**Goliath Application Availability Monitor Prerequisites**

This article was updated to support v12.0.1 of Goliath Application Availability Monitor.

**Goliath Server**

**Please disregard this section if this will be integrated into Goliath Performance Monitor.**

* Virtual Machine or Physical Server
* Windows Server 2012 R2 – 2022 64bit
  + Windows installation English OS required w/o any language packs installed
* Minimum of 4 vCPU
* Minimum of 8 GB RAM
* Minimum of 25 GB Disk Available

**Database**

**Please disregard this section if this will be integrated into Goliath Performance Monitor**

* Microsoft SQL Server 2014 – 2022
  + Microsoft SQL Express 2017 is the embedded database option packaged with the product
* SQL Server Sizing Recommendations:
  + 4 vCPU
  + 8 GB RAM
  + # of TempDB's: 4
* Windows Service Account with DBO rights to our database is required for Remote SQL Server
  + This account must also be a Windows admin on the Goliath Server

**Launch Endpoint**

**General Requirements**

* Virtual Machine or Physical Server
* Windows Server 2012 R2 – 2022 64 bit, Windows 8-10
  + English version of Windows required
* Minimum of 2 vCPU
* Minimum of 2 GB RAM
* User Account Control disabled at the System level, not through Control Panel
* **Required Trusted Websites**: If using Google Chrome with GAAM, add the following to trusted sites
  + https://apis.google.com
  + https://www.googletagmanager.com
* **Windows Account**: Dedicated Windows Admin account that must be logged in or disconnected to the endpoint at all times.
  + This can be the same as the platform account mentioned in the next section
* **Screenshot Feature**: In order for the technology to capture screenshots, an active console session must be open.
* **Maintenance**: Reboot schedule suggested; frequency depends on launch schedule

**Platform Specific Requirements**

**Citrix Virtual Apps & Desktops**

* Citrix Receiver version 4.12 and newer
* Dedicated Citrix test account with rights to applications or desktops to be launched
* Google Chrome installed on the GAAM Endpoint
* Powershell version 5.0 or newer on the GAAM Endpoint

**VMware Horizon**

* VMware Horizon Client version 5.X and 8.X supported
* Dedicated VMware Horizon test account with rights to applications or desktops to be launched

**Microsoft RDS**

* Dedicated Microsoft RDS test account with rights to applications or desktops to be launched
* Google Chrome installed on the GAAM Endpoint
* Powershell version 5.0 or newer on the GAAM Endpoint

**Cerner Patient Portal**

* Dedicated Cerner Patient Portal test account with rights at least one Allergy assigned
* Google Chrome installed on the GAAM Endpoint
* Powershell version 5.0 or newer on the GAAM Endpoint

**Firewall**

* *Goliath Server*
  + HTTPS 443/TCP 47629 opened inbound and outbound for web console connection
  + HTTPS 443 opened inbound for agent connection to agent location
  + TCP 135, 445, 49164 open outbound for remote agent installation via web console
* *Goliath Intelligent Agent*
  + HTTPS 443 opened outbound for agent connection to the Goliath Server
  + TCP 135, 445, 49164 open inbound for remote agent installation via web console

**Antivirus and Monitoring Solution Exclusions/Filters**

While not a-typical, we have been exposed to client environments which require antivirus filtering, or exclusion rules needing implemented due to the antivirus software conflicting with the Goliath Intelligent Agent. For that reasoning, we do recommend implementing exclusion rules which consist of the following. **Please Note**: Directory level exclusions are required on the Goliath Server due to the fact that some files are created dynamically in the Goliath application directories.

* **Main Goliath Server** 
  + Directory Exclusions:
    - \Program Files\MonitorIT\\*\* – This is the install directory of the Goliath Server, the local Agent, and relevant files (please include all subfolders/files)
    - Ensure recursive exclusions for the subfolders is allowed
  + Process Exclusions:
    - RPMAgent.exe – This is the process which is launched by the Agent’s Service
    - RPMCCS.exe – This is the process which is launched by the Server’s Service
    - AgentService.exe – Process supporting the Agent’s Windows Service
    - RestartService.exe – Process supporting the Agent’s Windows Service
    - MonitorITService.exe - Process supporting the Goliath Server’s Windows Service
    - Stunnel.exe – (Optional component) Used to support sending alerts and notifications via SSL/TLS enabled mail servers
    - LogonSimulator.exe - (Optional Component) Used if GAAM is running locally
* **Launch Endpoints**
  + Directory Exclusions:
    - Path “\Program Files\MonitorIT”
    - Ensure recursive exclusions for the subfolders is allowed
  + Process Exclusions:
    - RPMAgent.exe – This is the process which is launched by the Agent’s Service
    - AgentService.exe – Process supporting the Agent’s Windows Service
    - RestartService.exe – Process supporting the Agent’s Windows Service
    - LogonSimulator.exe - used for launching GAAM

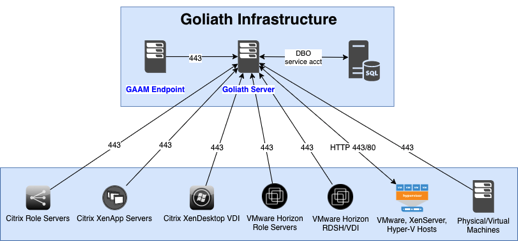
**Supported Browsers**

For the best experience accessing the Goliath web console, we recommend using the latest version of your preferred browser from the list of supported browsers below.

* Chrome v63 and later
* Firefox v50 and later

**Deployment Architecture**

**Goliath Performance Monitor w/ Application Availability Monitor**



**Goliath Application Availability Monitor**

