The eG Enterprise Logon Simulator for Amazon WorkSpaces

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

Amazon WorkSpaces is a fully managed, secure Desktop-as-a-Service (DaaS) solution which runs on AWS. With Amazon WorkSpaces, you can easily provision virtual, cloud-based Microsoft Windows desktops for users, providing them access to the documents, applications, and resources they need, anywhere, anytime, from any supported device.

A typical user logon in an Amazon WorkSpaces infrastructure begins with the user attempting to access the URL of the Amazon WorkSpaces over the web. Once the user conects to the Amazon WorkSpaces, he/she provides his/her login credentials at the login prompt. As soon as the credentials are validated, he/she will be allowed to access the desktop provisioned for him/her.

Many factors impact a user's logon experience. Slowness/failure of the web interface, authentication failures/delays, and network latencies can contribute to a sub-par logon experience. Because the failure points are one too many, proactive detection of a failed/slow logon and precise isolation of its root-cause is often a challenge for administrators. Another bottleneck to effective troubleshooting is the fact that logon issues do not come to light until a user actually logs in.

Collecting logon metrics of real user activity is challenging. Metrics have to be collected from the different tiers involved - the web interface, the network, and the Amazon WorkSpaces.

The eG Enterprise Logon Simulator for Amazon WorkSpaces, a part of the eG Enterprise suite, is a purpose built solution for delivering proactive visibility into the logon performance in Amazon WorkSpaces infrastructures. Using an agentless approach, the eG Enterprise Logon Simulator for Amazon WorkSpaces simulates a user logging into an Amazon WorkSpaces client portal through a browser and accessing his/her desktop. By emulating the exact same process that users go through when they logon to Amazon WorkSpaces, the eG Enterprise Logon Simulator for Amazon WorkSpaces provides a realistic measure of the user experience during logon. Since every simulation tests the entire Amazon WorkSpaces infrastructure, the results represent the cumulative health of all of the tiers supporting user logons.

Unlike traditional simulation tools that require recording of a script that captures the typical steps a user performs, the eG Enterprise Logon Simulator for Amazon WorkSpaces requires no recording and hence, is simple to implement. Installed on any physical or virtual machine, the simulator targets the configured logon URL and the desktop at pre-configured intervals and tests the logon availability and performance. When a problem is detected, the offending step is clearly highlighted, so administrators can start working on a resolution immediately.

The simulation can be configured to run from different remote locations to understand the logon performance from each location. By testing the simulated session from different locations and at different times, administrators can diagnose and resolve logon issues before users experience them and call up the helpdesk. Licensing is based on number of simulation locations, not on the number of logons simulated.

1.1 How does the eG Enterprise Logon Simulator for Amazon WorkSpaces Work?

A light-weight eG Logon Simulator Agent drives the logon simulation. This agent periodically runs a **Amazon WorkSpace Logon Simulator** test that emulates the entire process of a user logging into an Amazon WorkSpace cloud and launching an application / desktop. Since the test is what performs the simulation, let's call it the **simulator**. To perform this simulation, the simulator has to be configured with the following:

- The URL of the Amazon WorkSpaces that it needs to access
- The credentials using which it needs to log into the Amazon WorkSpace;
- The desktop that it needs to launch
- The registration code, since the Amazon WorkSpaces is enabled with two- factor authentication, by default.

Once the Logon Simulator Agent is configured, it runs at a pre-configured frequency. Every time it runs, it simulates the logon process, as detailed below:

- The Logon Simulator Agent first opens the Chrome browser and connects to the configured URL.
- It then logs in through the web interface (Client URL of the Amazon WorkSpaces) and captures the time taken to login. The success/failure of the login is also determined.
- The agent next opens the provisioned desktop and records the duration of the access. In the process, it figures out whether/not the mailbox was accessed successfully.
- Finally, the agent logs out of the desktop and the Amazon WorkSpaces infrastructure. The log out duration is also captured.
- Steps 1 to 4 are then repeated for every user that has been configured for monitoring.

1. The simulator first opens the Chrome and connects to the configured Amazon WorkSpace Site URL

2. It then logs in through the web browser and captures the time taken to login. The success/failure of the login is also determined.
3. The simulator next waits for the applications/desktops to be enumerated and records the time it took for the enumeration to complete. The success/failure of this step is also ascertained.
4. The configured application/desktop is then launched and the duration of the launch is recorded. In the process, the simulator also figures out whether/not the launch was successful.
5. Finally, the simulator closes the application and logs out of the Amazon WorkSpace session. The log out status and duration is also captured.
6. Steps 1 to 5 are then repeated for every application/desktop that has been configured for launching.

The simulator then reports the metrics so collected to the eG manager. The manager captures these metrics into an **Amazon WorkSpaces Logon Simulator** component and presents them in the eG monitoring console for analysis. Refer to the **Analyzing the Simulation Results** topic for a detailed discussion on the **Amazon WorkSpaces Simulator** model.

1.2 Pre-requisites for Using eG Enterprise Logon Simulator for Amazon WorkSpaces

Before attempting to use the simulator, make sure that the following pre-requisites are fulfilled:

Category	Pre-requisites
Logon Simulator Agent / Simulation Endpoint	• Client Session Simulation capability should be enabled on the eG license. • The logon simulator agent/external agent should be installed on a dedicated virtual machine or a physical server running Windows 2008/2012/2016/2019 or Windows 7/8/10 operating system. • The logon simulator agent/external agent should only run on an English version of Windows operating system. • No other eG agent should exist on the same host on which the logon simulator agent has been installed. • .Net 3.5 (or above) should pre- exist on the system hosting the logon simulator agent. • The simulator requires a user account with local administrator rights

	on the simulation endpoint - i.e., on the system hosting the Logon Simulator Agent. This user should be logged in at all times for the simulator to run continuously. **Note:** • The logon simulation will not work if the session is closed.
Environment	• One/more valid and dedicated email IDs on the Amazon WorkSpaces infrastructure is required for the purpose of the simulation. • To perform the simulation, the simulator needs to be configured with the URL of the Amazon WorkSpaces that it needs to access. **Ensure that the Web Access check box is enabled for that URL for which the simulation is to be performed.** To know more on how to enable the Web Access, click here. • If a firewall separates the simulation endpoint from the web interface, then make sure you configure the firewall to allow two- way communication between the endpoint and the web interface.
Browser	• Chrome browser v81 (and above) should be available on the dedicated endpoint. **Note:** In some environments where browsers are automatically updated to their latest versions, incompatibility is cited between the browser version and the Chrome drivers. This may sometimes hamper the start of the simulation. Therefore, ensure that the Chrome drivers are also updated whenever the browser is updated to the latest version. Chrome is capable of automatically applying updates and upgrading itself to higher versions. Sometimes, when Chrome auto- upgrades, some drivers that the eG Logon Simulator Agent uses may suddenly be rendered incompatible with Chrome. This can cause problems in simulation. To avoid this, the eG Enterprise Logon Simulator for Exchange, by default, prevents Chrome upgrades/updates (both automatic and manual) from being applied at the simulation endpoint. However, whenever a new version of the eG agent with updated drivers is released, you will have to manually upgrade Chrome to ensure continued compatibility. In this case therefore, you will have to make sure that the simulation endpoint allows Chrome upgrades. To achieve this, before manually upgrading Chrome, follow the steps

	below: • Login to the eG agent host. • Open the Windows command prompt as Administrator. • Switch to the <EG_AGENT_INSTALL_DIR>\lib directory, and issue the following command: ChromeUpgradeHandler.exe enable

Note:

To ensure that all the pre-requisites of the Amazon WorkSpaces Logon Simulator is fulfilled, you can execute the **LogonSimulatorChecks.exe** which is available in the **<eG_INSTALL_DIR>\lib** folder. This executable should be executed by a user with administrator privileges from the command prompt of the target agent host. If any pre-requisite has not been fulfilled, failure will be highlighted in Red (as shown by Figure 1.1).

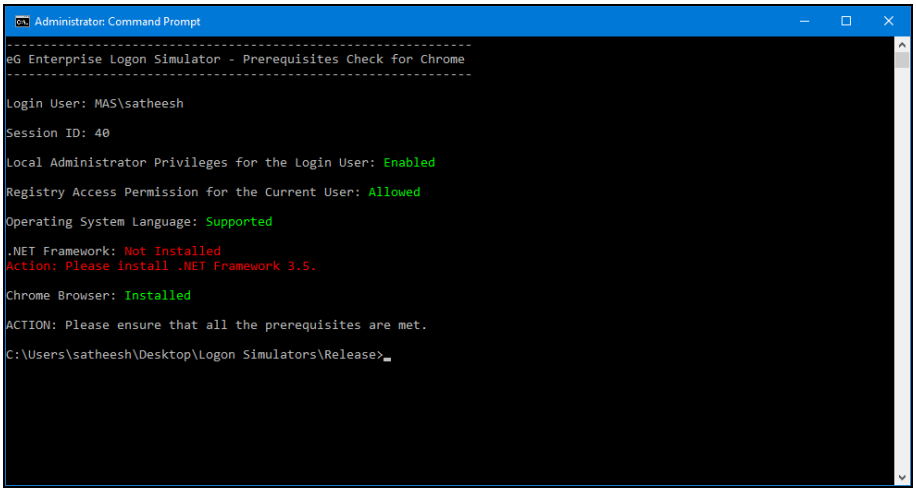

Figure 1.1: Setup script where a pre-requisite has failed

Use the pointers provided in Figure 1.1, just below the failed pre-requisite, to know how to fulfill that requirement. Then, rerun the **LogonSimulatorChecks.exe** to make sure that all pre-requisites are fulfilled, and then proceed.

If all pre-requisites are fulfilled, then Figure 1.2 will appear.

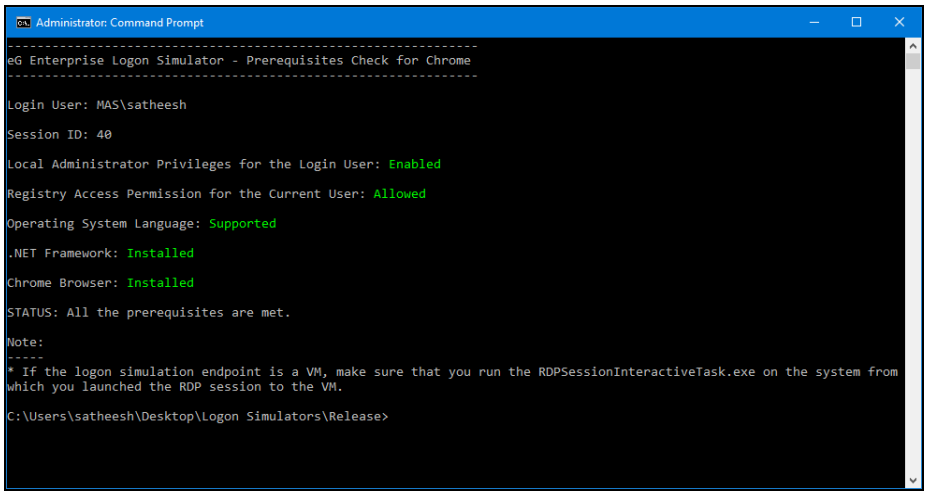

Figure 1.2: All pre-requisites are fulfilled

1.2.1 Enabling Web Access for Simulation

One of the key pre-requisites for starting the simulation is, the simulator should be configured with the URL of the Amazon WorkSpaces that it needs to access. By default, only certain device types are enabled to access the WorkSpaces using this URL. Sometimes, the simulation may fail to start even though all the required pre-requisites are fulfilled. In such cases, administrators should check for the device types that are enabled to access the WorkSpaces using the configured URL. eG Enterprise by default, uses web based access for simulation of the Amazon WorkSpaces. This Web based access option should be chosen by the administrators to ensure that the simulation starts. To enable the web based access option do the following:

1. Login to the Amazon Web Service console. Click the **Services** drop down and select the WorkSpaces option as shown in Figure 1.3.

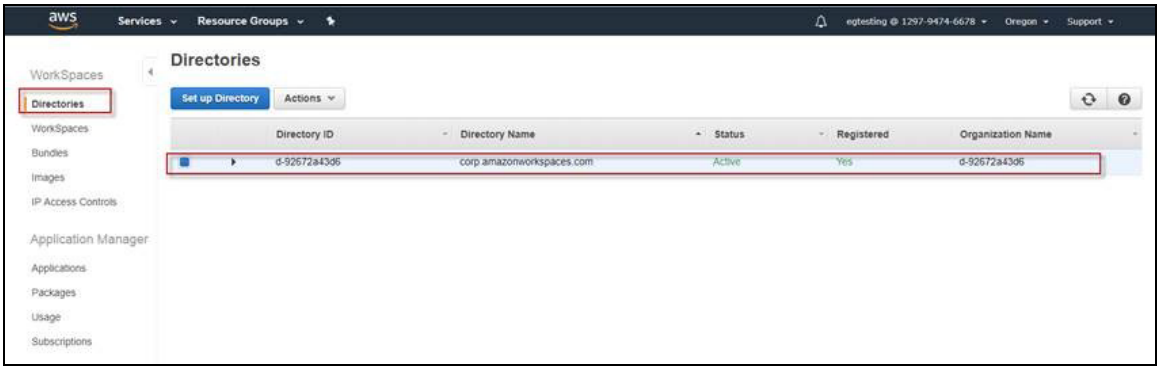

Figure 1.3: Clicking the Directories option

2. In Figure 1.3, click the **Directories** option from the **WorkSpaces** list. The URLs that is to be used to perform the simulation will then be listed there. Choose the URL by checking the check box and click the **Actions** drop down button.

3. Now, Choose the **Update Details** option as shown in Figure 1.4.

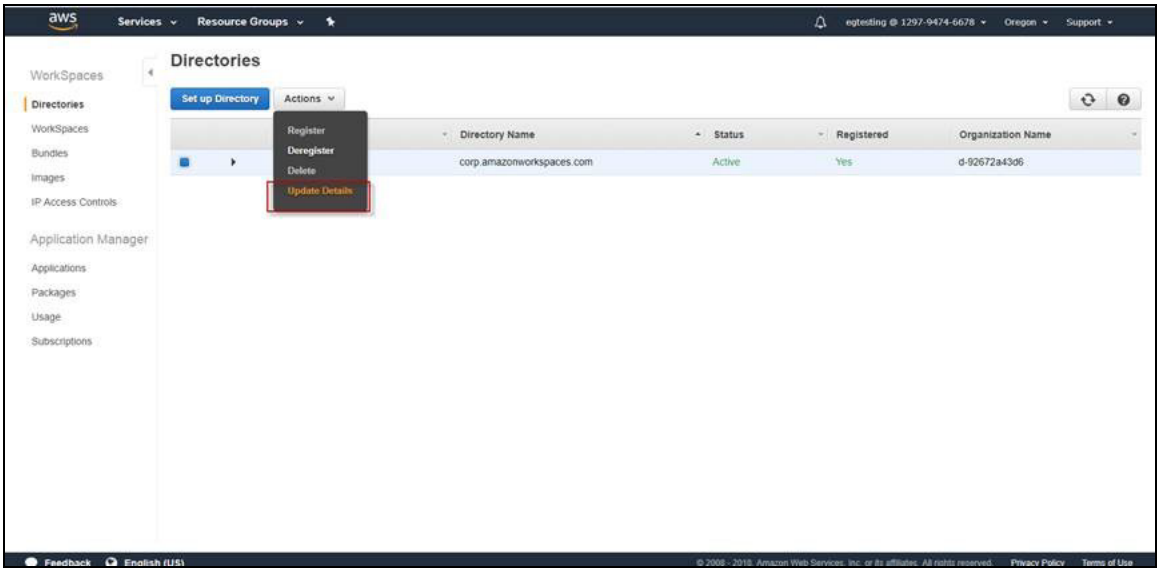

Figure 1.4: Updating the details of the chosen URL

4. Figure 1.5 then appears. Expand the **Access Control Options** list.

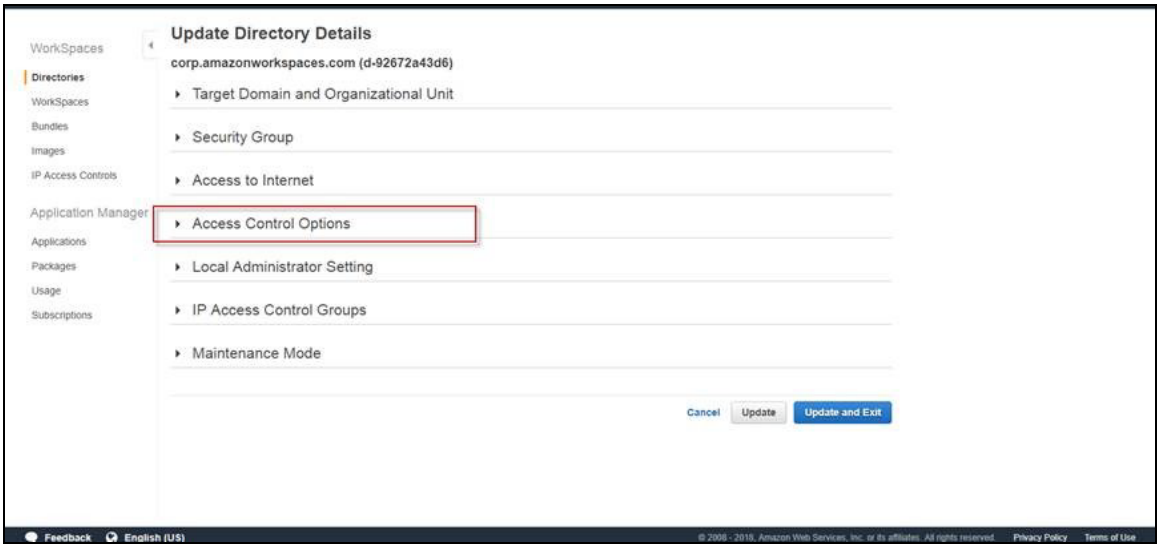

Figure 1.5: Expanding the Access Control Options list

5. In Figure 1.6 that appears, you need to enable the **Web Access** option under the **Other**

Platforms section.

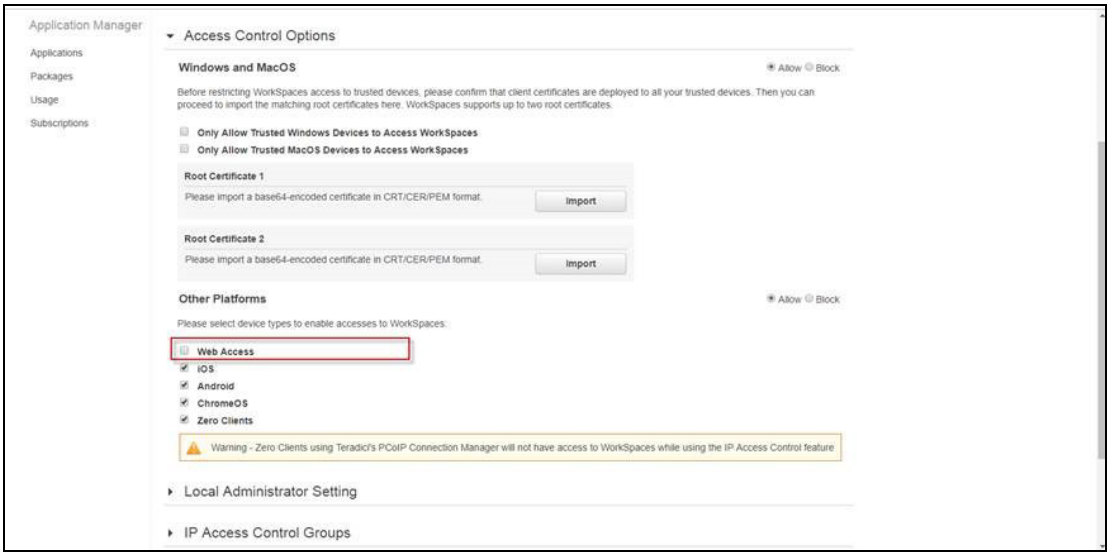

Figure 1.6: Locating the Web Access option

6. Simply check the check box in front of the **Web Access** option and click the **Update and Exit** button as shown in Figure 1.7.

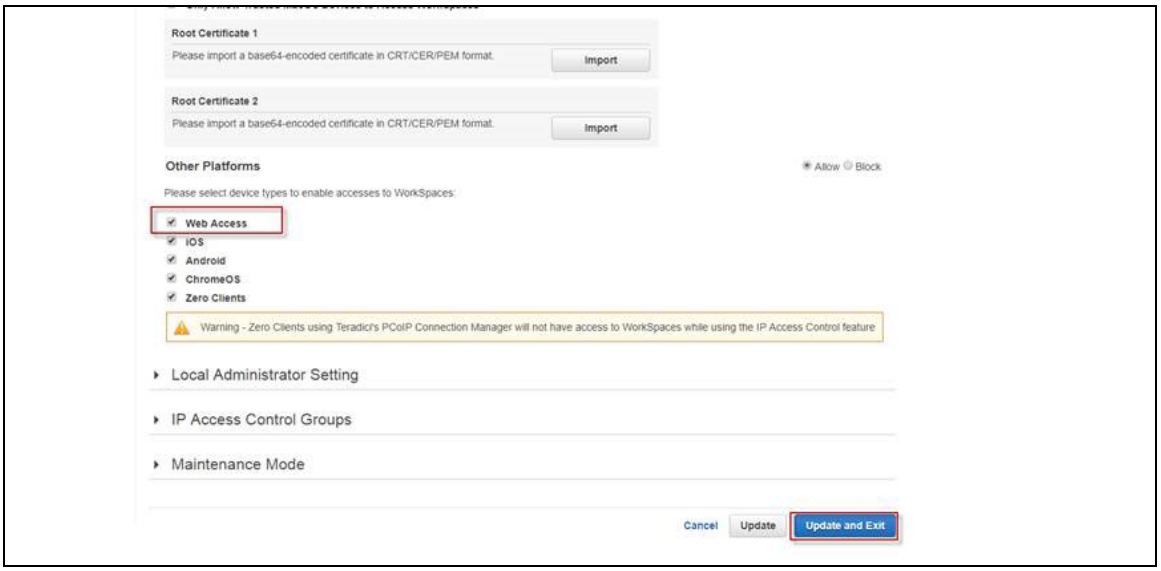

Figure 1.7: Checking the check box in front of the Web Access option

7. Now the URL is ready to perform the simulation.

Chapter 2: Configuring the Amazon WorkSpaces Simulator to Perform the Simulation

Once the pre-requisites listed in Section **1.2** are fulfilled, follow the steps detailed below to get the simulator up and running.

1. Log into the eG administrative interface.
2. Add a dedicated external agent for the purpose of the simulation. For that, follow the Agents -> External Agents menu sequence and click on the **Add New Agent** button. Then, specify the IP address/host name of the system that is hosting the dedicated external agent, and also provide a **Nick name** for the agent (see Figure 2.1).

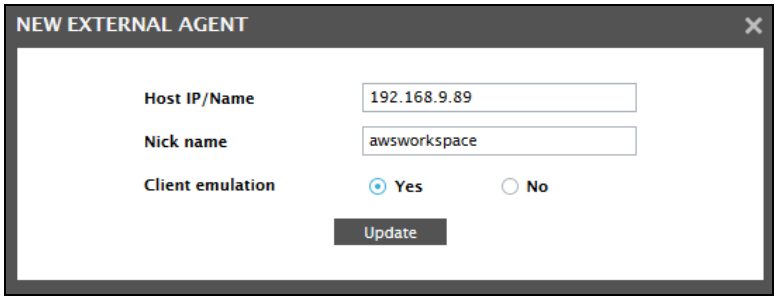

Figure 2.1: Adding a dedicated external agent for the simulation

3. Also, make sure that the **Client emulation** flag is set to **Yes** for the agent.
4. Finally, click the **Update** button in Figure 2.1 to save the changes.
5. Once this external agent is started, it simulates the entire logon process by periodically running a **Amazon WorkSpaces Logon Simulator** test. It is this test that serves as the **eG Amazon WorkSpaces Logon Simulator** . Since this test is mapped to an Amazon WorkSpaces Simulator component, you now need to manage a component of that type. For this, follow the Infrastructure -> Components -> Add/Modify menu sequence, and then pick **Amazon WorkSpaces Simulator** from the list of **Component types**. Then, click **Add New Component**. When Figure 2.2 appears, add an Amazon WorkSpaces Simulator using any IP address and nick name you want.

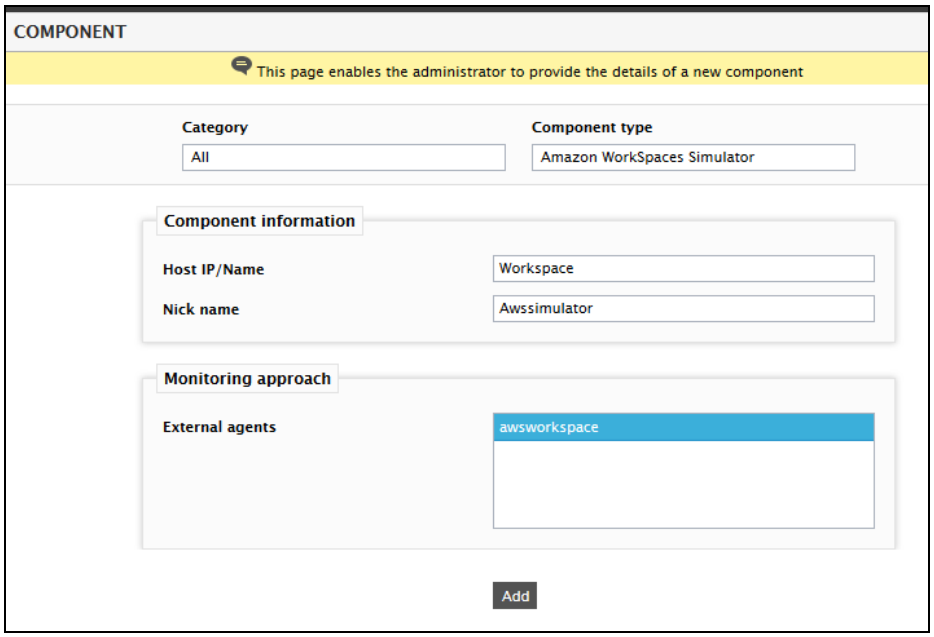

Figure 2.2: Adding an Amazon WorkSpaces Simulator

6. When adding, make sure you assign the dedicated external agent, which you had previously installed and configured for the sole purpose of this simulation, to the simulator component.
7. After clicking **Add** in Figure 2.2, proceed to sign out of the eG administrative interface. You will then be prompted to configure the **Amazon WorkSpaces Logon Simulator** test for this component. Click on the test to configure it.
8. Figure 2.3 will then appear. Click on each of the parameters in the figure below to know how to configure it.

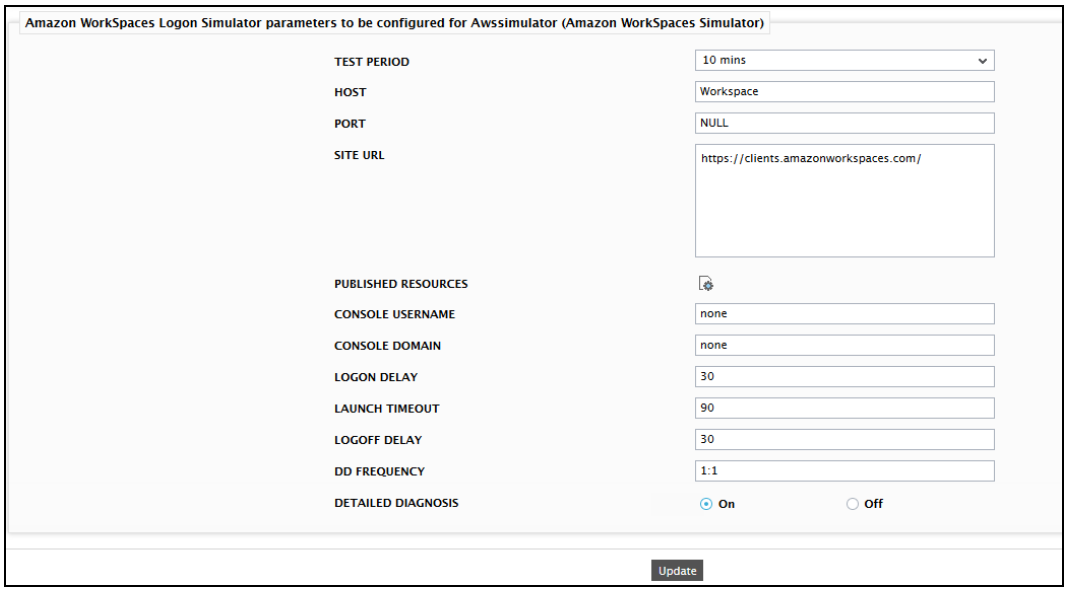

Figure 2.3: Configuring the Amazon WorkSpaces Logon Simulator test

9. To know how to configure the test, refer to the Section **Chapter 3** topic.
10. Once all parameters are configured, click the **Update** button to save the configuration.

Chapter 3: Analyzing the Simulation Results

Once the simulation ends, the logon simulator agent sends the availability and duration measures it collects to the eG manager. Using a specialized **Amazon WorkSpaces Simulator** monitoring model, the eG manager captures these metrics and publishes them in the eG monitoring console for analysis.

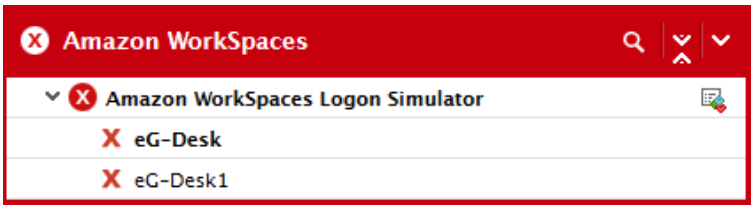

Figure 3.1: The layer model of an Amazon WorkSpaces Simulator component

As can be inferred from Figure 3.1 , this monitoring model consists of a single **Amazon WorkSpaces** layer, to which the **Amazon WorkSpaces Logon Simulator** test is mapped. Section **3.1** describes how this test works and the measures it reports.

3.1 The Amazon WorkSpaces Logon Simulator Test

This test emulates a user logging into an Amazon WorkSpaces cloud infrastructure and launching a desktop. In the process, the test reports the total duration of the simulation, time taken for the login to be authenticated, duration of desktop launch, and log out duration. Additionally, the test also captures failures (if any) at each step of the simulation. Using the insights provided by this test, the administrators can proactively detect logon slowness/failures and precisely pinpoint the root-cause of the anomaly - is it login authentication? desktop launch? or logout? This way, administrators are enabled to isolate the probable pain-points of their virtual infrastructure, even before users begin to actively use the cloud desktops.

Target of the test : Amazon WorkSpaces

Agent deploying the test : An external agent

Outputs of the test : One set of results for every virtual desktop configured for monitoring

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed. The default is 15 minutes.

Parameter	Description
	Note: Some parameter changes can sometimes impact the simulation duration. Most often, this can happen in the following situations: • If multiple desktops are configured for launching against PUBLISHED RESOURCES: In this case, the test will repeat the entire sequence of steps for every configured desktop - i.e., after a desktop is launched, the test will logoff and then log in again to attempt the launch of the next desktop. This can increase the duration of the simulation. • If the value of the Launch Timeout and/or the Logoff Delay parameters of the test is significantly increased: If this is done, then the simulator will wait that much longer for the desktop launch or logoff to happen, thereby increasing simulation duration. Sometimes, these changes can cause the simulation to take more time than the configured Test Period.
Host	The host for which the test is to be configured.
Port	Specify the port used to connect to the Amazon WorkSpaces here. By default, this will be *NULL*.
Site URL	Specify the URL for connecting to the virtual private cloud associated with the Amazon WorkSpaces here. You can provide either an HTTP or an HTTPS URL.
Published Resources	To know how to configure the resources to be monitored, refer to the Section **3.1.1** .
Console Username	The simulator needs to run in the account of a user who has local administrator rights on the simulation end point - i.e., the system on which the external agent has been installed. Specify the name of this user in the Console Username text box. This user should also be logged in at all times for the simulator to run continuously.
Console Domain	Specify the domain to which the user belongs to here.
Logon Delay	By default, this parameter is set to 30 seconds. This implies that the simulator will wait for a maximum of 30 seconds (by default) during each resource launch, for the logon to actually occur. If the logon does not happen even after the lapse of 5 seconds, then the simulation will be automatically terminated, and the

Parameter	Description
	simulator will mark the logon attempt as 'failed'. A logon duration will hence not be computed or reported in this case.
Launch Timeout	By default, this parameter is set to 90 seconds. This implies that the simulator will wait for a maximum of 90 seconds (by default) for a desktop to launch. If the desktop does not launch even after the 90 seconds have elapsed, then the simulation will be automatically terminated, and the simulator will mark that desktop launch as 'failed'. Accordingly, the *Application launch availability* measure for that published resource (i.e., desktop) will report the value 0, and no launch duration will be reported for the same. In some environments, one/more published desktops may take a little longer to launch than the rest. In such environments, you can instruct the simulator to wait longer for launching each of the configured published resources, by increasing the launch timeout. The high time out setting for resource launch ensures that the simulator captures and reports only genuine launch failures, and does not treat a launch delay as a failure.
Logoff Delay	By default, the Logoff Delay parameter is set to 30 seconds. This implies that the simulator will wait for a maximum of 30 seconds (by default) after each resource launch, for the logoff to occur. If the logoff does not happen even after 30 seconds have elapsed, then the simulation will be automatically terminated, and the simulator will mark the logoff attempt as 'failed'. A logoff duration will hence not be computed or reported in this case. In some environments, even during normal operation, logoff may take longer. In such environments, you can instruct the simulator to wait longer for the logoff to occur, by increasing the web logoff delay. The high time out setting for logoff ensures that the simulator waits for the log off to complete and captures and reports the accurate logoff duration.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against dd frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG

Parameter	Description
	agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

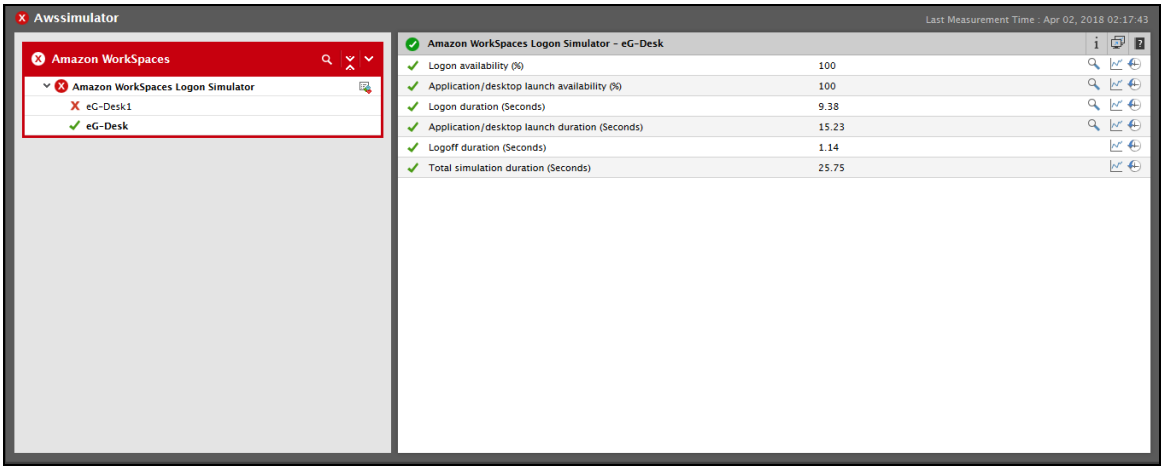

Figure 3.2: The measures reported by the Amazon WorkSpaces Logon Simulator test

Measurement	Description	Measurement Unit	Interpretation
Logon availability	Indicates whether/not the simulator logged into the directory of the virtual private cloud successfully, when attempting to launch this desktop.	Percent	The value 100 for this measure indicates that logon was successful, and the value 0 indicates that logon failed. If this measure reports the value 0, then no other measures will be reported for that desktop. You can also use the detailed

Measurement	Description	Measurement Unit	Interpretation
			diagnosis of this measure to view the output of the simulation script, scrutinize it, and isolate the failure and problem points of the Amazon WorkSpaces infrastructure at first glance.
Logon duration	Indicates the time taken by the simulator to login to the directory of the virtual private cloud, when attempting to launch this desktop.	Secs	If the *Total simulation duration* for a desktop exceeds its threshold, compare the value of this measure with that of the other duration values reported by the test to know where the bottleneck lies - in login authentication? desktop launch? or log out?
Application/desktop launch availability	Indicates the time taken by the simulator to launch this desktop.	Percent	The value 100 for this measure indicates that the desktop launch was successful, and the value 0 indicates that the launch failed. By comparing the value of this measure across desktops, you can quickly identify which desktop could not be launched.
Application/desktop launch duration	Indicates the time taken by the simulator to launch this desktop.	Secs	If the *Total simulation duration* for a desktop exceeds its threshold, compare the value of this measure with that of the other duration values reported by the test to know where the bottleneck lies - in login authentication? desktop launch? or log out?
Logoff duration	Indicates the time taken by the simulator to log out of the virtual private cloud.	Secs	If the *Total simulation duration* for a desktop exceeds its threshold, compare the value of this measure with that of the other duration values reported by the

Measurement	Description	Measurement Unit	Interpretation
			test to know where the bottleneck lies - in login authentication? desktop launch? or log out?
Total simulation duration	Indicates the total time taken by the simulator to simulate the launch of this desktop.	Secs	An abnormally high value for this measure could indicate a logon slowness. In such a case, compare the value of all the duration values reported by the test to know where the bottleneck lies - in login authentication? desktop launch? or log out?

Use the detailed diagnosis of the Logon availability measure to view the output of the simulation script, scrutinize it, and isolate the failure and problem points of the Amazon WorkSpaces infrastructure at first look. A summary of the simulation is also provided as part of the detailed diagnostics. This includes the Site URL configured for monitoring, the user name used for the simulation, the exact time at which the simulated user logged into the site, and the published resource that was accessed as part of the simulation.

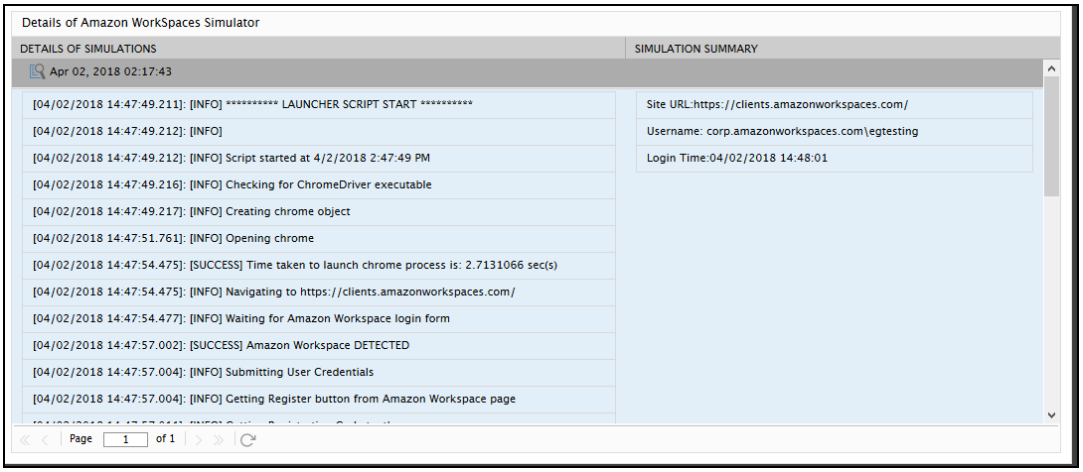

Figure 3.3: The detailed diagnosis of the Logon availability measure

3.1.1 How to Configure Published Resources for Monitoring?

To configure the applications / desktops that the simulator has to launch, click on the icon against **Published Resources** in 3.1.1.

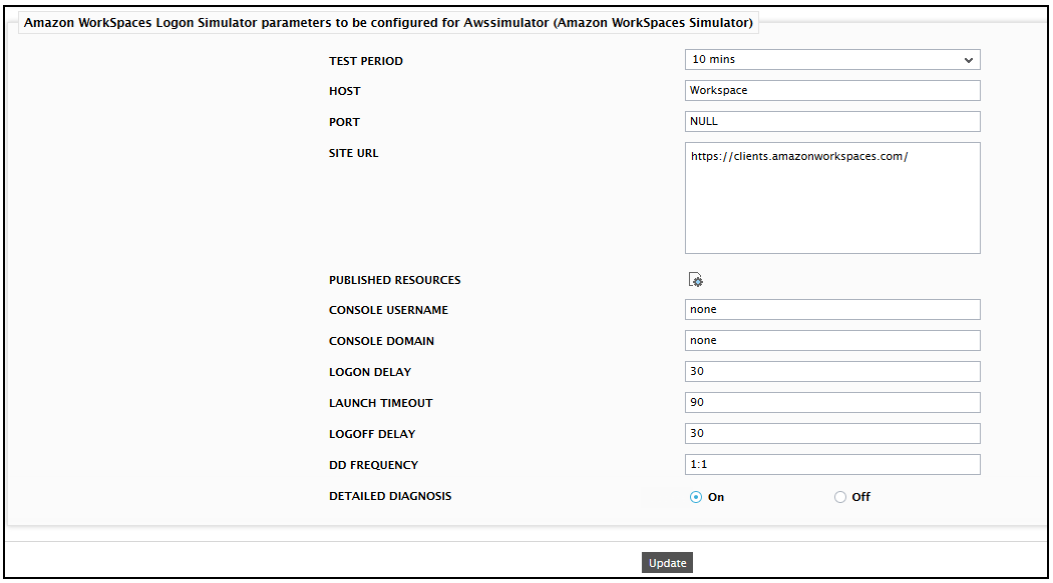

Figure 3.4: The Amazon WorkSpaces Logon Simulator Test configuration page

Figure 3.5 will then appear.

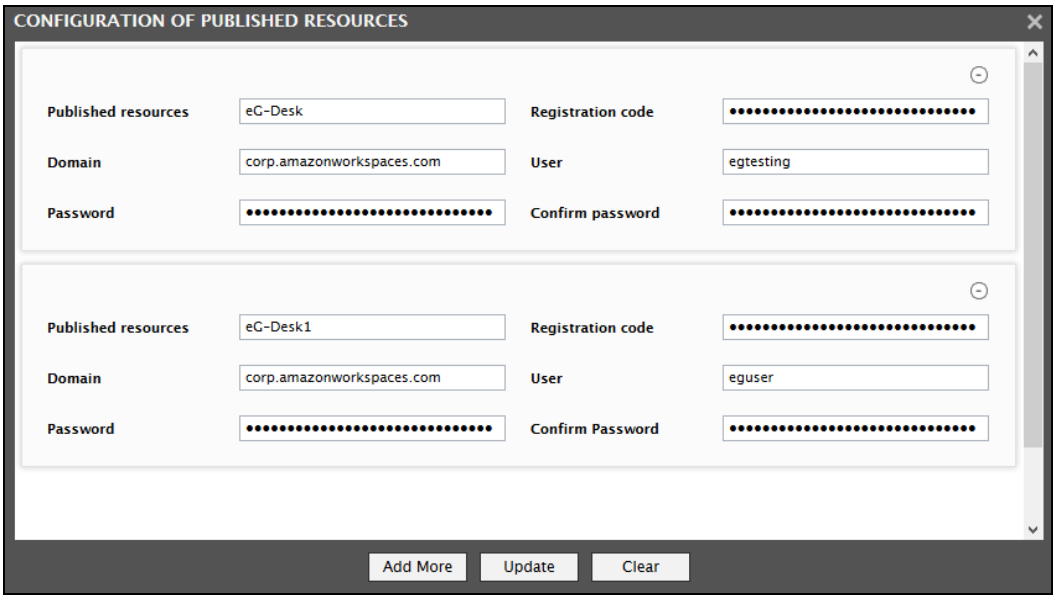

Figure 3.5: Configuring the published resources to be launched

Using Figure 3.5, you can easily configure multiple resources that you want the simulator to launch and also the valid user credentials for accessing each resource. For this, follow the steps below:

1. In the **Published resources** text box, specify the published resource that is to be launched. The resource should be a virtual desktop. When providing the desktop name, make sure you provide the same name using which the desktop on the web console of the virtual private cloud. Also, make sure that the User you specify is authorized to launch the desktop configured in the **Published resources**.

   Note:

   The resources can be specified either in lower case or upper case or a combination of both.

2. Then, using the **Registration code**, **Domain**, **User**, **Password**, and **Confirm Password** parameters, configure the credentials of the user who is authorized to launch the configured resources.
3. Registration code verification, is a security process in which the user provides an authentication to verify who they say they are. By default, the Amazon WorkSpaces is enabled with a registration code authentication. To authenticate the specified User login, the Amazon WorkSpaces client will require an additional layer of security other than the Password you have provided. This is the piece of information that only the User knows or has immediately in hand - such as a registration code that the AWS WorkSpace provides.
4. If you do not want to configure any more resources for launching, then click the Update button to save the changes. To add another resource for launching, click the Add More button. This will add an empty record in the **CONFIGURATION OF PUBLISHED RESOURCES** pop up window. Here, specify the names of more Published resources, and then use the Registration code, Domain, User, Password, and Confirm Password parameters to provide the credentials of a user who is authorized to launch those resources.
5. If you do not want to configure any more resources for launching, then click the **Update** button in Figure 3.5 to save the changes. To add another resource for launching, click the **Add More** button. This will add an empty record to Figure 3.5. Here, specify the names of more **Published resource**s, and then use the **Domain**, **User**, **Password**, and **Confirm Password** parameters to provide the credentials of a user who is authorized to launch those resources.
6. At any given point in time, you can exclude/delete a resource from the simulation by clicking the button corresponding to that resource in Figure 3.5.
7. You can also clear all the configured resources and their launch details at one shot, by clicking the **Clear** button in Figure 3.5.

3.2 Simulator Dashboard

Where two/more Amazon WorkSpaces Simulator components are managed, clicking on the *Amazon WorkSpaces Simulator* component-type in the **Components At-A-Glance** section of the Monitor dashboard automatically opens the **Simulator Dashboard**.

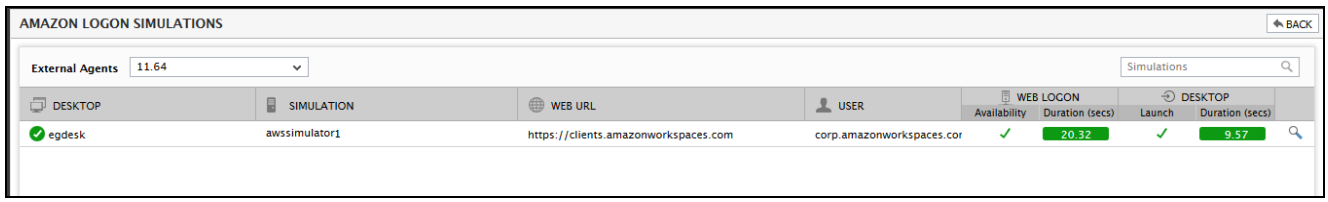

Figure 3.6: The Simulator Dashboard

By default, the dashboard displays all the simulations performed by all the simulators configured in an environment. For each simulation, the dashboard displays the applications accessed and metrics captured by that simulation. This way, the simulations that failed and the precise failure points - whether login, enumeration, application launch, or logoff - of each simulation can be instantly and accurately isolated. You can even click on the 'magnifying glass' icon corresponding to a simulation for a graphical view of the logon process. Using this graphical representation, administrators can clearly identify which step of the logon process has caused slowness.

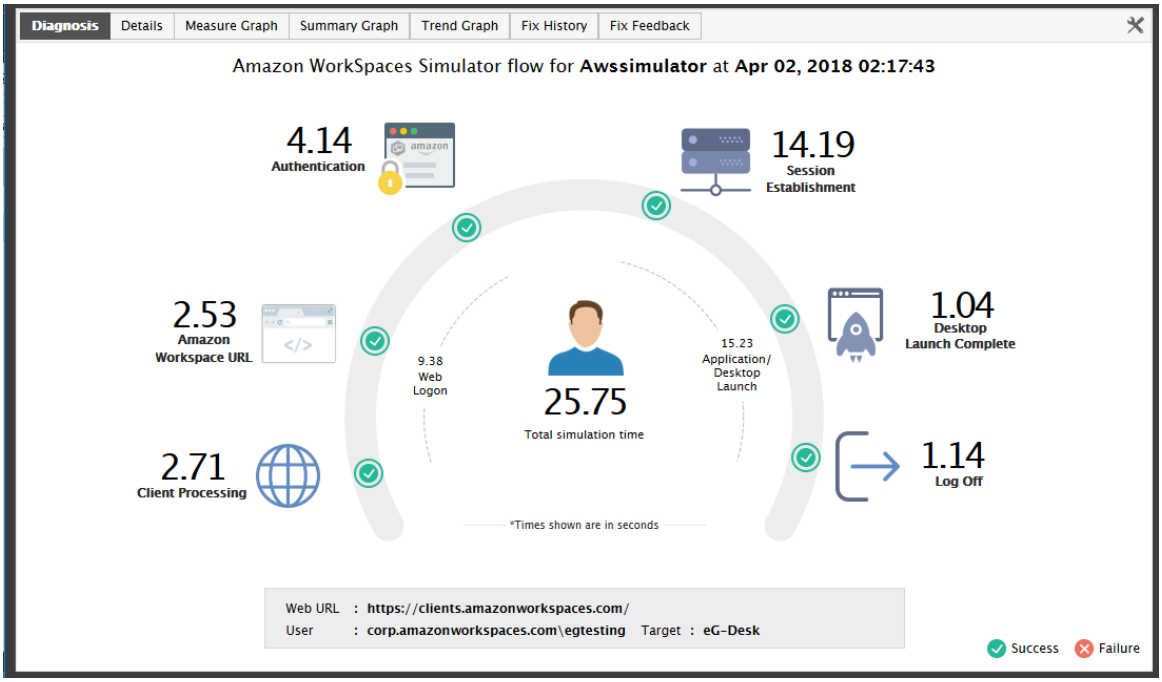

Figure 3.7: A graphical view of the logon process

You can click on the **Details** tab page in Figure 3.7 to view the output of the simulation script, scrutinize it, and isolate the failure and problem points of the Amazon WorkSpaces infrastructure (see Figure 3.8).

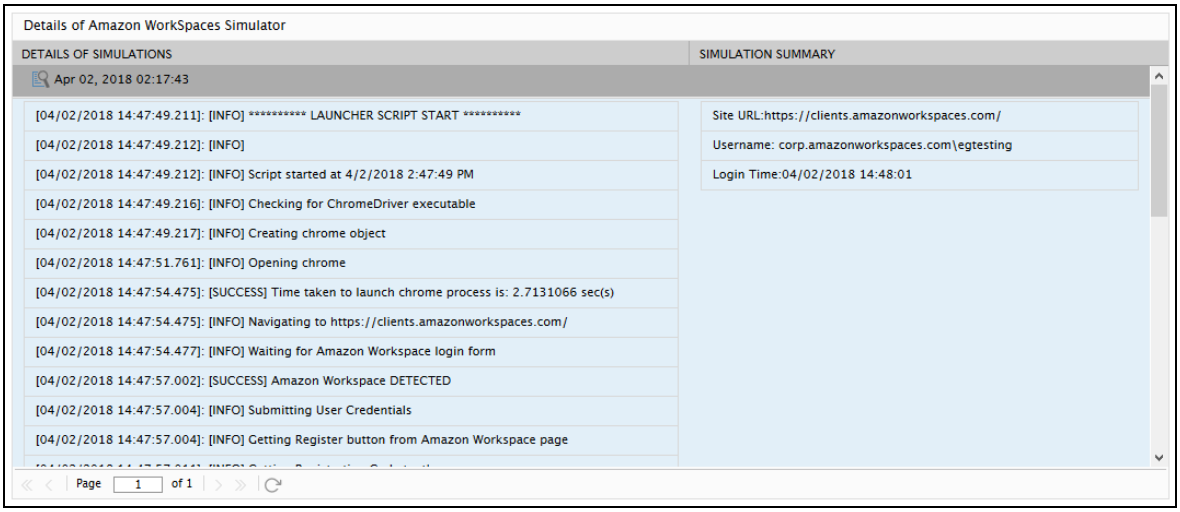

Figure 3.8: The simulation script highlighting the success and failure points of the simulation

You can even filter the details displayed in the dashboard by picking the simulator for which you want to view the details. This can be achieved by picking a particular external agent from the **External Agents** drop-down.

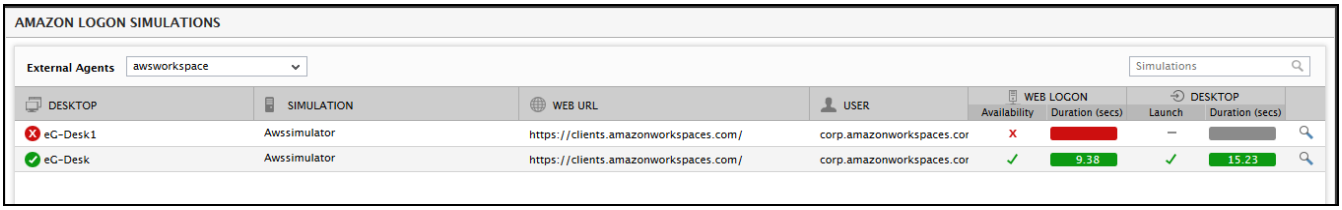

Figure 3.9: Viewing the details of a particular simulator alone

Alternatively, you can filter the dashboard contents on the basis of the *Amazon WorkSpaces Simulator* component that you managed. You can specify the whole/part of the component name in the **Simulations** search text box (see Figure 3.10) and click the 'magnifying glass' icon alongside. This will display the details of only those components with names that contain the specified search string.

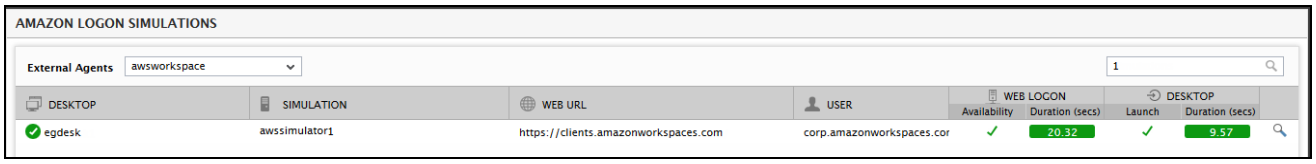

Figure 3.10: Viewing the details of only those simulations that were performed using Amazon WorkSpaces Simulator components that match the specified search string

Clicking on any simulation in the dashboard will lead you to the **Layers** tab page, where you can view the metrics reported by the simulation and the current state of each metric.

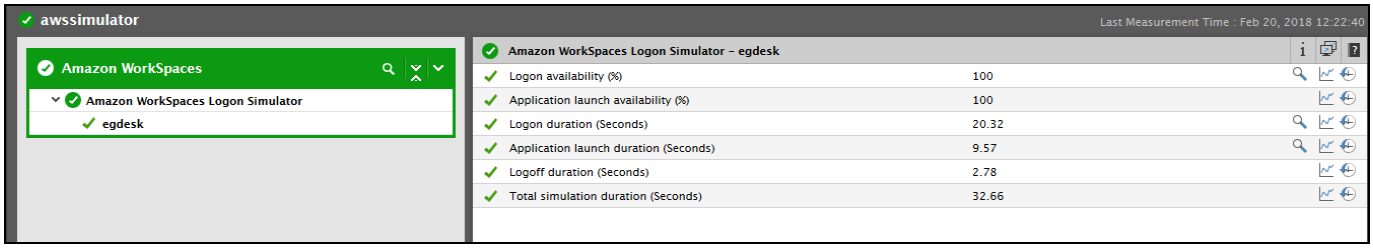

Figure 3.11: The layer model of the Amazon WorkSpaces Simulator component that was clicked on

Chapter 4: Fine-tuning the Simulation

One of the key pre-requisites for the simulation is a user account with local administrator rights on the simulation endpoint. This user should also be logged in at all times for the simulator to run continuously. Sometimes however, this user session may get disconnected. For instance, if the simulation endpoint is rebooted due to automatic updates, scheduled reboots, power failure etc., the user session on the simulation endpoint may get disconnected.

Every time a session disconnect occurs owing to reasons cited above, the administrator will have to login to the endpoint by manually providing the user credentials at the login prompt, while the system boots. If this is not done, then the user session will not get up and running; consequently, the simulation will not occur.

To save the time and effort involved in manually typing the login credentials everytime the endpoint reboots, and to make sure that a user is always logged into the endpoint (even when it reboots) for the purpose of the simulation, you can automate a user login at the time of a reboot. To achieve this, you can either run *Autologon.exe* or manually *edit the windows registry*.

4.1 Fine-tuning the simulation using Autologon.exe

If you wish to automate the user logon by executing Autologon.exe, follow the steps below:

1. Download the **Autologon.zip** file from the **Download Autologon** link from the following location:

   https://docs.microsoft.com/en-us/sysinternals/downloads/autologon

2. Extract the contents of the **Autologon.zip** file.
3. Once extracted, run the **Autologon.exe** file.

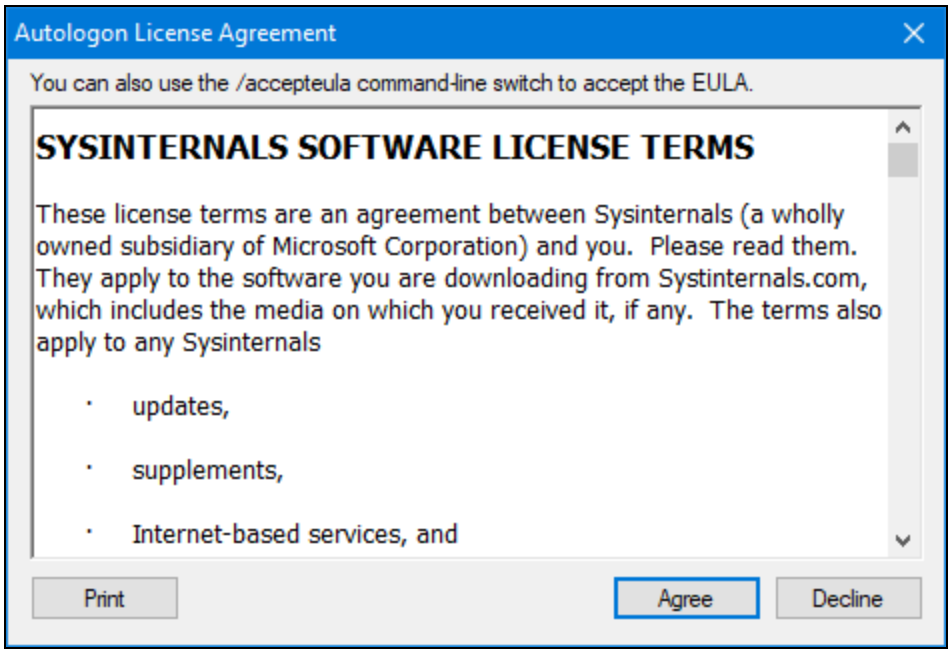

Figure 4.1: Agreeing to the Software License Terms

4. Figure 4.1 then appears. Click **Agree** to accept the Sysinternals Software License Terms.

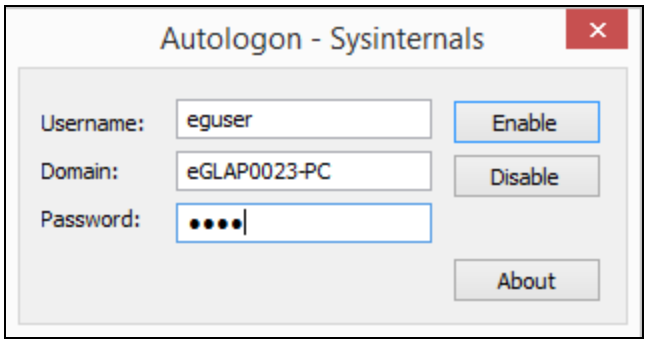

Figure 4.2: Provide the password in this form

5. In Figure 4.2 that appears next, the name of the user and the domain to which the user belongs will be automatically populated against the **Username** and **Domain** fields. Specify the password that should be used for automatic user logon against the **Password** text box.
6. Click the **Enable** button.
7. Ensure that the **eGurkhaAgentServices** are delayed for a period of 5 minutes (using Automatic (Delayed Start) Service properties) before restarting the simulation endpoint.
8. Finally, restart the simulation endpoint.

4.2 Fine-tuning the simulation by editing the windows registry

If you wish to automate the user login by editing the windows registry, follow the steps below:

1. Open the Windows Registry Editor.
2. Locate the following registry entry:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon
3. In this registry entry, add the following REG_SZ string values:
   - **AutoAdminLogon:** To enable automatic user logon on the simulation endpoint, set this string value to 1.
   - **DefaultUserName:** Specify the name of the user who is authorized to login into the simulation endpoint.
   - **DefaultPassword:** Specify the password for the user mentioned in the DefaultUserName. **Note that the password should be entered in plain text.**
   - **DefaultDomainName:** Specify the domain to which the user belongs to.
4. Ensure that the **eGurkhaAgentServices** are delayed for a period of 5 minutes (using Automatic (Delayed Start) Service properties) before restarting the simulation endpoint.
5. Finally, restart the simulation endpoint.

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

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.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.