longer than the usual time and figure out if they are genuinely accessing the applications or are just idle and consuming the resources alone. The **Long-Running Sessions** report helps administrators identify such users who have initiated longer sessions. The total sessions initiated in the environment

and the sessions that are running for a longer duration are highlighted. The concurrent user sessions and the long running sessions are identified on a day to day basis so that administrators can figure out the date/time on which too many long sessions and concurrent sessions have been initiated.

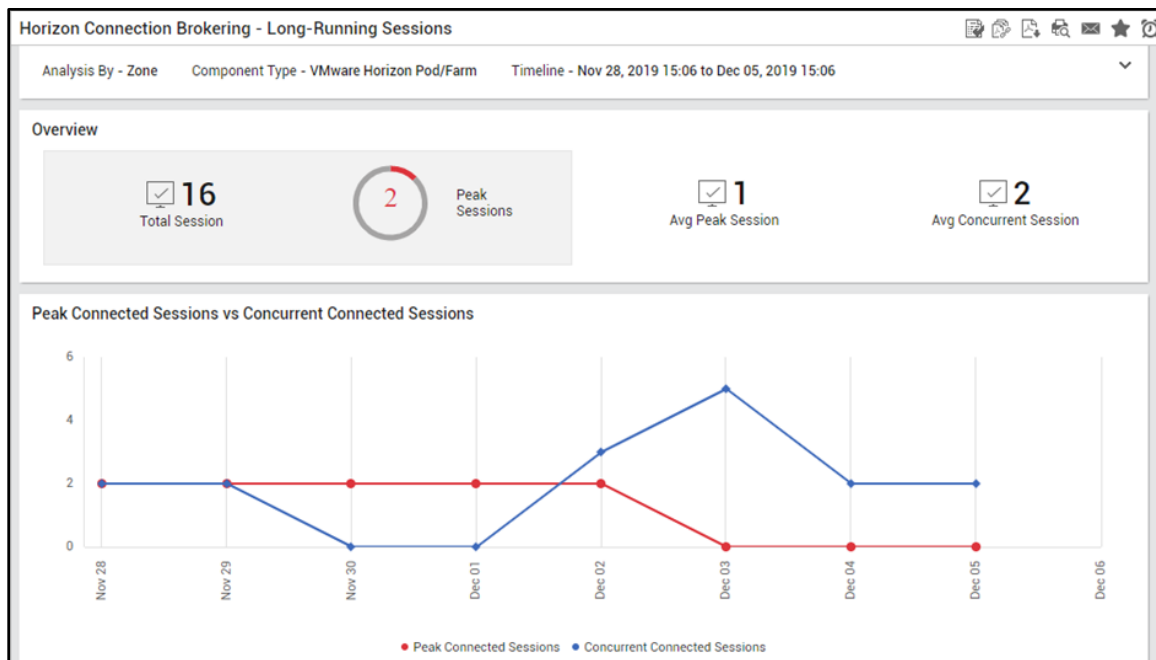


Figure 34: The Horizon Connection Brokering – Long-Running Sessions report

- **Sessions by Desktop/App Pools Report:** Administrators can use this report offered by eG Enterprise v7 if they want to historically analyze all Horizon sessions. Comparing session activity by pool, indicates the pools that are receiving the highest workload.

Administrators can also analyze session start time metrics by protocol type. This may shed light if session start up slowness is limited to specific protocols.

Details of sessions by desktop/app pools provide who accessed the desktop/app, when, using what protocol and host, etc. This information is required for auditing accesses to the Horizon farm.

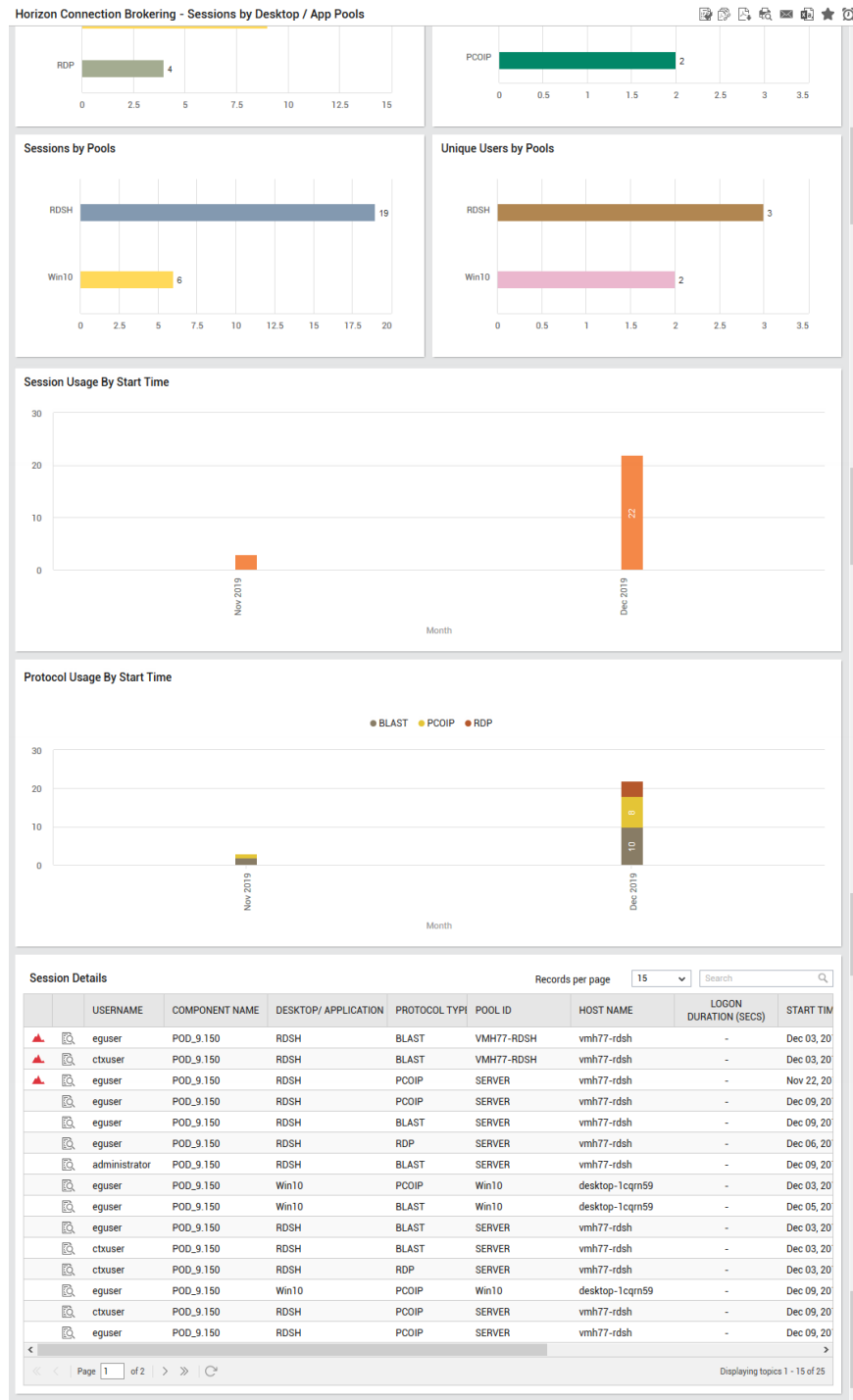


Figure 35: The Horizon Connection Brokering – Sessions by Desktops / App Pools report

4. Web Application Performance Monitoring

4.1 Synthetic Monitoring Capability for Web Applications

- **Web App Simulation:** As IT infrastructures evolve into being business-critical, high availability and peak performance of the IT infrastructure is also becoming very critical. In today's modern age of digital transformation and cloud deployments, it is essential to proactively monitor the user experience of web applications in IT infrastructures which are into competitive business services such as eCommerce. Frequent slowness or downtime of the web applications may directly impact the user experience which will in turn affect the business in terms of production and revenue. To improve the user experience on such web applications, eG Enterprise v7 has a purpose-built tool named a Web App Simulator. This tool comprising a Web App Simulation Recorder and a Web App Simulation Playback Engine is an easy to use record and playback tool, which can be used to simulate web application access.

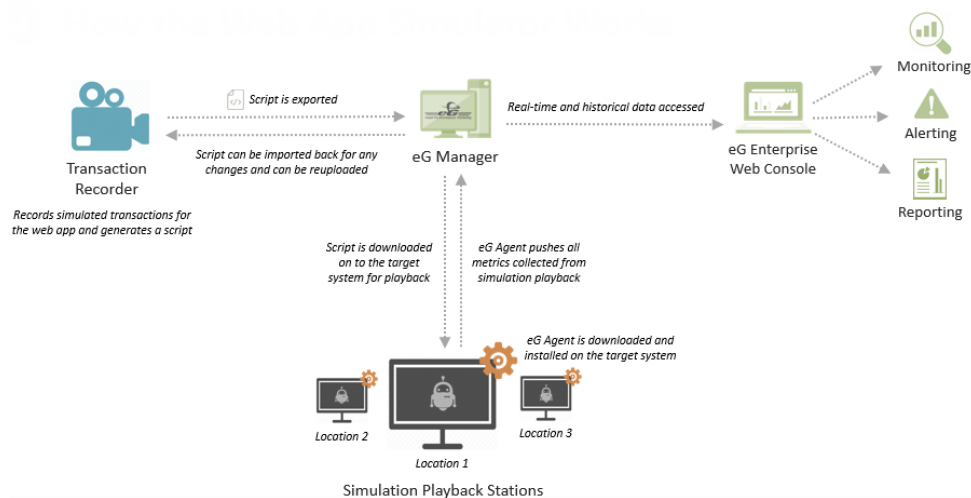


Figure 36: The architecture of the Web App Simulator

The Web App Simulator Recorder is used to record the script by emulating the transactions on the web application, and this script will be played back at periodic intervals to collect the required metrics.

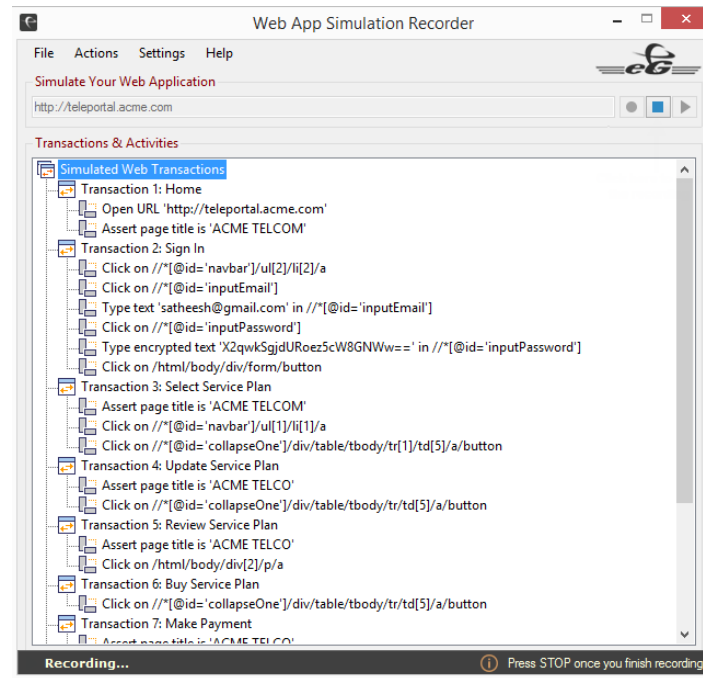


Figure 37: The Web App Simulation Recorder

The Web App Simulator is a standalone desktop tool that is packaged with the eG agent and is installed on the computer/VM from where the simulation will happen.

The Web App Simulation Playback Engine is an executable that is bundled with the eG Agent and is installed on remote locations from where the simulation playback happens. The Web App Simulation Playback Engine runs the script and executes the simulation playback based on the test frequency configured in the eG Manager.

A specialized monitoring model named Web App Simulation has been built by eG Enterprise to periodically playback the simulations and collect the required metrics. In the process, the success/failure of the simulation and the time taken for each transaction in the simulation are tracked and reported.

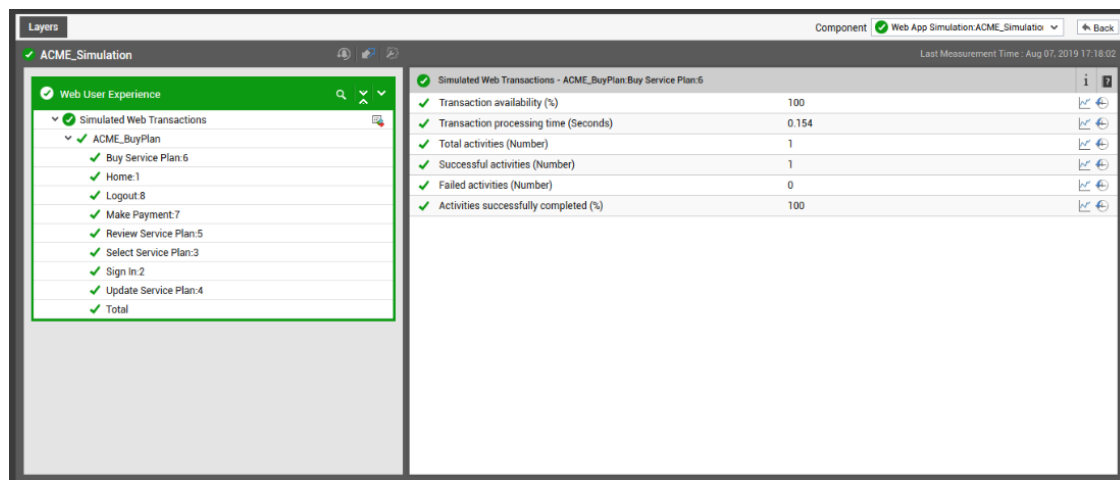


Figure 38: Measures reported by simulating the web transactions

Using the results, administrators can identify times when slowness was detected and they can clearly see why – is it due to abnormal transaction processing time or is it due to abnormal simulation time or is it due to an increase in the count of activities that failed for the transactions. Since the simulation is done periodically, the Web App Simulator can alert administrators to potential issues proactively.

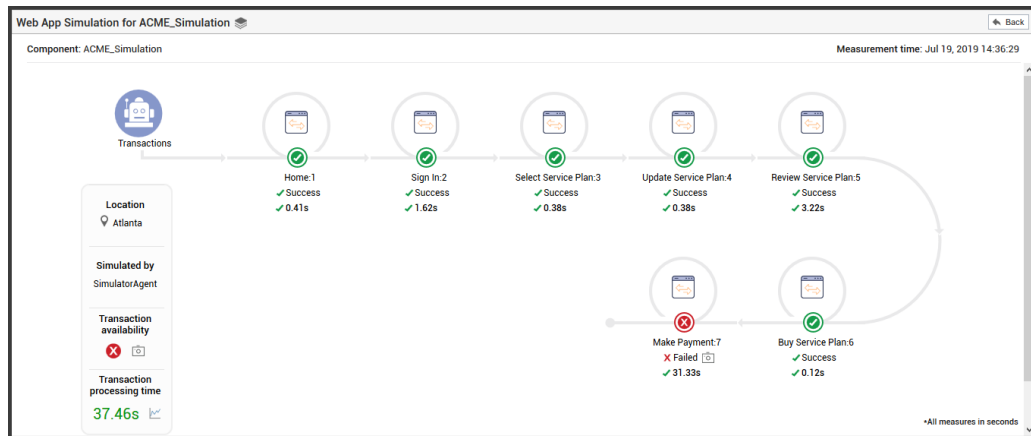


Figure 39: The transaction flow graph

eG Enterprise v7 also includes a brand-new report based on the results of Web App Simulation named the Web App Simulation Report. This report allows application teams to understand simulation trends over time and identify bottlenecks for a given period of time.

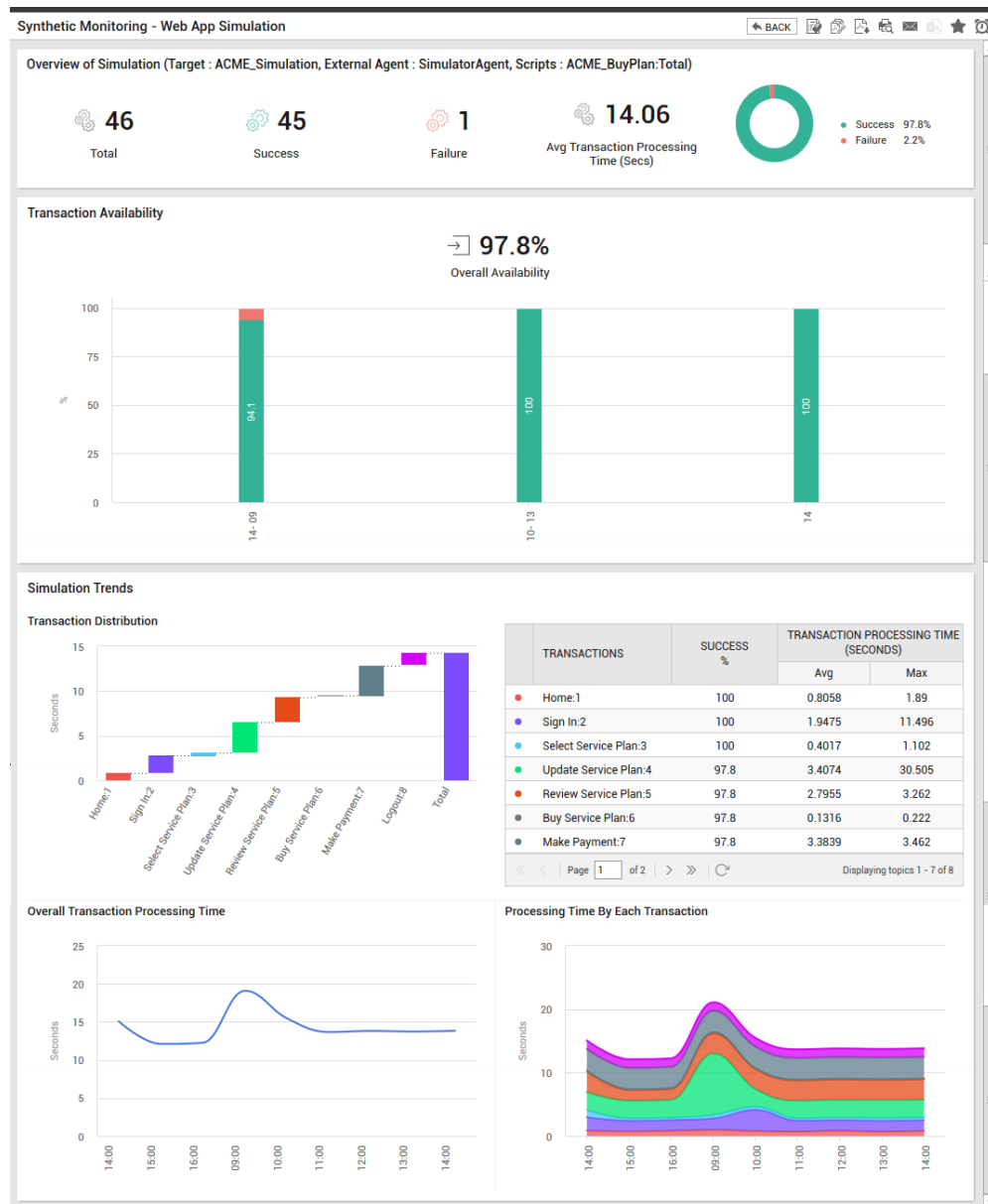


Figure 40: The Web App Simulation report

- **New Dashboards introduced for Protocol emulation:** In today's world where IT administrators need to resolve issues at a faster pace to keep hold of the business, it is necessary for the administrators to monitor the applications end to end. This type of monitoring is done from an external perspective. Administrators may often get complaints regarding slow access to certain pages in the target environment. This may not be due to the issues with the applications but may be due to the protocol (HTTP/HTTPS, TCP, FTP, MAPI, Network) that is used for accessing the application. It is therefore necessary for the administrators to monitor the accessibility and responsiveness of the applications over a protocol. Protocol emulation, one of the ways of external monitoring is a technology that mimics a network/application protocol's behaviour to test the availability / performance of real applications. Administrators need to use the protocol emulation technique to periodically measure the QoS of real applications from an external perspective (for e.g., from a client's perspective) and figure out accessibility and latency issues if any, much before end users experience them. By default, eG Enterprise monitors the availability and responsiveness of the server/

application from an external perspective and reports metrics. In environments where multiple servers/ applications are monitored, administrators had to traverse between multiple pages to check for the availability and responsiveness. To ease the pain of the administrators, eG Enterprise v7 has introduced a Synthetic Monitoring dashboard where administrators can view the metrics obtained via protocol emulation of all the servers/applications in a single page. The new user interface, dashboards and historical reports provide real-time and historical insights about protocol performance to the administrators.

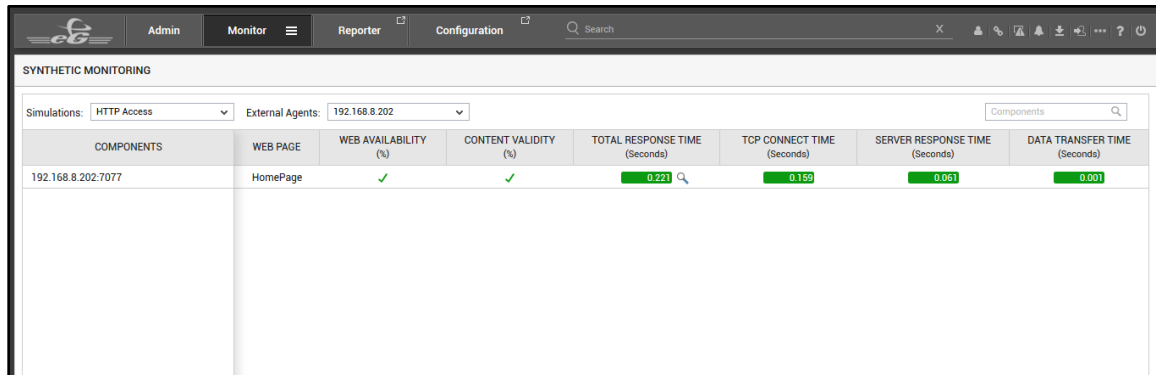


Figure 41: The Synthetic Monitoring dashboard that appears when the HTTP Access simulation is chosen

- **New Reports introduced for Protocol emulation:** Following are the reports that have been included in eG Enterprise v7 to provide real-time and historical insights about protocol performance:
 - Network Access
 - HTTP Access
 - Oracle Performance
 - SQL Performance
 - Client Session Simulation

4.2 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.

- **In depth visibility into Web page load time and network time:** In version 7, the eG Real User Monitor has been enhanced to provide more granular metrics on page load time, so that administrators can accurately deduce the root-cause of slow page views.

For instance, in this version, eG RUM reports the time requests spent at the browser end, and thus enables administrators to understand how browser activities can impact overall page load time. Additionally, eG RUM breaks down browser time further based on browser-side activities such as redirection, App caching, and resource fetching. With the help of this break-up, administrators can accurately isolate which browser activity is affecting user experience. Likewise, in v7, the average time spent in SSL handshakes is reported as an additional component of network 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, and thus enables precise root-cause diagnosis.

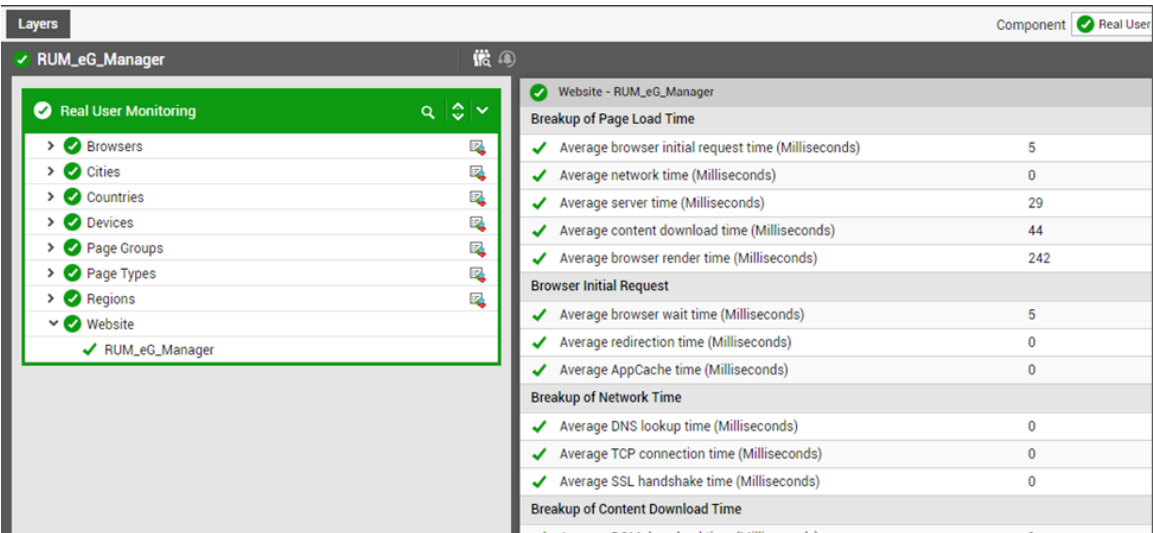


Figure 42: Additional metrics showing the breakup of page load time and network time

- **Enhancements to RUM Transaction Topology:** The eG Real User monitor is now capable of showing the name of the user who is currently accessing the monitored web page as part of the RUM transaction topology. The eG Real User Monitor captures the name of the user if the website that is being monitored requires the user to login with valid user credentials. Alternatively, if the eG Real User Monitor is used alongside eG's Java/.Net Business Transaction Monitor (BTM), then the name of the user is retrieved from the detailed diagnostics offered by eG BTM.

In previous versions, if a web page took too long to load, administrators drilled down the detailed diagnostics offered by eG Enterprise to view the load time of each resource in that page that was accessed. This enabled the administrators to identify the exact resource that was delaying the content download from the RUM Transaction flow diagram. Though the administrators obtained the overall browser time taken for downloading and displaying the content, they were not able to figure out when exactly delays were noticed in the browser - whether during the initial request to the browser or when the browser response was serviced for the request. To accurately pinpoint the when exactly browser delays were noticed, eG Enterprise v7 provides a granular split up of the browser time into Browser Initial Request time and Browser Response time.

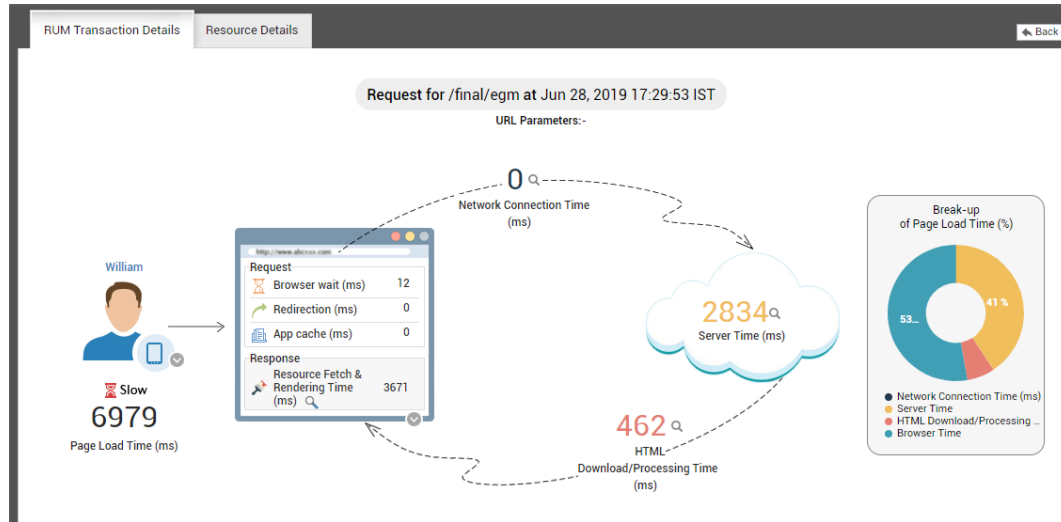


Figure 43: The name of the user and breakup of browser time taken to load the contents of the page

Sometimes, the requested page may load longer than usual. This may be due to the resources of the page being downloaded each time during page load instead of being served from the browser cache. To identify the CSS or JavaScripts that are causing such delayed load time, eG Enterprise v7 has introduced a Resource Details Tab in the RUM Transaction flow diagram. Clicking the magnifying glass icon against the HTML Download/Processing Time measure in Figure 40 will lead you to the Resource Details tab where users can view a detailed breakdown of the time taken to load every resource on the web page. By carefully analyzing the resources, administrators can figure out the resources that need to be minified so that page load is faster.

- **RUM Topology for AJAX Web Pages:** Starting with eG Enterprise v7, page load time breakdown and topology is now supported for AJAX web pages also.

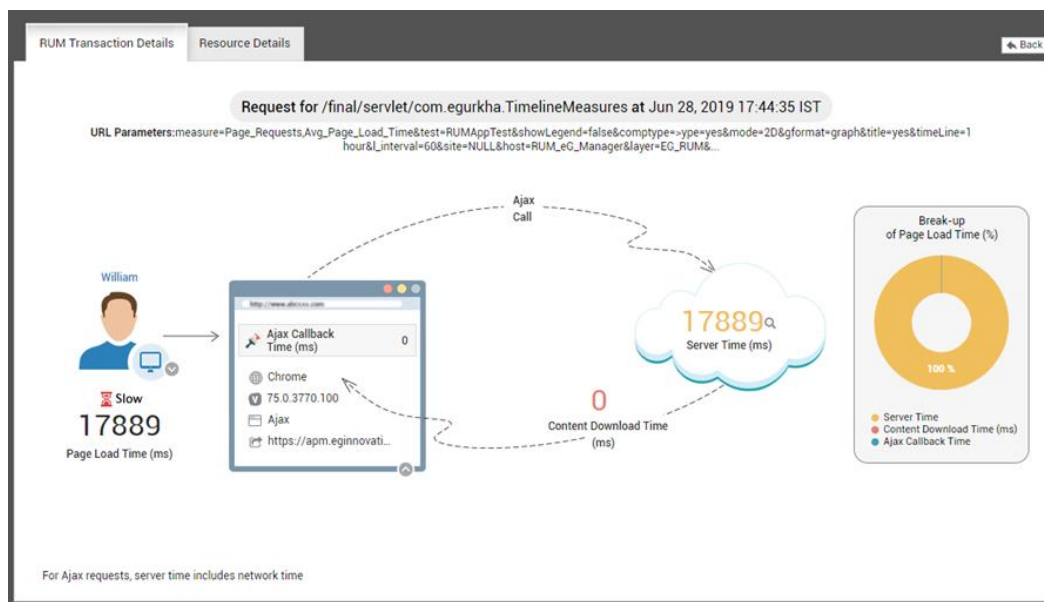


Figure 44: The RUM Topology for AJAX Web pages

- **Monitoring Page load time of Single Page Applications:** A Single Page Application (SPA) is a web application or website that loads all the resources required to navigate throughout the site on

the very first time the page loads. As the user clicks links and interacts with the page, subsequent content will be loaded dynamically. A perfect example of the Single Page Application is a mobile application with a scorecard or stock ticker where the content of the page refreshes without refreshing the URL. Starting with eG Enterprise v7, the eG Real User Monitor supports a new page type called Virtual Page which allows monitoring transactions to a SPA. eG Enterprise will not show the topology and breakdown of page load time for requests of such applications. Drilling down to the detailed diagnosis shows will help administrators identify the transactions that are healthy, slow, or error prone.

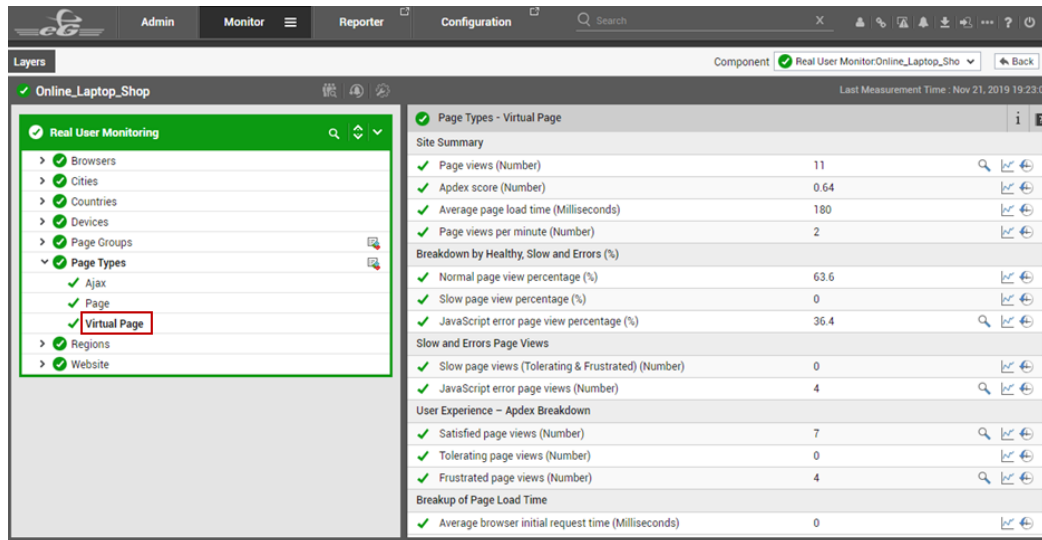


Figure 45: Monitoring the page load time of Single Page Applications (SPA)

- **Improved RUM Dashboard:** With version 7, administrators have a fluid, multi-dimensional RUM Dashboard at their disposal! On demand, this new, improved dashboard presents to you that perspective to user experience that you choose! For example, if you want to analyze the experience of your web site users from different geographies, then you can click the Geo icon in the left panel of the RUM dashboard. The Geo Map that is available as part of this view is also capable of displaying user experience data pertaining to the country of your choice.

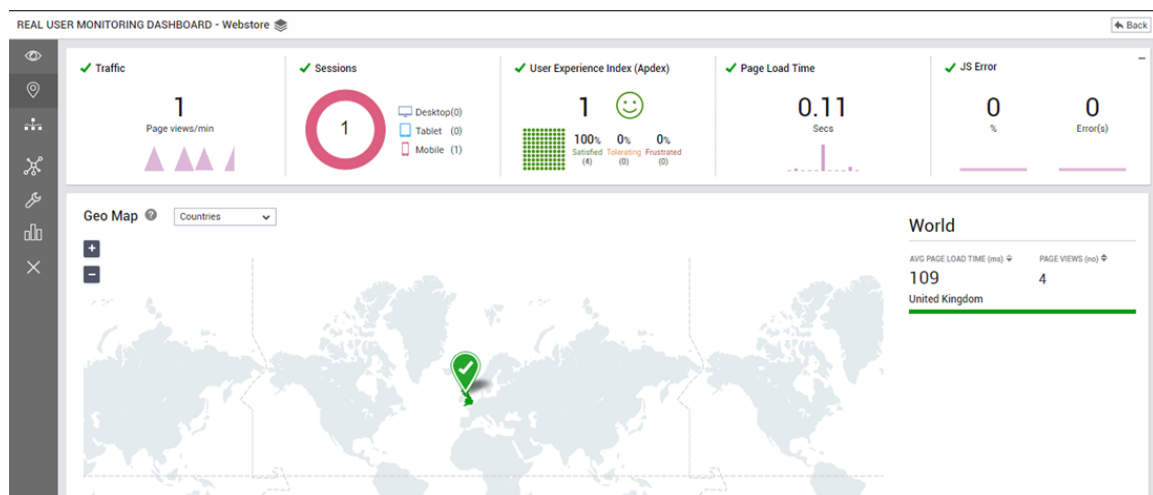


Figure 46: The improved Geo RUM Dashboard allowing to choose different countries

Similarly, if you want a quick summary of the experience of the different device users or page groups, then use the Omni channel option. Likewise, you can easily toggle the icons in the left panel of the dashboard to closely study Response Time Breakup, analyze Usage trends, check the health of individual Page View requests in real-time, or keenly focus on Errors. By default, however, the dashboard provides an overview of user experience with a target web site/application, pointing you to those countries and page groups that have been consistently experiencing slowness. As part of this default view, the dashboard also provides an all-new, web site-level break-down of page load time, across all URLs in the target web site. This serves as a good indicator of where problems lie – at the browser end? in the network? in content downloading? or at server end?

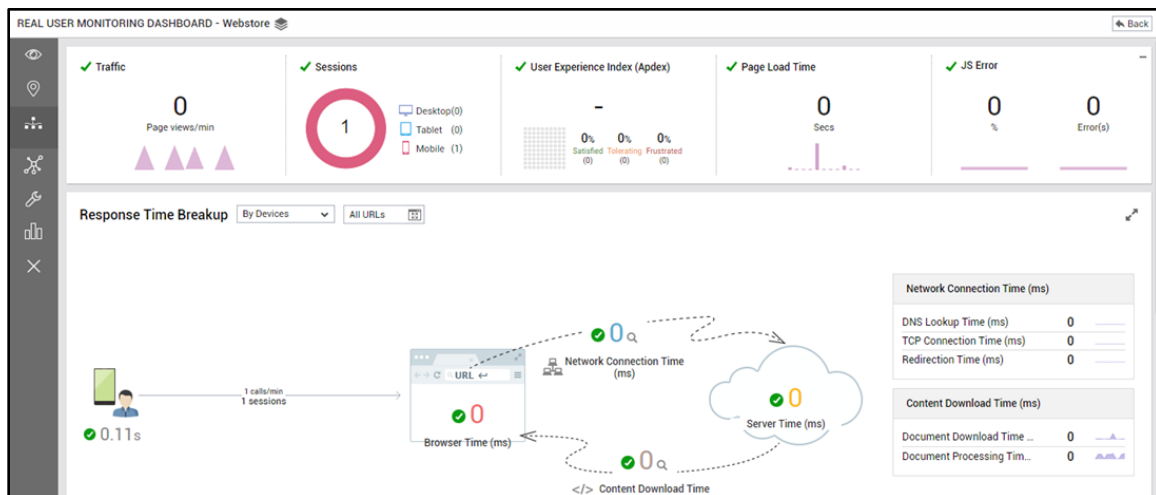


Figure 47: The improved RUM Dashboard with different accordions

- **Drilling down from RUM to transaction tracing:** In environments where the eG Real User Monitor and the eG BTM are configured for monitoring the accessed URLs, eG Enterprise v7 provides insights into the server side issues from the RUM Transaction flow diagram. The slowness in the server side can be analyzed with a single click on the Server Time measure displayed in the RUM Transaction flow diagram. For the same transaction displayed in the RUM Transaction flow diagram, the Transaction flow call graph traced by the eG BTM appears using which slowness in the server can be ascertained with ease.
- **New Reports for Real User Monitor:** Following are the RUM reports that have been included in eG Enterprise v7 for historical performance analysis of the web applications monitored by the eG Real User Monitor:
 - **User Experience Assessment report:** To view the overall user experience on a web application that is being monitored and to historically assess the user experience, eG Enterprise v7 offers the User Experience Assessment report. By generating this report, administrators can obtain a summary of user experience in an easily understandable format, figure out the user experience and identify the web application that generated the maximum traffic (desktop or mobile or tablet). Recommendations are offered based on the analysis in this report. Administrators can provide a consolidated analysis of user experience to the application teams to analyze the slow transactions and to the top-level management.



Figure 48: The User Experience Assessment report

- User Satisfaction Trend Report:** To evaluate user experience with a web application over time, administrators can use the User Satisfaction Trend report. A quick glance at this report will reveal the precise days/times during the given timeline when user experience has been less than satisfactory.

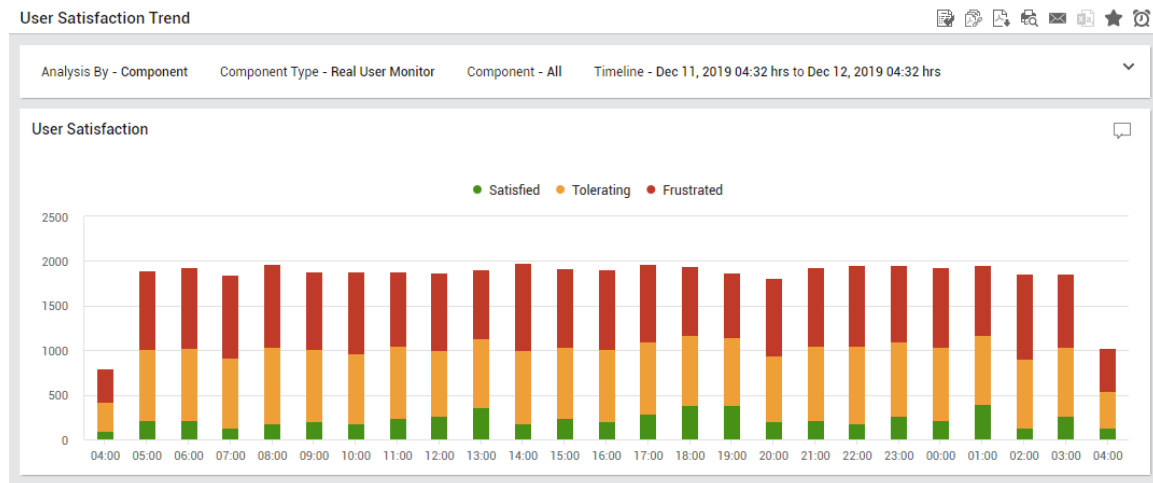


Figure 49: The User Satisfaction Trend report

- Page Visit Health Trend Report:** Use the Page Visit Health Trend report to historically analyze the health of the pages visited by the users of the web application. In the process, you can quickly identify the precise dates/times (during the specified timeline) when the maximum number of pages visited were loading slowly. This way, you can identify when user experience with the web application was poor and investigate the reasons for the same.

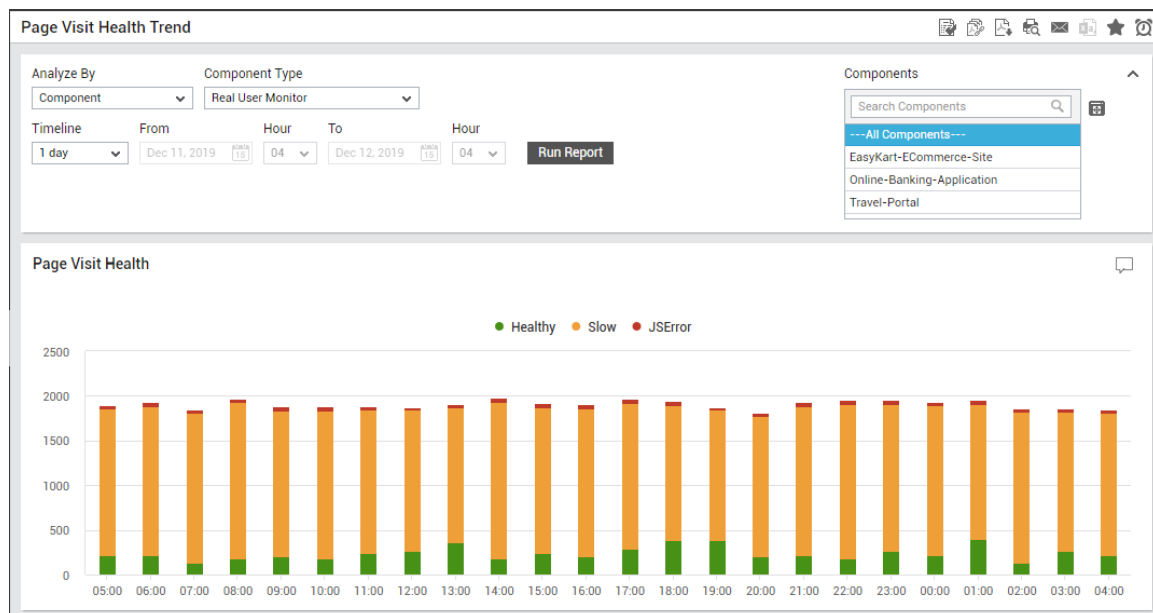


Figure 50: The Page Visit Health Trend report

- Device Usage Trend report:** Use the Device Usage Trend report to analyze device usage over time, and identify which device was used the maximum (during the said timeline) for accessing the web application - is it desktop? or mobile? or tablet?

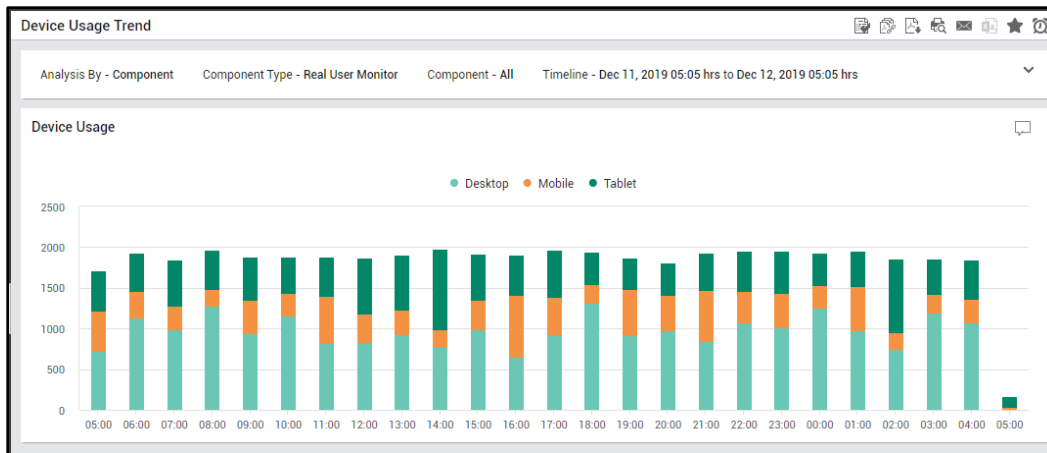


Figure 51: The Device Usage Trend report

- Slice and Dice Analytics Report:** By default, the Slice and Dice Analytics report provides administrators with an overview of the user experience with a web application, for a given period of time in the past. Besides displaying the total number of transactions that were performed on the chosen web application during the given period, the report also reveals the percentage of transactions that were healthy, slow, and error-prone, thus clearly indicating to administrators if overall user experience with the web application was satisfactory or not. Additionally, the report also allows administrators to easily pick and choose what perspectives to user experience they want to view and analyze in the report. For instance, administrators can choose to focus on slow pages alone, or historically analyze how specific page groups / URLs have performed over time. Likewise, they may need insights on page view requests coming from specific client IP addresses. This report supports such granular/focused analysis as well, so that administrators can view only what they want to in the report, exclude statistics that may distract them, isolate bottlenecks to user experience quickly and precisely, and troubleshoot efficiently.

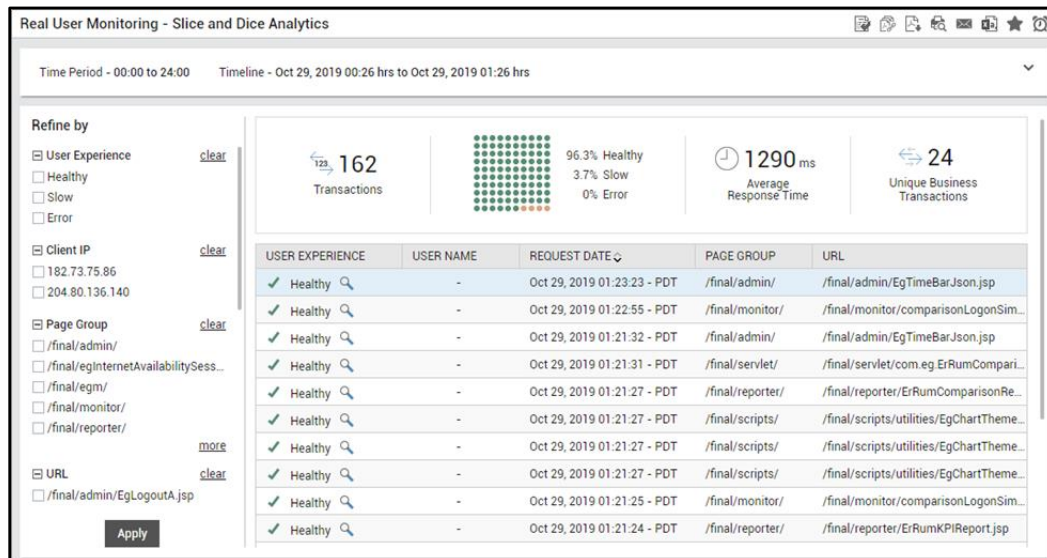


Figure 52: The Slice and Dice Analytics report

4.3 Enhancements to Business Transaction Monitor

- **Support for new point cuts:** Starting with eG Enterprise v7, eG Java BTM is capable of accurately capturing the time taken by external calls/queries to Mule ESB, Redis, MongoDB, SAP HANA, LDAP backends, and mailer server backends. Also, using eG BTM, you can now trace transactions passing through JMS message queues and JMS topics. The addition of these point cuts 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.
- **In-depth visibility into .NET CLR using .NET Profiler installed on a Microsoft IIS Web Server:** In version 7, the eG .NET Profiler has been engineered to provide in-depth insights into the health of the Common Language Runtime (CLR), a virtual machine component of Microsoft's .NET framework. Using the detailed diagnostics that the Profiler reports for the .Net CLR test, administrators can quickly detect if garbage collection has been taking longer than usual. The module name of the top assemblies, system and application classes are revealed using which administrators can troubleshoot application soft hang issues. The memory used by the .NET CLR is monitored and the size of the large object heap memory is tracked continuously. Abnormal growth of the large object heap memory can be tracked with the detailed diagnostics offered by eG Enterprise. The class name, class size, instance name and module name are reported as part of the detailed diagnostics using which administrators can analyze memory related constraints with ease.
- **.Net Business Transaction Monitor now supports monitoring of multiple websites:** In previous versions, if a single IIS web server hosted multiple web sites, each web site had to be managed as a separate IIS web server component in eG Enterprise to enable business transaction monitoring. From eG Enterprise v7, a comma-separated list of web sites on the target IIS Web Server can be configured for transaction monitoring. This allows one component in eG Enterprise to monitor transactions pertaining to all of the web sites hosted on an IIS web server.
- **New PHP Business Transaction Monitoring Capability:** PHP is a programming language for web applications. Starting with v7, eG extends its business transaction monitoring capabilities to web applications built on the PHP framework.

The eG PHP BTM module is installed on the Zend Engine by the eG agent installed on the PHP server. The PHP BTM module employs a unique tag-and-follow technique 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.

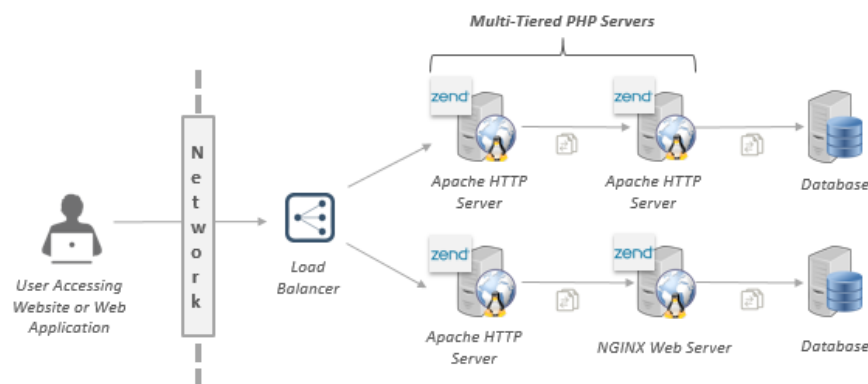


Figure 53: The distributed transaction tracing of PHP servers

Once the transaction path is determined, the eG PHP BTM measures the total response time of each

transaction, the time spent by the transaction on each web server (Apache / NGINX) that supports the PHP framework, and the time taken for processing every external service call (including SQL queries). Using these analytics, the eG PHP BTM precisely pinpoints the slow, stalled, and failed transactions to the PHP web application server. Intuitive icons and color-codes used in the graphical transaction flow enables administrators to accurately isolate where – i.e., on which PHP web application 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 PHP BTM facilitates rapid problem resolution, which in turn results in the low downtime of and high user satisfaction with the PHP web application.

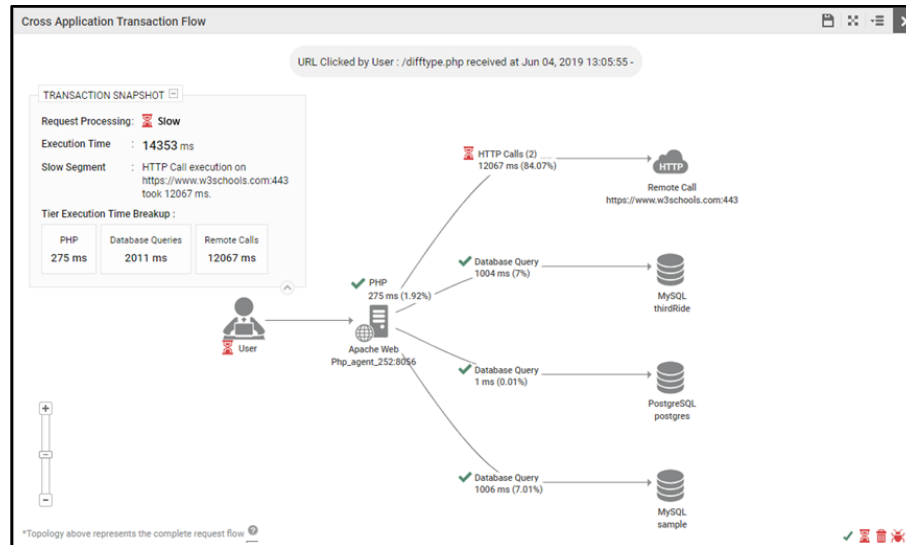


Figure 54: The cross-application transaction flow of a slow transaction

Note that the eG PHP BTM capability is applicable only on Linux environments.

- **Scalability Optimizations for Java Transaction Tracing:** Previously, in some environments, memory overheads were noticed on the Application server when the metrics were being pulled by the eG agent. Additionally, to pull the necessary metrics, a port on each JVM node should be opened by the eG agent. This was becoming tedious when metrics were to be collected round the clock for effective monitoring of environments where JVM nodes are scaled up and down. In order to avoid opening the ports for collecting the metrics and reduce memory overheads, starting with eG Enterprise v7, the **eg_btm.jar** available on the eG agent host pushes the metrics to the eG manager directly while the eG agent acts just as a listener. This method of pushing the metrics directly is best suited for Docker/Kubernetes and microservices environments where JVMs are scaled up and down based on business needs.
- **Communication Changes between eG manager and eG agent for Transaction Tracing:** In older versions, the eG agent collected the data by executing the tests relevant to transaction tracing and stored the data as a single file. When stored in such a way, the stack trace in the detailed diagnosis increased the size of the file considerably. This led to a decrease in the speed of data transmission between the eG agent and the eG manager and increased the overheads in processing large files. To optimize the speed of data transmission and decrease the overheads in processing the files, starting with eG Enterprise v7, the eG agent stores the collected data in multiple files before transmitting to the eG manager. The eG manager is also optimized to process the data using multiple threads as against a single thread in previous versions.

- **Database space has been optimized for eG BTM:** In previous versions, whenever slow queries were discovered during transaction tracing, each query was stored as a separate record in the eG backend database. When the same query was encountered for multiple transactions, the storage space in the database increased manifold resulting in space crunch. To optimize the database space, starting with eG Enterprise v7, each distinct query is stored only once in the eG backend database. A pointer is used to fetch the query and display in the detailed diagnosis.
- **New Reports for eG Java and .NET Business Transaction Monitor:** Following are the new reports that have been included in eG Enterprise v7:
 - **Overview Report:** Administrators can view the health status of business transactions for a given period in time. This report also provides administrators with insights into the traffic statistics, response time and error statistics in a single page. This report helps administrators in an overview of the transactions that are too slow/error prone at a single glance.

Business Transactions Health Report

| BUSINESS TRANSACTION | TRAFFIC STATS (NUMBER) | | RESPONSE TIME (MSECS) ⚙ | ERROR STATS (NUMBER) | | Healthy |
|---|------------------------|-----------|-------------------------|----------------------|------------|---------|
| | Calls | Calls/min | | Errors | Errors/min | |
| /final/servlet/com.eg.hghChartServlet | 497 | 1.2 | 18350 | 0 | 0.0 | 0.0 |
| /final/admin/EgViewUser/ | 2 | 0.3 | 838 | 0 | 0.0 | 100.0 |
| /final/admin/DeleteUsers/ | 3 | 1.0 | 786 | 0 | 0.0 | 100.0 |
| /final/servlet/com.eg.ErRumHealthServletC | 5 | 0.4 | 464 | 0 | 0.0 | 100.0 |
| /final/admin/EgChangeUserProfile/ | 35 | 1.7 | 424 | 0 | 0.0 | 100.0 |
| /final/servlet/com.eg.UploadImage | 69 | 0.3 | 405 | 0 | 0.0 | 100.0 |
| /final/monitor/EgRUMTopology.jsp | 3 | 0.5 | 386 | 3 | 0.5 | 0.0 |
| /final/servlet/com.eg.myDashboardController | 366 | 4.1 | 351 | 0 | 0.0 | 100.0 |
| /final/monitor/EgTestStatusInfo.jsp | 2 | 0.7 | 315 | 0 | 0.0 | 100.0 |
| /final/admin/EgAdminOperations.jsp | 10 | 0.3 | 254 | 0 | 0.0 | 100.0 |

<< < | Page 1 of 12 | > >> | 🔄

Displaying topics 1 - 10 of 119

Figure 55: The BTM Health Overview report

- **Health Trend Report:** Measuring business transaction performance in real-time and capturing transaction slowness instantly, is important. Equally important is to analyze how healthy the transactions are. Using this report, you can historically analyze the health of individual business transactions to a web site / web application. In the process, you can quickly identify transactions that have been consistently slow or have encountered errors very often. Such transactions can then be marked for closer scrutiny.

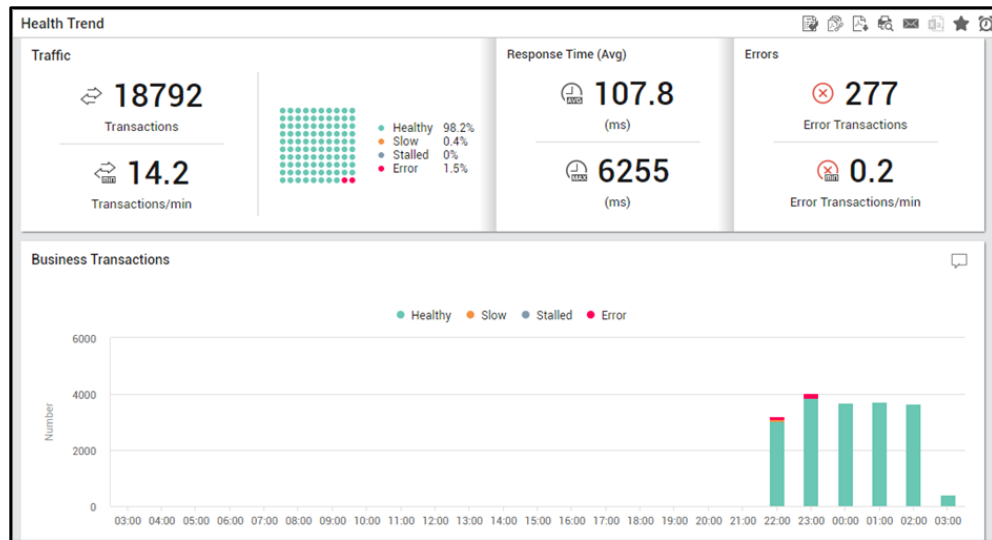


Figure 56: The Health Trend report

- Unique User/Session Analysis Report:** In environments where multiple business transactions are initiated, administrators should fairly have an idea of which user is initiating the business transaction and through which session the transaction was initiated. This report helps administrators understand the user load to each transaction in correlation with the response time. Also, this report helps application architects in optimizing performance and capacity needs.

| Unique User/Session Analysis | | | |
|---|-----------------|------|------------------------|
| Analysis By - Component Component Type - eG Manager Component - eGDP129:7077 Timeline - Dec 12, 2019 13:56 hrs to Dec 13, 2019 13:56 hrs | | | |
| Business Transactions by Session Identifier | | | |
| BUSINESS TRANSACTION | UNIQUE SESSIONS | HITS | AVG RESPONSE TIME (MS) |
| /final/reporter/ErPdfSaveStatus.jsp | 5 | 24 | 6343 |
| /final/servlet/com.eg.ErPdfDownloadC | 5 | 24 | 5690 |
| /final/admin/EgConfigEnv/ | 1 | 15 | 4951 |
| /final/admin/NewComponent/ | 2 | 31 | 4163 |
| /final/servlet/com.eg.ErJvmCpuC | 4 | 42 | 3497 |
| /final/servlet/com.eg.ErSessionUsageRep | 1 | 48 | 3240 |
| /final/servlet/com.eg.ErJvmOverviewC | 12 | 80 | 3191 |
| /final/servlet/com.eg.ErVMSessionUsage | 1 | 15 | 3091 |
| << < Page 1 of 21 > >> | | | Total Records : 164 |

Figure 57: The Unique User/Session Analysis report

- Code-level Exceptions report:** Use the Code-level Exceptions report offered by eG Enterprise v7 to map exceptions encountered with the business transaction URLs. This report allows the application teams to easily understand which URLs were affected due to a code-level exception and what were the exceptions that were frequently encountered by a business transaction.

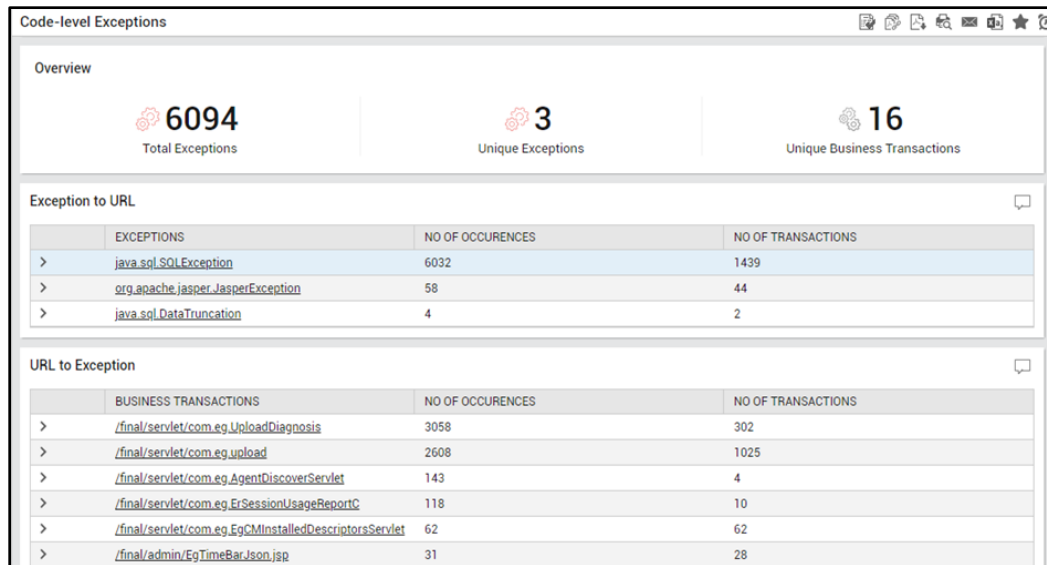


Figure 58: The Code-level Exceptions report

- **Transaction Health Analysis Report:** By default, the Transaction Health Analysis report provides administrators with an overview of the user experience with a web application, for a given period of time in the past. This report graphically (using a scatter chart) represents the transactions that were healthy, slow, and error-prone, thus clearly indicating to administrators if overall user experience with the web application was satisfactory or not during the designated period. Additionally, the report also allows administrators to easily pick and choose what perspectives to user experience they want to view and analyze in the report. For instance, administrators can choose to focus on slow requests alone, or historically analyze how specific business transactions / URLs have performed over time. Likewise, they may need insights on page view requests coming from specific client IP addresses. This report supports such granular/focused analysis as well, so that administrators can view only what they want to in the report, exclude statistics that may distract them, isolate bottlenecks to user

experience quickly and precisely, and troubleshoot efficiently.

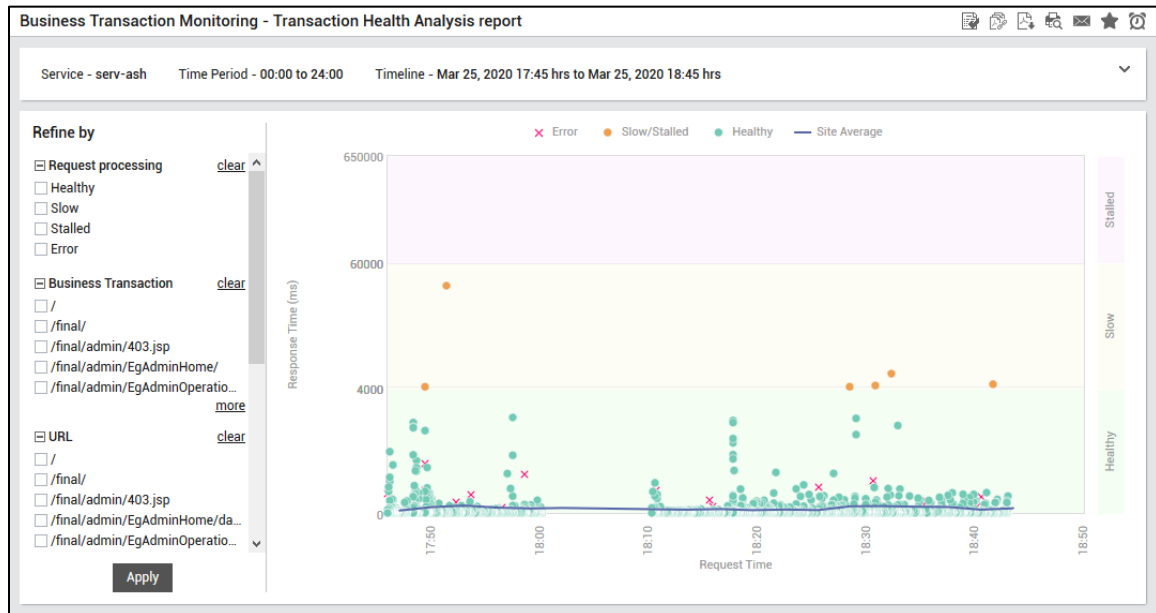


Figure 59: The Transaction Health Analysis report

- **Monitoring Azure App Service:** A new monitoring model named Microsoft Azure App Service is offered by eG Enterprise v7 to monitor the .NET applications built on Azure cloud using the Azure App service. The transactions are monitored and the statistics pertaining to slow transactions, stalled transactions and error transactions are revealed.

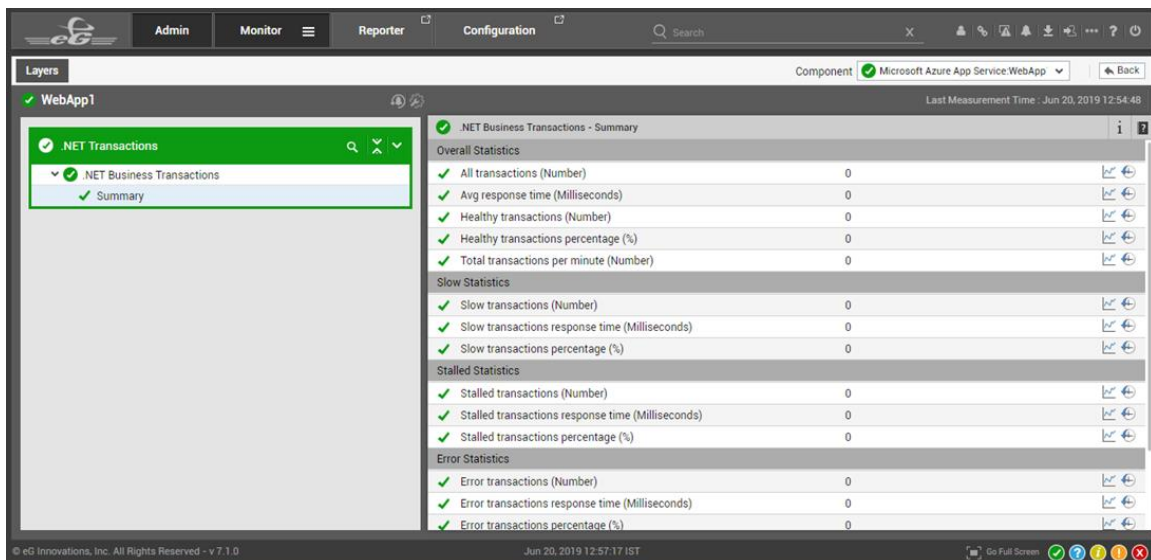


Figure 60: Monitoring the Azure App Service

- **Monitoring NodeJS:** Node.js is an open-source, cross-platform runtime environment built on Chrome's V8 javascript engine. It is used to build fast, scalable server-side web applications. The event-driven, non-blocking I/O model makes Node.js lightweight and efficient. Performance setbacks suffered by the NodeJS server can affect the availability of critical services it supports. To avoid such an eventuality, you need to continuously monitor the performance of the NodeJS server.

eG Enterprise v7 helps administrators in this regard. The CPU and memory utilization of the server is monitored to figure out if the server is resource hungry. The garbage collection activity of the server is continuously monitored by taking count of how often garbage collection was performed and how much of memory was released due to garbage collection activity. The errors encountered in the server are captured and reported. The event loops executing on the server are monitored periodically and time delays encountered while the event loop is executing is captured and reported for further analysis.

4.4 Deeper Visibility of the JAVA Virtual Machine (JVM)

Following are the enhancements that have been included in eG Enterprise v7 for monitoring the JVM:

- **Identifying the JVM threads causing CPU issues:** In previous versions, administrators identified the resource hungry threads by continuously monitoring the JVM threads. However, administrators could not effectively troubleshoot the threads because they could not figure out the CPU utilization of the threads which was important for analysing the real reason. For greater visibility and troubleshooting, eG Enterprise v7 offers to report the CPU utilization of the threads and identifies the type of thread – is it web/HTTP thread? or RMI thread? or GC thread? that is consuming the maximum CPU.
- **New Reports included for performance analysis of JVM components:** Following are the new reports that have been included in eG Enterprise v7 for analysing the JVM components:
 - **JVM – Overview Report:** The prime concern of administrators of Java applications is knowing how well the application was functioning over a period of time, and how to troubleshoot issues (if any) in the performance of these applications. For this purpose, eG Enterprise v7 offers a JVM – Overview report. By generating this report, administrators gain considerable knowledge on the overall performance, availability, incidents, top issues and resource constraints in JVMs in their environment over a period of time. Administrators can also historically analyze the CPU, memory, GC and thread incidents, figure out the times when the incidents peaked and start troubleshooting the issues effectively. The Top N JVMs that are impacted by blocked threads,

runnable threads, garbage collection etc can also be identified using this report.



Figure 61: The JVM – Overview report

- JVM - Uptime/Downtime Analysis Report:** Uptime is a key measure of the general health and availability of the critical JVMs in an IT infrastructure. Periodic uptime values that the eG agent reports for target JVMs can alert you to unscheduled reboots that occurred recently; however, to effectively assess JVM 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 a JVM and the total number of reboots it experienced over a period of time is necessary. To enable such an analysis for one/more critical JVM components of an IT infrastructure, eG Enterprise provides the Uptime/Downtime Analysis report.

Using the Uptime/Downtime Analysis reports, you can figure out the following:

- Which JVMs are the healthiest, in terms of availability?
- Which JVMs have been down for the longest period of time? How long was each JVM unavailable during the specified timeline?
- How many times during the designated period did a JVM reboot? How many of these were scheduled reboots? How long was the JVM down before every reboot?
- Which servers had the least uptime/downtime and how many JVMs were available in the target environment?

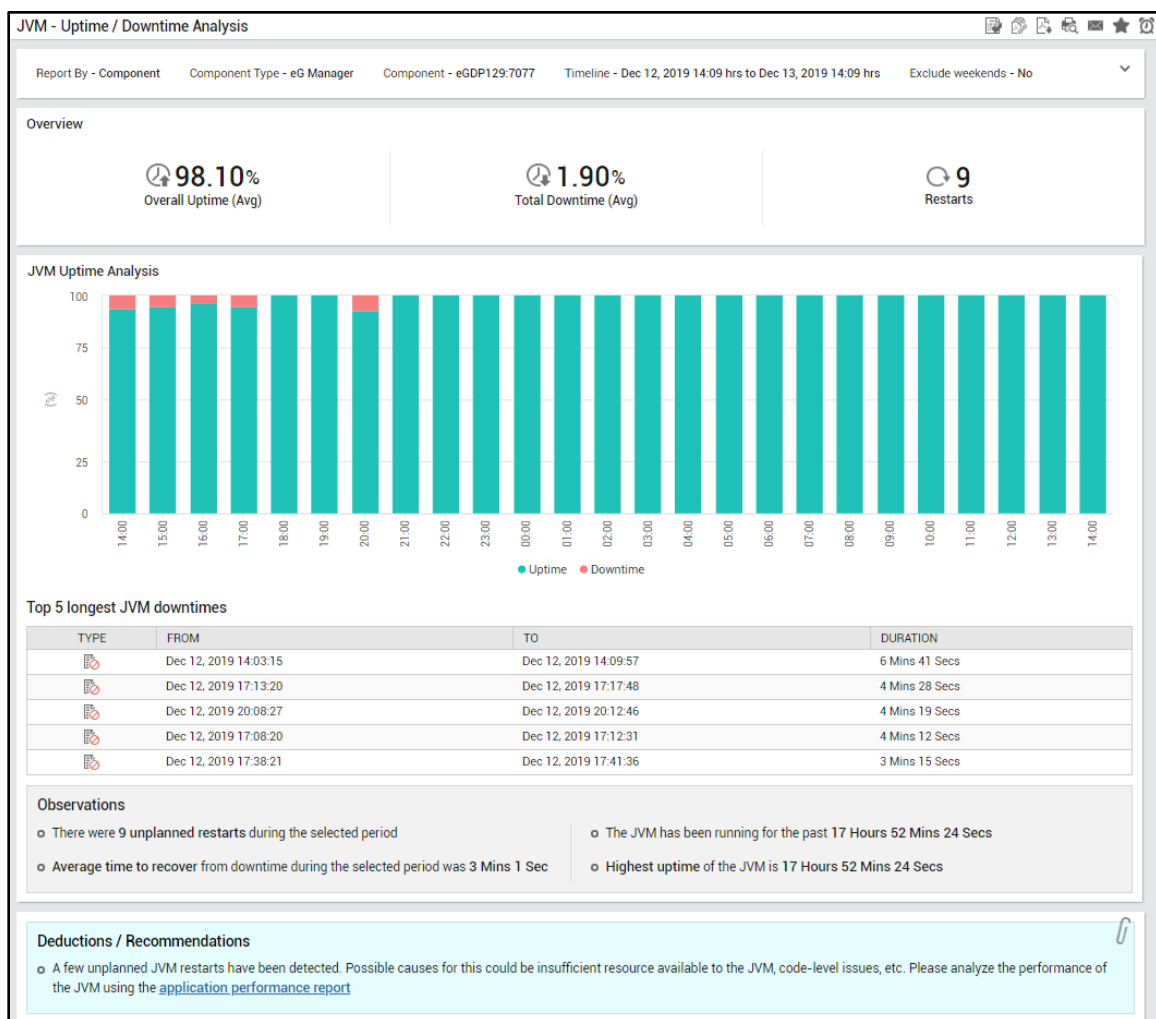


Figure 62: The JVM – Uptime/Downtime Analysis report

- **JVM - Memory Analysis Report:** Use the Memory Analysis report to view historical trends of memory usage in terms of Heap Memory and Non-Heap Memory. By closely analyzing the

historical trends, administrators can infer sudden spikes in memory usage and start investigations on optimizing the memory utilization.

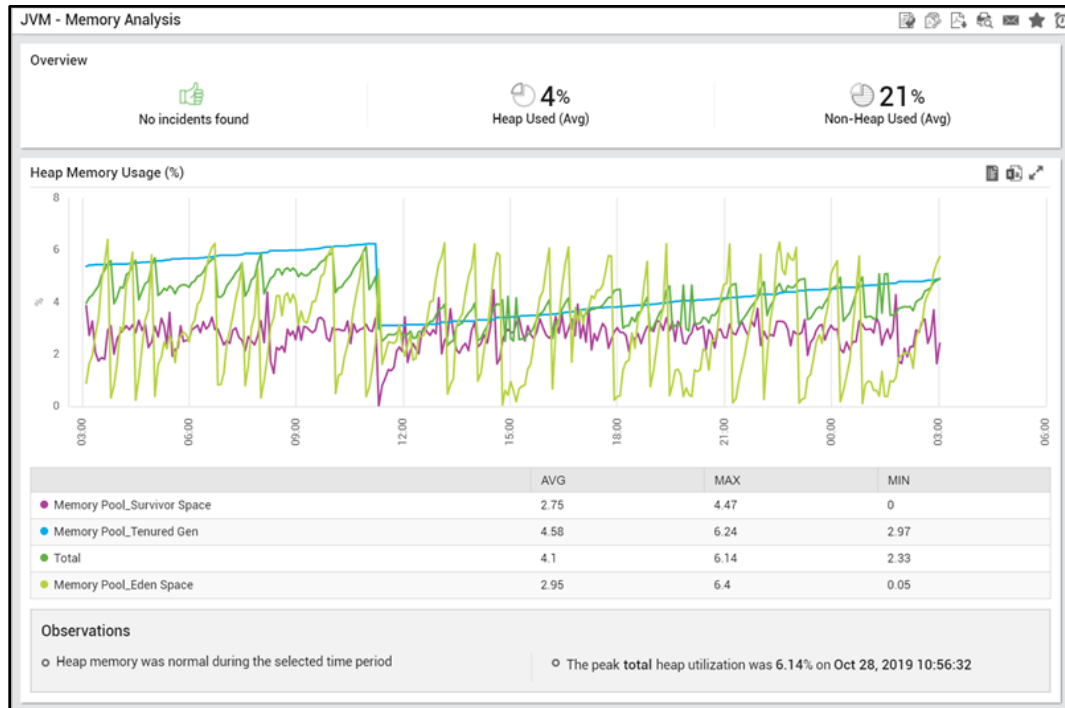


Figure 63: The JVM - Memory Analysis Report

- JVM - GC Analysis Report:** Administrators can use the JVM - GC Analysis report to historically analyze how much time was spent on garbage collection and analyze whether there were any SLA violations. For easy understanding of the report, users are pointed out to recommendations/conclusions regarding GC issues.

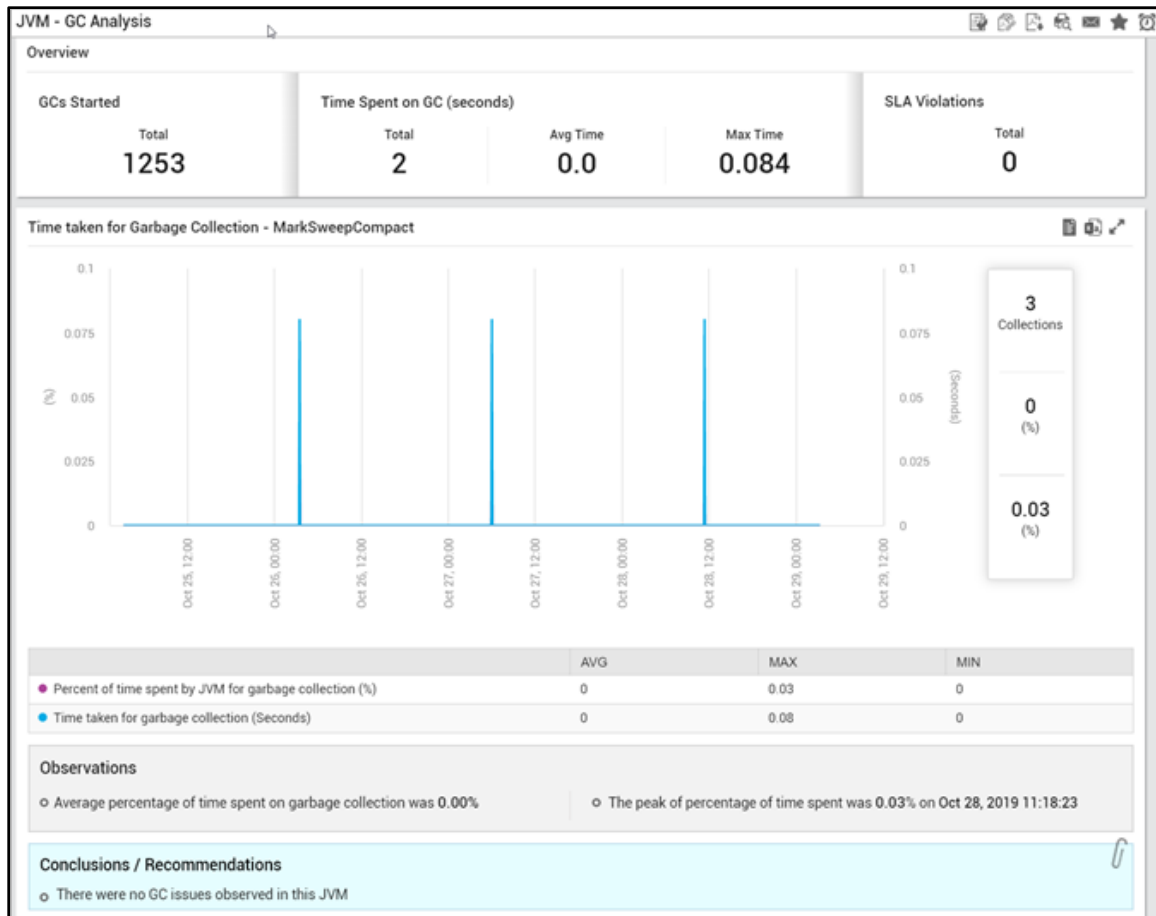


Figure 64: The JVM – GC Analysis report

- JVM - CPU Analysis Report:** Use the JVM - CPU Analysis report to historically analyse the CPU utilization of the thread types. The thread type that consumed maximum CPU is identified and administrators are alerted to that thread type through the recommendations offered by eG Enterprise v7.

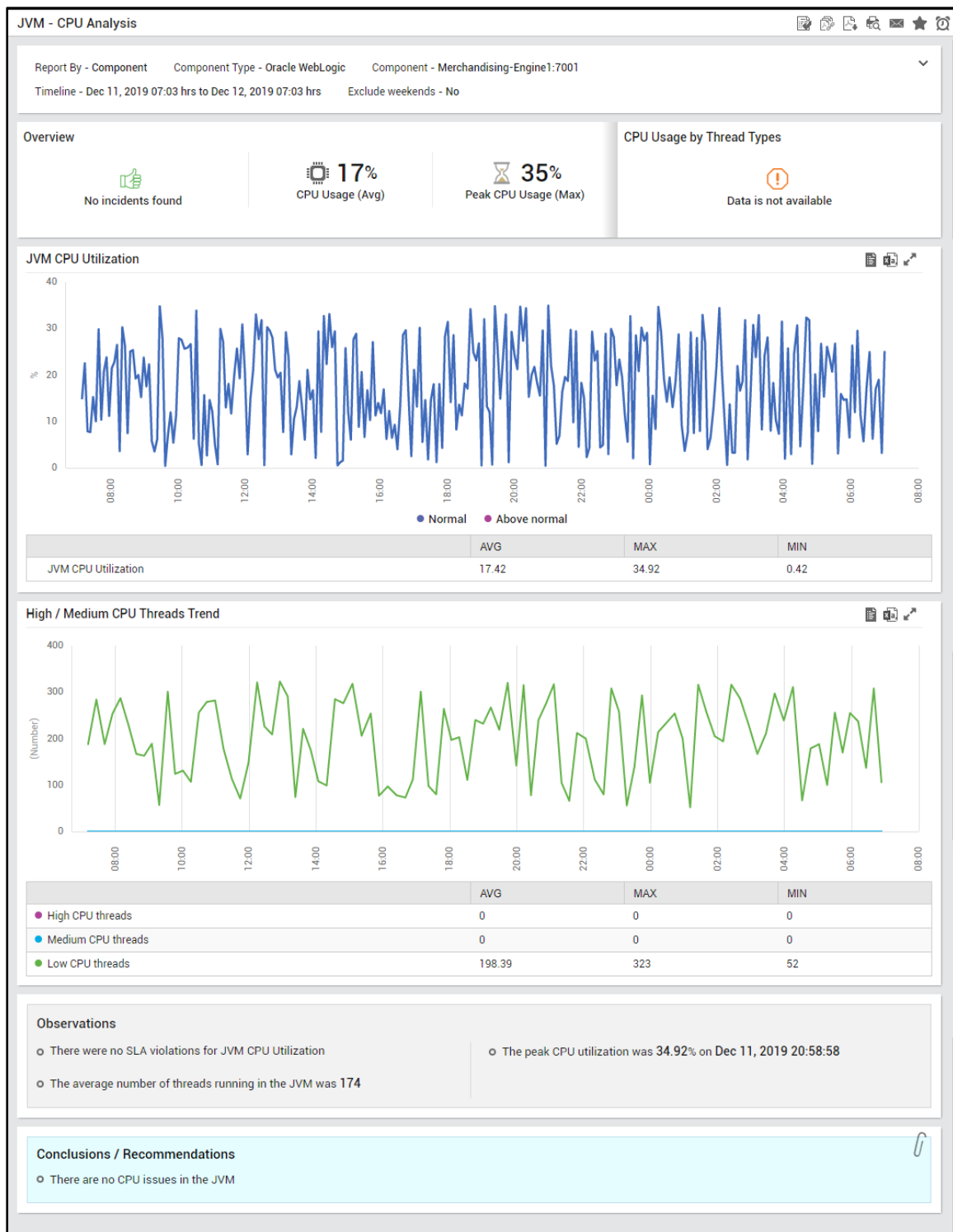


Figure 65: The JVM – CPU Analysis report

- JVM - Thread Analysis Report:** The JVM - Thread Analysis report helps administrators in historical analysis of the thread activity. By generating this report, administrators can analyse the waiting/blocked/deadlocked threads and high CPU threads over a period of time. Administrators are enlightened to the exact recommendation of which type of thread was

causing problems in the target environment so that they can start working on rectifying the issues at a faster pace.

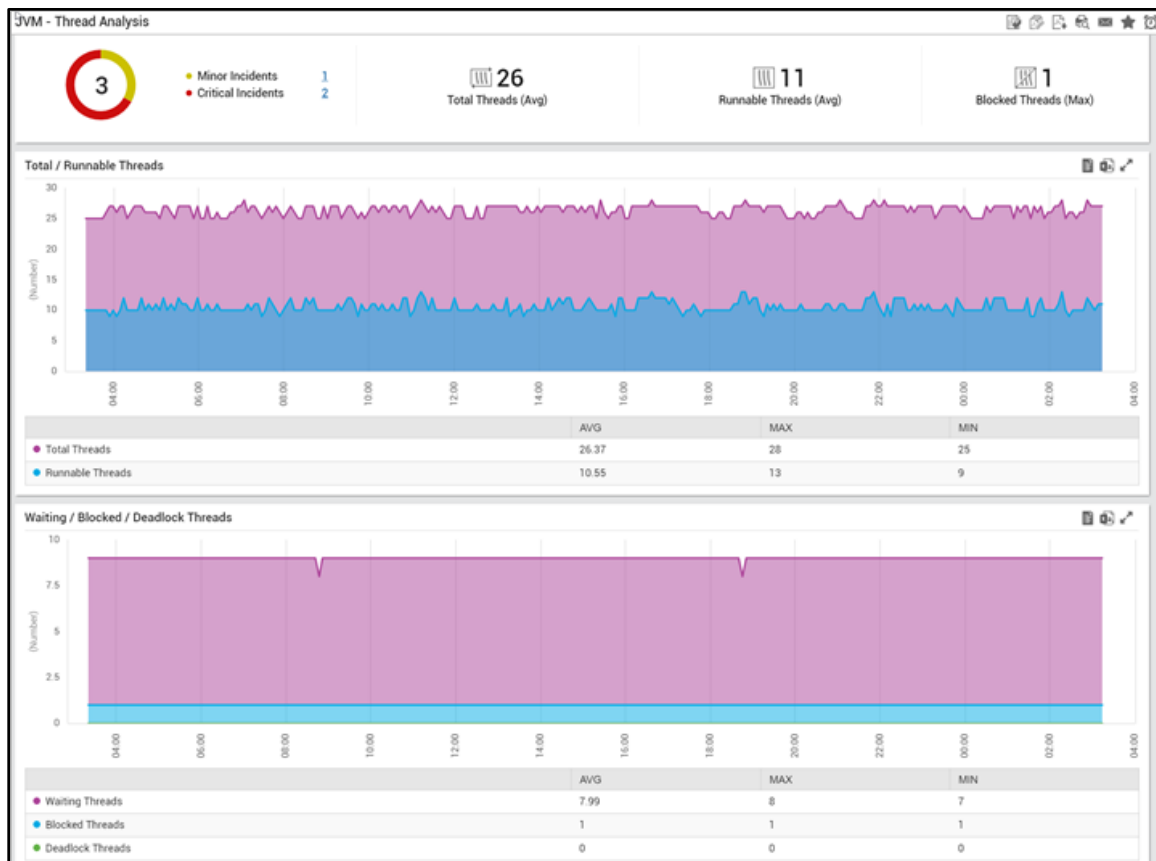


Figure 66: The JVM – Thread Analysis report

5. Enterprise Application Monitoring

5.1 Enhancements for SAP Monitoring

eG Enterprise v7 has expanded its SAP monitoring capabilities to support new SAP applications such as Fiori, BusinessOne, Hybris, Business Warehouse and Business Objects Data Services.

- **Monitoring SAP Business One:** eG Enterprise v7 is capable of monitoring the SAP Business One application. The SAP Business One application offers an affordable way to manage your entire business – from accounting and financials, purchasing, inventory, sales and customer relationships, and project management, to operations and human resources. Version 7 of eG Enterprise performs in-depth monitoring of the SAP Business One application and in the process, for each IPO URI, reveals the top 5 executions that were slow. User login failures are detected and the reason for the failure is analyzed. The error-prone workflow instances and cancelled instances are identified with ease. The failed tasks of each task type are identified and reported alongside the throughput of the tasks. The error and warning messages are captured and reported by monitoring the DI API logs, SAP BI Business logs. This way, abnormalities are brought to light and errors are rectified by the administrators before users start to complain.

- **Monitoring SAP Business Warehouse Instance:** SAP Business Warehouse (BW) is a model-driven data warehousing product based on the SAP NetWeaver ABAP platform. It collects, transforms and stores data generated in SAP and non-SAP applications and make it accessible through built-in reporting, business intelligence and analytics tools, as well as third-party software. Slowness experienced in data collection and storage may lead to incorrect report generation and wrong report analysis which may lead to loss of business. To avoid such slowness and to maintain the performance of the SAP Business Warehouse instance throughout, eG Enterprise v7 monitors the SAP Business Warehouse Instance. The open hub destinations are monitored to figure out if there are any error requests and if responsiveness is poor. The process chains that are currently running on the server are discovered and for each process chain, the error prone processes, slow processes, and those that are in an abnormal execution state are promptly captured and reported. The queries executing on the server are discovered and slow running queries are highlighted. The templates are monitored and those that have been running for a long time are pinpointed, so the reason for the same can be determined. The workbooks are monitored, so that administrators can quickly identify the slow running workbooks and diagnose the source of slowness by closely analyzing executions and queries.
- **Monitoring SAP Hybris:** SAP Hybris is a complete customer engagement and multichannel e-commerce solution with fully integrated tools and capabilities. eG Enterprise v7 monitors the SAP Hybris solution. The current status of each Data Source is monitored and reported. Open connections are highlighted. The usage of the Entity Region Cache and Query Region Cache are monitored, and cache hits and misses are captured. The maximum number of entries in flexible query cache helps administrators in analyzing the efficiency of the cache. The main cache is monitored and the hits and misses to the cache are reported. This way, the cache that is most frequently being used is identified.
- **SAP Platform Dashboard:** In recent years, SAP has emerged as a one stop solution for Enterprise Application and Business needs - from analytics to human capital management to ERP, and everything in between. As with any application/product, service disruptions, downtime and slow connectivity/transaction issues are bound to affect business continuity and SAP administrators require actionable insight to proactively alert them when performance starts to degrade and to help them resolve problems quickly. eG Enterprise v7 helps administrators in this regard! eG Enterprise empowers SAP administrators to continuously monitor health and performance metrics, diagnose issues, and isolate the root cause of SAP performance problems. eG Enterprise offers a new SAP landscape dashboard that allows administrators to monitor high-level performance metrics of all SAP tiers/SAP components on a single console.

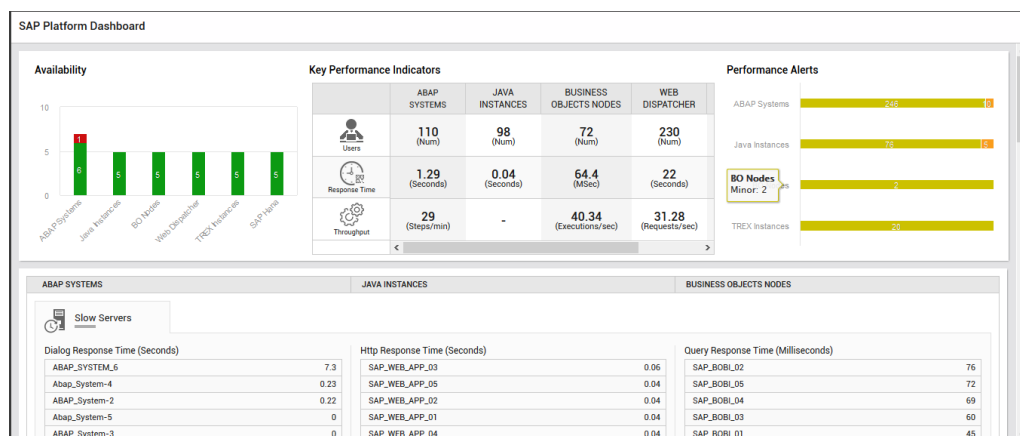


Figure 67: The SAP Platform Dashboard

By closely monitoring the servers of SAP applications/products in the target environment, eG Enterprise tracks the availability, reports how many alerts were raised for each SAP server, how many users were logged in and the response time and throughput of each SAP server. The servers

that are termed as slow and busy are identified for each SAP application/product with ease! The resource utilization (CPU, memory, disk) of each server is tracked continuously and the servers that are consuming high resources are promptly identified.

Further navigating down the dashboard will lead you to separate sections for each of the SAP application monitored in your environment. Each section will display a few key performance insights using which you can figure out how well the servers are performing. For example, when you drill down to the ABAP Systems section, you can identify the work processes that remain free in each of the SAP ABAP servers, the top SAP ABAP servers that are generating tRFC traffic and the top low transactions identified in each SAP ABAP server.

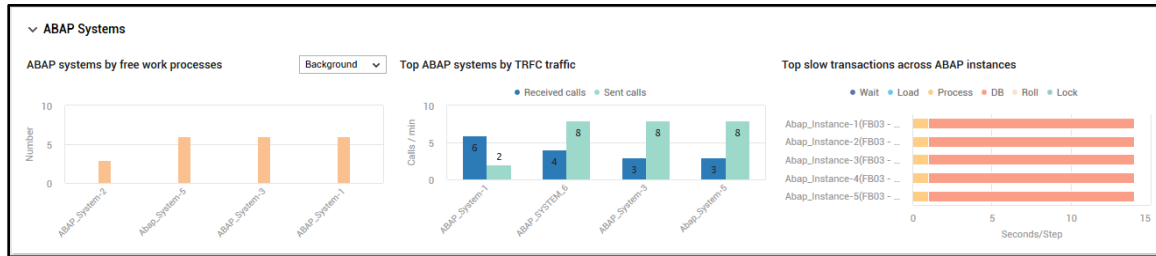


Figure 68: The ABAP System section detailing the key performance metrics of SAP ABAP servers

- **SAP Monitoring Dashboard:** While the SAP Platform Dashboard provides a one stop solution of the SAP environment in a single console, SAP administrators are required to analyse the performance of individual SAP ABAP instances frequently. To cater to the needs of such SAP administrators, eG Enterprise v7 offers a brand-new SAP Monitoring Dashboard. eG Enterprise empowers SAP administrators to continuously monitor the health and uptime of each SAP ABAP instance, identify the user distribution across the instance, figure out the dumps generated in the instance, identify the worker processes that are held for long, diagnose issues, and isolate the root cause of SAP performance problems. This dashboard also helps administrators visualize transaction processing by ABAP instances and figure out the transaction that is taking too long to respond. The long running jobs and cancelled jobs are identified with ease along with the details of top transactions, users and applications in terms of high response time. The resource consumption of the SAP ABAP instance

can also be monitored from this dashboard with ease.

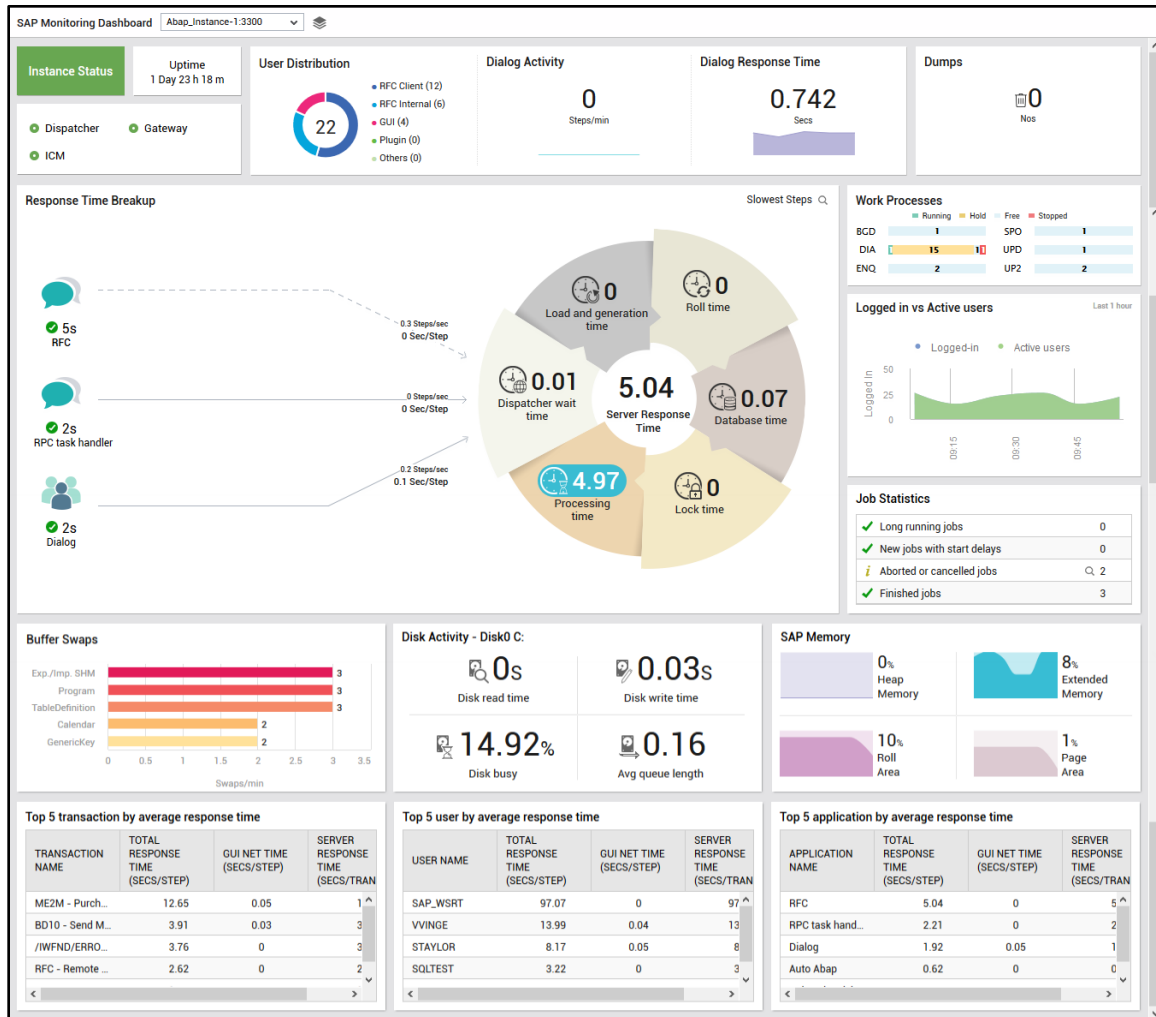


Figure 69: The SAP Monitoring Dashboard

- **ABAP Dumps Report:** In any environment, one of the reasons for performance degradation of the servers is errors encountered by the servers. These errors when left unnoticed may even collapse the entire environment. Similarly, in SAP environments, when unhandled exceptions occur while an ABAP program is executed, an ABAP runtime error is triggered, and the execution of the program is terminated. The error encountered is then logged as a short dump in the Syslog file which can be further used for post-mortem analysis on how to rectify such errors. eG Enterprise v7 monitors such errors or dumps encountered in the SAP ABAP Instance. The ABAP Dumps report offered by eG Enterprise v7 provides information on top dumps by source, types of dumps encountered, top hosts encountering dumps and user accounts that are impacted. This report thus helps administrators in figuring out the users who are frequently impacted by the dumps and take remedial measures accordingly.

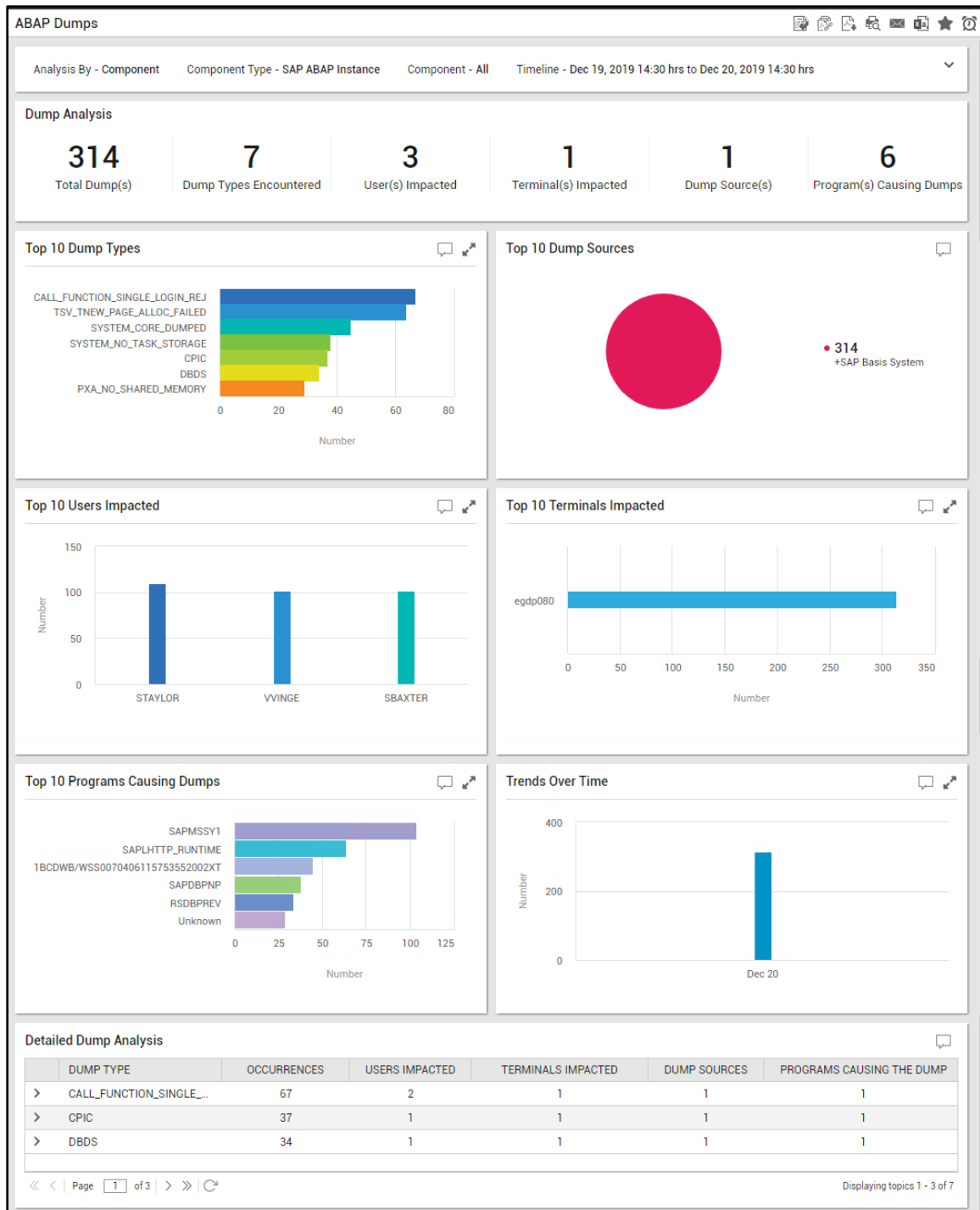


Figure 70: The ABAP Dumps report

5.2 Enhancements to Office 365 Monitoring

eG Enterprise v7 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 offers the following capabilities for O365 customers:

- **Synthetic Checks for Proactive Monitoring of Office 365 Applications:** In most IT infrastructures, Office 365 products play a major role. Office 365 administrators must always be able to detect problems and start troubleshooting before users start complaining. In environments where users are scattered across different zones and geographies, administrators have an additional onus of monitoring the connectivity of the users to the Office 365 products round the clock. To help administrators with these checks and troubleshoots, eG Enterprise v7 has built a new monitoring model named O365 Synthetic Monitor. This model emulates the user connections to the Office 365 products and reports anomalies proactively. Each Office 365 product in the environment (Microsoft Teams, SharePoint Online, Exchange Online, Skype for Business and OneDrive for Business) is monitored and the user connectivity, file operations, Mail deliverability, user MAPI connectivity, logon connectivity, call quality checks are reported by emulating a user periodically. This helps administrators in getting alerted on critical issues before users notice them in real time.
- **Office 365 Dashboard:** In recent years, Office 365 has eclipsed all other cloud providers to emerge as the most widely used enterprise cloud service. As with any cloud-hosted service, service disruptions, downtime and slow connectivity issues are bound to affect business continuity and Office 365 administrators require actionable insight to proactively alert them when performance starts to degrade and to help them resolve problems quickly. eG Enterprise v7 helps Office 365 administrators in this regard! eG Enterprise empowers Office 365 administrators to continuously monitor health and performance metrics, diagnose issues, and isolate the root cause of Office 365 performance problems.

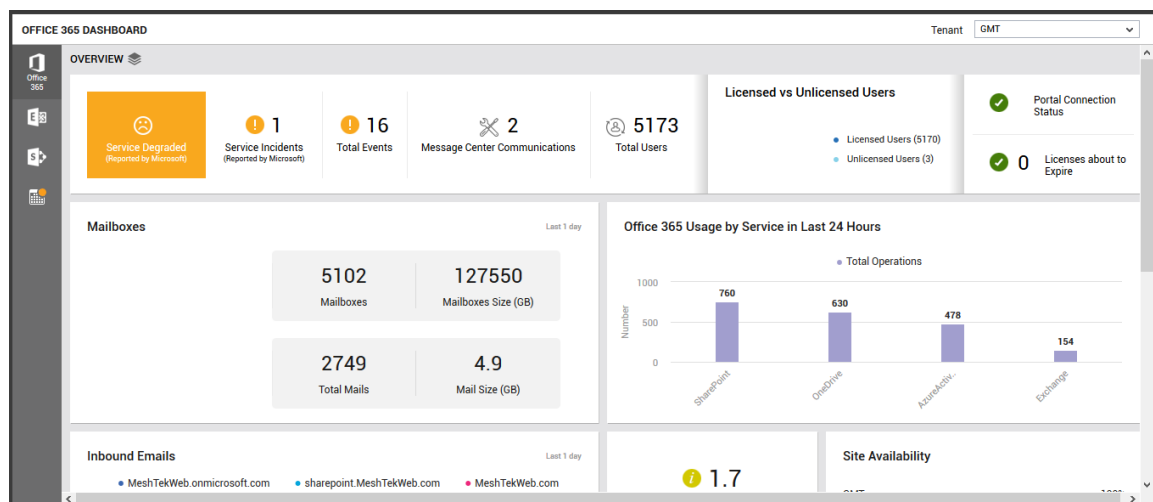


Figure 71: The dashboard displaying the Microsoft Office 365 health

By closely monitoring the Microsoft Exchange Online, eG Enterprise tracks the amount and size of emails sent/received, reports how many emails were delivered/failed/rejected, how many were filtered as spam. The users accessing each mailbox are tracked, the mailboxes that are inactive/archived are identified and the mailboxes that have reached quota limits are also identified with ease! The MAPI connectivity of a mailbox is checked, and the proper functioning of the Exchange Online servers is ensured. The built-in logon simulator synthetically tests logon connectivity to

Exchange Online and proactively helps catch issues before users complain.

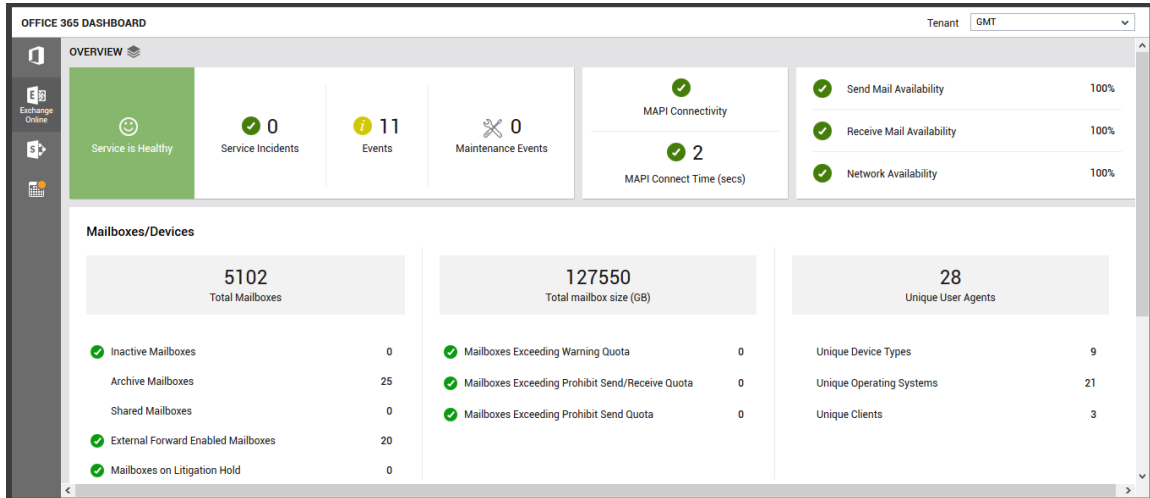


Figure 72: The dashboard providing insights into the Exchange Online Service Health

eG Enterprise v7 also monitors real-time digital experience of users connecting to SharePoint Online sites and measure user satisfaction levels. In-depth visibility into site administration, synchronization, and sharing and access request operations can be obtained. The file, page, and folder activities (uploads, downloads, deletions, modifications, etc.) are tracked so that administrators can stay compliant with audits.

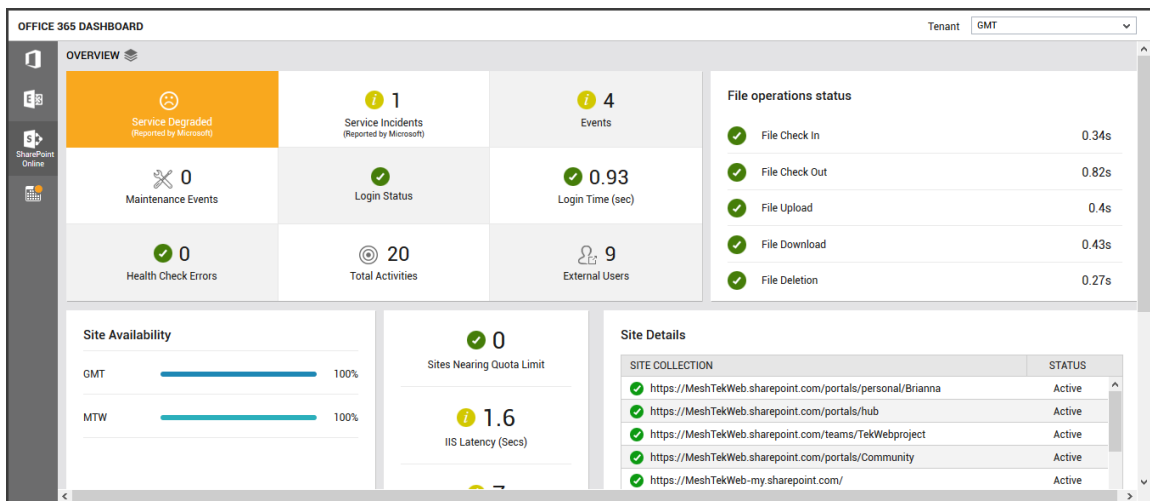


Figure 73: The dashboard displaying the SharePoint Online Service Health

eG Enterprise v7 also monitors real-time experience of users connecting to Microsoft Teams and measures user satisfaction levels. In-depth visibility into connection status, connection time, call trends, user activities and the device usage trends can be obtained. The call quality analysis helps

administrators figure out the type of call streaming (audio, video or VBSS) that was poor consistently.

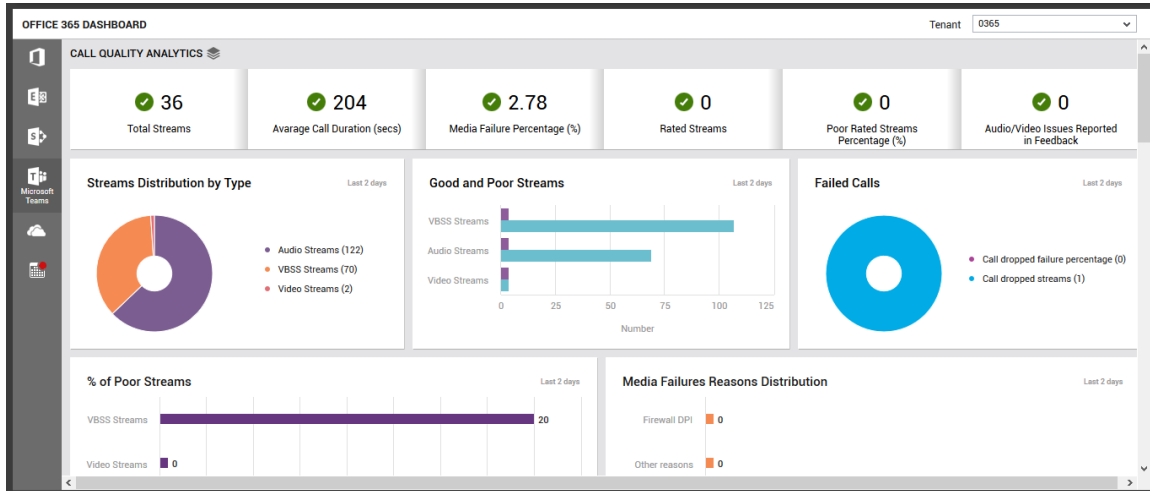


Figure 74: The dashboard displaying the Microsoft Teams health

eG Enterprise v7 also monitors in real-time, the digital experience of users connecting to Microsoft OneDrive, and measures user satisfaction levels. In-depth visibility into site administration, synchronization, and sharing and access request operations can be obtained. The file, page, and folder activities (uploads, downloads, deletions, modifications, etc.) are tracked so that administrators can stay compliant with audits.

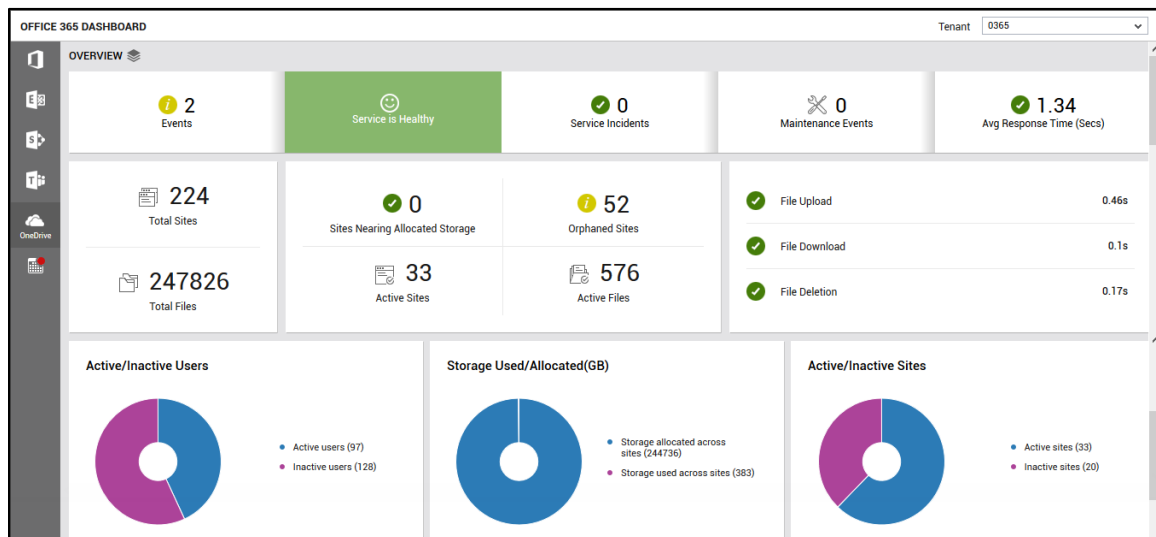


Figure 75: The dashboard displaying the Microsoft OneDrive health

Moreover, using in-built machine learning intelligence, eG Enterprise automatically baselines the performance of your Microsoft services across locations and helps analyze the impact of moving to the cloud. Out-of-the-box reports and actionable analytics deliver insights for historical trending, capacity planning and cloud scaling. Events that have occurred in the Office 365 environments are

also captured and reported with the start time of the event, severity and description.

| | COMPONENT TYPE | COMPONENT NAME | DESCRIPTION | START TIME | | |
|----|-----------------------------|----------------|---|--------------------|---|---|
| 1 | Microsoft Office 365 | GMT_365 | SharePoint Online service health has degraded for GMT_365 | Dec 02, 2019 00:38 | 🔍 | 🔗 |
| 2 | Microsoft Exchange Online | GMT_exo | Inactive users detected on Microsoft Exchange Online GMT_exo | Dec 02, 2019 00:44 | 🔍 | 🔗 |
| 3 | Microsoft Exchange Online | GMT_exo | Inbound spam items detected on Microsoft Exchange Online GMT_exo | Dec 02, 2019 00:00 | 🔍 | 🔗 |
| 4 | Microsoft Exchange Online | GMT_exo | Outbound spam items detected on Microsoft Exchange Online GMT_exo | Dec 02, 2019 00:00 | 🔍 | 🔗 |
| 5 | Microsoft Exchange Online | GMT_exo | DLP Policy Hits detected on Microsoft Exchange Online GMT_exo | Dec 02, 2019 00:00 | 🔍 | 🔗 |
| 6 | Microsoft Exchange Online | GMT_exo | Many delivery failed messages found on Microsoft Exchange Online GMT_exo | Dec 02, 2019 00:00 | 🔍 | 🔗 |
| 7 | Microsoft Exchange Online | GMT_exo | Many delivery pending messages found on Microsoft Exchange Online GMT_exo | Dec 02, 2019 00:00 | 🔍 | 🔗 |
| 8 | Microsoft Exchange Online | GMT_exo | Alert detected for Unknown of Mail Traffic Statistics | Dec 02, 2019 00:00 | 🔍 | 🔗 |
| 9 | Microsoft Exchange Online | GMT_exo | Inbound malware items detected on Microsoft Exchange Online GMT_exo | Dec 02, 2019 00:00 | 🔍 | 🔗 |
| 10 | Microsoft Exchange Online | GMT_exo | Inbound malware items detected on Microsoft Exchange Online GMT_exo | Dec 02, 2019 00:00 | 🔍 | 🔗 |
| 11 | Microsoft Exchange Online | GMT_exo | Inbound malware items detected on Microsoft Exchange Online GMT_exo | Dec 02, 2019 00:00 | 🔍 | 🔗 |
| 12 | Microsoft Exchange Online | GMT_exo | Outbound malware items detected on Microsoft Exchange Online GMT_exo | Dec 02, 2019 00:00 | 🔍 | 🔗 |
| 13 | Microsoft SharePoint Online | GMT_spo | IIS latency is high on Microsoft SharePoint Online GMT_spo | Dec 02, 2019 00:03 | 🔍 | 🔗 |
| 14 | Microsoft SharePoint Online | GMT_spo | Health score indicates the Microsoft SharePoint Online service GMT_spo is ... | Dec 02, 2019 00:03 | 🔍 | 🔗 |
| 15 | Microsoft SharePoint Online | GMT_spo | Request processing duration is high on Microsoft SharePoint Online GMT_spo | Dec 02, 2019 00:03 | 🔍 | 🔗 |
| 16 | Microsoft SharePoint Online | GMT_spo | Service is not healthy for Microsoft SharePoint Online GMT_spo | Dec 02, 2019 00:03 | 🔍 | 🔗 |

Figure 76: The events that have been captured in the Office 365 environment

- **Monitoring Microsoft Teams:** Microsoft Teams is a hub that brings everything together in a shared workspace where users can chat, meet, share files, and work with business apps. To ensure that user experience with Microsoft Teams remains above-par all the time, eG Enterprise v7 monitors Microsoft Teams and reports the call quality of various Teams services like audio, video, AppSharing, File transfers, IMs, and more. The streams 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, and meetings are monitored, so that administrators can assess the level of activity on Microsoft Teams. The Tabs, bots and connectors of Microsoft Teams are monitored periodically to figure out the additions, removals and modifications. The activities of the team member, team owner and global admin activities are also monitored, and activities that are 'suspect' are highlighted.
- **Monitoring Skype for Business Online:** eG Enterprise v7 monitors Skype for Business Online and reports critical metrics to administrators. The Skype sessions are monitored and the top users who are engaged in Instant Messaging and File transfers are identified. By monitoring Skype video sessions, eG accurately captures the top users in terms of the number of video streams they sent/received. eG also alerts administrators if the provisioning health status is abnormal and if there are one/more pending activations.
- **Monitoring OneDrive:** Microsoft OneDrive helps you to easily store, access and discover your personal and shared work files in Office 365, including Microsoft Teams, from all the devices. The edits users make offline are automatically uploaded next time they connect. eG Enterprise v7 provides extensive monitoring support to OneDrive. The storage space allocated to Microsoft OneDrive is reported and the storage space usage is tracked, so that administrators are proactively alerted to a potential storage space crunch. During such times, eG also leads administrators to the exact sites that are contributing to the storage crunch. Additionally, eG reveals inactive and orphaned sites to administrators, so that they can decide if such sites can be removed to release storage space. The user activity on OneDrive can be monitored, and in the process, the inactive users can be pulled up. The File/folder/site sharing requests are monitored to figure out the blocked invitations. The unique client IPs, destinations, operations and users frequently sharing the files/folders are identified. The sites that are inactive and those that do not perform synchronization activities are revealed. The

users, client IPs that are frequently performing synchronization activities are identified.

5.3 Reporter Enhancements for Exchange Online

- **Exchange Online Health Report:** To historically analyse the uptime and performance of the Exchange Online service over a period of time and to improve the diagnosis of problems detected in the Exchange Online service, eG Enterprise v7 offers the Exchange Online Health report. The service incidents detected over a period of time helps administrators identify the pattern of the occurrence of service incidents and detect if there was a history of unplanned incidents in the past.

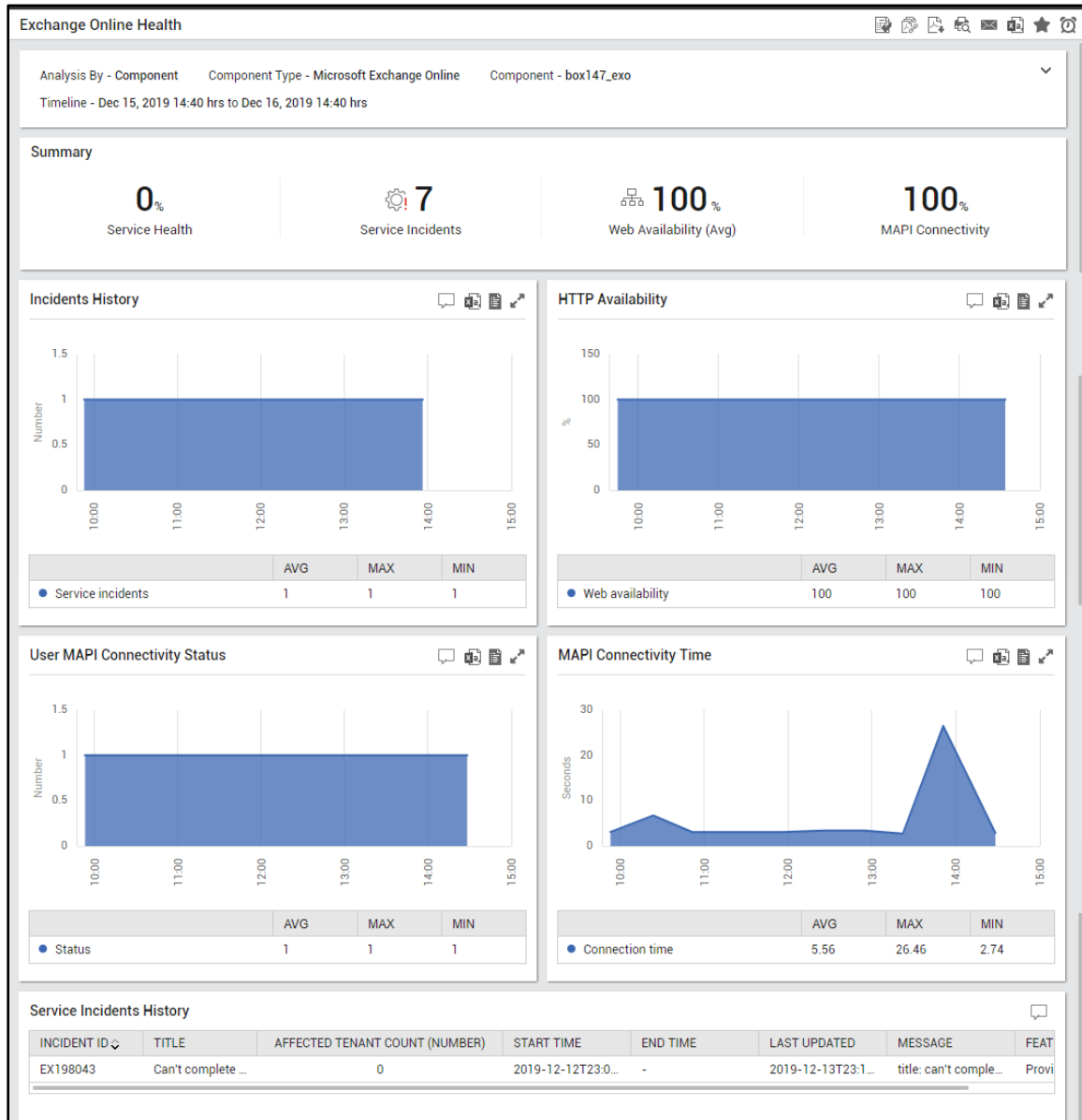


Figure 77: The Exchange Online Health report

- **Mailboxes Report:** To efficiently manage the user mailboxes, administrators must audit the user

mailboxes and detect the pattern of the following with respect to the user mailboxes:

- The mailboxes that were newly created, and the ones that were modified / soft-deleted over a period of time;
- The mailboxes that were on hold, the type of hold – whether it is Litigation hold or In-place hold;
- The mailboxes that are shared;
- The mailboxes that have been enabled for forwarding mails to external addresses.

The Mailboxes report offered by eG Enterprise v7 helps administrators perform such audit analysis with ease.

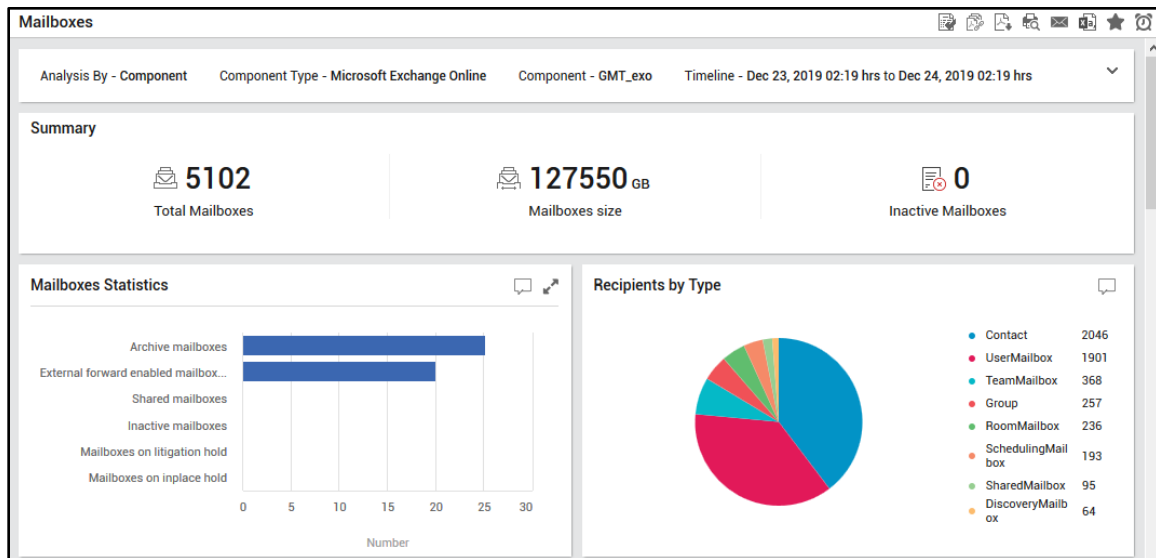


Figure 78: The Mailboxes report

- **Groups Report:** In Exchange Online environments, administrators often find it challenging to analyse the distribution groups, dynamic distribution groups and Office 365 groups during audits. To manage the groups in a much better way and to generate an audit report on the groups that are available in the Exchange Online environments, eG Enterprise v7 offers a Groups report. By generating this report, administrators can identify those groups (distribution/dynamic distribution/Office 365) that contain the maximum number of orphaned groups and empty groups, analyse the ownership of the groups and delete then groups that are inactive for a long period as part of optimizing the environment. Administrators will also be in a better position to historically

analyse the activity of the groups and figure out when exactly the groups were more productive.

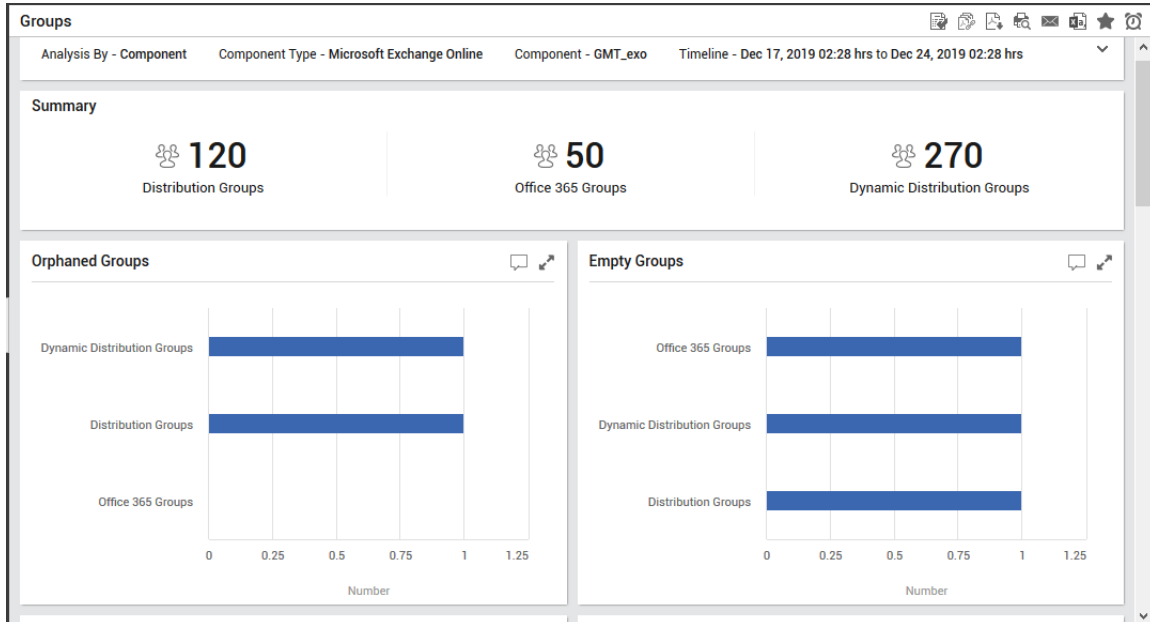


Figure 79: The Groups report

- **Mail Traffic Statistics Report:** In Exchange Online environments, it is necessary to monitor the mail traffic at all times and administrators need to analyse the trend in mail traffic, figure out when there was a surge in mail activity and when the mail delivery was sluggish. The Mail Traffic Statistics report offered by eG Enterprise v7 helps administrators determine such patterns and helps administrators in understanding mail delivery failures/slowness and identify pain points using which the efficiency of mail delivery in Exchange Online environments can be improved considerably.

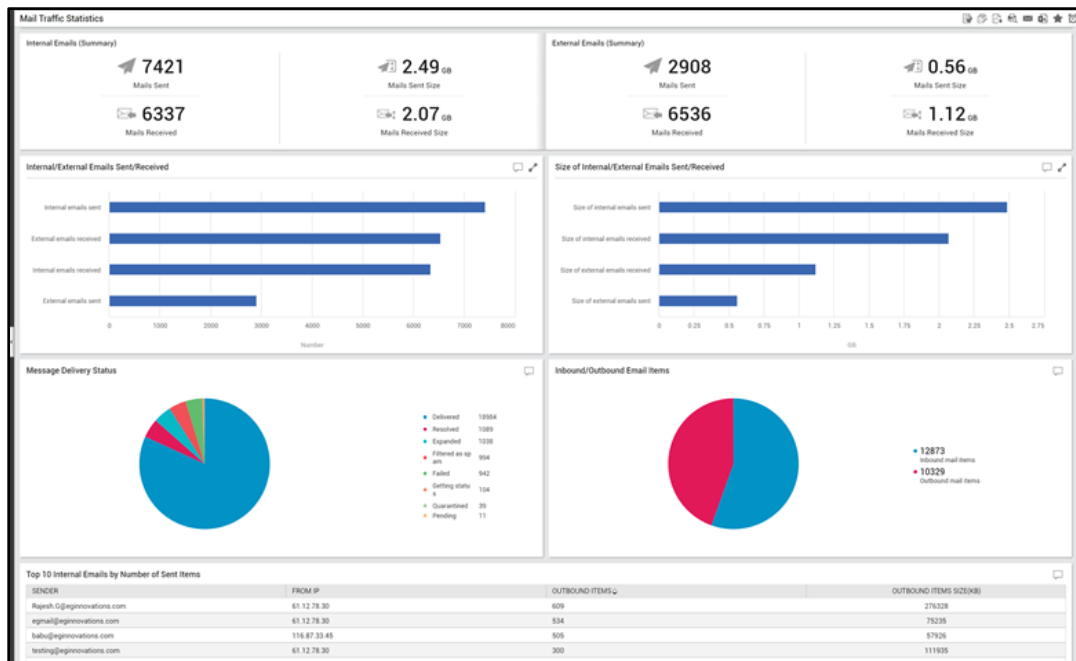


Figure 80: The Mail Traffic Statistics report

- **Spam Detections:** In real-time, for any Exchange Online administrator, detecting spam mails and keeping those mails at bay is a huge task. To achieve this, administrators should periodically filter out spam mails and identify the unique senders sending the spam mails. Analysing the trend over a period of time will help administrators in realizing the spam mail patterns and also in gaining more control over the mail traffic in their environments by removing the spam mails then and there. The Spam Detections report helps administrators in this regard.

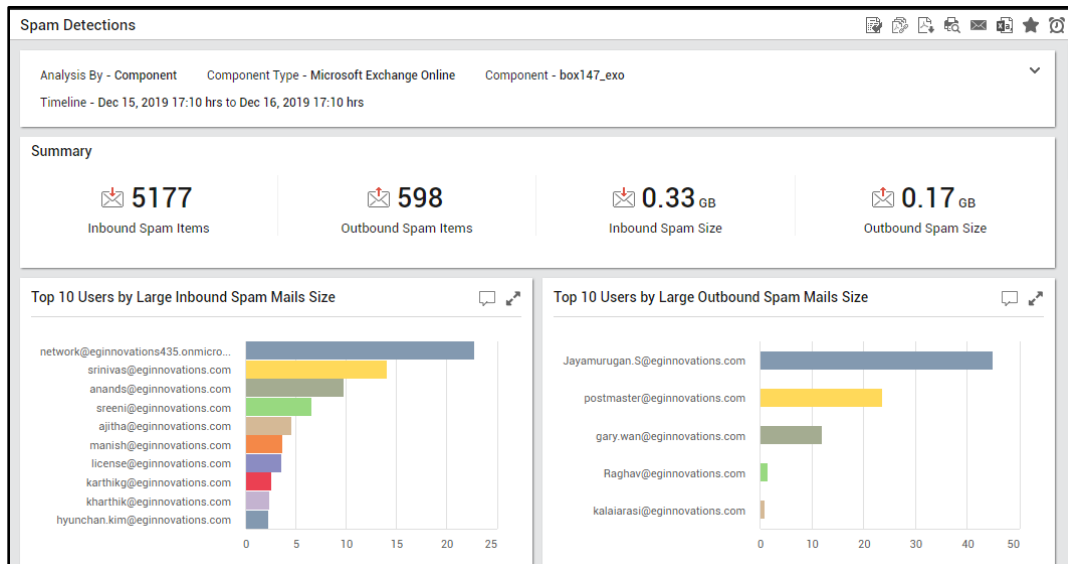


Figure 81: The Spam Detections report

- **Malware Detections Report:** One of the challenges faced by an Exchange Online administrator is to isolate vulnerable mailboxes that may get infected by malware. Administrators also need to analyse the trend of the mailboxes that were infected by malware and identify the senders sending the malware and the receivers who are receiving the malware. Analysing the pattern of malware detection helps administrators in assessing the severity of malware infection and review the configuration of malware protection policies of Exchange Online from time to time. The Malware Detections report offered by eG Enterprise v7 helps administrators in this regard. Using this report, administrators can strengthen the security of their Exchange Online environment and proactively

protect the environment.

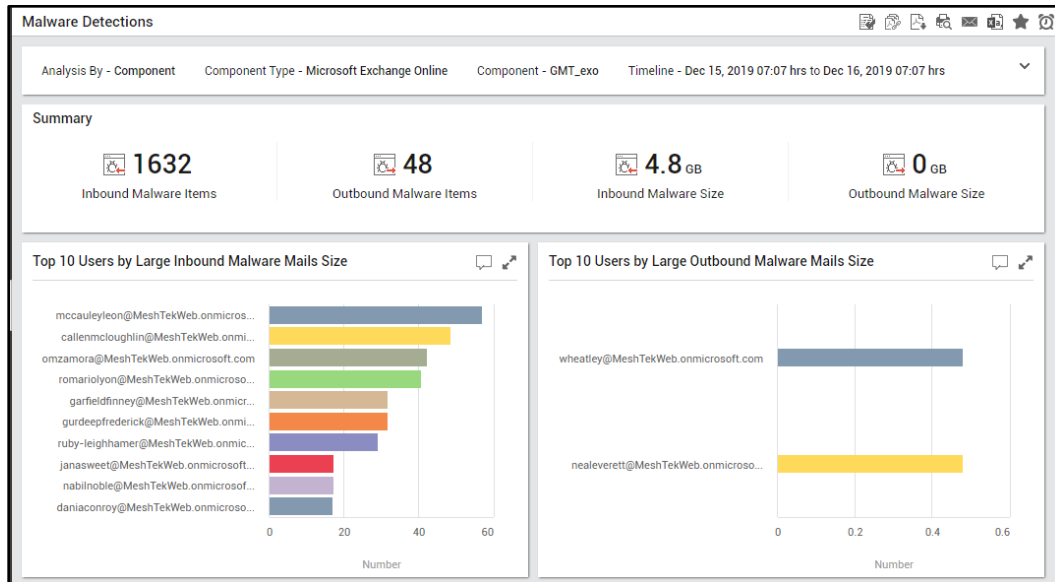


Figure 82: The Malware Detections report

- **Exchange Online Activity Report:** For effective functioning and smooth performance of the Exchange Online, it is necessary for the administrators to constantly analyse the trends noticed in the activities performed by both administrators and users alike. The Exchange Online Activity report helps administrators in performing such audits. By analysing the activities performed by the administrators, the operations that were performed the most by the administrators can be detected. The unique users performing the operations are identified and operation failure patterns are

analysed.

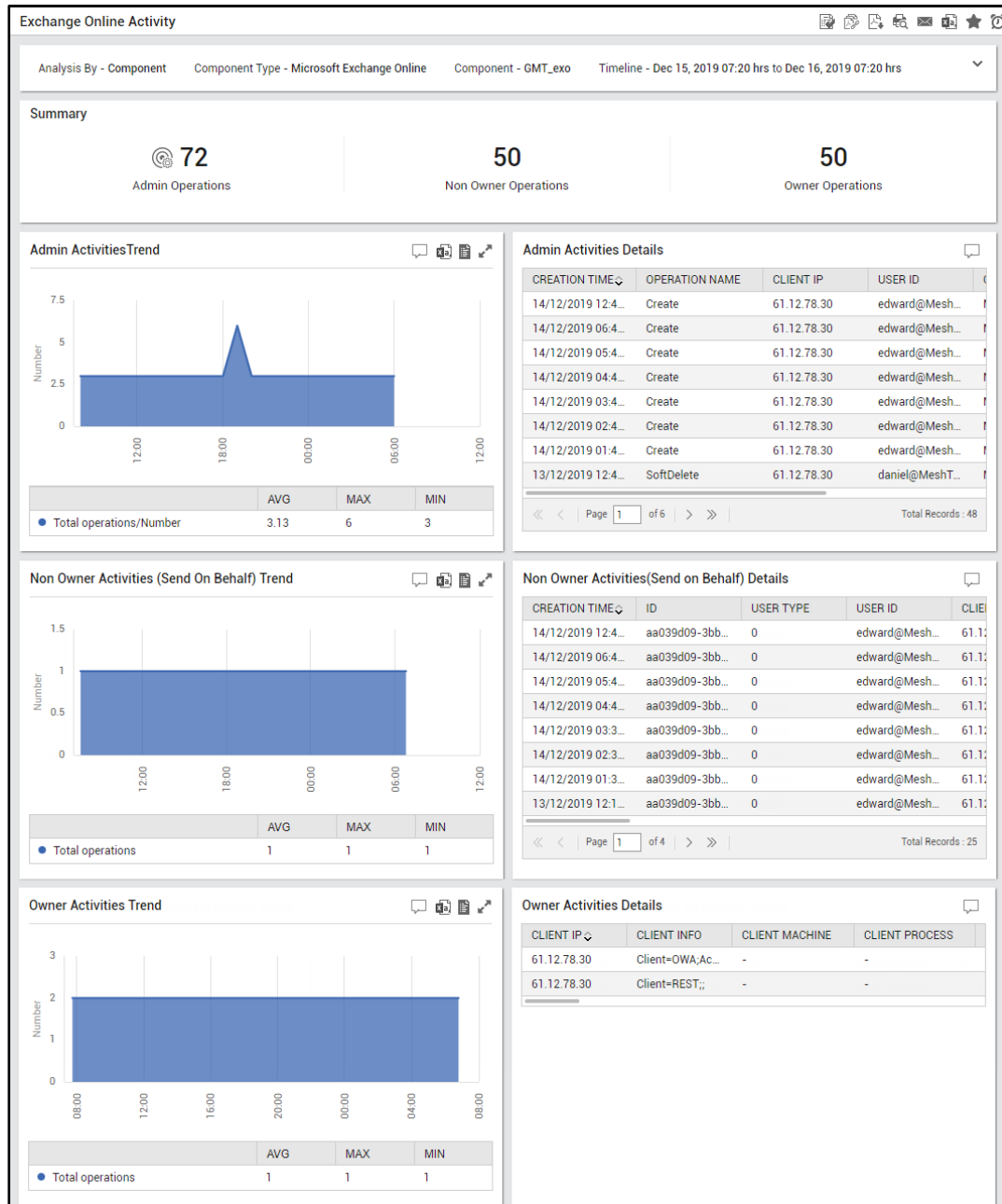


Figure 83: The Exchange Online Activity report

5.4 Reporter Enhancements for Microsoft Office 365

- **Service Health Report:** As with any cloud-hosted service, service disruptions, downtime and slow connectivity issues are bound to affect business continuity and Office 365 administrators require actionable insight to proactively alert them when performance starts to degrade and to help them resolve problems quickly. eG Enterprise v7 helps Office 365 administrators generate a Service Health report which throws light on the service health and incident history over time. This report also helps administrators in post-mortem analysis of the data which in turn would help administrators in

understanding the pattern of Office 365 performance problems.

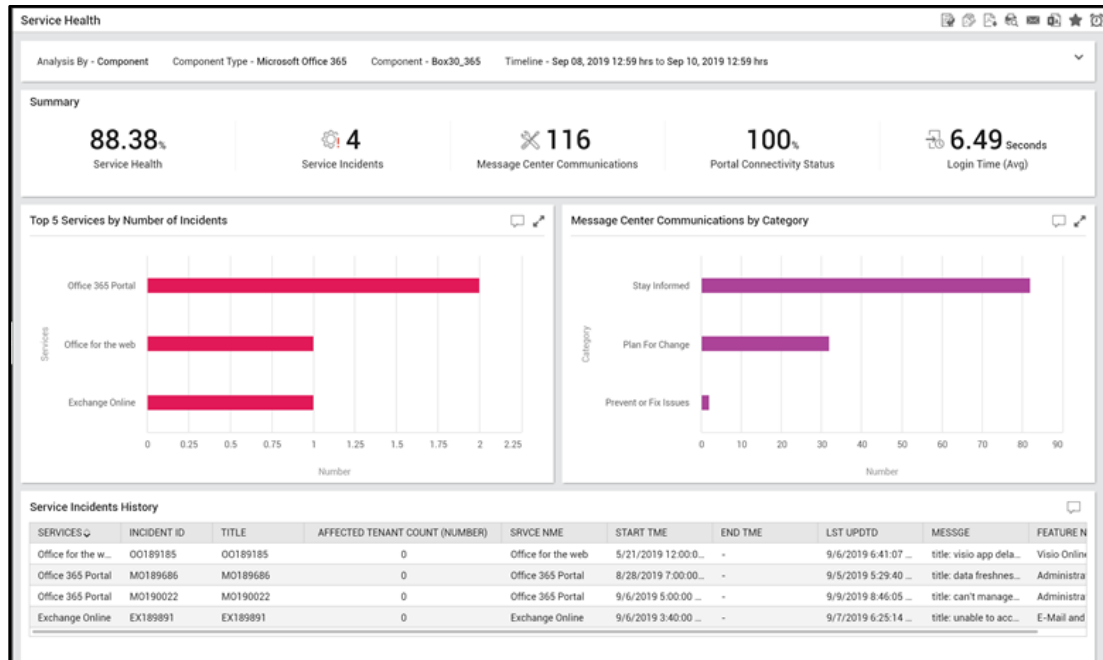


Figure 84: The Service Health report

- **License Usage Report:** When you buy an Office 365 subscription, you specify the number of licenses that you need, based on how many people you have in your organization. eG Enterprise v7 tracks the validity and usage of these licenses and proactively alerts administrators to any potential license shortage / expiry. To analyze the trend of applications/services that the users have subscribed for under the Office 365 product, administrators can use the License Usage report.

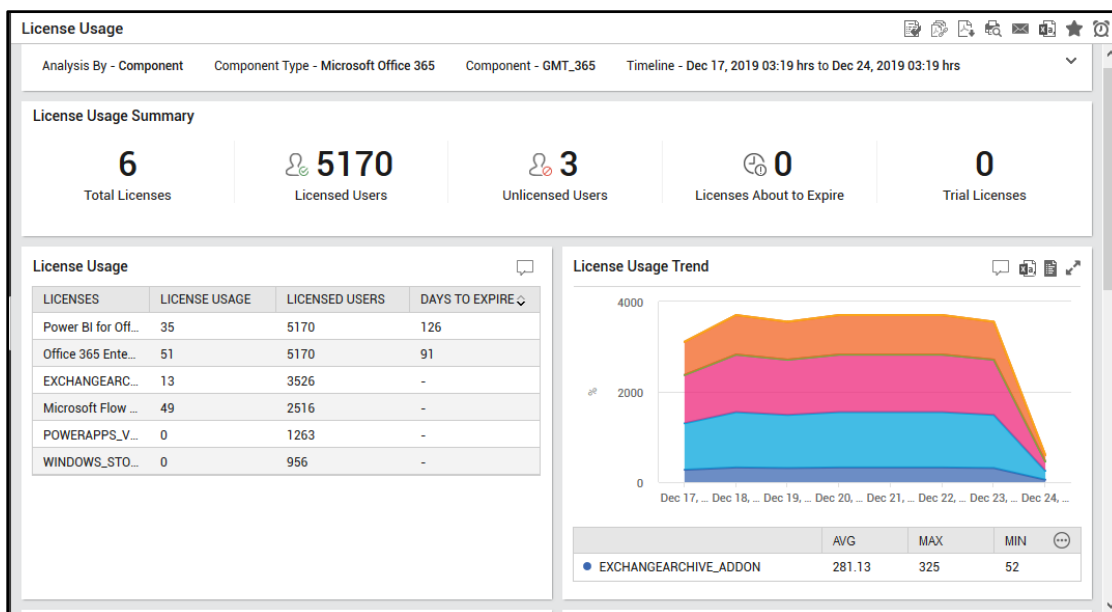


Figure 85: The License Usage report

- **User Activities Report:** Administrators can use the User Activities report offered by eG Enterprise

v7 to view the trends of user activities on the Office 365 products by operations and logons. By closely observing the generated report, administrators can infer when exactly the successful/failed logins peaked, who are the top users/client IPs by number of operations etc.

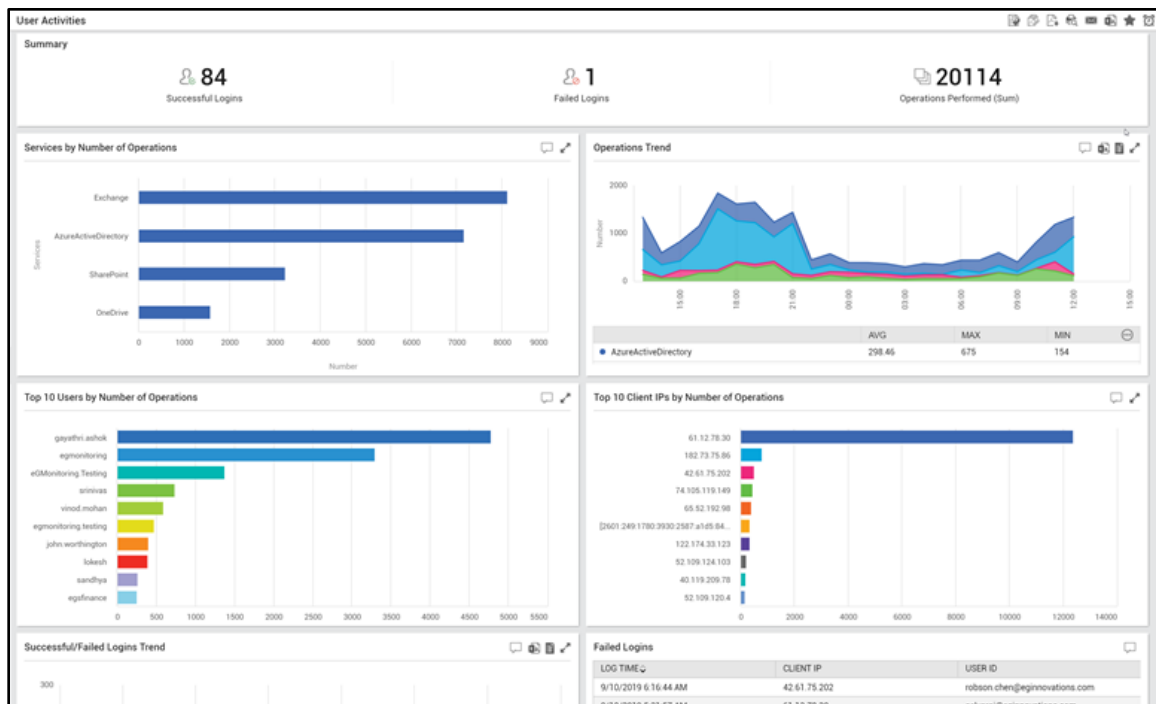


Figure 86: The User Activities report

- **Groups Report:** The Groups report offered by eG Enterprise v7 helps administrators in performing historical audit analysis on distribution groups, dynamic distribution groups, Office 365 groups, and security groups.

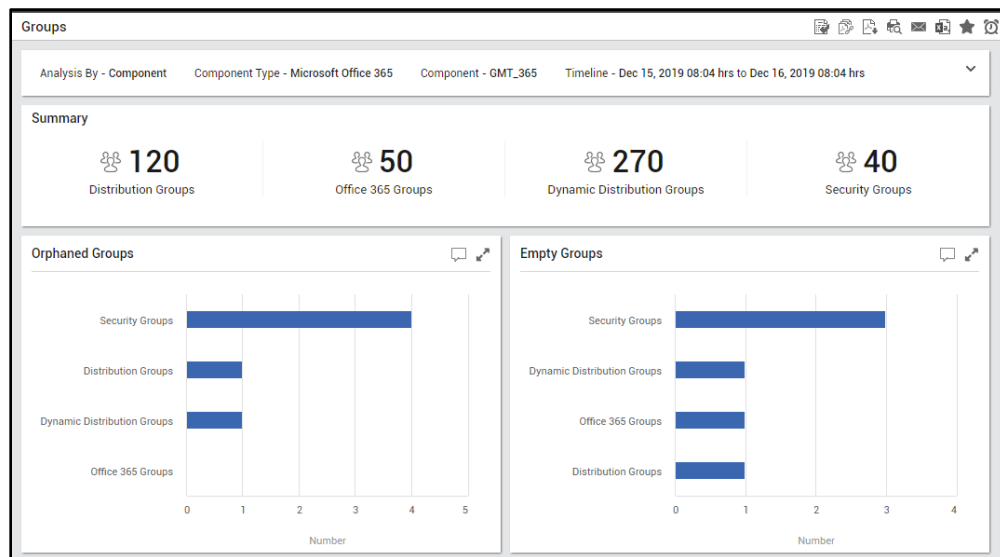


Figure 87: The Groups report

5.5 Reporter Enhancements for Microsoft SharePoint Online

- **SharePoint Online Health Report:** To historically analyse the uptime and performance of the SharePoint Online service, and to detect/diagnose service incidents, eG Enterprise v7 offers the SharePoint Online Health report. Analysis of the service incidents that occurred during a given period of time helps administrators to trace patterns and see if there was a history of unplanned service incidents in the past.

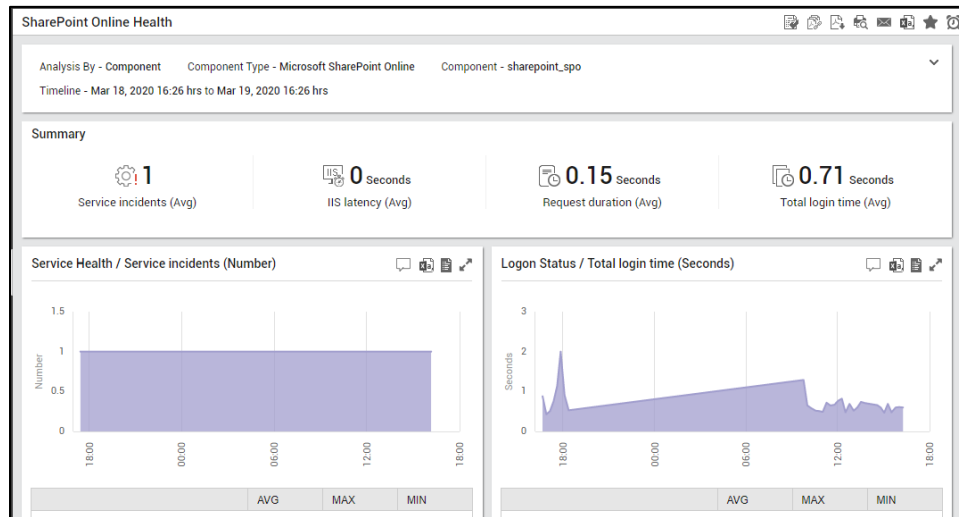


Figure 88: The SharePoint Online Health report

- **Site Administration Activities Report:** In SharePoint Online environments, there may exist multiple administrators (for e.g., Global Administrators, SharePoint Administrators). Each administrator has his/her own privileges and restrictions. There may always be a probability that changes made by one administrator get inadvertently overridden by another! To analyse the changes made across SharePoint Online over a period of time, and most importantly, to identify which administrator effected what change, eG Enterprise v7 offers the Site Administration Activities report. This report helps administrators in auditing the administrative operations performed on SharePoint Online over a period of time, identify the administrators who effected the changes, the clients from

which the changes were performed and the sites that were impacted.

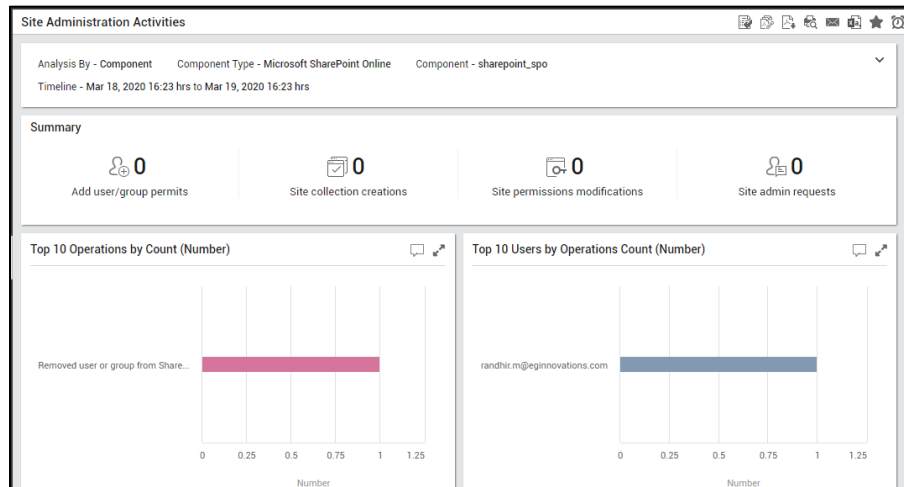


Figure 89: The Site Administration Activities report

➤ **Site Usage Summary Report:** This report provides a quick summary of usage across SharePoint Online sites over time. A single look at this report will point you to:

- Sudden/steady surges in activity levels across sites;
- Sites that experienced a high level of activity during the given period, in terms of page views and visits;
- Sites that consumed more storage space than the rest, during the chosen period;

With the help of these insights, administrators can correlate the load on the individual sites with their storage allocation and usage. In the process, you can figure out if any site requires additional storage space to handle its current/future demand.

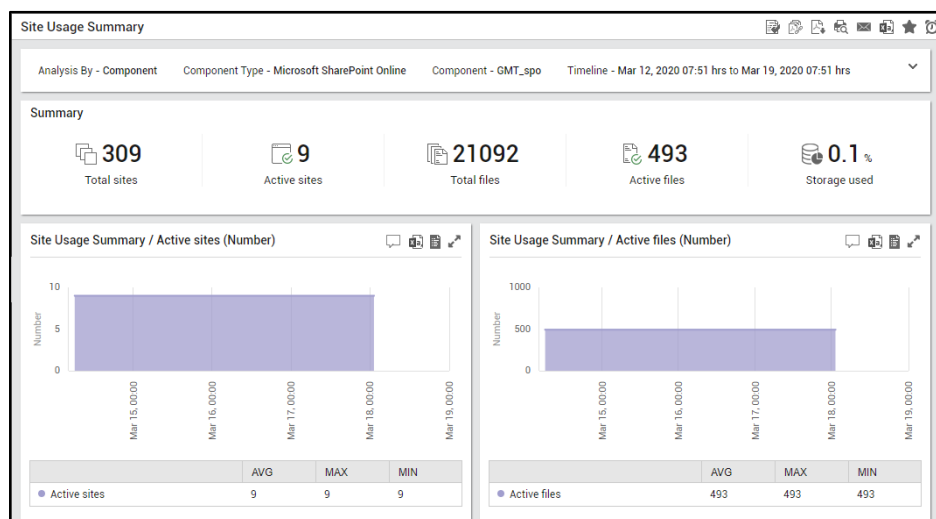


Figure 90: The Site Usage Summary report

➤ **Content Growth Analysis Report:** A SharePoint administrator should constantly keep track of the growth of the SharePoint and Content databases to proactively detect and if possible, avert, abnormal growth in database size. For this purpose, eG Enterprise v7 offers the Content Growth Analysis report.

By generating this report, administrators can identify the growth rate of the content database over a period of time. The storage space used by the recycle bin and the content databases are analysed to figure out if the database has recorded abnormal growth over a period of time. The growth rate of the site collections and the sites are also analysed for abnormalities. The top active site collections and the sites in terms of growth helps administrators in identifying site collections/sites that may require additional storage space.

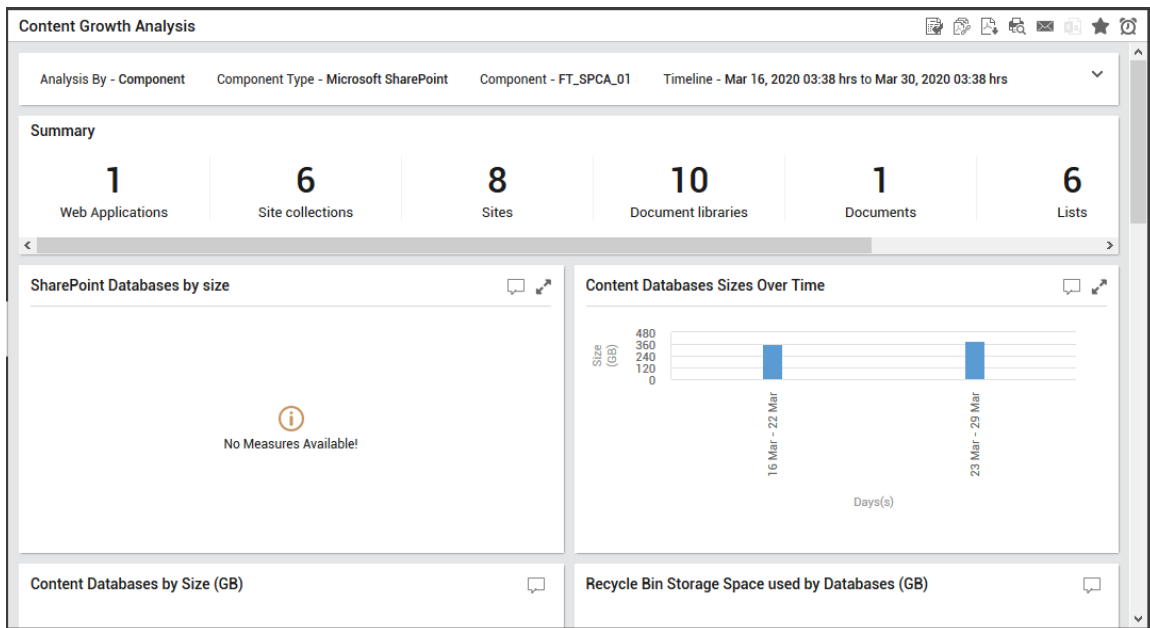


Figure 91: The Content Growth Analysis report

- **Synthetic File Operations Report:** One of the key factors influencing user experience with SharePoint Online are file operations. If critical file operations such as checkin, checkout, upload, download etc., fail frequently or take too long to complete, it will impact user productivity and may result in many 'unhappy' users. To improve user experience with SharePoint Online, it is imperative that administrators make sure that file operations are successful and execute rapidly at all times. For this purpose, eG Enterprise v7 simulates file operations to the site at pre-configured intervals, using the SharePoint REST API, and proactively alerts administrators to issues before real users start complaining. The results of these simulations are used for generating the **Synthetic File Operations** report. By generating this report, administrators can easily figure out when exactly the operations performed on the files failed and what type of operation failed frequently. This would help administrators in troubleshooting issues related to the file operations!

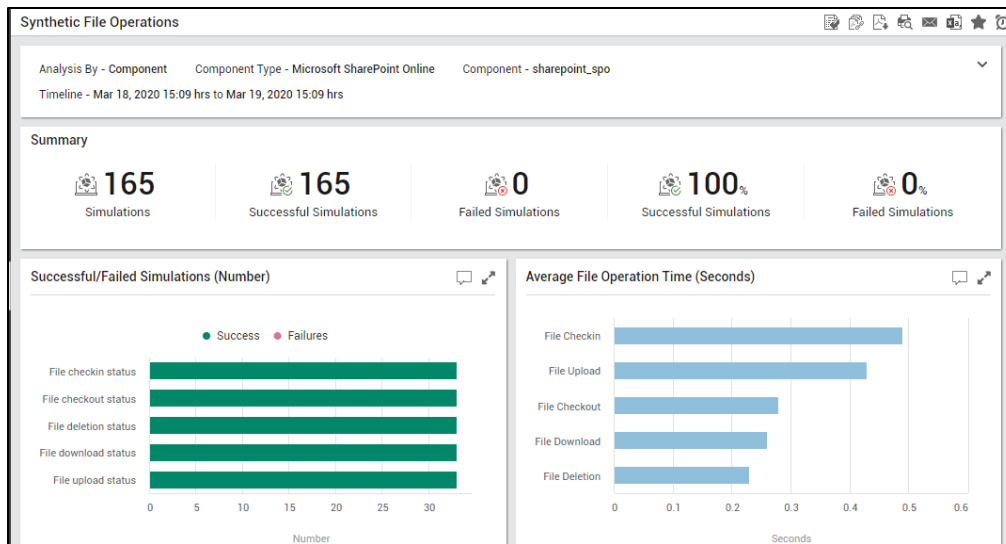


Figure 92: The Synthetic File Operations report

- **File and Page Activities Report:** Use the File and Page Activities report offered by eG Enterprise v7 to analyze the file and page operations performed by the users on Microsoft SharePoint Online 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.

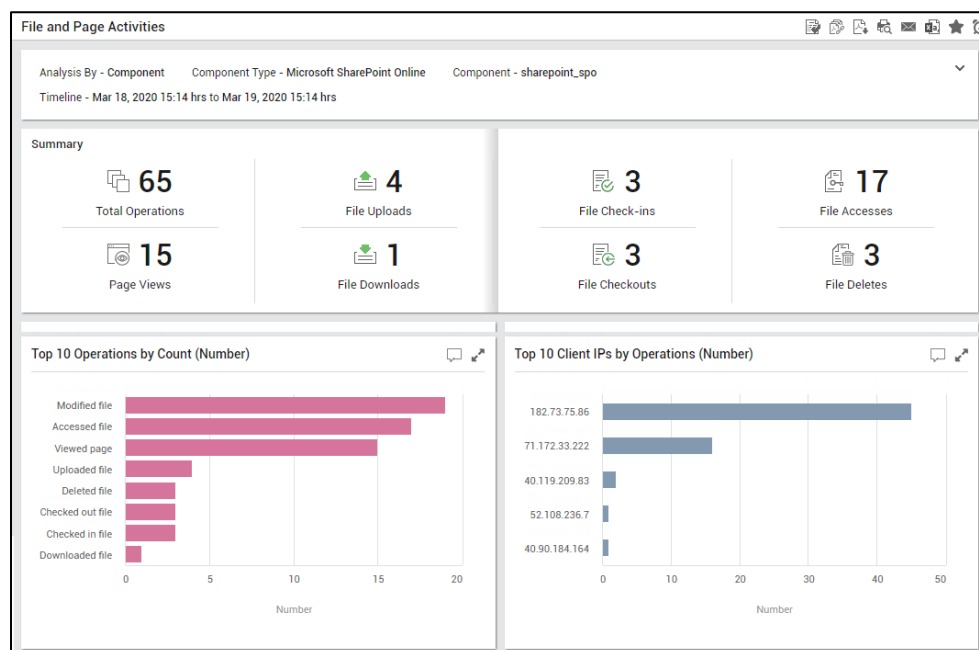


Figure 93: The File and Page Activities Report

- **Synchronization Activities Report:** The Synchronization Activities Report offered by eG Enterprise v7 helps administrators in effectively auditing the synchronization activities that users perform on files. 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 on the file as part of

synchronization, the unique users performing synchronization etc.

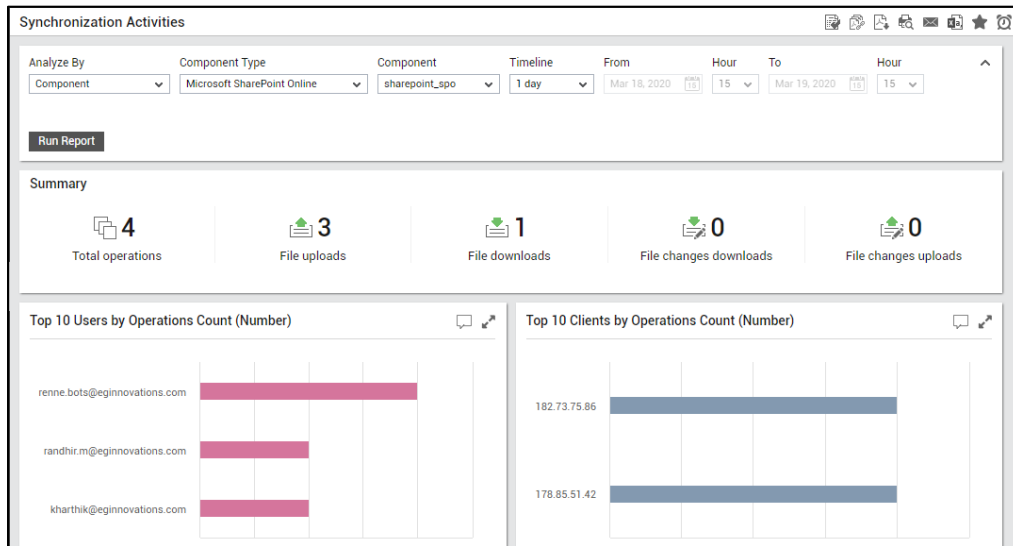


Figure 94: The Synchronization Activities Report

- **Folder Activities Report:** To historically analyze the folder operations performed by users on Microsoft SharePoint Online, administrators can use the Folder Activities report offered by eG Enterprise v7. 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.

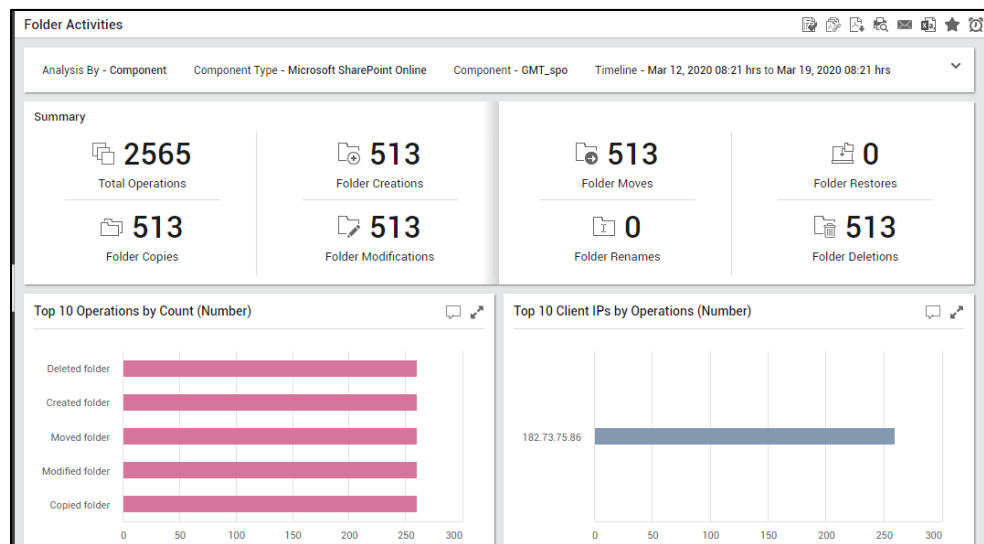


Figure 95: The Folder Activities Report

- **Sharing and Access Request Activities Report:** In SharePoint Online environments, administrators need to maintain the security and integrity of the data stored in the sites regardless of how the contents of the site are accessed (whether it is by requesting access, or via sharing invitations, or via sharing links). A security lapse may expose the contents of the site to malicious attacks. To ensure that sensitive activities are performed by authorized individuals alone, administrators need to periodically audit these sensitive activities. For this purpose, eG Enterprise v7 offers a Sharing and Access Request Activities Report. By generating this report, administrators can

historically analyze the access requests, sharing invitations and sharing links, and closely scrutinize them to understand who initiated the operation frequently, on which site, and from where.

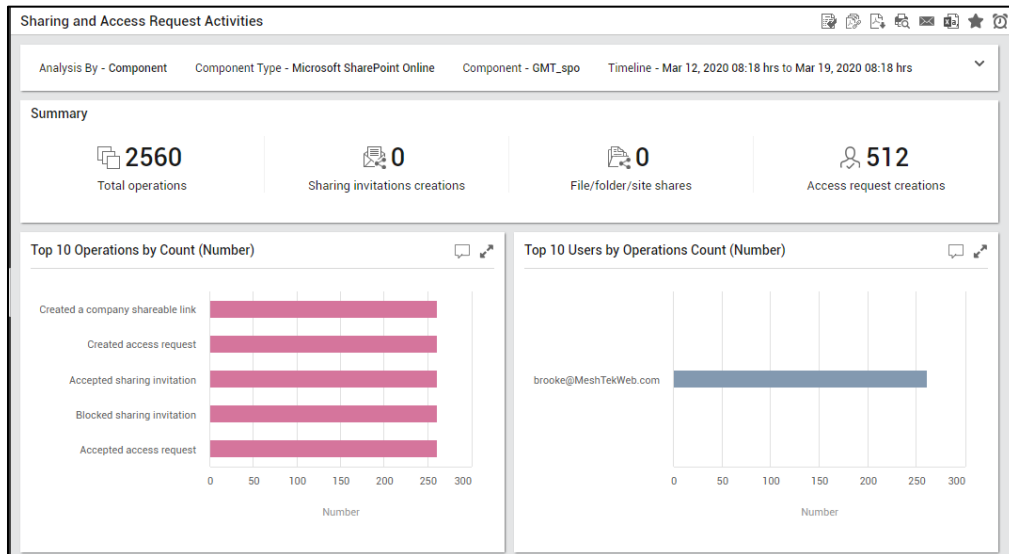


Figure 96: The Sharing and Access Request Activities Report

5.6 Additional Monitoring Support for SaaS Applications

In addition to the above enhancements, eG Enterprise v7 adds out-of-the-box monitoring support for Salesforce.

- **Monitoring Salesforce:** Salesforce offers customer-relationship management service through cloud platforms. Salesforce provides companies with an interface for case management and task management, and a system for automatically routing and escalating important events. The Salesforce customer portal provides customers the ability to track their own cases, includes a social networking plug-in that enables the user to join the conversation about their company on social networking Web sites, provides analytical tools and other services including email alert, Google search, and access to customers' entitlement and contracts. For the businesses that use cloud platforms like Salesforce to thrive, it is of utmost importance for the components of Salesforce to be available round the clock. eG Enterprise v7 helps administrators monitor the availability and performance of the critical components/systems of Salesforce, so that glitches can be captured and fixed, before they challenge business continuity. Using the metrics reported by eG, the inactive users and users who are removed can be identified with ease. The user sessions that are initiated frequently and are currently active are identified and reported for each type of network connection, so as to ascertain network latencies during session initialization. The Salesforce objects are monitored, and administrators alerted to a sudden/unusual increase in the number of objects. Network availability to the Salesforce portal is also monitored, and any break in the network connection is immediately reported. The storage of Salesforce is monitored, so that administrators are alerted to shortage of storage space before it is too late. The top users of data and file storage are monitored and reported at periodic intervals. The validity of licenses to the Salesforce portal is also tracked and administrators alerted to licenses that are about to expire.

6. Extended Monitoring Reach to Support

New IT Infrastructure Components

To provide more extensive coverage of IT infrastructures, eG Enterprise v7 has added monitoring support for an array of new components. The following sections provide a detailed report on the components

6.1 Network Monitoring Enhancements

The following enhancements have been made to eG Enterprise's network monitoring capabilities in 7:

- **Monitoring Cisco Meraki:** The Meraki MX is an enterprise security & SD-WAN appliance designed for distributed deployments that require remote administration. Meraki MX appliances are equipped with SD-WAN capabilities that enable administrators to maximize network resiliency and bandwidth efficiency. eG Enterprise v7 offers complete monitoring support to the Cisco Meraki. Using the metrics collected, the count of clients connected to the access point, status of the uplink interface, latencies in data transmission and reception by each client connected to the security appliance/switch, the count of clients connected to the switch and failures on the appliance can be detected.
- **Enabling BGP monitoring on Cisco Routers:** BGP (Border Gateway Protocol) is an interdomain routing protocol designed to provide loop-free routing links between separate routing domains that contain independent routing policies (autonomous systems). BGP is designed to run over a reliable transport protocol, preferably TCP. A network administrator usually manually configures the relationships between BGP-speaking devices. A peer device is a BGP-speaking device that has an active TCP connection to another BGP-speaking device. This relationship between BGP devices is often referred to as a neighbor. When a TCP connection is established between peers, each BGP peer initially exchanges all its routes - the complete BGP routing table - with the other peer. eG Enterprise v7 is now capable of auto-discovering the BGP peers through the Cisco routers and reporting the status of each BGP peer. This way, the BGP peer that is too busy processing messages can be identified with ease.
- **Monitoring Big-IP Access Policy Manager:** Access Policy Manager secures, simplifies, and protects user access to apps and data, while delivering the most scalable access gateway in the market. In version 7, the Access Policy Manager module offers vital statistics on the sessions initiated using the Access profile and statistics relating to transmitting/receiving data to/from the connectivity profile. The users experiencing slowness while being connected to the F5 appliance using access profiles can be identified. The sessions initiated by Citrix users can also be identified.
- **Monitoring McAfee Email Gateway:** McAfee Email Gateway integrates comprehensive inbound threat protection with outbound data loss prevention, advanced compliance, detailed reporting, and simplified administration. This is why, the McAfee Email Gateway is commonplace in high-security environments, where security of the mailing infrastructure cannot be compromised! In such environments, any degradation in the performance of the email gateway can expose the environment to malicious attacks and potential security risks. To avoid such an outcome, eG Enterprise v7 provides deep insights into the performance of the McAfee Email Gateway and proactively alerts them to probable security threats. The status of the sensors of the hardware components such as temperature, voltage, cooling units, and UPS are monitored and reported. The CPU and memory utilization of the email gateway is continuously monitored and administrators alerted potential resource constraints. Disk space usage of the different partitions – e.g., deferred partition, logging partition, etc. – is tracked, and the partitions that may soon run out of disk space are pinpointed. The overall health of each process on the server is reported so that processes in corrupt and critical states can be identified. The status of the inbound / outbound email messages is tracked, so that administrators are notified if any message has bounced, has been blocked, or has been quarantined by the email gateway.

- Starting with eG Enterprise v7, host level metrics such as processes executing on the server, CPU and memory usage of each process executing on the server are reported for the following component types:
 - F5 Advanced Firewall Manager
 - F5 Application Delivery Controller
 - Forcepoint firewall
 - McAfee Network Security Manager
 - McAfee Enterprise Firewall
 - Imperva manager
 - Imperva Gateway
 - CheckPoint Firewall Manager

In addition, by polling the NetSNMP MIBs administrators can figure out the disks that are running out of space. Dwindling memory resources can be identified, and administrators can be prompted to add additional memory. The user processes and system processes consuming too much of CPU resources are tracked and reported.

- **Specialized Monitoring of Juniper MX Router:** Powered by the Junos operating system and the programmable Trio chipset, Juniper MX Series Routers provide powerful routing, switching, security, and services features that help network operators transform their networks - and their businesses - in a hyper-connected world. eG Enterprise is capable of performing specialized monitoring of Juniper MX Routers. The metrics reported includes monitoring the CPU and memory of the router at periodic intervals to track the utilization levels. The status of each hardware component is monitored, and hardware failures promptly captured. In environments where BGP neighbors are connected to the router, the data transmitted and received through each BGP neighbor are monitored and reported periodically. Various latency metrics are reported to enable administrators to capture slowness and diagnose its source.
- **Monitoring Peplink WAN Router:** Peplink WAN Router is an ideal single box solution for medium to large business environments and allows service providers to enable highly available multi-network services without any complexity. eG Enterprise v7 monitors the Peplink WAN Router and reports a slew of metrics which includes determining the uptime of the router, CPU and memory monitoring to determine the utilization levels of the router, determining the current state and throughput of each VPN profile, and reporting the current state and throughput of each WAN connection. Administrators can also keep a vigil on the count of dropped packets to ascertain if there is any malicious activity over the router.
- **Monitoring HP Procurve Switch:** HP Procurve Switch is an IP switch that provides reliable port connectivity with uplinks to increase secure and fast business traffic. Using eG Enterprise v7, 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, power supply and temperature probes of the switch is also periodically monitored and reported. The status of the sensors in the switch is continuously monitored and sensor failures are promptly captured. If accesses to packet buffers fail, administrators are duly notified.
- **Monitoring Dell Force 10 Switch:** The Dell Force10 Switches bring core-like resiliency in a compact form factor to the network edge, enabling cost-effective scalability. These high performance and low latency Gigabit Ethernet switches deliver the critical functionality that advanced data center network edges demand. Using eG Enterprise v7, you can monitor the resource usage of the switch and determine if the switch has been sized right. Hardware failures come to light. The overall status and uptime of the stack unit is tracked and abnormalities (if any) are highlighted.

- **Monitoring of Nokia IPSO Firewall:** Nokia IPSO firewall appliance is built based on the IPSO operating system, which was developed from a branch of the FreeBSD operating system, with numerous hardening features applied. This basis makes the Nokia IPSO firewall very stable and more secure to the environments. Nokia IPSO firewall helps organizations that are determined to keep control over their network resources from endlessly increasing security threats. The IPSO firewall reliably protects the environment, provides the ability to sustain the malicious attacks and assures the data confidentiality, integrity and availability of the resources in the environment. Monitoring of Nokia IPSO Firewall includes capturing hardware failures, detecting potential CPU contentions, checking whether the temperature of the chassis is at acceptable levels, and measuring the resource usage of each virtual system process to identify the resource-hungry ones. The status of the Secure XL feature is also monitored periodically, and the count of connections added/deleted to the firewall by the Secure XL is reported.
- **Monitoring Crypto Server HSM:** CryptoServer HSM is the Hardware Security module that was developed to ensure the efficiency and security for the cryptographic operations. eG Enterprise v7 performs in-depth monitoring of the crypto server HSM, and in the process, points to delays in the processing of service authentication requests, reports ineffective cache usage, and captures authentication failures.
- **Monitoring Brocade FastIron Switch:** The Brocade FastIron switches provide a superior scalable foundation for improved operational efficiency and faster response to business opportunities today and into the future, extending control from the network edge to the backbone with intelligent network services, including superior Quality of Service (QoS), predictable performance, advanced security, comprehensive management, and integrated resiliency. To ensure the high availability and peak performance of this switch at all times, you can use the advanced monitoring capabilities that eG Enterprise v7 provides. Using these capabilities, you can proactively detect probable resource contentions on the switch and promptly detect hardware failures, so that the problems can be fixed before any irreparable damage is done.
- **Monitoring D-Link DGS Switch:** The D-Link DGS Series gives new meaning to flexibility and scalability. Featuring high port densities, switch stacking, and easy management, the switches are ideal for a variety of applications at every scale. With eG Enterprise v7, you can monitor the availability and 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 resource usage of the switch and warns you of potential resource contentions. eG also sends out alerts if hardware components such as fans, PSUs, temperature probes fail.
- **Monitoring Cyberoam Firewall:** Cyberoam UTM and NGFW appliances, available as hardware and virtual security platforms, offer next-generation security to SOHO, SMBs and Enterprise. The Cyberoam Firewall monitoring model offered by eG Enterprise v7 tracks the status of critical firewall services, and alerts administrators if any service stops suddenly or dies. eG also monitors the protocols generating traffic to the firewall, and points to those protocols that are popular. In addition, the count of antivirus alerts that were generated per protocol is also reported, so you can quickly identify the protocol that is vulnerable to virus attacks. Additionally, eG also periodically checks how the firewall is using its CPU, memory, and disk space resources, and sounds off administrators if it anticipates a serious resource contention.
- **Monitoring JetNexus Load Balancer:** JetNexus load balancer/ADC (Application Delivery Controller) ensures that your core business applications are always available and delivered securely to end users with speed and efficiency. To ensure that JetNexus delivers on these promises, eG Enterprise v7 provides a specialized monitoring model for JetNexus that keeps tabs on the availability and overall health of the load balancer and notifies administrators if there are any lapses in its operations. For instance, the CPU and memory of the Switch Processor and Management Processor are monitored and unusual usage patterns are brought to the administrator's attention. The current workload of the load balancer is measured and reported in terms of number of connections, so that administrators can promptly detect a connection overload. The session related

statistics related to the real servers and virtual servers are also reported, so that load-balancing irregularities can be promptly detected and remedied.

- **Monitoring IBM Blade Chassis:** The IBM BladeCenter Chassis unit is a high-density, high-performance, rack-mounted blade server system. To ensure the high uptime of the blade and the virtualization benefits it provides, eG Enterprise v7 periodically monitors the health, power supply status, current voltage and power consumption of the server and each chassis on the server, and promptly reports abnormalities. The operational status of the fan pack and the colors emitted by the LED switches are also periodically tracked, so that administrators can rapidly detect deviations and take appropriate remedial action.
- **Monitoring Riverbed Steelhead:** Riverbed SteelHead offers secure optimization and acceleration of all applications whether it is on-premises or hosted on cloud or offered as a SaaS to enhance workforce productivity anywhere. To ensure the high availability and peak performance of Riverbed Steelhead and dependent applications, eG Enterprise v7 provides specialized monitoring capabilities. The health and uptime of the Steelhead device is monitored round the clock, so that unscheduled boots come to light. CPU, memory, and bandwidth usage is monitored, and usage excesses are promptly reported. The top application ports, top sources, top talkers, and top destinations in terms of traffic flow are accurately pinpointed, so administrators can easily troubleshoot high bandwidth usage conditions. Disk usage is tracked and hits and misses to disk are reported.
- **Specialized Monitoring for Maipu Router:** As a multi-purpose universal data processing and routing platform, Maipu routers provide operators, government, finance, energy, transportation, education, military and other industrial users and large/medium-sized enterprise users with a full range of WAN solutions, widely applied at the core backbone layer and core aggregation layer of the above industries. Monitoring the Maipu router includes analyzing the status and CPU utilization of each task and identify the task that is consuming excessive CPU. The CPUs of the router are monitored to figure out the CPU that is frequently utilized to the maximum. The stack memory utilization levels are monitored and abnormalities if any, are rectified. The overall memory utilization of the router alerts administrators to memory crunch.
- **Monitoring Packet Shaper Load balancer and Packet Shaper S Series Load Balancer:** PacketShaper provides management for web-connected applications such as Cloud applications, social media, recreational video, and audio/video communication. For your popular web/multi-media applications to deliver on their service level guarantees, you need to make sure that the Packet Shaper Load Balancer managing these applications is available, is error-free, and efficiently averts overload conditions. This is why, specialized monitoring capabilities for the Packet Shaper Load Balancer have been embedded in version 7 of eG Enterprise. In this version, the resource usage of the load balancer is continuously monitored and reported, so that administrators can figure out if the load balancer is sized right or not. The health of hardware components is periodically verified, and failures are promptly reported. Data transmissions to and from the class, link, and partition are also monitored, so that unusual traffic flows can be rapidly spotted and investigated.
- **Improved Monitoring of Network Elements Supporting AES Encryption:** In earlier versions, if the Encrypt type parameter of SNMP-based tests was set to AES192 or AES256, the SNMP tests failed to report metrics. To resolve this issue, SNMP tests now take an additional Engine ID parameter. By default, this parameter is set to No. Administrators are required to set this flag to Yes, if they choose AES192 or AES256 as the Encryption type.

6.2 Database Monitoring Enhancements

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

- **Cassandra Database:** Apache Cassandra™ is a massively scalable open source NoSQL database. Cassandra is perfect for managing large amounts of structured, semi-structured, and unstructured

data across multiple datacenters and the cloud. Cassandra's built-for-scale architecture means that it is capable of handling petabytes of information and thousands of concurrent users/operations per second. Cassandra is designed from the ground up as a distributed database with peer-to-peer communication. eG Enterprise v7 provides in-depth insights into the health, response time and overall performance of the Cassandra database servers. The growth of the commit logs and database logs are monitored and abnormalities, if any are detected with ease! The errors logged in the log file are frequently monitored and rectified. Monitoring the compaction activity of the Cassandra database helps administrators identify how frequently compactions are performed on the disks of the Cassandra database server and how many are pending. The status of the nodes of the Cassandra database server helps administrators understand if the node is upto date. Data inconsistencies on the nodes are detected by monitoring the running status of the Gossip protocol service and the native protocol service of each node. Thread pools are monitored and the thread pool that lags in completing the tasks are identified.

- **Hadoop:** The Apache™ Hadoop® project develops open-source software for reliable, scalable, distributed computing. The Apache Hadoop software library is a framework that allows for the distributed processing of large data sets across clusters of computers using simple programming models. eG Enterprise v7 monitors the Hadoop Big Data and provides in-depth insights into the availability and uptime of the key components such as Resource manager and Hadoop name node. Job queues are monitored and failed and killed jobs are highlighted. Corrupt and missing data blocks of the Hadoop HDFS are captured and reported. The I/O processing capability of each data node and each data block are reported, and, in the process, block verification failures are captured. Failed RPC calls and the processing time of the failed calls are periodically tracked so as to analyze failure patterns. The data node on which write operations are taking too long to complete are identified. Journal transactions and the time taken by the journal transactions are monitored and reported periodically. Kerberos logins are periodically monitored to identify frequent login failures. Storage of Hadoop is monitored, and space constraints are identified at the earliest. Containers in the node manager are monitored to figure out the containers that failed. Anomalies are brought to light by monitoring shuffle errors in the jobs processed by Hadoop.
- **Monitoring MySQL Cluster:** MySQL Cluster is the distributed database combining linear scalability and high availability. It provides in-memory real-time access with transactional consistency across partitioned and distributed datasets. eG Enterprise v7 monitors the MySQL 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 processed that were stopped and those processes that failed are identified. The memory utilization of each cluster node is monitored the cluster node that is space-hungry is identified. The locking activity on each cluster node, the I/O activity of the buffers on each node are monitored and reported. The queries serviced from the cache are monitored to figure out the workload on the node. The node from which the maximum number of queries are registered with the cache is also identified. 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 are isolated and the reason for such long execution can be investigated.
- **Microsoft SQL Integration Server:** SQL Server Integration Service (SSIS) is a component of the Microsoft SQL Server database software that can be used to conduct a wide range of data integration tasks. SSIS is a fast & flexible data warehousing tool used for data extraction, loading and transformation like cleaning, aggregating, merging data, etc. eG Enterprise v7 monitors the SQL Server Integration Service and provides insights into the health and overall performance of the service. By continuously monitoring the Microsoft SQL Integration Server, the packages that failed, cancelled, and stopped are captured and communicated to the administrator. The SSIS messages are monitored and errors (if any) are highlighted. The memory utilization during continuous

integration deployment of the SQL server is monitored and abnormalities if any, are reported.

- **Monitoring Microsoft SQL Report Server:** SQL Server Reporting Services (SSRS) provides a set of on-premises tools and services that create, deploy, and manage mobile and paginated reports. The SSRS solution flexibly delivers the right information to the right users by providing an interface into Microsoft Visual Studio so that developers as well as SQL administrators can connect to SQL databases and use SSRS tools to format SQL reports. Users can consume the reports via a web browser, on their mobile device, or via email. If the SSRS solution fails to deliver the right information, then the user experience may suffer! To avoid this, version 7 of eG Enterprise performs in-depth monitoring of the Microsoft SQL Report Server. In the process, eG reports the availability and responsiveness of the server, pinpoints the status of the SSRS report, captures busy sessions, alerts administrators to errors and poor cache utilization.
- **Monitoring Microsoft SQL Analysis Server:** SQL Server Analysis Services is an analytical data engine used in decision support and business analytics. SQL Server Analysis Services supports tabular models at all compatibility levels (depending on version), multidimensional models, data mining, and Power Pivot for SharePoint. eG Enterprise v7 monitors the SQL Analysis Services and provides insights into the hits and misses of the cache, connection failures and currently logged in user sessions. The data process is monitored continuously by frequent evaluation of rows that are converted, read and written. The query processing ability of the storage engine is monitored and abnormalities (if any) are detected when query execution time takes longer than usual. The thread pools are monitored to identify the thread pool in which the threads are busy processing the jobs. The memory utilization is continuously monitored when Multidimensional Online Analytical Processing is performed. The locking activity on the SQL Server Analysis Services are monitored to determine the deadlocks at the earliest. The memory utilization of the SQL Analysis Services on the SQL server is monitored and abnormalities if any, are reported.
- **Monitoring Apache CouchDB:** Apache CouchDB is an open-source document-oriented NoSQL database. A CouchDB server hosts named databases, which store documents in JSON format. Each document is uniquely named in the database, and CouchDB provides a RESTful HTTP API for reading and updating (add, edit, delete) database documents. eG Enterprise v7 provides in-depth insights into the health, response time and overall performance of the Apache CouchDB servers. The growth of the commit logs and database logs are monitored and abnormalities, if any are detected with ease! Monitoring the compaction activity of the Apache CouchDB helps administrators identify how frequently compactions are performed on the disks of the Apache CouchDB server. The requests to the Apache CouchDB server are monitored and the type of requests (HTTP, Bulk, Purges, View and Temporary Index) that are frequently served are identified. The hits and misses to the database server are monitored to figure out how well the requests are serviced by the cache. The document write failures are monitored in the replica databases to identify the database that is not in sync with the updated data. The Design Document cache and the Shared cache are monitored to figure out how efficiently the cache services the requests. The Indexing activity and the I/O activity of the Apache CouchDB server are monitored and discrepancies if any, are rectified at the earliest.
- **Object growth monitoring:** eG Enterprise v7 is capable of monitoring the objects (in both the Oracle database server and the Microsoft SQL server) that are larger than the size configured by the administrators. Objects that are growing in size uncontrollably can be identified and the root cause of the growth can be detected.
- **In-depth analysis of SQL Jobs:** eG Enterprise v7 provides in depth analysis of the SQL jobs. Additional metrics provided in version 7 enables administrators to figure out if the SQL jobs were consistently slow or if slowness was sporadic in nature.
- **Monitoring SQL Server Log Shipping:** SQL Server Log shipping allows you to automatically send transaction log backups from a primary database on a primary server instance to one or more secondary databases on separate secondary server instances. By keeping the primary and secondary instances in sync at all times, SQL Server Log Shipping ensures that there is no data loss during

disaster recovery. On the other hand, if this feature takes too long to apply the logs to the secondary instances, then the data in the primary and secondary instances will be out of sync, thus increasing the risk of data loss! To avoid this, administrators should be proactively alerted to any latency in the application of logs to the secondary databases, so that they can take appropriate action well before disaster strikes. For this purpose, the eG Microsoft SQL Server Monitor now runs an additional SQL Log Shipping Status test. This test monitors and reports the time taken by SQL Server Log Shipping to apply transaction logs on each secondary database instance. This way, administrators can be instantly be alerted to the secondary databases that took too long to be updated with the data.

- **Detailed insights into monitoring the backups performed on the DB2 servers:** Starting with version 7, statistics pertaining to the backups performed on both DB2 DPF server and DB2 UDB server respectively, are monitored and reported. By closely monitoring the backups performed, administrators can pinpoint the backup jobs that failed and the jobs that were successfully completed. Additionally, the maximum time duration taken to complete a backup job is also reported, so that latent jobs can be captured.
- **Identifying the availability of additional database instances of the DB2 UDB server:** eG Enterprise version 7 is now capable of reporting the availability and responsiveness of more than one database instance hosted on the DB2 UDB server. For this purpose, an ADDITIONAL DATABASE parameter has been included while configuring the DB2 Service test. By specifying a comma-separated list of database instances, administrators can obtain the availability and responsiveness of those databases. If additional databases are specified, then, each database instance will be the descriptor of the test.
- **Enhancements to SAP HANA Database server monitoring:** eG Enterprise v7 is now capable of monitoring the different high availability mechanisms of SAP HANA. The Storage and System replication mechanisms are monitored, and the replication status is reported. Administrators can also figure out if the secondary server is active or not during high availability. Administrators can also determine the time taken for replication and in the process figure out if the data on the secondary server is in sync with same on the primary at all times.
- **Enhancements to Progress Database server monitoring:** eG Enterprise's Progress Database server monitoring capabilities have been enhanced in v7 to provide in-depth insights into the transaction activity performed by each user. The unused/useless indexes are identified with ease. The level of locking activity performed by each user is monitored and the user with maximum locks are identified. Resource intensive queries are identified and isolated. The session utilization of each user is tracked and the user who is consuming the maximum load on the server is identified. The size of the after-image and before-image log files are monitored periodically to check for abnormal growth of the files.
- **Monitoring Managed Cloud Database Instances:** A Managed Cloud Database Instance is a cloud computing service in which the end user pays a cloud service provider for accessing a database. These managed databases simplify the tasks associated with provisioning and maintaining a database. eG Enterprise v7 monitors the databases hosted on both AWS and Microsoft Azure cloud platforms. The Oracle, Microsoft SQL, My SQL and PostgreSQL database instances hosted on AWS cloud platform are monitored and critical metrics such as availability and responsiveness are reported. The space utilization of each database instance is closely monitored, and administrators are proactively alerted to potential space crunches, missing indexes and top tables in terms of size. The SQL Azure hosted on the Microsoft Azure cloud platform is monitored and the availability of the Microsoft Azure is reported. SQL Azure sessions that are prolonged, top queries that take longer than usual for execution and root blockers are identified. Memory consumption status is tracked and potential space crunch is identified by monitoring the size of the SQL Azure database, the memory grants and the resources available for use in the SQL Azure Instance. eG Enterprise v7 is also capable

of monitoring SQL managed Instances and Maria Database on Cloud.

- **Configuration tests for Sybase ASE Servers:** eG Enterprise version 7 is capable of reporting configuration metrics related to the Sybase objects, Sybase deadlocks, user connections to the Sybase server, quorum heartbeats, cluster heartbeats, plan cache, databases, Sybase devices, license name, version and the memory allocation.
- **Monitoring EnterpriseDB Postgres:** Postgres versions 9.4 to 11.1 are collectively referred to as EnterpriseDB Postgres. Starting with v7, eG extends monitoring support to EnterpriseDB Postgres.
- **Troubleshooting SQL Root Blocker Processes is now easier:** eG Enterprise is capable of capturing root blocker processes 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 query plan. A query plan is a set of steps that are executed to complete a query. By analyzing the query 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 query plan, administrators can build better queries and eliminate root blockers. This is why, starting with eG Enterprise v7, the detailed diagnostics of the SQL Blocker Processes test includes an Execution Plan column, which will detail the steps that were executed to complete the query.

6.3 Storage Monitoring Enhancements

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

- **HPE StoreOnce Backup:** HPE StoreOnce offers disk-based backup with deduplication for longer term on-site data retention and off-site disaster recovery with best-in-class scalability and performance for larger midsize and enterprise data centers. eG Enterprise v7 extends monitoring support for HPE StoreOnce Backup. The status and capacity of the HPE StoreOnce Backup server is monitored and reported. The status and health of the Catalyst switch on the HPE StoreOnce Backup is reported. The Virtual Tape Libraries that are in abnormal state are identified and anomalies brought to light. The NAS Shares are monitored periodically and the NAS Share that is functioning abnormally is identified. The replication services are monitored round the clock to identify discrepancies in replication performed on the NAS Shares and Virtual Tape Libraries.
- **Monitoring Hitachi Content Platform:** Hitachi Content Platform (HCP) is an object storage software solution that connects data producers, users, applications and devices into a central cloud storage platform. eG Enterprise v7 is capable of monitoring the Hitachi Content Platform. Each node in the platform is monitored, and those nodes that are in an abnormal state are highlighted. eG also measures how each node is utilizing the storage space available to it, thus turning the spotlight on those nodes that are running out of space. Additionally, eG also periodically checks the health of the hardware supporting the Hitachi Content Platform and notifies administrators of anomalies – e.g., failure of battery backup units and PSUs, erratic temperature and voltage fluctuations, and so on. Abnormalities are reported by frequently measuring the temperature and voltage. The space utilization of each tenant is monitored, so administrators can accurately identify the tenants that are space-hungry. Node replication is monitored, and errors (if any) encountered during replication are pinpointed.
- **Monitoring Progress OpenEdge Server:** The Progress Application Server (PAS) for OpenEdge is an efficient, highly-scalable, secure and standards-based application server requiring fewer system resources and easing installation, configuration and management. Using eG Enterprise v7, you can monitor the state of the server and capture errors encountered during read and write operations. The sessions on the server are monitored and the idle sessions are identified.
- **Monitoring Dell Isilon:** Dell EMC Isilon is a scale-out network-attached storage system, designed for demanding enterprise file workloads. eG Enterprise v7 performs in-depth monitoring of the Dell

Isilon storage system, and in the process, points to delays in accessing the data, reports low throughput, and captures hardware failures and I/O overload conditions.

- **Monitoring Oracle Exadata Storage Server:** The Oracle Exadata Storage Server runs the Exadata Storage Server Software and provides the unique and powerful Exadata software technology of the Database Machine including Smart Scan, Smart Flash Cache, Smart Flash Logging, IO Resource Manager, Storage Indexes and Hybrid Columnar Compression. eG Enterprise v7 offers complete monitoring support for Oracle ExaData Storage Server. Using the metrics collected, the status of each grid disk is determined and the error prone disks if any, are identified. The host to which maximum amount of data was dropped during transmission is identified with ease. By monitoring the Oracle ExaData Storage Server, the cell disks that are unavailable are promptly reported. The I/O processing ability of each cell disk is monitored and the I/O errors if any, are reported. The space utilization of each cell disk is monitored and the cell disk that is running out of space is identified. The status of each cell disk is monitored along with the current status of the fans, temperature and power of each cell disk. The CPU utilization of each cell disk is measured, which will help administrators in identifying the cell disk that is consuming abnormal CPU resources.
- **Monitoring Dell EMC Elastic Cloud Storage:** Dell EMC Elastic Cloud Storage is an object storage software designed to adhere to several tenets of object storage, including scalability, data resiliency and to take advantage of existing or new commodity server hardware in order to manage costs. eG Enterprise v7 is capable of monitoring the Dell EMC Elastic Cloud Storage. Using the metrics collected, key performance of the disks in the Virtual Data Center such as the health, the I/O processing ability, garbage collection capability and replication ability are monitored and abnormalities, if any are reported. The nodes in the Virtual Data Center are also monitored and the I/O processing ability of the nodes along with the workload of the nodes are reported. The storage pools are monitored and the storage pool that is lacking proper resources (disk space, bad disks, bad nodes etc) is identified. Inactive namespaces, locked buckets and the replication groups in which large amount of user data is pending are identified with ease! The nodes that are running out of disk space are determined so that administrators can provision additional disk space. You can also take appropriate actions on the nodes that are exhibiting poor I/O processing ability and workload.

6.4 Cloud Monitoring Enhancements

eG Enterprise supports monitoring two main public cloud environments out of the box: AWS and Azure. eG Enterprise leverages APIs from these vendors to get performance metrics about the cloud infrastructure and services. In addition to this, by installing the eG Agent in a cloud VM or virtual desktop, eG Enterprise can monitor the performance of applications and desktops running in the cloud.

- **Enhancements to Microsoft Azure monitoring:** With v7, eG's Microsoft Azure monitoring capabilities have been significantly enhanced to report a slew of metrics relating to Azure Billing, Enterprise Integration, Internet of Things, Azure Data Services and Azure Active Directory.
 - Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service, which helps your employees sign in and access resources in various external resources such as Microsoft Office 365, Azure portal etc and internal resources such as apps in the local network. The primary purpose of Azure Active Directory is to help user authentication through the network. Administrators can easily monitor the users, groups, directory role and audit logs that are part of the Azure Active Directory. The inactive users and non-membered users accessing the active directory are identified. The status of each active directory group is tracked to identify inactive groups, the members and owners of the active directory groups are also enumerated as part of the detailed diagnostics offered. The directory roles are frequently monitored to figure the directory roles that are unassigned to any user. The directory ID and the directory name to which the directory role is associated can be identified from the detailed diagnostics. Failure activities logged in audit logs pertaining to user/group/application are captured and the user initiated that activity

can be identified. Critical activities of Microsoft Azure Active Directory such as adding a user, deleting a user, deleting a group or policy etc are tracked and unauthorized changes captured at periodic intervals.

- Azure Billing Services are monitored continuously and for each Azure account, eG Enterprise v7 periodically tracks the monthly utilization of resources and the cost related to the utilization. This helps administrators in planning the environment accordingly.
 - Logic Apps is a cloud service that helps you schedule and automate tasks, business processes and workflows when you need to integrate apps, data, systems, and services across enterprises or organizations. The status and workflow of each Logic App is monitored and the Logic App that had encountered more failures and throttled events are identified.
 - IOT is a network of physical objects or things embedded with electronics, software, sensors and network connectivity, which enables these objects to collect and exchange data. eG Enterprise v7 is capable of monitoring both Azure IoT Hubs and Event Hubs. The Azure IoT Hubs and Event Hubs are cloud services that can ingest large amounts of data and process or store that data for business insights. IoT Hub addresses the unique requirements of connecting IoT devices to the Azure cloud and the Event Hubs addresses the need for big data streaming. By closely monitoring each of the Azure IoT Hubs and the Event Hubs, eG Enterprise v7 reveals the status of the hubs, the message processing capability, and the errors (if any) recorded in the hubs. In the process, orphaned messages and dropped messages are also identified.
- **Monitoring Alibaba Cloud:** Alibaba Cloud provides cloud computing services to online businesses. A sudden non-availability of the cloud, no matter how brief, or a slowdown/failure of any of its regions/availability zones/instances, can make it impossible for cloud providers to build and launch mission-critical services on the cloud and for consumers to access these services for prolonged periods. To detect such non-availability of the Alibaba cloud and to ensure all the regions/zones/instances/services are accessible, eG Enterprise v7 helps administrators with a specialized monitoring model to monitor Alibaba Cloud. The availability and responsiveness of the cloud is monitored continuously. The regions and zones are monitored and the zones that are unavailable are identified. For each Alibaba account, the Alibaba billing is monitored continuously. The monthly utilization of the resources and the cost related to the utilization are calculated and reported. Each Alibaba service billing reveals the cost incurred upon using the service. This helps administrators in planning the environment accordingly. The ECS instances are monitored round the clock to identify the instances that were removed and powered off. The irregularities in instance sizing is brought to light by analyzing the CPU, disk and network resources that the instance is configured with. The operational state of each VPN that connects a VPC with your network is reported. The status and size of each Cloud disk in a region is reported.

6.5 DevOps Monitoring Enhancements

DevOps adoption is growing in organizations. DevOps is focused on bringing in a collaboration between Dev and Ops teams towards improving productivity, efficiency and speed of software development from code commit to deploy. There are various tools used for various stages of DevOps implementation. eG Enterprise v7 now supports monitoring some key DevOps tools to ensure all stages of application development to deployment happens seamlessly.

- **Monitoring Jenkins:** eG Enterprise v7 is capable of monitoring Jenkins which is an open source Continuous Integration server. Jenkins is capable of orchestrating and automating a chain of actions that enables developers to reliably build, test, and deploy their software. This means that any snag in the operations of Jenkins may impact the stability and performance of applications/software built using the same. To avoid this, administrators must monitor Jenkins, capture the snags, and fix them, before its users notice. With eG Enterprise v7, this is now possible! Using eG Enterprise v7,

administrators can monitor the status of each job and promptly spot aborted builds and failed executions. Blocked jobs and jobs that are stuck in queue are highlighted, so they can be pulled up for scrutiny. Irresponsive nodes and memory-starved nodes are pinpointed, so administrators can resize such nodes for improved performance.

- **Monitoring Ansible:** Ansible Tower is Ansible at a more enterprise level and is designed to be the hub for all your automation tasks. Synchronized and failure-free functioning of the Ansible Tower is therefore a key requirement for the continuous delivery of critical applications/services. To ensure that the Tower is always accessible and is performing to peak capacity, it is necessary to constantly watch over the performance of the Tower and detect and resolve failure conditions before they cause serious impact. This can be easily achieved using the specialized Ansible Tower monitoring model offered by eG Enterprise version 7. Using the specialized Ansible Tower Monitor that eG provides, administrators can instantly determine the number of hosts in a Tower and accurately figure out how many of those hosts are unable to successfully perform jobs. If any job execution caused project/inventory syncing process to fail, administrators are promptly notified of the same. Administrators can also zoom into the job that was run last on the Tower and determine its status – i.e., whether it was a success/failure and whether/not it was slow. eG also tracks the status of job templates, and accurately points to the job template that may have caused a host/group to fail.
- **Monitoring GitHub:** GitHub is a web-based version-control and collaboration platform for software developers. It allows developers to collaborate on a project more effectively by providing tools for managing possibly conflicting changes from multiple developers. GitHub environment is hosted on the cloud and shared across multiple users. To ensure reliability and data integrity of the cloud-based GitHub account, it is important for every GitHub account owner to keep track of the changes happening in his/her account at regular intervals. This can be easily done using eG Enterprise v7. Using eG, a GitHub account owner can closely monitor the repositories and accurately identify those where a large number of issues are still unresolved. Repositories with many commit operations are also highlighted and the details of these operations are revealed to the owner, so that he/she can figure out if the committed changes were made by authorized personnel only. The growth in the size of each repository can be tracked, so that the owner can rapidly identify those repositories that are growing uncontrollably, figure out the reason for the growth, and fix it. Furthermore, with the help of eG, administrators can easily ascertain the number and names of organizations managed by the owner and the constitution of each organization. Additionally, the owner can track the storage space usage of his/her GitHub account, and proactively detect probable storage space constraints.
- eG Enterprise v7 is also capable of monitoring Jira Software and Bitbucket.

6.6 Other Monitoring Enhancements

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

- **Monitoring Raspberry Pi Devices and Systems:** Raspberry Pi is a series of single-board computers that is developed to educate people in computing and create easier access to computing education. eG Enterprise v7 offers two different monitoring models for Raspberry Pi – namely Raspberry Pi Device and Raspberry Pi System. By monitoring the Raspberry Pi System, the voltage of each hardware component on the system is monitored and the hardware component that is experiencing erratic voltage fluctuations is detected. The temperature of the system is constantly monitored to avoid overheating issues. The Raspberry Pi device is monitored and components that are overclocking are highlighted.
- **Monitoring Redis:** Redis is an open source (BSD licensed), in-memory data structure store, used as a database, cache and message broker. It supports data structures such as strings, hashes, lists, sets, sorted sets with range queries, bitmaps, hyperlog logs, geospatial indexes with radius queries and streams. Redis has built-in replication, Lua scripting, LRU eviction, transactions and different levels of on-disk persistence, and provides high availability via Redis Sentinel and automatic

partitioning with Redis Cluster. To ensure high reliability and outstanding performance of the Redis Cluster, it is important of the administrators to keep track of the performance of the Redis cluster at periodic intervals. This can be achieved using eG Enterprise v7. Using eG Enterprise, the Redis cluster can be closely monitored and the health of the cluster can be tracked continuously. The idle time of each client on the cluster is tracked and the blocked clients identified with ease. The state of the cluster is periodically monitored and the nodes and slots that were in 'fail' state are identified. The resource utilization of the Redis cluster is monitored and CPU hungry background processes are identified. Memory consumption of the Redis cluster is also periodically monitored so that administrators could be proactively alerted to potential memory crunch. The replica of the Redis cluster is also monitored to ensure high availability. The command executions that are slow are identified and the reason behind such slowness is analyzed. The command processing ability of the Redis cluster is monitored and reported. Partial synchronization failures are captured and reported for further analysis.

- **Monitoring Mule ESB:** eG Enterprise v7 monitors the Mule Enterprise Service Bus which is a runtime engine of Anypoint Platform and a lightweight Java-based enterprise service bus (ESB) and integration platform that allows administrators to connect applications together quickly and easily, enabling faster and reliable data exchange. By monitoring application transactions processed by Mule ESB, eG Enterprise helps administrators in identifying slow and error prone transactions. The cross-application transaction flow and call graph offered by eG Enterprise helps administrators in drilling down the exact cause of transaction slowness.
- **Monitoring Apache ActiveMQ servers:** Apache ActiveMQ is an open source message broker written in Java together with a full Java Message Service (JMS) client. eG Enterprise v7 is capable of monitoring the Apache ActiveMQ servers. Each host on the broker is monitored and the workload on the host is determined. The queues are monitored and the queue that is busy processing the messages is identified. The protocol through which connections were established are monitored and the protocol that is establishing the maximum number of connections is revealed. The frequently used topic is also determined by continuously monitoring the topics in the message broker.
- **Monitoring Veritas NetBackup:** Veritas NetBackup is a backup and recovery software suite designed for enterprise users. To protect applications deployed in containers, Veritas now provides a NetBackup Client that can be deployed as a container. eG Enterprise v7 is capable of monitoring the Veritas NetBackup. For each scheduled backup type, the total jobs, files that are on hold during backup and the files that are backed up are reported. The total number of tasks performed for each task status code is monitored and reported using which administrators can get a clear idea on the frequently used task status code in their environment. The errors encountered by the backup server are captured and reported periodically. Media servers are periodically monitored to figure out the media server on which the media tape drives are active for backup, tape drives that are frozen/suspended and encrypted. Administrators can figure out the Media server that is inactive for most of the time and drill down the exact cause of inactivity.
- **Monitoring Proxmox Virtual Environment:** Proxmox VE is a complete open-source platform for all-inclusive enterprise virtualization that tightly integrates KVM hypervisor and LXC containers, software-defined storage and networking functionality on a single platform, and easily manages high availability clusters and disaster recovery tools with the built-in web management interface. eG Enterprise v7 offers two different monitoring models for Proxmox Virtual Environment – namely Proxmox Cluster and Proxmox Hypervisor.
 - **Monitoring Proxmox Hypervisor** reveals the status of the virtual machines provisioned by the Proxmox hypervisor is monitored and the VMs that are not running and the VMs that are removed are identified. The session load on the hypervisor is determined by constantly monitoring the logins to the hypervisor. The resource utilization of each node is monitored to figure out the node that is consuming too much of resources. The space utilization of each storage is monitored and the storage that is space-hungry is identified. The resource and

memory utilization of each VM provisioned through the hypervisor is monitored and the VMs that are resource-hungry are identified.

- **Monitoring Proxmox Cluster** reveals the status of each cluster; the nodes that are offline, the VMs and containers that are stopped and the users within the cluster. The status of each node in the cluster is monitored and the node that is resource and memory hungry is isolated. The storage space utilization of each storage is monitored to figure out the storage that is consuming too much of memory resources. The Logs are monitored to figure out the tasks that have failed and the errors encountered are determined.
- **Detailed diagnostics on disk activity provides insights into file-level IOPS:** Previously, for a Windows host, the detailed diagnosis of the Disk Activity test provided details of the top-10 I/O-intensive processes on the host. This enabled administrators to identify the exact process that was responsible for any abnormal disk activity on the host. However, to effectively troubleshoot abnormal disk I/O, Windows administrators required insight into file-level I/O activity – i.e., they needed to know the precise files the processes read from or wrote to when disk activity violated its thresholds. With eG Enterprise v7, administrators can easily configure the Disk Activity test to obtain this information! The Disk Activity test now takes an additional TRACE parameter, which when set to Yes, displays the details of every file that is read from / written to, as part of detailed diagnostics of the Disk busy measure. To ensure that these detailed metrics do not clutter the display or the eG database but make problem areas apparent, administrators can even control when they want the file-level metrics to be collected, how much information should be collected, and for what files. Towards this end, the Disk Activity test now supports the following parameters:
 - Disk Busy Percent: The detailed diagnosis will include file-level I/O operations only if the Disk busy measure reports a value higher than the percentage specified here. This ensures that file-level insight is available to administrators only if disk activity is abnormally high.
 - Read Size in KB: If data read from a file is greater than the value specified here, then detailed diagnosis will include the I/O metrics of such a file. This ensures that detailed diagnosis includes only those files that are experiencing a high level of read activity.
 - Write Size in KB: If data written to a file is greater than the value (in KB) specified here, then detailed diagnosis will include I/O metrics of such a file. This ensures that detailed diagnosis includes only those files that are experiencing a high level of write activity.
 - Disk Response Time Secs: If the time taken to read from/write to a file is greater than the duration (Secs) specified here, then detailed diagnosis will report the I/O usage of such a file. This ensures that detailed diagnosis includes only those files that respond slowly to I/O requests.
 - Event Capture Interval In Secs: This parameter is set to 10 seconds by default. This means that, by default, the test will pull file-level I/O metrics only from the disk activity that occurs during the last 10 seconds. This ensures that the most 'current' I/O metrics are captured.
- **Monitoring Mosquitto MQTT:** eG Enterprise v7 is capable of monitoring the Mosquitto MQTT, which is an open source (EPL/EDL licensed) message broker that implements the MQTT protocol versions 5.0, 3.1.1 and 3.1. The uptime of the server is monitored and reported. Client related statistics are reported so that administrators can easily identify the clients that expired. The subscriptions that are active on the broker are also reported. The data transmission and reception through the broker is monitored and reported along with the count of messages that are dropped. The message transmission and reception are also monitored and reported.
- **Enhancements to eG Syslog:** The eG Syslog monitoring has been enhanced in eG Enterprise v7. Administrators can now extract the error/warning messages pertaining to each rule configured in the eG Syslog file. Warning, Critical and error prone messages can now be isolated with ease from the Syslog file. In older versions, the detailed diagnosis fetched all the relevant messages from the syslog file for each measurement period. This increased the overhead of the eG backend database.

To avoid such overheads, an additional “**NO OF MESSAGES IN DD**” parameter has been introduced in v7 while configuring the tests. By default, this parameter is set to 50 which implies that the top 50 messages alone will be displayed for each measurement period in the detailed diagnostics reported by the test.

- **Monitoring CommVault Backup:** Commvault Complete Backup & Recovery is a single, powerful backup software solution for data protection irrespective of where the data resides. eG Enterprise v7 offers complete monitoring support for CommVault Backup. Using the metrics collected, the pending jobs and jobs that are suspended can be identified. Inactive clients can be identified and isolated. The count of backup jobs and jobs that were restored can be determined with ease.
- **Monitoring Fortinet Sandbox:** Fortinet Sandbox is an advanced threat detection solution that performs dynamic analysis to identify previously unknown malware. With eG Enterprise v7, you can monitor the hardware of the Fortinet Sandbox such as CPU, disk and memory to identify resource constraints, if any. You can also determine the count of the files (e.g., exe files, PDF files, web files etc) that are pending in the job queue and figure out which type of file are mostly pending in the job queue. The uptime of the Fortinet Sandbox and the count of traps are also tracked periodically.
- **Monitoring Oracle Primavera:** Oracle Primavera is an enterprise project portfolio management software which includes project management, scheduling, risk analysis, opportunity management, resource management, collaboration and control capabilities, and integrates with other enterprise software such as Oracle and SAP’s ERP systems. In eG Enterprise v7, the Oracle Primavera is monitored to figure out the count of projects handled, the activities, resources and users accessing the projects. The total users logged into the Oracle Primavera are reported along with the count of users with access to various services such as P6 EPPM API Services, P6 EPPM Web Services, P6 EPPM Power client, P6 EPPM Resource Access field, P6 EPPM Project sections, P6 EPPM Portfolios section, P6 EPPM Reports, P6 EPPM Team Member modules and P6 EPPM Team Member Interface modules. The user sessions are monitored and the sessions that are most frequently initiated by the users are identified. The connection pools are monitored round the clock to identify the latent and busy connection pools. By monitoring the job services, the pending jobs and the jobs that failed can be easily determined. The job service that is busy processing the jobs can also be identified.
- **Monitoring Microsoft Certificate Authority Server:** A certification authority (CA) is responsible for attesting to the identity of users, computers, and organizations. eG Enterprise v7 is capable of monitoring the Microsoft Certificate Authority Server. The active connections that are requesting the certificates are monitored periodically. The certificate request processing ability of the server is monitored and the certificate requests that failed or are pending processing are identified promptly. By monitoring the SSL certificates, the certificates that have expired and are nearing can be pinpointed.
- **Ability to report the name of the NFS client as the descriptor of the Disk Space test:** In previous versions, if an NFS drive on an NFS server was used by multiple Linux/Solaris hosts, then the Disk Space test for all the hosts reported the drive name on the NFS server as the descriptor. Some administrators however preferred to have the test display the drive name on the NFS client as the descriptor, instead of the drive name on the server. To offer this flexibility to administrators, the Disk Space test now takes an additional REPORT LOCAL NFS NAME parameter. If this parameter is set to true, then the Disk Space test of a Linux/Solaris host will display the NFS drive name on that host as the descriptor of the test.
- **Introduced self-monitoring capability for eG VM agent:** Starting with eG Enterprise v7, the self-monitoring and recovery capabilities of the eG agent have been extended to the eG VM Agent. The eGVMAgentMon process has been included to ensure that the eG VM agent is up and running. Whenever the eG VM agent is down, the eGVMAgentMon process starts the eG VM agent. This helps the eG VM agent in collecting metrics from the core components without any disruption.
- **JVM Monitoring for the eG Agent Simplified:** In previous versions, to pull JVM metrics from a target eG Agent component, JMX had to be enabled for the eG agent. To monitor the eG agent's

JVM without requiring a cumbersome JMX configuration or an eG agent restart, eG Enterprise v7, by default, polls local Mbean attributes to collect the JVM metrics. To this effect, in eG Enterprise v7, a **MODE** parameter has been introduced for the JVM tests of the eG Agent component. By default, this parameter is set to **Local**. However, if administrators prefer to use the JMX approach for collecting the metrics, they can still do so by setting the **MODE** flag to **JMX**.

6.7 Monitoring Container Environments

With the rising popularity of applications built with microservices architecture, resource provisioning has become on-demand. An application will be created on demand and it would need to be provisioned with resources to support it. Once the application/workload is switched off, the resource needs to be reclaimed. Docker containers provide this modular and scalable auto-scaling architecture to support code pipeline management in the microservices world. Kubernetes is a popular open source platform that is used for container orchestration (deployment, management, scaling, etc.).

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

- **Enhancements to Docker:** eG Enterprise already had support for monitoring Docker containers. While earlier, an agent-based monitoring approach was recommended, starting with eG Enterprise v7, an eG agent container is now used on each node for monitoring. In a Kubernetes environment, the eG agent container is configured as a DaemonSet so that the agent container is automatically created and deployed on each Docker node when it comes up. In a non-Kubernetes environment, the agent container can be downloaded from the Docker hub and deployed on each Docker host. This eG agent container when deployed on the Docker host is capable of monitoring the Docker host, its containers and the containerized applications.
- **Monitoring Kubernetes:** Kubernetes is an open-source system for managing - i.e., running and co-ordinating - containerized applications across a cluster of machines. It allows users to define how their applications should run and how they should interact with other applications or the outside world. At its base, Kubernetes brings together multiple physical or virtual servers into a cluster using a shared network to communicate between them. Though the cluster can contain any host that runs containerized applications, the most common or popular deployment of Kubernetes has it managing a cluster of Docker hosts. This cluster is the physical platform where all Kubernetes components, capabilities, and workloads are configured. eG Enterprise v7 provides a dedicated monitoring model for those Kubernetes clusters that manage Docker hosts and containers. This model continuously monitors the status of the cluster nodes, the Kubernetes control plane services running on the master node, and the workloads and application services on the worker nodes. In the process, administrators are alerted to real/potential operational failures that may cause a mismatch between the actual state of objects and the desired cluster state. The health of the deployments is monitored and the deployments that failed to create the desired number of Pod replicas are identified. The autoscalers that are unable to compute scales are identified and the reason for such inability can be debugged. Administrators are alerted to jobs that are running for a longer duration. Failure/problem events are detected in the Kubernetes cluster periodically and the administrators are alerted to the exact events that caused the Pod creation to fail. Additionally, administrators can proactively detect probable resource utilization constraints by identifying the nodes that are running out of resources.
- **Monitoring OpenShift Clusters:** RedHat OpenShift is a secure and enterprise-grade container application platform based on Kubernetes for traditional and cloud-native applications. The OpenShift Container Platform contains the following:
 - Kubernetes that is used for Orchestration
 - Containers that are hosted on RHEL CoreOS/CRI-O Engine
 - Applications that run on containers

Starting with eG Enterprise v7, monitoring support has been provided for OpenShift Clusters. The Kubernetes monitoring model offered by eG Enterprise can be used to monitor OpenShift Clusters.

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

7.1 SaaS Enhancements

eG Enterprise is now truly Multi-Tenant: By default, eG Enterprise supports the following deployment options:

- Fully on-premises (eG manager is hosted by the customer purchasing eG Enterprise)
- Fully SaaS based (eG manager is hosted by eG Enterprise)
- MSP deployment (eG manager is hosted by MSP)

In previous versions, when the eG manager is hosted in SaaS and MSP deployments, the admin user who is the super user of eG Enterprise had all the administrative control i.e., the tenants of those deployments had limited control in setting up the environment and hence had to rely on the admin user to even do simple tasks such as managing the components, setting thresholds etc. In environments where components were dynamically managed, the tenants found it difficult to contact the eG admin user for the smallest of their needs. Equally, the admin user also felt that he/she was constantly setting up the environment by performing mundane tasks. To strike a balance between the tenants and the admin user on this issue, eG Enterprise v7 now empowers tenants to perform a few administrative tasks, thus making eG Enterprise truly self-provisioned and multi-tenant.

Starting with eG Enterprise v7, tenants of SaaS and MSP environments are empowered to self-register with eG Enterprise and download the eG agents. The tenants are also allowed to create, manage and administer the components on their own. By offering these capabilities, eG Enterprise provides more control to the tenants than ever. The deployments are easier and are more automated with this setup.

The first step towards automating the deployment in SaaS and MSP environments starts with a change in the installation of eG Enterprise v7. Users are now empowered to choose how they want to install the eG manager. Users are allowed to choose the Enterprise model of eG Enterprise or the SaaS model as the case may be.

Manager Configuration

General Settings

eG manager set-up for monitoring

☐ Enterprise ☒ SaaS

* Mail ID for admin user

To

Enable auditing?

☐ Yes ☒ No

Minimum password length

Password complexity (should contain)

☒ Lowercase alphabets

☐ Numbers

☐ Uppercase alphabets

☐ Special characters

Mail Server Settings

Mail protocol

SMTP mail host

SMTP mail port

eG Administrator mail ID

Alternative mail sender IDs

SMTP server requires authentication? ☐ Yes ☒ No

Do you want to configure mail receiver settings? ☐ Yes ☒ No

Figure 97: Deploying the eG manager in a SaaS environment

A broad overview of eG Enterprise's approach to being truly multi-tenant is discussed underneath:

- Self-Registration is allowed for the users:** Previously, the tenants had to entirely rely upon the eG admin user to register them on the eG Enterprise. Starting with eG Enterprise v7, the users are empowered to self-register as a tenant on the eG Enterprise without having to involve the eG admin. The Register tab in the eG Enterprise's sign in page governs the self-registration process. In high security environments, administrators may need to centrally manage and control user registrations; naturally therefore, they may not want tenants to self-register. To facilitate such a need, administrators can disable self-registration by setting the **Allow users to self-register** flag to **No** in the **MANAGER MODEL** page of the eG administrative interface.

eG Enterprise Cloud
Converged Application and Infrastructure Monitoring as a Service

John

Acme

(UTC-5:00) America/Havana

© eG Innovations, Inc. All Rights Reserved. [*Terms and conditions *](#)

Figure 98: Self-registration portal for tenants

- **eG agent download process is simplified:** Once the user is self-registered with eG Enterprise as a tenant, he/she can directly get started towards discovering the environment and managing the components. For this purpose, 3 simple steps are offered by eG Enterprise v7.

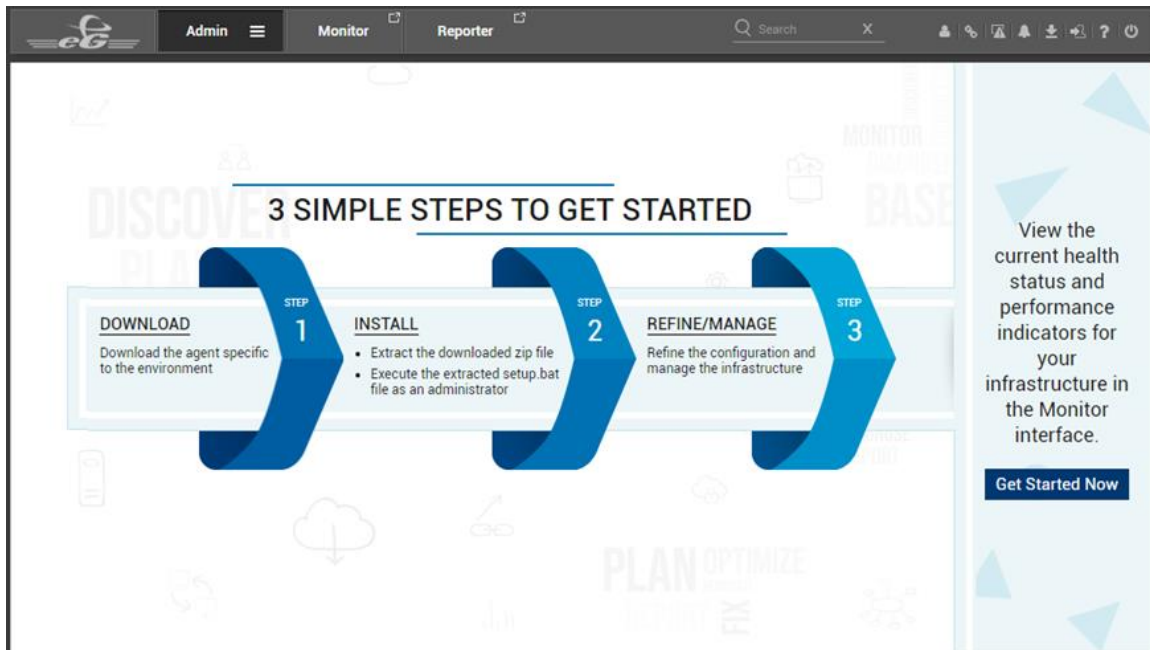


Figure 99: The steps to get started with eG Enterprise

The first step to get started in discovering and managing the components is to choose the type of the environment. A tenant can choose the type of his/her infrastructure from **the What would you like to Discover/Monitor?** page introduced in eG Enterprise v7.

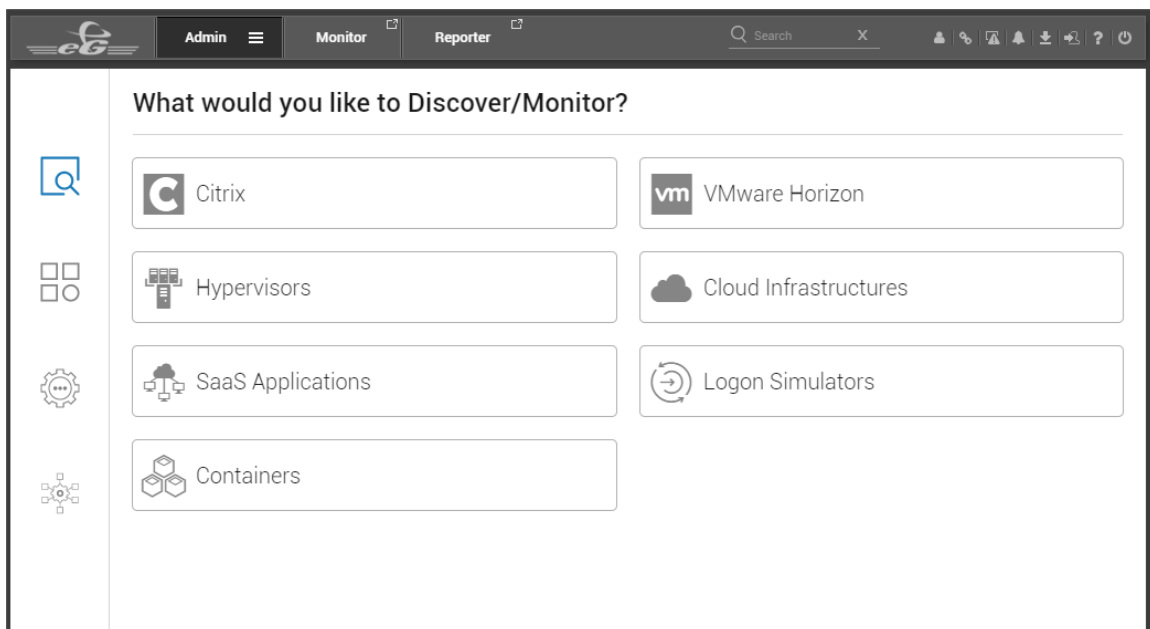


Figure 100: Choosing the type of environment to be monitored

Once the environment is chosen, the tenant can download the appropriate eG agent directly from the eG manager.

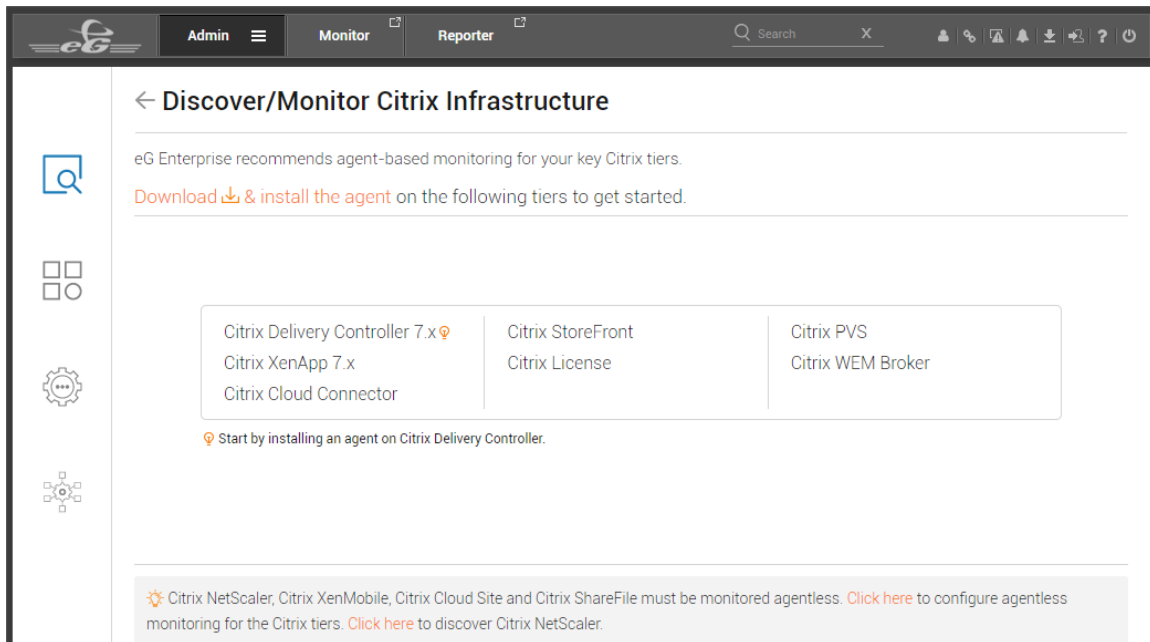


Figure 101: Downloading the eG agent relevant to the chosen environment

In SaaS environments, there may be hundreds of tenants who may be downloading different eG agents. In such environments, mapping the eG agent with the eG manager is a tedious process. To have a smooth mapping between the eG agent and the eG manager, a unique Universal Unique Identifier (UUID) is generated automatically when a user registers as a tenant. Once the UUID is generated, the tenant is allowed to download the eG agent directly from the eG manager. The UUID is used for auto-associating the user's infrastructure elements to the organization. With the help of this UUID, the information of the eG manager is automatically available to the downloaded eG agent. The components are then auto-discovered, auto-managed and auto-associated to the tenants.

- **Automatic Discovery of components:** eG Enterprise v7 has improved the scope of discovering the components to a great extent. In SaaS and MSP deployments, the eG agent discovers the components based on a pre-defined list of component types. If all the components in the environment belong to the component types that can be automatically discovered by eG Enterprise by default, then, the components will be added to the eG manager and monitoring will be enabled by default. If there are components that cannot be discovered in the target environment or if the components are discovered but still remain unmanaged, the tenants have the option to manually manage the components for monitoring.
- **Automatic creation and management of components:** In previous versions, components that are automatically discovered were in an unmanaged state. Administrators had to deliberately manage the components for monitoring using the MANAGE/UNMANAGE COMPONENTS page available in the eG admin console. Starting with eG Enterprise v7, the components that are automatically discovered will be managed automatically. This way the components will be ready for monitoring the minute they are discovered.
- **Components managed in SaaS environments are auto named:** In Enterprise model offered by eG Enterprise, components can be managed with either the IP address or the host name. Until the previous version, the same logic applied to SaaS and MSP environments too where the eG admin user had to cautiously provide a unique nick name for the component that is to be managed in each

environment. Starting with eG Enterprise v7, components are auto assigned with a unique nick name based on their host names. As a best practice, in SaaS and MSP environments, IP addresses should not be used for configuring a component for monitoring.

- **Automatic assignment of components to tenants:** eG Enterprise v7 has a built-in capability to create a zone specific to the tenant who has self-registered on eG Enterprise in SaaS and MSP deployments. The components that are assigned to the tenant are also automatically mapped to the created zone. This feature helps tenants in obtaining a high-level of overview for the components managed by them. Also, eG admin user is also benefitted as he/she can view the tenant-level view of all the components.
- **License Assignment is more flexible:** In previous versions, licenses allocated to the tenants and licenses consumed by the tenants were only reported at the eG admin level. The tenants could not allocate the licenses to the users in their environment and had to solely rely on the eG admin. In SaaS and MSP deployments, the license allocation needed to be more flexible since the tenants needed to have the ability to allocate licenses and figure out the license utilization in their environments. To grant this flexibility, starting with eG Enterprise v7, tenants can themselves allocate the license to the users within their environment. The tenants can also view the license consumption of each user.
- **Increased management control for Tenants:** With the introduction of new user interface in the eG admin console for managing the components, managing the users and setting maintenance policies, the tenants of SaaS and MSP deployments are empowered to perform management tasks with ease without having to rely on the eG admin user.
- **Auto-deleting inactive tenants and their associated components:** In SaaS and Multi-tenant environments, there may be many self-registered users who may not be using eG Enterprise any longer. To maintain the users in a better manner and simplify the admin management, it is necessary for the administrators to frequently identify inactive users and remove them. This can be achieved using the **DELETE USER ACCOUNTS** page. The users who remain inactive for a default period of 30 days can be auto deleted. The elements associated with the users will also be auto deleted.
- **Additional roles are introduced to support SaaS and MSP deployments:** Additional roles are introduced in eG Enterprise v7 to enable the administrators to manage the components in a more rationale manner. The roles and responsibilities offered in eG Enterprise v7 are explained in the table below:

| Roles | Responsibilities |
|------------------|--|
| OrgAdmin | User possessing this role has unrestricted access to monitor the components in the eG monitor interface along with certain administrative privileges to configuring tests, thresholds, alarm policies, manage components, configure external/remote agents, configure zones/services etc. |
| OrgAdminNoConfig | User possessing this role has unrestricted access to monitor the components in the eG monitor interface along with certain administrative privileges to configuring tests, thresholds, alarm policies, manage components, configure external/remote agents, configure zones/services etc. The user possessing this role does not have the privilege to access the eG Configuration Management interface. |

| | |
|------------------------------|--|
| OrgAdminWithUserMgmt | User possessing this role has unrestricted access to monitor the components in the eG monitor interface along with administrative privileges to configuring tests, thresholds, alarm policies, manage components, configure external/remote agents, create users, manage users, provide user roles etc. |
| OrgAdminWithUserMgmtNoConfig | User possessing this role has unrestricted access to monitor the components in the eG monitor interface along with administrative privileges to configuring tests, thresholds, alarm policies, manage components, configure external/remote agents, create users, manage users, provide user roles etc. The user possessing this role does not have the privilege to access the eG Configuration Management interface. |

7.2 Architecture Enhancements

7.2.1 Installation Enhancements

- **Faster and simplified eG manager installation:** Until eG Enterprise v7, the eG database configuration was part of the eG manager installation i.e., the credentials for creating the eG backend database were to be provided even before the eG manager installation was complete. If the eG backend database creation failed, then, eventually the eG manager installation also failed. This forced the users to initiate the installation process all over again from the beginning. This was time consuming and was becoming more unfriendly to the users. To ease the pain of the users and simplify the installation process, eG Enterprise v7 has segregated the installation of the eG manager into two – eG manager installation and eG backend database configuration. The eG manager installation and the eG database configuration are now taken up sequentially i.e., the eG database

configuration is taken up only after the eG manager installation is complete.

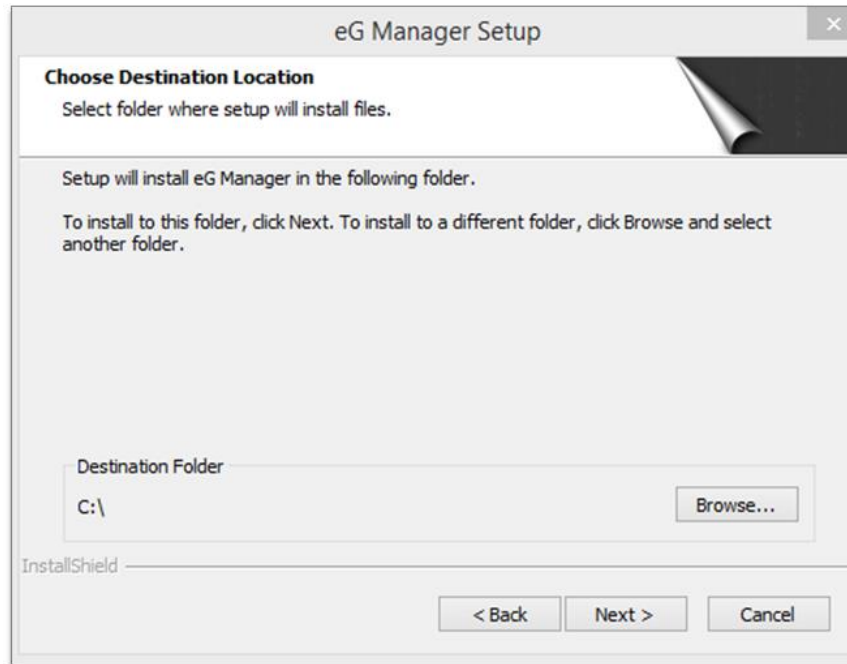


Figure 102: eG manager installed on the destination folder

Figure 103: The eG database is created after eG manager installation is complete

This sequential process helps in reducing the time of eG manager installation.

- **Robust Manager Installation Includes Providing Certain Mandatory Settings:** In older versions, administrators were able to key in certain settings such as Enabling audit logs, setting the password length and the mail server settings of the users logging into the eG manager only after the eG manager installation was complete. If the administrator failed to provide any of these, then, support personnel of eG Enterprise found it difficult to resolve issues that were raised since there would not be any audit logs logged, password could not be changed since the email ID was not configured. To enable the eG administrators spend lesser time in resolving issues and to provide

greater flexibility to the IT administrators who are installing eG managers in their environments, the above-mentioned settings are presented to the IT administrators as part of the eG manager installation process. Starting with eG Enterprise v7, the eG manager setup for monitoring (Enterprise or SaaS) can be chosen upfront during the installation process.

The screenshot shows the 'Manager Configuration' window. It is divided into two main sections: 'General Settings' and 'Mail Server Settings'.

General Settings:

- eG manager set-up for monitoring:** Two radio buttons are present: 'Enterprise' (selected) and 'SaaS'.
- * Mail ID for admin user:** A text input field with the placeholder 'To'.
- Enable auditing?** Two radio buttons: 'Yes' and 'No' (selected).
- Minimum password length:** A text input field with the value '8'.
- Password complexity (should contain):** Four checkboxes: 'Lowercase alphabets' (checked), 'Numbers', 'Uppercase alphabets', and 'Special characters'.

Mail Server Settings:

- Mail protocol:** A dropdown menu showing 'SMTP'.
- SMTP mail host:** A text input field.
- SMTP mail port:** A text input field with the value '25'.
- eG Administrator mail ID:** A text input field.
- Alternative mail sender IDs:** A text area.
- SMTP server requires authentication?** Two radio buttons: 'Yes' and 'No' (selected).
- Do you want to configure mail receiver settings?** Two radio buttons: 'Yes' and 'No' (selected).

At the bottom of the 'Mail Server Settings' section is a 'Validate' button. At the bottom of the entire window is an 'Update' button.

Figure 104: Specifying the eG manager setup for monitoring

Until the previous version, the eG manager license needed to be manually added by the administrators for the manager installation to be complete. Similarly, the JDK needed for running the eG manager too need to be configured separately. Starting with eG Enterprise v7, the license is automatically uploaded to the eG manager. The Open JDK bundled by default with the eG manager eliminates the need of configuring the JDK separately.

- **Other Installation Changes:** To reduce the risk of malicious attacks and to promote better security, step up with the end of life of versions that were already being used, the eG manager is bundled with Tomcat v9 and Open JDK from eG Enterprise v7. The eG agent and eG manager on Windows and Linux 64-bit systems are also bundled with Open JRE starting with eG Enterprise v7. With this change, administrators need not subscribe to Oracle support services to use Oracle JREv1.9 and above thus eliminating the need of license requirements for the same. The eG agent on Windows and Linux 32-bit systems will continue to use Oracle JRE.

7.2.2 Administration Enhancements

- **Simplified User Interface with helpful indicators:** Starting with eG Enterprise v7, the eG administrative interface sports some helpful intuitive indicators which will guide the users of eG Enterprise to the next step of configuration. The **What's Next** dialog box as shown in Figure 94 helps administrators in this regard.

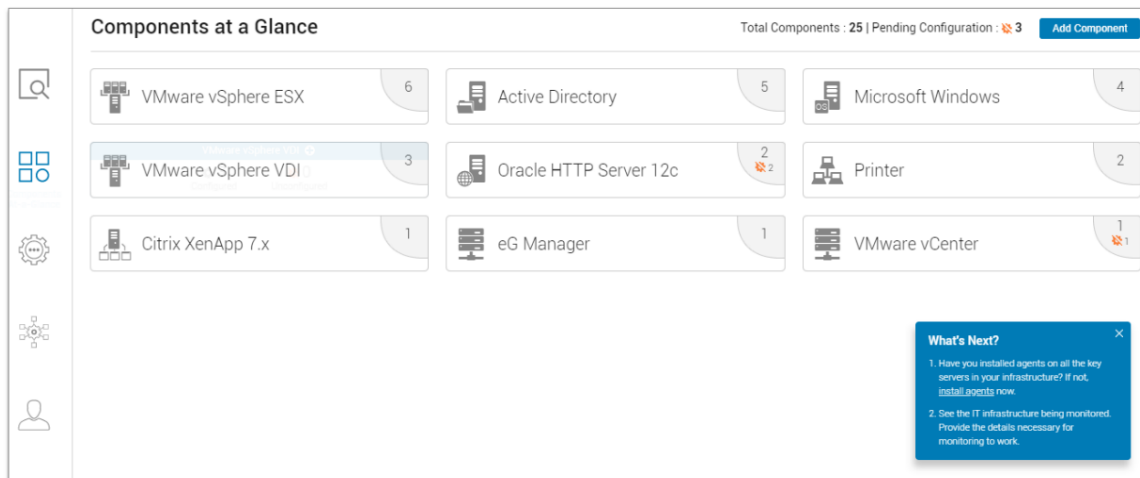


Figure 105: A sample page showing the indicator on what to do next

- **Extending the privileges of the LimitedAdmin role:** In older versions, LimitedAdmin users could configure tests, thresholds, alarm policies and maintenance policies for the components in their purview. Even, they were allowed to view the maintenance policies created by other users. However, they were restricted from creating Zones/Services/Segments, add a remote agent and perform user management functions. The LimitedAdmin users had to rely on the administrators solely for this purpose. For the LimitedAdmin to act independently and to perform better monitoring at a faster pace, eG Enterprise v7 has enhanced the capabilities of the LimitedAdmin user. Such users can now create Zones/Services/Segments, add a remote agent and also perform user management functions for the users under his/her purview.
- **Enhancements to Discovery using the eG manager:** In previous versions, network devices were discovered by the eG manager only if the SNMP version used by the network devices were v1 or v2. Nowadays, more network devices use SNMP v3. Starting with eG Enterprise v7, the eG manager is capable of discovering the network devices that use SNMP v3. From this version, the discovery process using the eG manager has also been improved to enable faster discovery of components.
- **Auto-creation of component groups:** When monitoring Citrix infrastructures, administrators often prefer to manage delivery groups on a Citrix Delivery Controller as Component Groups in eG. Previously however, to achieve this, administrators had to manually create a component group in eG for every delivery group managed by the controller. This meant that every time the delivery group configuration changed; the configuration of the corresponding component group had to be manually changed. Version 7 saves the time and effort involved in this exercise by completely automating this cumbersome process!

If an eG agent is installed on a Citrix Delivery Controller and is monitoring it, then this agent can now auto-discover all the delivery groups managed by that controller and the XenApp servers in each group. The eG manager uses the details so discovered to accurately identify the delivery group to which a managed XenApp server belongs. With this knowledge, the eG manager then automatically creates a component group in eG, adds the managed XenApp server to it, and also assigns the delivery group's name (by default) to that component group. If later, XenApp servers are added/removed from a delivery group, eG Enterprise auto-detects this change and updates the corresponding component group configuration accordingly. This eliminates the need for any manual intervention in component group maintenance.

- **Discovery using eG Remote agents is now possible:** Starting with eG Enterprise v7, the eG remote agents too can perform discovery of components. If a remote agent is configured to monitor a VMWare vCenter, then this remote agent is now capable of discovering all the VMWare vSphere

ESX servers in the target environment. The underlying topology of the servers too are discovered and displayed.

- **Filters introduced for filtering SNMP traps:** In previous versions, the eG manager sent the SNMP traps by default for all the components managed in the environment to the configured SNMP manager. In some environments where there were too much of SNMP traps to be sent, administrators were not given the liberty to filter out the components/tests for which SNMP traps can be excluded. To provision such filtering option, a separate SNMP Trap Filters tab has been introduced in the SNMP MANAGER CONFIGURATION page of the eG administrative interface. Using this page, administrators can exclude the Component Types/Components/Layers/Tests/Descriptors from sending SNMP traps.
- **Component Administration in bulk is now possible:** In environments where a large number of components need to be added, administrators either added components one by one or used the eG CLI to add multiple components. The process of adding one component at a time was time consuming and left the administrator frustrated. To initiate faster administration of components through the eG administrative interface, eG Enterprise v7 has introduced a special capability which lets the administrator add the components in bulk.

The screenshot shows a web interface titled 'Components'. It features two dropdown menus: 'Category' with 'All' selected, and 'Component type' with 'Choose a component type' selected. To the right of these is a checkbox labeled 'Show managed component types only'. Further right are two buttons: 'Add New Component' and 'Bulk Add/Modify'.

Figure 106: Adding components in bulk

Starting with eG Enterprise v7, components can be added, modified, managed, unmanaged and deleted in bulk. For this, a special CSV format has been devised by eG Enterprise. The sample CSV file can be downloaded from the eG console. The administrators need to specify all the necessary details of the components as mentioned in a separate file, save it in CSV format and upload the file. The components will then be added/modified or managed/unmanaged/deleted according to the option chosen by the administrator.

The screenshot shows a modal dialog box titled 'ADD/MODIFY COMPONENTS IN BULK'. It has a close button (X) in the top right corner. Inside, there is a 'Select action' section with two radio buttons: 'Add' (which is selected) and 'Modify'. Below this is a 'Choose file' section with a text input field and a 'Browse' button. Underneath the input field is a link that says 'Download sample CSV'. At the bottom of the dialog is a large 'Upload' button.

Figure 107: Uploading the CSV file to add components in bulk

- **Providing/Changing user credentials made easier while configuring/reconfiguring the tests:** In environments where hundreds of components are monitored, administrators found it difficult to configure the tests of each component by providing appropriate user credentials like domain name, name of the user, password etc. To ease the pain of such administrators, a new **PASSWORD PROFILES** page has been introduced using which you can add a Password profile and associate the profile with a domain name, name of the user and password.

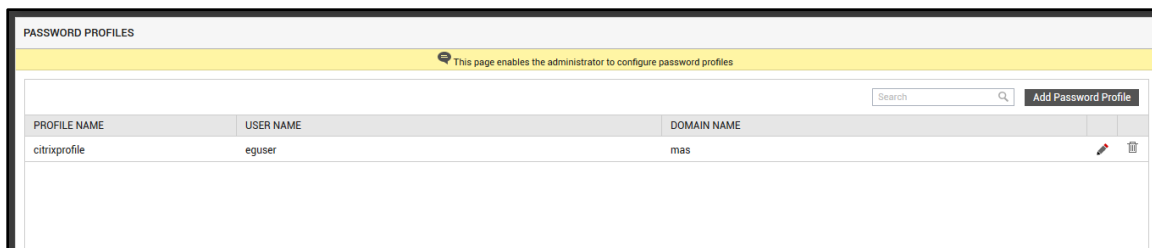


Figure 108: The PASSWORD PROFILES page

Once these credentials are associated with the password profile, whenever administrators configured the tests, choosing the appropriate password profile from the PASSWORD PROFILE list will auto-populate the credentials associated with the profile to the test.

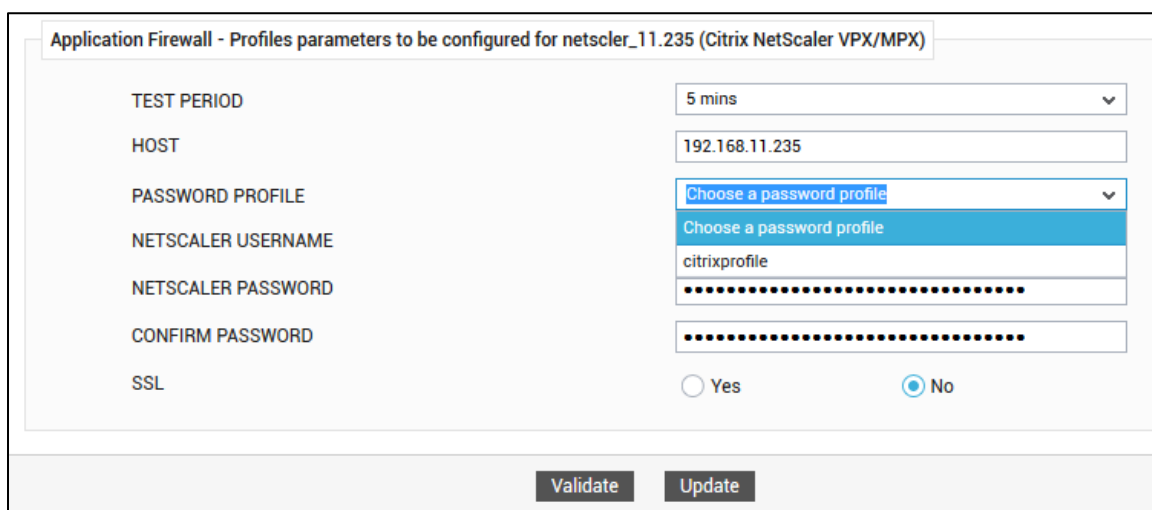


Figure 109: Choosing the appropriate password profile

This will save administrators a considerable amount of time in keying the credentials. Also, whenever administrators wanted to reconfigure the test with another user, they can do so by adding a new password profile and associating that password profile to the test.

- **Maintenance Policy can now be set from the layer model:** Until the previous version, administrators were allowed to set maintenance policies only from the eG administrative console. In environments where tests had multiple descriptors and administrators needed to put only a descriptor under maintenance, they still had to navigate to the eG administrative interface. For ease of use of the administrators, eG Enterprise v7 has introduced an icon which can be used to set maintenance policies from the layer model page of the eG monitor console. Administrators are also allowed to modify an existing maintenance policy from the eG layer model page.
- **Improved criteria to set Maintenance Policies:** In previous versions, administrators could set the maintenance policies only for a chosen day in a week. Though this was useful for the administrators, they wanted to set the maintenance policies in a more granular manner i.e., administrators wanted to set the maintenance policies for a chosen day of a chosen week in a month. eG Enterprise v7 allows administrators set maintenance policies by choosing a day of the week and the week of the month. Starting with eG Enterprise v7, maintenance policies can also be set for a chosen date of every month.
- **Maintenance policies can be reconfigured directly from the alert emails:** Starting with eG Enterprise v7, users are allowed to reconfigure the maintenance policies from the alert emails. This configuration can be performed without the users being able to login to the eG manager console.

To this effect, a link to configure the maintenance policy is specified in the alert emails wherever applicable. Note that users with admin role alone will be entitled to receive the alert emails and hence admin users alone are entitled to change the maintenance policies.

- **REST API test type is introduced in Integration Console:** With the growth of the IT industry, new technologies are introduced frequently. One such technology is the REST API which is more frequently used nowadays. Users of eG Enterprise v7 are now provided the option to build a test using the REST API test type. When choosing this type, the user provides the output of the REST API to be used and the Integration Console takes care of integrating the API into the eG framework.
- **Automatically Deleting/Unmanaging the components that are not reporting:** In dynamic environments where servers/devices are constantly added/removed, eG agent will not be able to collect metrics from components that have been uninstalled/removed from the environment. Previously however, such components continued to be visible in the eG Enterprise console, cluttering the view unnecessarily. To avoid this, eG Enterprise v7 has introduced an option to either delete or unmanage the components that are removed from the environment after a default period of 8 days. The **COMMON SETTINGS – AUTO UNMANAGE/DELETE** page in the eG administrative interface helps administrators in this regard. By default, administrators are allowed to unmanage/delete the components of the component types that are specified in the **Component types to be automatically managed** section of the **COMMON SETTINGS – AUTO MANAGE** page of the eG administrative interface.

7.2.3 Improved Alerting

- **Actionable Email Alerts:** In older versions, email alerts sent were not descriptive and nonexperts found it difficult to understand the alerts. Starting with eG Enterprise v7, the email alerts sent to the users are more descriptive, user friendly and smart. Apart from mentioning the actual problem which led to the generation of the alert, the severity is also mentioned in the email. Besides, an alert description is also provided along with the trend graph of the measure that violated the thresholds. The detailed diagnosis and the configuration changes, if any to the measure/component specific to the alert are also now reported in the email. This would help non-experts easily understand the context of the alerts. The users are also provided with actionable insights and recommendations on resolving the alerts. Note that such descriptive alerts will be available for html emails only.

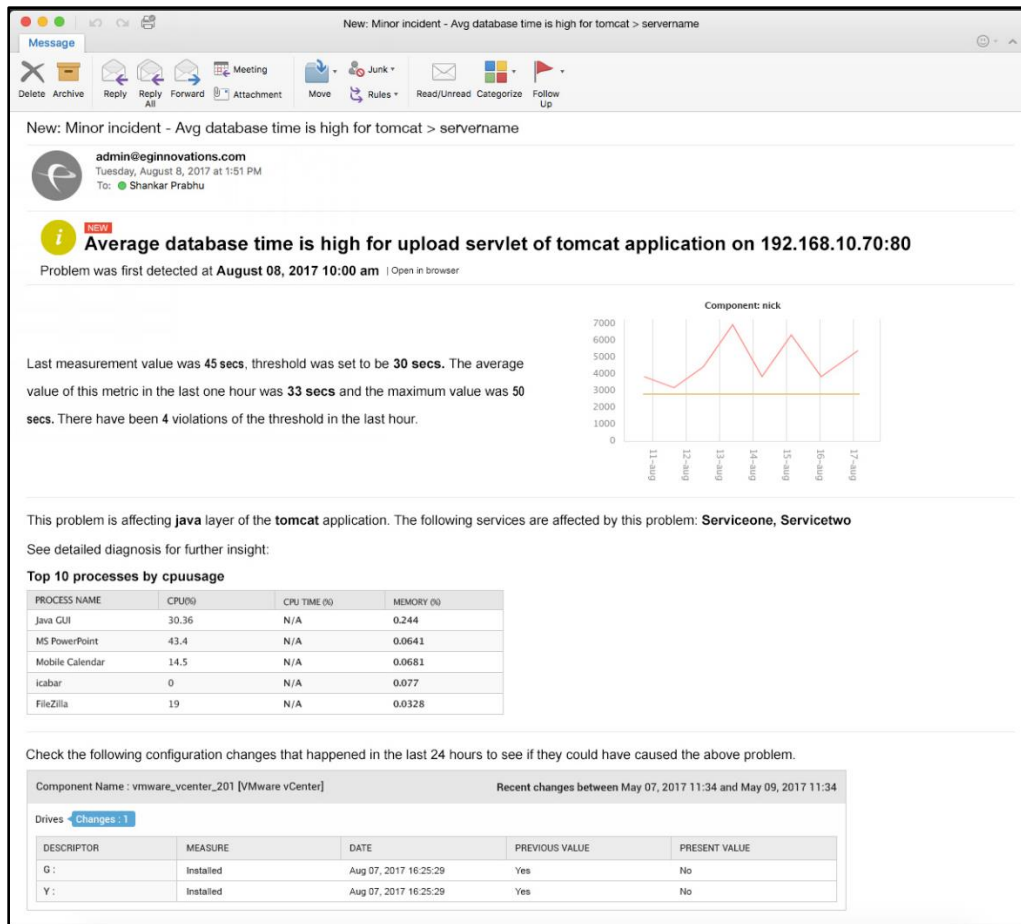


Figure 110: A sample email sent with a detailed alert description

- **Daily Performance Overview Email:** eG Enterprise v7 is now capable of sending a user-wise report on a daily basis as an email for a set of key performance metrics of the servers assigned to each user in the target environment. The generated report can be compared on the fly with the report generated for the previous day. This report helps administrators in understanding the overall health of the target environment without having to view the dashboards. The Daily Performance overview report emailer can be customized based on the needs of the user as well as based on the component types monitored in the target environment. The History of Alerts, system resource utilization for each day, average user experience metrics are some of the few panels that are offered by default in the report.

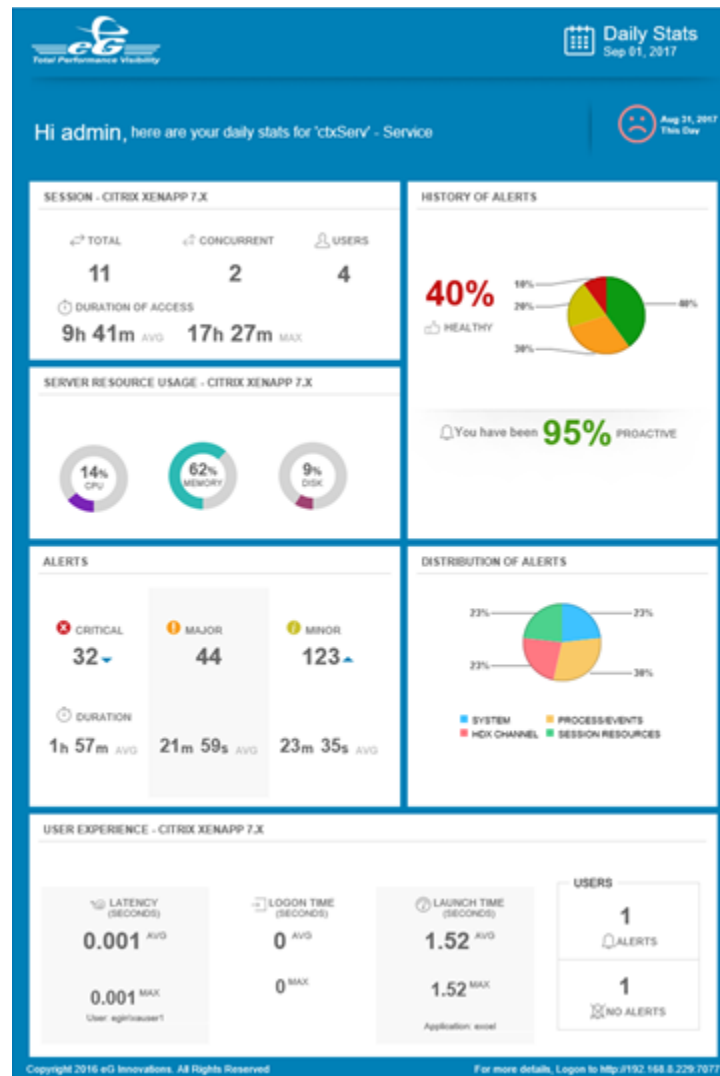


Figure 111: The Daily Performance Overview email

- **Ability to Acknowledge/Delete Multiple alarms:** Until the previous version of eG Enterprise, administrators were able to acknowledge or delete only a single alarm at a time. In environments where administrators handled a large quantity of alarms, it was difficult for them to choose each alarm for acknowledgement/deletion. Also, in some environments, certain administrators focus only on application level alarms while some other administrators focus on operating system level alarms. For such administrators, it was tedious to scroll through each application level alarm and acknowledge/delete the alarm which was also time consuming. To fasten the process of acknowledging/deleting the alarms, eG Enterprise v7 offers the ability to choose multiple alarms from the **CURRENT ALARMS** page for acknowledgement/deletion. With the introduction of this capability, administrators can select multiple alarms for acknowledgement/deletion in a single shot.

| TYPE | COMPONENT NAME | DESCRIPTION | LAYER | START TIME |
|------|-----------------------------|---|-----------------------|--------------------|
| | eG Manager | Database insert time is high for servlet Upload on eG Manager 192.168.8.30:7077 | eG Application | Jul 16, 2019 13:45 |
| | VMware vSphere ESX | ESX temperature status is abnormal for Processor/IO Module 1 PCH Temp on VMware vSphere... | Hardware | Jul 16, 2019 13:04 |
| | VMware vCenter | License utilization is high (VMware vCenter Server 6 Standard) | vCenter Services | Jul 16, 2019 13:00 |
| | VMware vCenter | License utilization is high (VMware vSphere 6 for Virtual SAN Witness for Embedded OEMs) | vCenter Services | Jul 16, 2019 12:55 |
| | eG Manager | Disk Disk0 C: on egMnager830 is very busy | Operating System | Jul 16, 2019 11:56 |
| | Microsoft Office 365 | Usage of Active Licenses for Office 365 BUSINESS PREMIUM is high for Microsoft Office 365 of... | Office Tenant | Jul 16, 2019 11:54 |
| | Citrix XenServer | Virtual CPU used by VM TEZ-WIN10-eG-(9.148) is high. This VM is hosted on Citrix XenServer X... | Outside View of VMs | Jul 16, 2019 11:54 |
| | Microsoft Windows | notepad's processes are not running on Microsoft Windows server 192.168.8.30 | Application Processes | Jul 16, 2019 11:54 |
| | eG Manager | Database insert time is high for servlet Upload Diagnosis on eG Manager 192.168.8.30:7077 | eG Application | Jul 16, 2019 13:54 |
| | eG Manager | Database insert time is high for servlet Upload Diagnosis on eG Manager egMnager830:7077 | eG Application | Jul 16, 2019 13:54 |
| | VMware vSphere ESX | Memory usage is high on VMware vSphere ESX host ESX134 | Operating System | Jul 16, 2019 13:26 |
| | VMware vSphere ESX | Space usage is high on datastore egVNXE-Lun03 of VMware vSphere ESX LOCALHOST1 | Operating System | Jul 16, 2019 13:02 |
| | Microsoft Office 365 | Exchange Online service health has degraded for Microsoft Office 365 office_365 | Office Tenant | Jul 16, 2019 12:35 |
| | Microsoft Exchange Online | Service degraded | Tenant | Jul 16, 2019 12:19 |
| | eG Manager | Response time is high for transactions to /final/servlet/com.eg.UploadDiagnosis on eG Manag... | eG Access | Jul 16, 2019 12:13 |
| | Microsoft Exchange Online | Service degraded | Tenant | Jul 16, 2019 12:11 |
| | Microsoft SharePoint Online | Percentage of storage usage is high (https://eginnovations435.sharepoint.com/) | Site Collections | Jul 16, 2019 11:55 |
| | Citrix XenServer | Usage of allocated memory by VM INF-NSVPX-12.1.48 is high. This VM is hosted on Citrix Xen... | Outside View of VMs | Jul 16, 2019 11:54 |
| | Microsoft Office 365 | Exchange Online service health has degraded for Microsoft Office 365 trail_365 | Office Tenant | Jul 16, 2019 11:54 |
| | eG Manager | Many recent slow transactions for /final/servlet/com.eg.UploadDiagnosis on eG Manager serve... | eG Access | Jul 16, 2019 14:04 |

Figure 112: Acknowledge/Delete multiple alarms

- **Introduced Alert notification plugin for Chrome browser:** To keep track of the alarms raised by eG Enterprise, administrators had to either depend on the mails sent to them or login to the eG console. This was the norm until the version prior to eG Enterprise v7. When administrators were focused on other websites/applications, and do not have the eG manager console open at that moment, they tend to miss important alerts by a few minutes. To enable the administrators in being up to date on the alerts raised and to be quick in identifying the alerts, starting with this version, alerts can be viewed by the administrators without needing access to the eG console. For this, eG Enterprise has developed a new extension which is integrated with the Google Chrome browser.

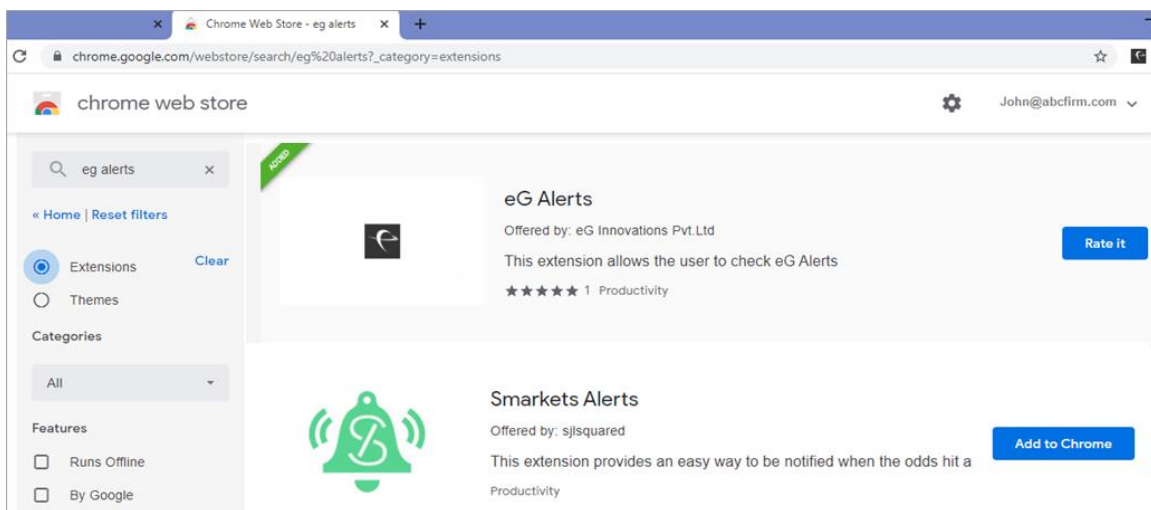


Figure 113: The eG Alerts extension on Google Chrome

Administrators need to enable this extension and provide the credentials of the eG manager.

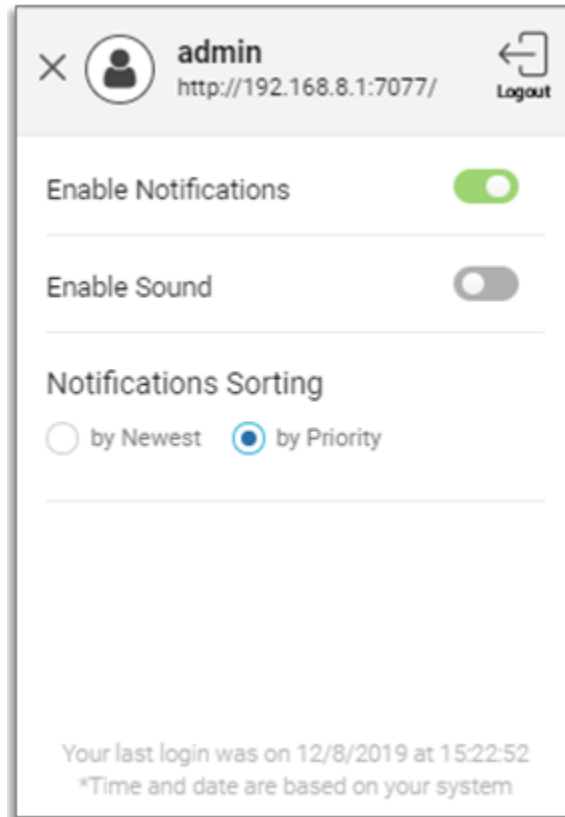


Figure 114: Specifying the eG manager IP in the eG Alerts extension

Then, the administrators will be notified of the alarms generated in that eG manager from the Google Chrome browser itself rather than logging into the eG console.

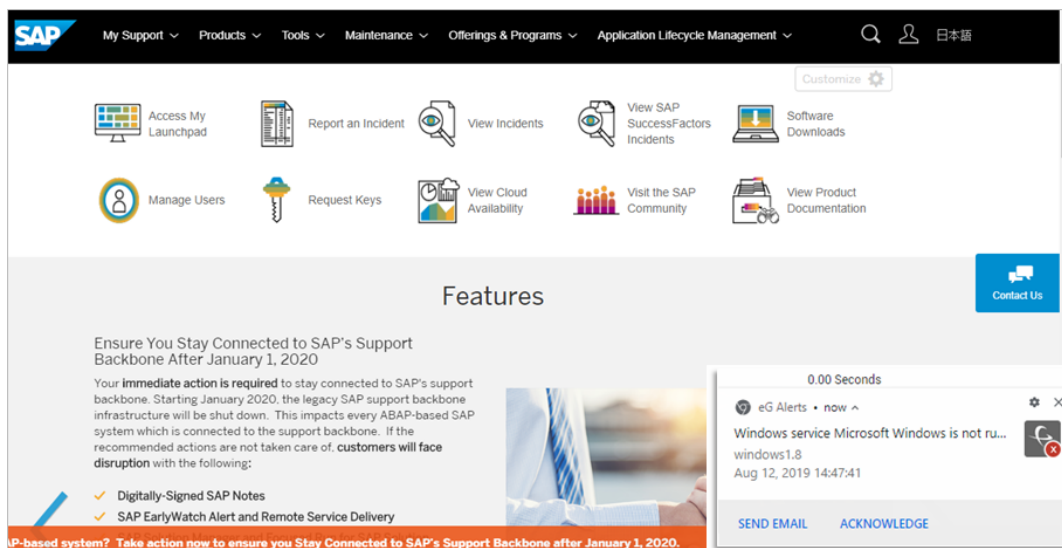


Figure 115: Alerts popping out on the browser

The notifications that appear on the Google Chrome browser can be sorted based on the newest alarms or based on alarm priority. Pop up notifications can also be enabled. Administrators can even

acknowledge/unacknowledge the alarm or send an email with the alarm details to the desired email ID.

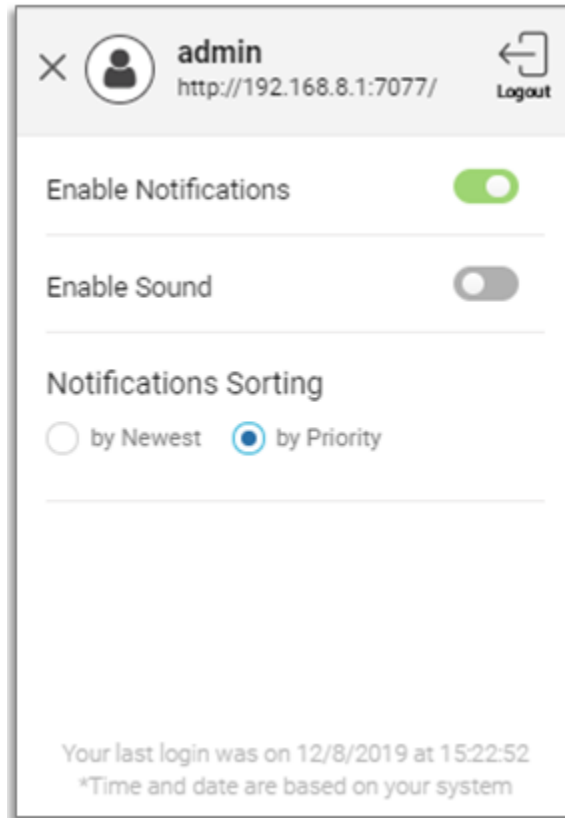


Figure 116: Enabling the Notifications

- **Alerts are now sent through WhatsApp:** To be on par with the technology world, eG Enterprise v7 offers to send alerts through WhatsApp. For this to take effect, administrators should first specify a valid mobile number in the USER PROFILE page.

USER PROFILE

USER ID
admin (login does not expire)

ALARMS BY MAIL/SMS
☒ Critical
 ☐ Major
 ☐ Minor

MAIL ID/MOBILE NO
 To
 CC
 BCC

Set Monitor Home
☒ Default
 ☐ Dashboard Templates

Infrastructure Overview

Submit Edit Profile

Specifying a valid mobile number

Then, administrators should enable the **Enable WhatsApp alerts** option from the **MAIL/SMS ALERT PREFERENCES** page in the eG administrative console. When the gateway (Chat API or WhatsMate) through which WhatsApp needs to be integrated with eG Enterprise is chosen and valid credentials are provided for the gateway, alerts are sent directly to the mobile number mentioned as a WhatsApp message. To avail this feature, note that the mobile number specified in the USER PROFILE page should already be registered with WhatsApp application. **Note that if administrators had enabled the Enable WhatsApp alerts flag, alerts will be sent only as a WhatsApp message and the SMS alerts will not be sent.**

WHATSAPP ALERT CONFIGURATION

Enable WhatsApp alerts ☒

Gateway ☒ Chat API ☐ WhatsMate

Gateway URL

Token

Update

Figure 117: Enabling alerts to be sent through WhatsApp

7.2.4 Enhanced Display

Support for Kiosk Mode: Often, administrators are required to keep track of their environment every other minute. Though the dashboards offered by eG Enterprise help administrators achieve this, they are forced to navigate through multiple dashboards to track what is hampering their environment. To ease the pain of the

administrators from juggling across different dashboards and to view the dashboards on a larger screen in a display loop, eG Enterprise v7 offers the Kiosk mode capability. The **KIOSK MODE** page in the eG monitor console can be played to view the dashboards offered by eG Enterprise on a larger screen. The default time delay of 10 seconds between each dashboard screen can be modified to suit the administrator's needs. Administrators can use the **Kiosk Filter** option to select the dashboards that they want to run in the Kiosk mode, or choose the infrastructure elements (e.g., components, services, zones etc.) for which dashboards need to be run in the Kiosk mode. This Kiosk filter is applicable to a few dashboards for e.g., Real user Monitoring, My Dashboard etc.

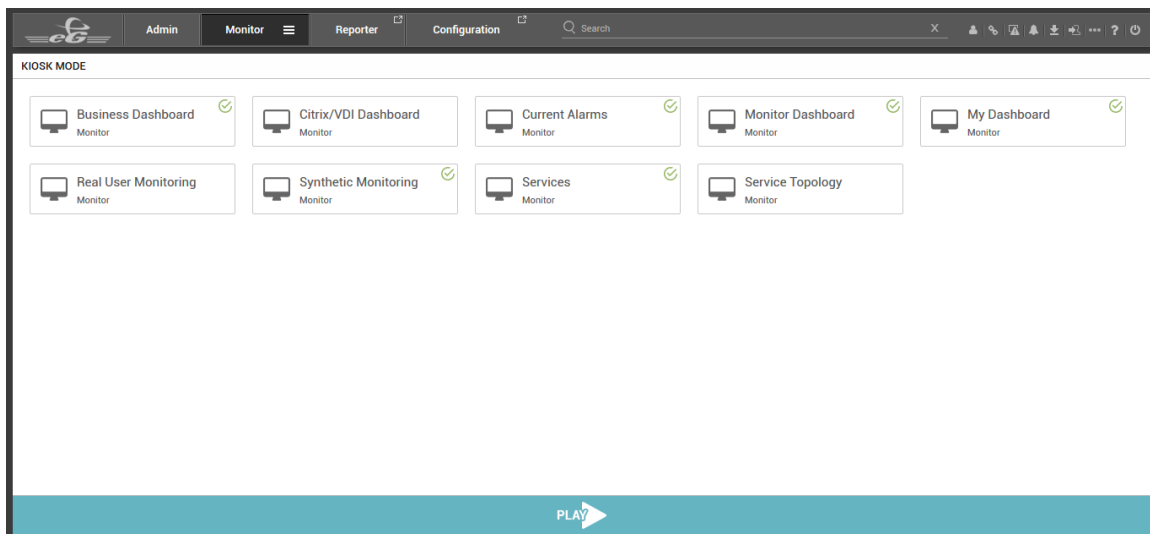


Figure 118: Setting the dashboards In Kiosk Mode

Improved Search UI: In previous versions, to use the **Search** feature available in the eG console, administrators were first required to choose an appropriate Search criterion (for e.g., User, Zone, Segment etc.). If the administrator failed to choose the correct search criteria, then the search results were inaccurate and sometimes, the search results did not include what the administrators were searching for. For an improved search performance, eG Enterprise v7 has enhanced the search functionality.

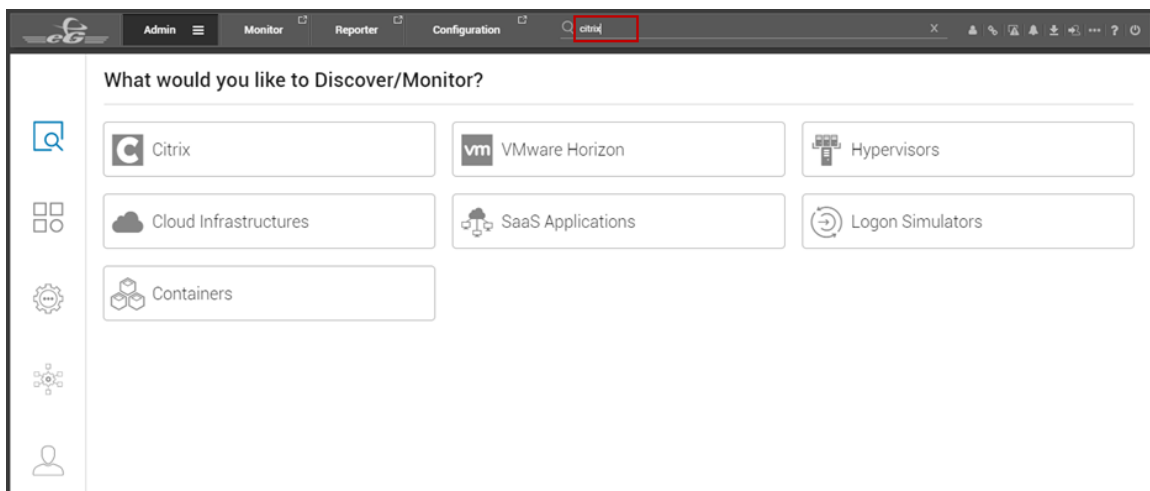


Figure 119: Specifying the name of the search

Upon inputting the name in the Search field, all criterions with that name will be automatically fetched and

presented to the administrators which make the Search capability much easier and reliable.

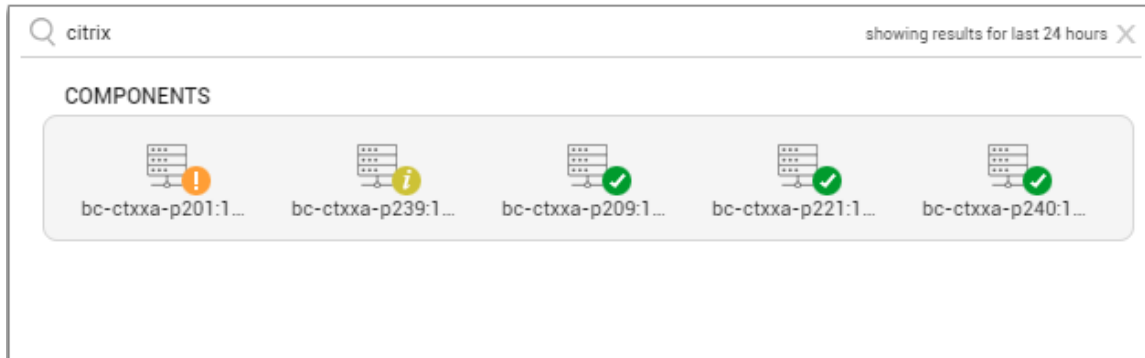


Figure 120: The results retrieved upon search

Improved Remote Control Actions: By default, the remote control commands can be executed from the layer model of each component. However, until the previous version, certain control actions can be initiated only at the server level and administrators had to deliberately define the commands needed to perform those actions. To offer more granularity in remote control command execution, eG Enterprise v7 gives you the ability to remotely initiate pre-built control actions for user sessions from web browsers. Now, certain actions (for e.g., to shadow a session, take a screenshot of a session, kill user GPO policies etc) can be initiated per user for Citrix XenApps, VMware Horizon and Microsoft RDS component types. eG Enterprise v7 has a pre-defined set of remote control commands for both user level and Operating System level.

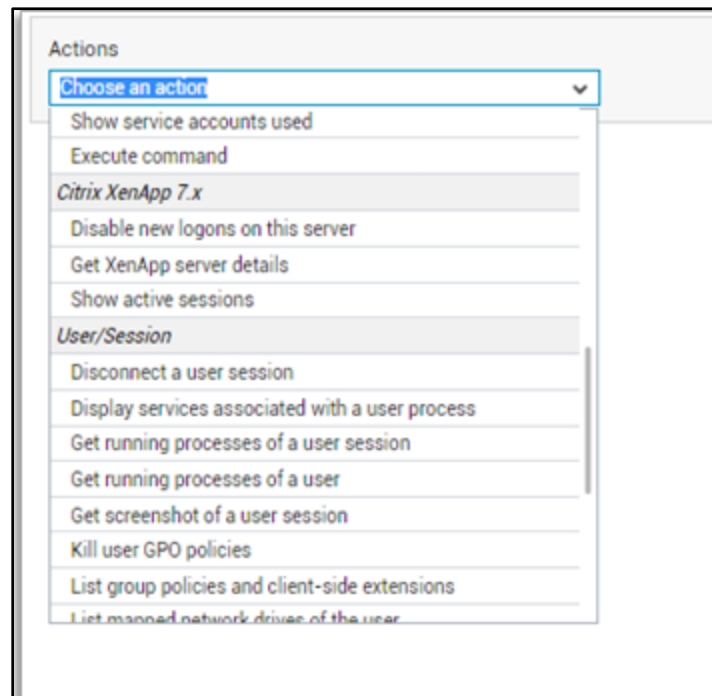


Figure 121: Choosing the remote control actions per user

Improved representation of virtual desktops and virtual servers in the Inside View Dashboard page: Until the previous version, the virtual servers and virtual desktops icon displayed in the Inside View of Servers and Inside View of Desktops page were the same. To enhance the visual appeal, starting with eG

Enterprise v7, different icons have been introduced for virtual servers and virtual desktops.

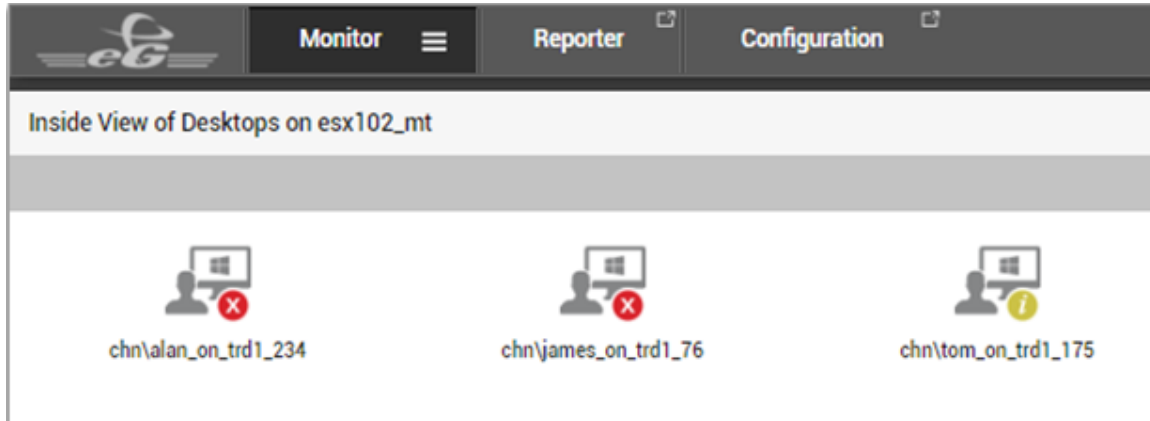


Figure 122: The representation of virtual desktops

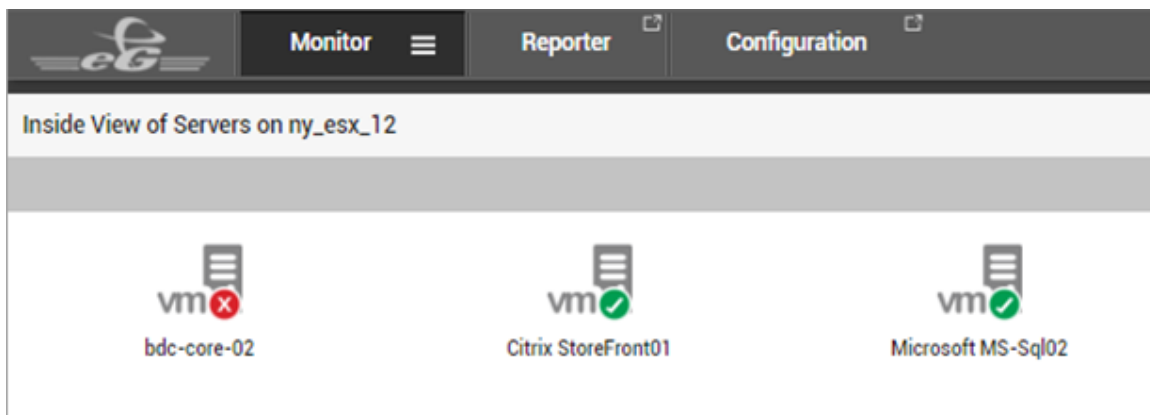


Figure 123: The representation of virtual servers

Enhancements to My Dashboard: Using My Dashboards, administrators can build a dashboard on their own or use the One click dashboard and create a brand-new dashboard. Though these features were of great help to the administrators, the dashboards could not be built with the data generated from an external source. For example, in environments spanning across multiple locations, data obtained in each location may be consolidated and stored in different forms (CSV, excel file, SQL database or as a REST API source). These data could not be accommodated earlier in the **My Dashboards** and therefore, administrators were unable to build a consolidated dashboard which spans all geographies. For the convenience of such administrators, eG Enterprise v7 has included a functionality where the eG manager integrates with an external source, pulls

the data and creates a new dashboard.

DSNSettings

DSN Name
salesforce

Integration Options

REST SQL EXCEL CSV

File: Browse file

Data Preview

| DATE | CUSTOMER | REGION | INVOICE ID | SALES PERSON | OPPORTUNITY | SALES PO | REVENUE |
|--------------|-------------------|--------|------------|--------------|-------------|----------|----------|
| 5/23/18 7:50 | EU Solutions P... | UK | BCD9790 | Jeol | 7 | 5 | 750000 |
| 4/20/18 7:55 | Timberlands P... | APAC | BCD9789 | Shaun | 18 | 12 | 18000000 |
| 3/16/18 7:59 | LKC Solutions ... | APAC | BCD9788 | Leon | 5 | 3 | 450000 |
| 3/12/18 8:05 | NSU Bank Pvt ... | US | BCD9787 | John | 8 | 8 | 1200000 |
| 2/10/18 8:09 | National Insur... | US | BCD9786 | Peter | 9 | 7 | 1050000 |

Save

Cancel

Figure 124: Integrating data from external sources in My Dashboard

- Setting a Global Timeline:** In previous versions, each widget was configured with a different timeline. Administrators of some environments wanted to have the current data in all the widgets of their dashboard. To cater to the need of such administrators, eG Enterprise v7 has included a Timeline drop down list in the Modify Dashboard page. When this global timeline is set, this timeline is considered across all the widgets. However, if administrators choose a different timeline in any widget, then that timeline will take precedence over the global timeline.
- Deleting Unwanted dashboards:** In previous versions, dashboards created by a user can be deleted by that particular user alone. However, if the user left the organization, administrators found it difficult to delete the dashboards and when there are multiple dashboards, it led to delays in loading the dashboards and constraints to space consumption. To avoid such hardship in dashboard loading and to regain the space consumed, starting with eG Enterprise v7, administrators are provided with the ability to delete the dashboards created by the users. Dashboards that are not accessed by the users for a long period of time can be chosen and deleted by the administrators.
- Widgets in My Dashboard are categorically restructured:** In versions prior to eG Enterprise v7, only a few widgets were offered for building the dashboard by default. Administrators needed to configure the widgets as and when required. Starting with this version, the widgets are grouped in a much convenient to use manner. The pre-built widgets are grouped separately while the widgets that need manual configuration are grouped under the **Configurable Widgets** section. Administrators are also provided the option to build their own widgets using the templates available and such widgets will be available under the **My Widgets** section.
- Introduction of new Widgets:** Starting with eG Enterprise v7, any custom dashboard that is built includes a **Zone map** widget in the Widgets Gallery section that houses all the pre-built widgets. With the Zone Map widget, you can have your dashboard display a zone map, using which you can figure out where exactly your zones operate, and what their current state is.
 - The **Problem Distribution** widget displays the history of problem events over a period of time in the environment. Using this, administrators can identify how many alerts are open, how many are acknowledged, the average duration of an alert and the maximum duration to resolve an

alert.

- Administrators can plot the **Activity Chart** graph to compare the performance of measures across servers/descriptors in a single graph.
- The **Scatter Plot** widget helps in historically analyzing the values of two closely related metrics and plotting their historical values in a single graph. For example, you can use the Scatter plot to analyze the free space vs used space in a server.
- The **Topology** widget can be used to display the real-time topology of your business-critical services, so that you can instantly determine service health and accurately isolate the root-cause of service slowdowns (if any).
- The **Text** widget helps administrators to write a note for their reference on the dashboard that they have created.
- The **Detailed Diagnosis** widget has been enhanced to plot the measures in a graph format. In addition to displaying the DD columns in a tabular format, the DD columns can also be plotted as either an Area Graph or a Bar Graph.

7.2.5 Reporter Enhancements

- **Enhancements to History of Alarms Report:** In previous versions, by generating the History of Alarms report, administrators could only perform historical analysis of alarms and detect problem patterns. Though this report was helpful in performing effective root-cause analysis, administrators could not generate a report for the alarms that were currently raised in the target environment. To aid administrators in generating a report for the open alarms, an **Alarms Type** list has been included in this report. Choosing the **Current** option from this list will generate a report that would list all the currently open alarms in the target environment. This would help administrators in identifying the problem-prone components and perform root cause analysis efficiently.
- **In-depth Visibility into the Logon Duration of Each User in the Sessions by Users Report:** Previously, administrators used the Sessions by Users report to figure out at what times the specified user logged into the Citrix XenApp server/virtual desktop, which server the user accessed, how much CPU/memory was utilized by the user, and the applications/VMs used by the user. However, administrators could not obtain in-depth visibility into the session start up details on the Citrix XenApp server/virtual desktop. This delayed the administrators in figuring out where exactly the slowdowns were noticed frequently – was that on the server side? or the client side? To aid administrators with this end to end visibility into the logon experience of each user session, a **needLogonSplitUp** flag has been introduced. If the administrators wish to generate the report with the end to end logon performance of each user session, he/she can set the **needLogonSplitUp** flag in the **[CITRIX_USER_REPORT]** section of the **eg_report.ini** file available in the **<eG_INSATLL_DIR>\manager config** folder to **yes**.
- **Brand-new report to check the Health of the eG Manager:** To determine at-a-glance how healthy the eG manager has been over a chosen time period and to quickly and accurately pinpoint performance 'hot spots', you can use the new **eG Manager Health** report that eG Enterprise v7 offers. This report when generated, runs a pre-configured set of health checks – i.e., rules - on the eG Manager. If even a single rule had failed in the given timeline, the report marks the eG manager's health as 'Not OK'. Using the report, you can also identify the exact rules that failed. This way, you can accurately isolate the problem-prone KPIs of eG manager performance.

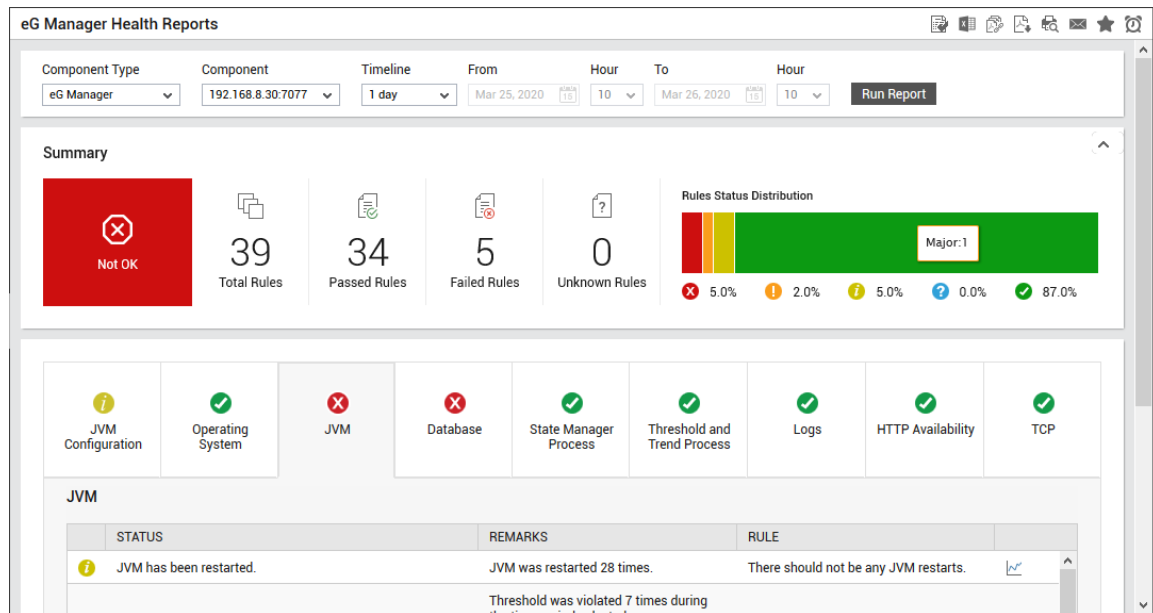


Figure 125: The eG Manager Health Report

- **Simplify Report Creation with the Report Builder:** eG Enterprise v7 now introduces a new built-in utility called **Report Builder** that empowers customers and service providers to build their own custom reports and add them to the Reporter console. Using an intuitive and easy-to-use interface, IT admins can build custom reports with different types of charts including bar chart, area chart, pie chart, stacked bar chart, heatmap, top-N chart and more and share the report with their team members or management. To avail this capability, administrators need to create a custom report template. This template will then be visible in the eG Custom Reports page which can then be used for generating the report that you want.

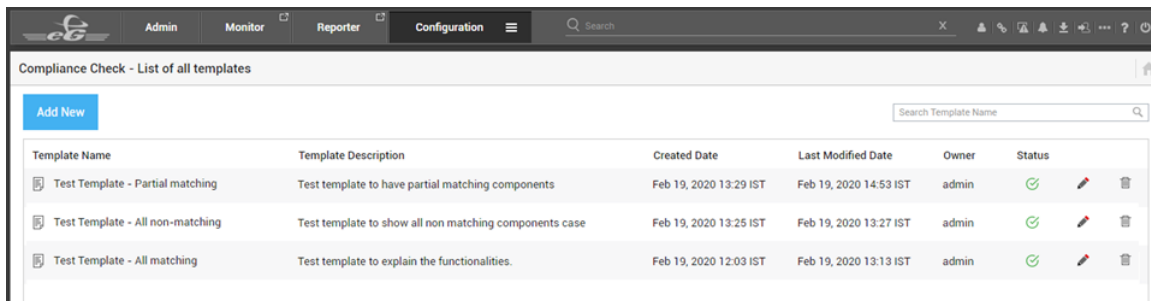
7.2.6 Configuration Management Enhancements

Starting with eG Enterprise v7, following components can be monitored to receive metrics related to configuration:

| | | |
|------------------------|----------------------------|----------------------------|
| IBM WebSphere MQ | Siebel Application Server | Juniper Net screen |
| SAP ABAP and BW | Synology NAS | Sonic Firewall |
| Citrix XenMobile | FortiGate Firewall | Checkpoint Smart Appliance |
| EMC VNXe | SAP Application Server | Hitachi Compute Blade |
| EMC Unity | HP ESKM SERVER | F5 Traffic manager |
| DHCP server | Palo Alto Firewall | F5 Analytics |
| Windows DNS | RSA Authentication Manager | |
| Sybase Adaptive Server | Bluecoat Proxy SG Server | |
| | | |

Introduction of Compliance Check: In environments comprising of numerous Windows machines, the biggest challenge for administrators is to verify whether/not the latest OS patches/fixes are installed on all the machines, and to identify the ones where the required patches/fixes do not exist. To ease the pain of

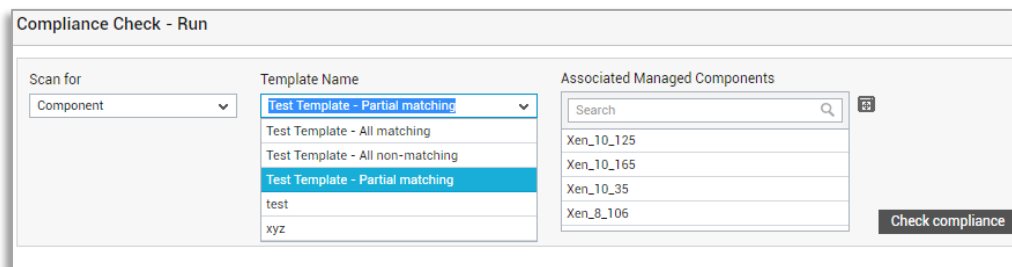
administrators, a gold template aka compliance check template is created and run on the eG Configuration module. While creating a template, administrators need to configure a few conditions based on which the compliance check should be performed. For example, an administrator may want to install an application on all Windows 10 machines that possess RAM of 6GB and above. To do this, the administrators need to create a template and configure a condition that checks for the RAM on all machines. Based on the condition that is configured on the template, compliance check is performed on all the machines in the target environment.



The screenshot shows the 'Compliance Check - List of all templates' interface. It includes a search bar, an 'Add New' button, and a table with columns: Template Name, Template Description, Created Date, Last Modified Date, Owner, and Status. There are three templates listed.

| Template Name | Template Description | Created Date | Last Modified Date | Owner | Status |
|----------------------------------|--|------------------------|------------------------|-------|--------|
| Test Template - Partial matching | Test template to have partial matching components | Feb 19, 2020 13:29 IST | Feb 19, 2020 14:53 IST | admin | ✓ |
| Test Template - All non-matching | Test template to show all non matching components case | Feb 19, 2020 13:25 IST | Feb 19, 2020 13:27 IST | admin | ✓ |
| Test Template - All matching | Test template to explain the functionalities. | Feb 19, 2020 12:03 IST | Feb 19, 2020 13:13 IST | admin | ✓ |

Figure 126: The list of compliance check templates



The dialog box shows the configuration for running a compliance check. It includes a 'Scan for' dropdown set to 'Component', a 'Template Name' dropdown with 'Test Template - Partial matching' selected, and a list of 'Associated Managed Components' including Xen_10_125, Xen_10_165, Xen_10_35, and Xen_8_106. A 'Check compliance' button is at the bottom right.

Figure 127: Checking for the compliance based on the template

Non-compliances are reported and the deviant machines are revealed to the administrators.

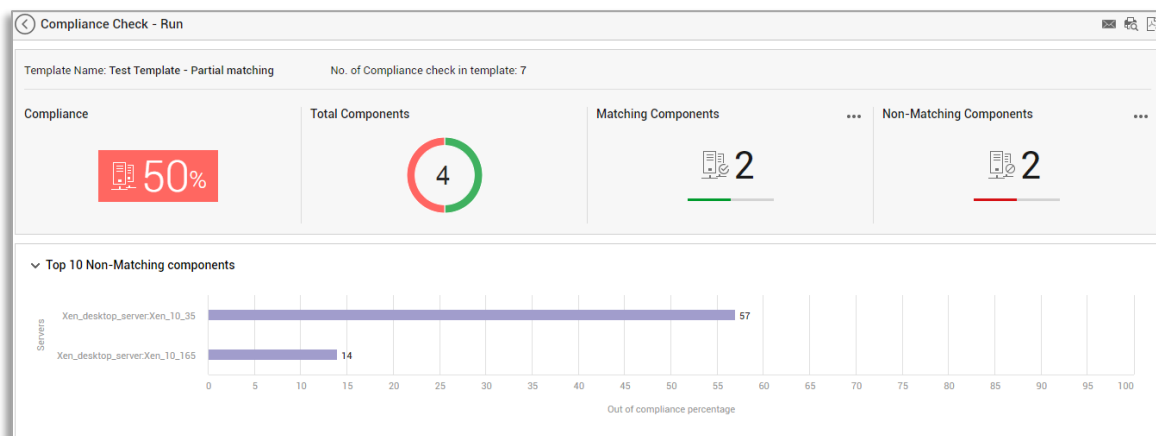


Figure 128: The result of Compliance Check

Optimizations to the eG Configuration Module: In previous versions, the eG agent used to store configuration metrics both in the memory as well as a local copy. This was useful because, whenever the eG agent restarted, the memory copy was no longer available; but, the eG agent continued to perform configuration change tracking using the local copy. This approach, however, may not be ideal for provisioned

environments. This is because, if a provisioned agent is restarted, the local copy may be wiped out along with the memory copy, or it may be overwritten with old configuration. Without a reliable copy of configuration metrics, the eG agent may not be able to perform configuration change tracking correctly. To overcome this issue, starting with eG Enterprise v7, the eG agent will not store the configuration metrics locally. The memory copy will be used to compare the current and previous configurations until such time the eG agent restarts. Upon a restart, the eG agent communicates with the eG manager to download the last known configuration from the eG database and uses this to detect configuration changes.

7.3 eG CLI Enhancements

Starting with eG Enterprise v7, administrators are allowed to add/modify groups in bulk using the eG CLI. With the help of an XML or CSV file that contain the exact details of the components that are part of the group, administrators can execute the commands in bulk. In a similar fashion, administrators are allowed to add/modify zones in bulk using the eG CLI.

7.4 Support for REST API for Administering the eG Manager and Retrieving Analytics

To perform critical configuration tasks on the eG manager without logging into the eG manager, eG Enterprise previously offered only an eG CLI capability. With eG Enterprise v7 however, a brand new eG REST API capability is also available for a similar purpose. From any REST client, you can hit the URL of the eG manager using the HTTP POST method to connect to the manager and perform configuration tasks on it. Moreover, using the eG REST API, you can also retrieve analytical data (for e.g., alarms raised in the target environment, the detailed diagnosis data of a chosen measure, health of the components in the target environment) from the eG manager. Commands can also be executed in bulk using this eG REST API.

7.5 Security Enhancements

Two Factor Authentication: Nowadays, with the advancement of technologies, IT infrastructures are becoming more and more vulnerable to unauthorized access and this vulnerability in particular, has increased the security worries of the IT administrators. The first step towards any security breach is that of the attacker's/hacker's ability to gain access to the login credentials of the servers in the environment and that of users logged into those environments. User authentications were commonly compromised to gain access to the IT environments. To avoid security breach and to firm up the authenticity of the users accessing the environments, providing an additional layer of security apart from the usual user authentication becomes a necessity. This additional layer of security is often provided by two-factor authentication across the technology world. eG Enterprise v7 incorporates this authentication mechanism. When two-factor authentication is enabled, the users logging into the eG manager are required to provide the user credentials along with a unique code.

Administrators can either enforce two-factor authentication as a mandatory step for all the users or let the users decide if they want to be verified with two-factor authentication. The **2-STEP VERIFICATION** page in the eG admin console helps administrators in enabling the two-factor authentication for the users in their environment.

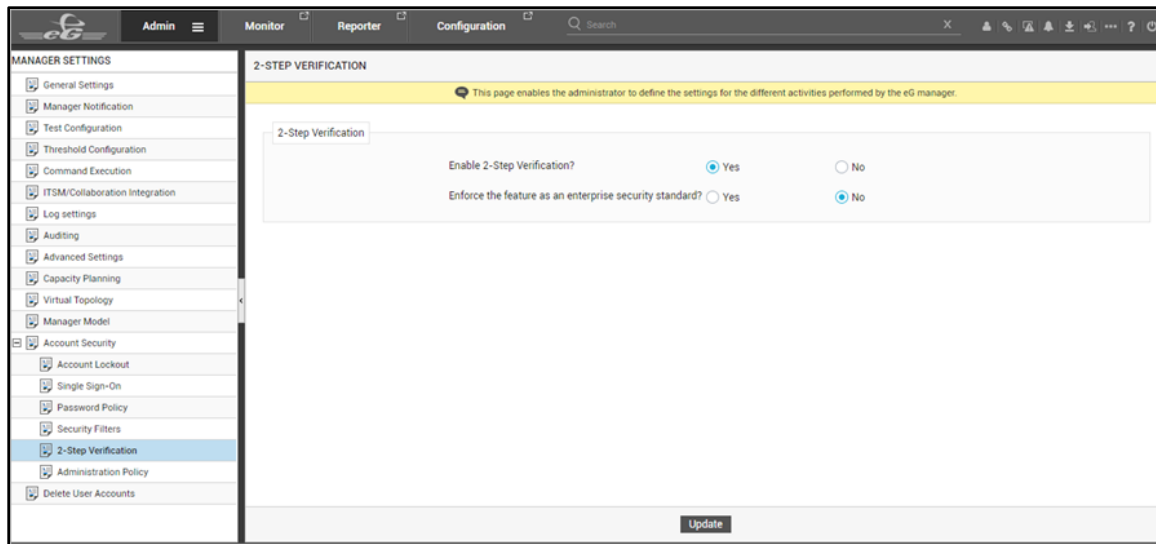


Figure 129: The 2-Step Verification page

If the administrator has enforced the two-factor authentication across the entire infrastructure, administrators are required to configure the email IDs of the individual users logging into the environment. Once this is complete, all the users in the environment will receive a One Time Password (OTP) in their email IDs which they need to provide mandatorily after specifying their passwords while logging in.

If the administrator has empowered the users to decide whether to use two-factor authentication or not, the users can enable two-factor authentication from the **USER PROFILE** page. Once the user enables two-factor authentication, he/she can choose to receive the One Time Password either through the registered email ID or through the Google Authenticator application installed on their verified mobiles. When the user chooses to generate the OTP through the Google Authenticator application, he/she will first receive a secret key to the registered email ID. The user should then input this secret key in the Google Authenticator application to generate the OTP.

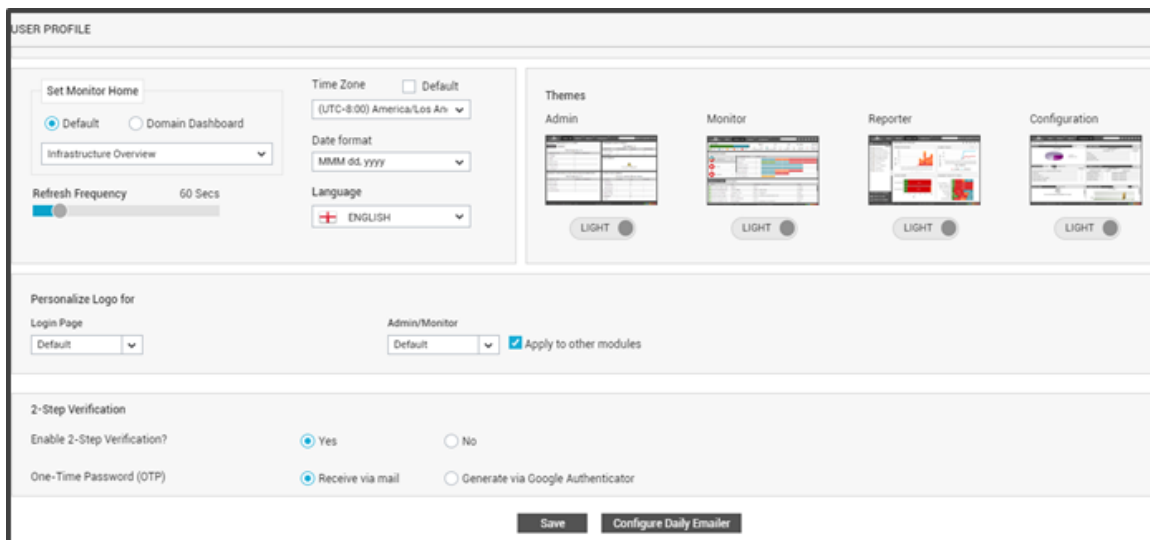


Figure 130: Enabling the 2-step verification in the User Profile page

- **Introduced Single Sign-on capability:** With the day to day increase in the applications accessed by the users, they are forced to remember multiple set of user credentials for logging into the applications.

Though login is a quick process, sometimes, users may either forget their password or may key in the wrong password. This would delay the login process considerably. To avoid the risk of keying in the wrong password and to improve the productivity of the user, it is necessary to eliminate the need for multiple logins. This can be achieved using Single Sign-On authentication process in the technology world. eG Enterprise v7 has incorporated this Single Sign-On authentication mechanism. The users logging in through various single sign-on systems such as Active Directory, AD FS, OKTA, OneLogin etc can now be authenticated using the Single Sign-On authentication. For this, users need to use the SINGLE SIGN-ON page in the eG admin console. To offer Single Sign-On authentication, eG Enterprise v7 uses the SAML authentication process. SAML authentication is the process of verifying the user's identity and guiding the service provider on what access is to be granted to the authenticated user.

MANAGER SETTINGS

- General Settings
- Manager Notification
- Test Configuration
- Threshold Configuration
- Command Execution
- ITSM/Collaboration integration
- Log settings
- Auditing
- Advanced Settings
- Capacity Planning
- Virtual Topology
- Manager Model
- Account Security
 - Account Lockout
 - Single Sign-On**
 - Password Policy
 - Security Filters
 - 2-Step Verification
 - Administration Policy
 - Delete User Accounts

SINGLE SIGN-ON

This page enables the administrator to define the settings for the different activities performed by the eG manager.

Single Sign-On

Enable single sign-on (SSO) ☒ Yes ☐ No

Allow the user to logout from the SAML Identity Provider (IdP) ☐ Yes ☒ No

Update

Figure 131: Enabling Single Sign-On

eG Enterprise v7 offers two types of Single Sign On logon mechanisms using SAML – namely Service Provider initiated Single Sign On and Identity Provider (IdP) initiated Single Sign On. Using the **SAML IDENTITY PROVIDERS** page in the eG admin console, administrators need to configure the details of Identity Providers i.e., Single Sign on systems such as OneLogin, OKTA etc.

SAML IDENTITY PROVIDERS

This page enables the administrator to configure the SAML Identity Providers for authentication.

View Metadata Configure SAML IDP Delete All SAML IDPs

| SAML IDP NAME | LOGIN URL | LOGOUT URL | IS DEFAULT IDP FOR LOGIN? |
|---------------|-------------------------------------|-------------------------------------|---------------------------|
| OneLogin | https://egadmin.onelogin.com/tru... | https://egadmin.onelogin.com/tru... | No |
| Demoldp | https://egadmin.onelogin.com/tru... | https://egadmin.onelogin.com/tru... | No |
| Vinodidp | https://egdemo.onelogin.com/trus... | https://egdemo.onelogin.com/trus... | No |

Figure 132: Configuring the SAML Identity Providers

Once the Identity Providers are successfully configured, administrators can use either of the two authentication mechanisms to login into the eG console. When Service Provider initiated Single Sign-On system is chosen, users are first required to choose the Identity Provider from the eG login page. The users will then be redirected to the login page of the chosen Identity Provider where they need to enter valid credentials. Once the credentials are authenticated, users gain access to the eG console.

When the users choose Identity Provider initiated Single Sign-On logon mechanism, they login through the Identity Provider and choose eG Enterprise from the listed services to gain access to the eG console.

Enhanced Security to prevent vulnerabilities: eG Enterprise v7 has been bundled with the latest versions of Tomcat server (v9) and JDK (v12). Which by default have inbuilt security features to prevent against critical vulnerabilities. eG Enterprise v7 also consists of a new security filter option which automatically turns on to protect against the vulnerabilities. With such powerful security filters, eG Enterprise is protected against certain types of vulnerabilities recommended by OWASP. Following are a few types of vulnerabilities that are protected by the security filters of eG Enterprise v7:

- Injection
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Insecure Direct Object Reference
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Components with Known Vulnerabilities
- Unvalidated Redirects and Forwards

Administration Policy: In environments such as banks, hospitals etc, administrators often struggle to ensure the security of the environment and they mostly succeed in providing top notch security. In order to maintain the security of the environment, administrators need to ensure that the users are denied access to the environment from remote locations. To help administrators in this regard, eG Enterprise v7 includes a special feature that allows the users of eG Enterprise log into the eG Enterprise console only from a particular IP address or an IP range or an IP address pattern to perform administrative tasks. For this, purpose, an **ADMINISTRATION POLICY** page has been included in the eG admin console. When an administrative policy is added, users are allowed access to the environment only from the IP address or IP range or IP address pattern that has been specified.

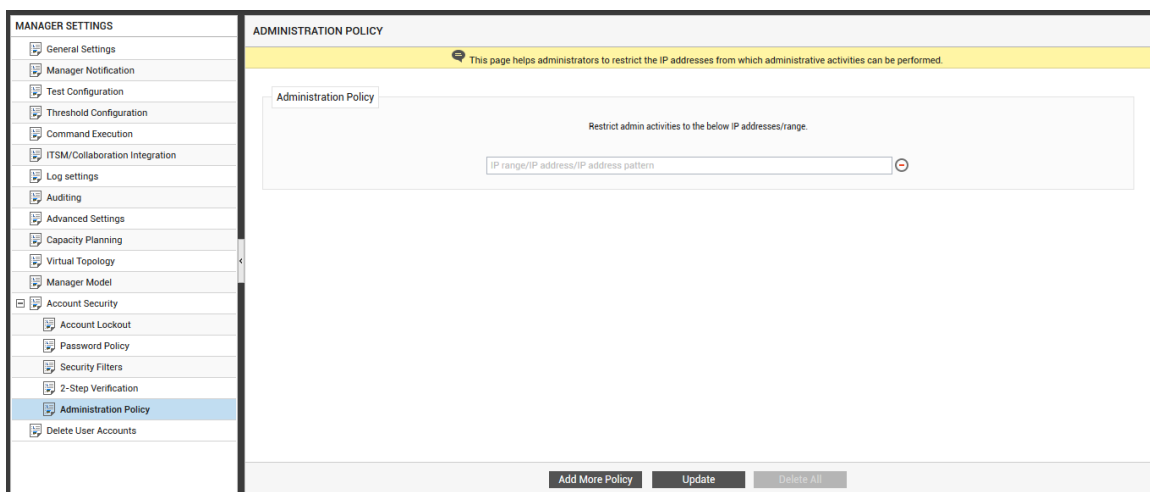


Figure 133: Specifying the IP address/range to restrict access to eG Enterprise

7.6 eG Mobile Application Enhancements

Following are the enhancements that are done with respect to the eG mobile application:

- Enabling Push Notifications is now available within the eG mobile application: Earlier, Push notifications were sent through the eG mobile application only if the user had registered for push notifications and had set the **EnablePushNotification** flag in the **eg_services.ini** file available in the **<eG_INSTALL_DIR>\manager\config** folder of the eG manager to which the eG mobile application is communicating to **Yes**. The users did not have the option to register for the same if they failed to register during installation. To avoid such hardship, starting with eG Enterprise v7, an **Enable Push Notification** option has been included in the **Settings** section of the eG mobile application. Users can enable/disable the push notification feature at their own will.

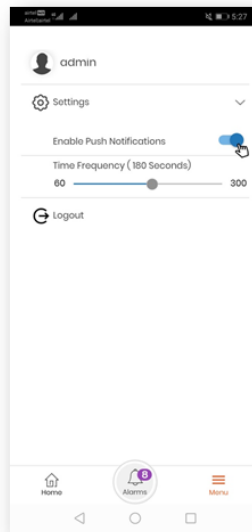


Figure 134: Enabling/Disabling Push Notifications

- **Support for Two-Factor Authentication:** Starting with eG Enterprise v7, the eG mobile application is automatically enabled with two-factor authentication. This is applicable only when the eG mobile application is configured with the credentials of an eG manager that is enabled with two-factor authentication. If the Google Authenticator application is used to generate the OTP for logging into the eG manager console, then you need to ensure the following in the eG mobile application.
 - The Google Authenticator application and the eG mobile application should be installed on the same mobile.
 - The timezone of the eG manager and the mobile on which the Google Authenticator and the eG mobile application is installed should be the same.
- **Ability to add maintenance policies:** Starting with eG Enterprise v7, maintenance policies can be set for components via the eG mobile app. To set a maintenance policy, administrators need to choose the alarms pertaining to the components that need to be put under maintenance. Alarms of

different component types can be chosen simultaneously while adding a maintenance policy.



Figure 135: Adding alarms of multiple components to maintenance policy

- Ability to delete multiple alarms: Starting with eG Enterprise v7, multiple alarms can be deleted simultaneously from the eG mobile application. Similarly, multiple alarms can be simultaneously acknowledged/unacknowledged.

7.7 Integration Enhancements

eG Enterprise v7 can now be easily configured to route its alarms to a trouble ticketing system such as SapphireIMS, OpsGenie, VictorOps, Webhook Integration, MS Teams, MoogSoft, Connectwise, ZenDesk and SNOW ITOM, via the web services framework.

7.8 Scalability Improvements

eG Enterprise v7 is now more scalable with certain improvements made in the eG manager and eG agent communication, redundancy and thresholds. Let us now have a more detailed discussion on these scalability improvements.

- **Compression of eG manager and eG agent data:** In environments where the communication between the eG manager and the eG agent was through SSL and the data packets communicated were large, the bandwidth usage was always on the higher side. This eventually slowed down the

data transmission. To facilitate faster data transmission and to reduce the bandwidth consumption, starting with eG Enterprise v7, the technique of compressing the data has been introduced. This technique has showed a considerable decrease in the bandwidth usage i.e., when experimented internally, we were able to reduce the bandwidth usage by 7% to 14%. Thus, the speed of data transmission between the eG manager and the eG agent has improved.

- **Threshold Changes:** In older versions, if a test/descriptor was configured with Static threshold, then, alerts were not raised until the threshold computation process was complete. The threshold computation process took up to an hour to complete. eG Enterprise did not alert the administrators when thresholds were violated during the very first measure period. Similarly, Static thresholds do not vary with time and when such thresholds are calculated once in an hour, the database consumed too much of space. To overcome these two limitations, eG Enterprise v7 has introduced a new capability that will ensure that the administrators are alerted even before the threshold computation was complete. To this effect, the **StoreAbsThresholdInDB** parameter in the **[MISC_ARGS]** section of the `eg_services.ini` file available in the `<EG_INSTALL_DIR>\manager\config` folder is set to **False**. This implies that the threshold computation process will not be carried out and hence threshold data will not be stored in the database.
- **Data Retention changes in redundant managers:** In previous versions, in environments where redundant managers were setup for monitoring, the data retention period of both the primary manager and the secondary manager was configured to be the same. Therefore, the data from both the managers were wiped out simultaneously. A few administrators however wanted to retain the data available in the secondary manager for a longer period. This is to avoid any data loss on both the managers as well as to archive the data for further analysis. To this effect, starting with eG Enterprise v7, administrators can set the **DifferentDataRetentioninClusterManagers** flag in the **[MISC_ARGS]** section of the `eg_services.ini` file available in the `<eG_INSTALL_DIR>\manager\config` folder to true. This will ensure that the same data retention period will not apply for redundant managers and administrators will be allowed to change the database settings of the secondary manager.
- Starting with eG Enterprise v7, Database Partitioning is supported on Oracle Database 12c Enterprise Edition also.

8. Conclusion

eG Enterprise v7 enables organizations take a 360° view of user experience. The many enhancements in this release help organizations quickly troubleshoot complex application and IT infrastructure problems without affecting user productivity and customer satisfaction.

Based on customer feedback and market analysis, eG Innovations will continue to build new monitoring, diagnosis and reporting functionality to address the performance management the needs of the modern technology landscape. We are committed to make eG Enterprise even more robust, intelligent, automated, scalable and easy to use in future product releases.

Contact Us

- To contact eG Innovations sales team, email sales@eginnovations.com.
- Get a free trial of eG Enterprise v7: <https://www.eginnovations.com/FreeTrial>.
- For support queries and feature requests, email support@eginnovations.com.

About eG Innovations

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments. To learn more visit www.eginnovations.com.