Goliath Application Availability Monitor for Microsoft RDS Prerequisites Guide

Goliath Application Availability Monitor Proof of Concept Limitations

Goliath Application Availability Monitor Proof of Concepts (POC) will be limited to launching a single Microsoft RDS application or desktop from one location.

If your evaluation or POC process requires a different configuration than the licensing allows for, please contact your account manager or Goliath Sales or Support as follows for assistance:

Sales
Email: sales@goliathtechnologies.com
Phone: 1-855-465-4284

Support
Email: support@goliathtechnologies.com
Phone: 1-855-465-4282

http://www.goliathtechnologies.com

Legal Notices

Goliath Technologies believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." GOLIATH TECHNOLOGIES MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any Goliath Technologies software described in this publication requires an applicable software license.

Linux is a registered trademark of Linus Torvalds.

Windows is a registered trademark of Microsoft Corporation.

VMware, ESX, ESXi, vCenter, and vSphere are either trademarks or registered trademarks of VMware Corporation.

Citrix, Xen, XenServer, and XenCenter are either trademarks or registered trademarks of Citrix Systems Inc.

All other trademarks and copyrights referred to are the property of their respective owners.

Support, Sales, Renewals and Licensing

- For information on new sales, licensing and support renewals you can email sales@goliathtechnologies.com
- For additional information about Goliath Technologies products and services, go to http://www.goliathtechnologies.com
- For customers and partners with an active support agreement, you can use the support web board or email support@goliathtechnologies.com for information about software patches, technical documentation, and support programs.

Note: A valid support agreement is necessary to receive new release and software updates.

Table of Contents

Goliath Application Availability Monitor for Microsoft RDS Prerequisites

Note: On the Goliath Server, if it is running **Windows Server 2012-2016**, .NET 3.5 needs to be installed from the Features Wizard as .NET 4.5 is not backwards compatible. Goliath can be accessed over the network or WAN to your local computer.

International users: For installations in environments requiring foreign language versions of Windows, Goliath requires that the base installation be performed with the English version of Windows OS. Localization should be done using language packs only, no localized Windows OS install.

Table 1 - Goliath Application Availability Monitor for Microsoft RDS System Requirements

Component	Requirement
Goliath Server (please disregard if also using Goliath Performance Monitor)	☐ Virtual Machine or Physical Server ☐ Windows Server 2008 R2 – 2016 64 bit ☐ .NET 3.5 Framework ☐ Static IP address ☐ Minimum of 4 vCPU ☐ Minimum of 8 GB RAM ☐ Minimum of 25 GB Disk Available ☐ **Dependencies**: ○ PowerShell 3.0 ○ Internet Explorer 11
Launch Endpoint	☐ **OS**: Windows Server 2008 R2 – 2016 64 bit, Windows 7-10 ☐ **Resources**: Minimum of 2vCPU and 2 GB RAM ☐ **Dependency**: Goliath Agent deployed ☐ **Web Browser**: Internet Explorer 11 ☐ **User Account Control**: Disabled at the System level, not through Control Panel ☐ **IE Enhanced Security**: Disabled for Administrators and Users ☐ **Trusted Sites**: Add Microsoft RDS Portal to whitelist for trusted sites and the security zone set to “Low” to bypass file downloads ☐ **Microsoft RDS Test Account**: Dedicated Microsoft RDS test account with rights to applications or desktops to be launched ☐ **Windows Account**: Dedicated account that must be logged in/disconnected to the endpoint at all times. This can be the same as the Microsoft RDS account, especially if you’re automating logons using integrated Windows authentication.
Firewall	*Goliath Server* ☐ HTTPS 443/TCP 80* opened inbound and outbound for web console connection ☐ TCP 8282* opened inbound for agent connection to agent location *Goliath Intelligent Agent* ☐ TCP 8282* opened outbound for agent connection to the Goliath Server * Default ports listed and can be modified.

Goliath Service Accounts

Infrastructure Component	Rights	Notes
Launch Endpoint	Local Admin Rights	This can be a local account or a domain account
Remote SQL (for Goliath DB)*	DBO	Needs to be applied to the Goliath Database.
Goliath Server*	Local Admin Rights	The account that has DBO rights to the Goliath database will also need local admin rights on the Goliath server.
Microsoft RDS Launch Account	Access to apps and desktops	Needs rights to launch the applications and desktops

*only needed for Application Availability Monitor Standalone (not integrated with Goliath Performance Monitor) if using an external database

Goliath Firewall Settings

A. Goliath Intelligent Agent for Launch Endpoint

Source	Destination	TCP Port	Traffic	Notes
Agent Location	Goliath Server	8282	Outbound	Agent connection. Default port listed, port can be modified.

Monitoring Endpoints/Workstations that reside **outside** your network will require the following:

- NAT policy on the firewall to allow agent communication inbound via TCP 8282 (default port, this can be changed)
- Public IP address of the firewall

B. Goliath Application Availability Monitor Server

Source	Destination	TCP Port	Traffic	Notes
(Anywhere)	Goliath Server	8282	Inbound	Agent connection. Default port listed, port can be modified.
(Anywhere)	Goliath Server	80	Inbound	Web console connection. Default port listed, port can be modified.
Goliath Server	(Anywhere)	80	Outbound	Web console connection. Default port listed, port can be modified.

Goliath Antivirus 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:

- Directory Exclusions:
  - \Program Files\MonitorIT – This is the install directory of the agent
  - \Program Files (x86)\MonitorIT – This is the install directory of the Goliath Server
- 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
  - LogonSimulator.exe – This is the process which is launching the Application Availability Monitor