Monitoring Radius Servers

eG Enterprise v6

Restricted Rights Legend

The information contained in this document is confidential and subject to change without notice. No part of this document may be reproduced or disclosed to others without the prior permission of eG Innovations Inc. eG Innovations Inc. makes no warranty of any kind with regard to the software and documentation, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Trademarks

Microsoft Windows, Windows NT, Windows 2000, Windows 2003 and Windows 2008 are either registered trademarks or trademarks of Microsoft Corporation in United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Copyright

Table of Contents

Table of Figures

Monitoring Radius Servers

Remote Authentication Dial In User Service (RADIUS) is an AAA (authentication, authorization, and accounting) protocol for controlling access to network resources. RADIUS servers and clients are commonly used by ISPs and corporations managing access to the internet or internal networks across an array of access technologies, including modems, DSL, wireless and VPNs.

In an era where corporates and end-users alike have come to look upon the Internet as a reliable medium for transacting business, ISPs have begun to depend a lot on the RADIUS server to ensure that such transactions are safe and secure. This only means that even a brief non-availability of the RADIUS server, or a slowdown in authentication experienced by the server, can expose the infrastructure and the business to untold harm. If such an adversity is to be prevented, then the RADIUS server has to be continuously monitored.

eG Enterprise presents a specialized *Radius* monitoring model (see Figure 1.1) that periodically checks the availability and responsiveness of the Radius server.
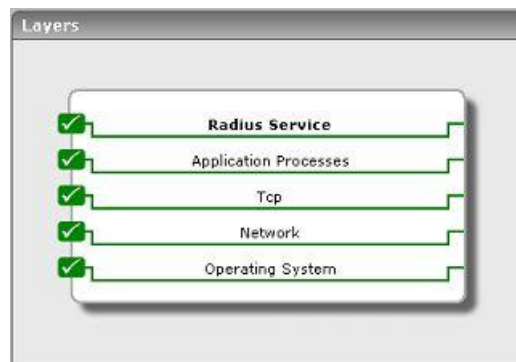

Figure 1.1: The layer model of a Radius server

Since the the bottom 4 layers of Figure 1.1 have already been discussed in ample measure in the *Monitoring Unix and Windows Servers* document, the section to come will discuss the topmost layer of Figure 1.1 alone.

1.1 The Radius Service Layer

This layer monitors the availability and responsiveness of the Radius server.

Figure 1.2: The test associated with the Radius Service layer

1.1.1 RadiusService Test

Purpose	Reports the availability and responsiveness of the Radius server
Target of the test	A Radius server
Agent deploying the test	An external agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **Host** - The host for which the test is to be configured 3. **port** - The port at which the specified **host** listens 4. **acctport** - The account port used by the Radius server 5. **authtype** - The type of authentication used by the Radius server for authenticating clients. Here, specify **PAP** if the type of authentication used by the Radius server is **Password Authentication Protocol**. If the authentication used is **Challenge Handshake Authentication Protocol**, then enter **CHAP** here. 6. **username** - For logging into the Radius server, the test requires a valid **USERNAME**. Specify the user name in the space provided. 7. **password** - The **PASSWORD** of the specified **USERNAME** 8. **confirmpassword** – Confirm the password by retyping it. 9. **sharedsecret** – The shared secret of the Radius server 10. **timeout** - The maximum duration (in seconds) for which the test will wait for a response from the server

Outputs of the test	One set of results for every Radius server being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Login status: Indicates whether the Radius server is available or not.	Percent	If the value of this measure is 100%, it indicates that the server is available. If the value of this measure is 0, then it means that the server is not available.
	Login time: The time taken by the Radius Sever to authenticate Radius clients using the configured protocol (PAP / CHAP).	Secs	

Chapter

2

Conclusion

This document has described in detail the monitoring paradigm used and the measurement capabilities of the eG Enterprise suite of products with respect to **Radius servers**. For details of how to administer and use the eG Enterprise suite of products, refer to the user manuals.

We will be adding new measurement capabilities into the future versions of the eG Enterprise suite. If you can identify new capabilities that you would like us to incorporate in the eG Enterprise suite of products, please contact support@eginnovations.com. We look forward to your support and cooperation. Any feedback regarding this manual or any other aspects of the eG Enterprise suite can be forwarded to feedback@eginnovations.com.