

Secure communication between a monitoring host Web service and monitored Web services

Skill Level: Intermediate

[Judith M. Myerson \(jmyerson@bellatlantic.net\)](mailto:jmyerson@bellatlantic.net)
System engineer and architect

15 Apr 2009

Should we have a Web service as a dedicated security monitoring host? Or should we have several Web services that work together as the distributed security monitoring host? In this article we look at the pros and cons of each host type and suggests how each can be used to solve security problems.

Introduction

In my article, "Dedicated vs distributed security monitoring Web service host," I suggest a monitoring plan to help decide whether we should have a dedicated or distributed security monitoring Web service. I reviewed the pros and cons of each alternative and suggested how each can be used to solve security problems. I also mentioned that for the first monitoring host type, secure communication is needed to transfer or access data from one Intranet to another, from one Intranet to a closed network or from one closed network to another.

In this article, I will discuss how to ensure the communication between a monitoring host Web service and monitored Web services are secure. I compare secure communication in Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6), which are Internet Protocol internetnetwork-layer protocols. I will provide a remote data center scenario on the merits of establishing secure communication between monitoring and monitored Web services in IPv6-based workstations and eventually in a global grid. I look at what we need to do when communicating with one another that's lags; resulting in security compromises, exploitation of vulnerabilities, resource waste, and even system crash. Finally, I provide some examples for overcoming these problems.

Monitor Web services

You can have more than one monitoring Web services to act as multiple hosts for monitored Web services. A lead monitoring host Web service can start at the top level of a hierarchy and have secure communication to another monitoring host service and one more monitored Web services in the lower levels of hierarchy. Designate failover monitoring host and monitored Web services as part of a disaster recovery plan. Always backup your applications and data periodically to avoid unnecessary delay and possible loss of business reputation and revenue.

At the top level, you should configure the lead monitoring Web service host as distributed running in a grid. The lower level monitoring host can be either dedicated or distributed depending on whether it is within an enterprise or in a grid. If the dedicated host is within an enterprise, it can be connected securely to other monitoring services in the grid.

You can configure monitoring Web services at three levels: local, regional and global. Some monitoring Web services run only at the local level; they have no parents. Other local monitoring Web services have parents at the regional and in turn at the global level. In some cases, there may be parent monitoring Web services on a global level, none at the regional level.

Specify requirements

In order for the security communication standards for monitoring and monitored Web services to work, you must specify requirements to accomplish secure communication. Here are some requirements you should include:

Table 1. Minimum requirements

Item	Description
Identification	Identify entities whether they are monitoring and monitored Web services, individuals or facilities.
Authentication	Confirm the credentials of a claimed identity.
Authorization	Ensure monitoring and monitored Web services and users are given permissions to perform the tasks assigned to them and are not given permission to perform the tasks not assigned to them.
Confidentiality	Ensure information is not exposed to unintended or unauthorized parties .
Integrity	Ensure information is not unintentionally or maliciously altered.
Non-repudiation	Ensure monitoring and monitored Web services

cannot deny sending or receiving specific messages.

Exchange credentials

It takes two steps to accomplish secure communication between monitoring and monitored Web services. First, each of the two parties -- monitoring and monitored Web services need to determine if they can trust the asserted security credential of the other by checking if the credential is in the library or by accepting the credential externally. Then the both parties exchange the credentials.

Applications that communicate using Web services can use WS-Trust to obtain and exchange security credentials. It can be done either directly or through a trusted third party--and use WS-SecureConversation to establish and maintain a secure session in which a monitoring Web service and a monitored Web service pass multiple rounds of secured messages.

WS-Trust provides methods for establishing, detecting, and brokering trust relationships. WS-SecureConversation overcomes the restriction of WS-Security to a round of a single secured message between a monitored Web service and a monitoring Web service. Together, WS-Trust and WS-SecureConversation can increase the overall performance and security of exchanges.

Secure with IPv4 or IPv6?

Let's compare secure communication needed to connect between monitoring and monitored Web services using IPv4 and IPv6. First, IPv4-based secure communication in the grid is available only for site-to-site connections between monitoring and monitored Web services. Secure communication is one-way due to Network Address Translation (NAT) problems and client/server business model. Security in LAN segments is low and it can be difficult to accomplish application interoperability between different vendors.

Second, IPv6-based secure communication in the grid is available not only site-to-site communication but also end-to-end connection. Some IPv6's improvements to provide for better network security includes large address space, neighbor discovery and address auto-configuration. IPsec is an integral part of IPv6 while IPv4 support for IPsec is optional.

In contrast to IPv4's one way approach, IPv6 achieves two-way secure communication between appliance and mobile. Not only does it provides a client/server business model, it also works with peer-to-peer and mobility models. IPv6 allows you to easily setup new communication.

Improved security in IPv6 is not necessarily more secure than IPv4, however. Like IPv4, it is subject to attacks when vulnerabilities are successfully exploited. While it is possible to fully migrate IPv4 to IPv6 on the local level, it will take longer for the regions and the world to accomplish full migration to IPv6. Monitoring Web service to switch to IPv6 from IPv4 in the grid depends on how unused resources are harnessed in the workstations participating in the grid.

Avoid performance lags

In addition to secure communication standards, we need to establish a system performance threshold to ensure that secure communication between monitoring and monitored Web services do not lag. If the system falls below the threshold, it will increase the risks of exploiting vulnerabilities, IPv6 migration security issues, and resource waste of secure communication that could impact SLAs and ultimately result in system crash.

When this happens, the monitoring Web service will send an alert to system administrators and security officers for immediate corrective action and move temporarily to a fail-over monitoring Web services. The monitoring Web service alert mechanism is triggered by monitored Web services not meeting the performance criteria at a particular point of time. These monitored Web services will move to fail over Web services temporarily.

Scenario: Remote control for data centers

Let's suppose at an operations center you use secure communication to connect monitoring Web services at the center remotely with monitored Web services at multiple data centers. You can remotely refocus, rotate, get pictures from the camera, reset and get data from the thermometer, receive alerts from thermometer when outside temperature drastically changes and adjust the speed of fans.

You need a monitoring Web service to track how well IPv6 is performing in remotely controlling multiple data centers and whether one data center is performing better than others. You need to establish system performance threshold both at the operations center and multiple data centers. You need to set the threshold at an optimal level that would most likely not to increase the risks of vulnerabilities, IPv6 migration issues and resource waste.

The lead monitoring host compares performances between monitored Web services. You can configure monitoring Web services to send alerts to systems administrators on unusual sensor and performance changes that could impact SLA guarantee on uptime availability even though the changes are at or above the performance threshold.

Conclusion

You need a team of developers, testers, and system administrators to establish secure communication between Web services. You must plan ahead on which Web services will be the monitoring hosts and which ones are to be monitored, specify what the requirements are and how credentials are to be exchanged. You must also determine how IPv6 security can be improved as shown in the scenario. Resolving these issues makes your job of monitoring Web services with secure communication a lot easier. You can use IBM Rational® ClearQuest, Quality, IBM Rational Functional Tester, and WebSphere® MQ Low Latency Messaging to increase productivity by reducing testing and defect tracking time at the grid level.

Resources

Learn

- Explore the [OASIS Consortium](#).
- See all of [Judith M. Myerson's](#) content, offering information on how to work with Web services in enterprise-wide SOAs.
- Read "[Dedicated versus distributed security monitoring as a Web services host in an SOA](#)" (developerWorks, Oct 2008).
- Check out Judith M. Myerson's developerWorks series, [Use SLAs in a Web services context](#), for details on service-level agreement.
- Read "[Tight coupling Web services in the SOA](#)" (developerWorks, Jan 2008).
- Read more about the use of [WS-SecureConversation v1.3](#) and [WS-Trust v1.3](#) as [OASIS standards](#)
- Get details about:
[IBM Rational ClearQuest](#)
[IBM Rational Functional Tester](#)
[IBM Webspheres MQ Low Latency Messaging IBM Rational Tester for SOA Quality](#)
- Read Judith M. Myerson's [The Complete Book of Middleware](#), which focuses on the essential principles and priorities of system design and emphasizes the new requirements brought forward by the rise of e-commerce and distributed integrated systems.
- Get the business insight and the technical know-how to ensure successful systems integration by reading [Enterprise Systems Integration, Second Edition](#).
- Bring your organization into the future with [RFID in the Supply Chain](#), which explains business processes, operational and implementation problems, risks, vulnerabilities, and security and privacy.
- IBM Redbooks: Read [Tivoli Manager for Domino V2.1 Fulfilling Service Level Agreements Using Tivoli Technology](#), for IBM Lotus Domino administrators, which goes into the nuts and bolts of developing a service-level agreement.
- The [IBM SOA Web site](#) offers an overview of SOA and how IBM can help you get there.
- Play in the [IBM SOA Sandbox!](#) Increase your SOA skills through practical, hands-on experience with the IBM SOA entry points.
- The [IBM SOA Web site](#) offers an overview of SOA and how IBM can help you get there.

- Stay current with [developerWorks technical events and webcasts](#).
- Visit the [Safari bookstore](#) for books on these and other technical topics.
- Check out a quick [Web services on demand demo](#).

Get products and technologies

- Download a [trial version of Rational ClearQuest](#).
- Download a [trial version of Rational Functional Tester](#).
- Download a [trial version of Rational Tester for SOA Quality](#).
- Download a [trial version of Websphere MQ Low Latency Messaging](#)
- Innovate your next development project with [IBM trial software](#), available for download or on DVD.

Discuss

- [Participate in the discussion forum for this content](#).
- [Participate in the discussion forum](#).
- Collaborate with others who are interested in SOA in the federal sector in the [Federal SOA Institute - SOA Certification Mentoring](#) discussion forum.
- Get involved in the developerWorks community by participating in [developerWorks blogs](#), including the following SOA and Web services-related blogs:
 - [Service Oriented Architecture -- Off the Record](#) with Sandy Carter
 - [Best Practices in Service-Oriented Architecture](#) with Ali Arsanjani
 - [WebSphere SOA and J2EE in Practice](#) with Bobby Woolf
 - [Building SOA applications with patterns](#) with Dr. Eoin Lane
 - [Client Insights, Concerns and Perspectives on SOA](#) with Kerrie Holley
 - [Service-Oriented Architecture and Business-Level Tooling](#) with Simon Johnston
 - [SOA, ESB and Beyond](#) with Sanjay Bose

About the author

Judith M. Myerson

Judith M. Myerson is a systems architect and engineer. Her areas of interest include middleware technologies, enterprise-wide systems, database technologies, application development, network management, security, RFID technologies, and project management.