SECURE WEB SERVICES:

Opening Up the NonStop Server while Keeping It Safe!

Andrew Price DirectorSales & Business Operations, APJ, NuWave Technologies

Web services, using SOAP initially, and more recently REST, have become immensely popular methods to allow disparate applications and platforms to communicate, and this communication allows you and your customers to do exciting things, like connect to IoT devices and access backend applications from mobile devices. The API directory website **www.programmableweb.com** now tracks over 19,000 web-based APIs, the vast majority of which are now REST-based. In the NonStop space, we've been able to utilize middleware based on these technologies since the early 1990s, and they are now the preferred method to integrate NonStop applications and data with other platforms and applications, both within the enterprise, and externally. Today, solutions from vendors such as NuWave, HPE, ACI, and Comforte have been widely deployed to help simplify access to NonStop applications and the valuable data that they contain, as well as to access public and private Web services from NonStop applications.

Of course, while "opening up" the NonStop environment has some significant benefits, it needs to be carefully planned and executed to avoid the risk of allowing unauthorized access to those valuable applications and data. In the past, the NonStop Server often benefited from "security through obscurity", the fact that most hackers didn't know enough about the NonStop environment to be able to successfully access it and its data. Web services are generally well-understood, and hence this "default" security is generally not enough, if indeed it ever was!

In addition to selecting the appropriate middleware solution for your environment (Do you prefer to work in Guardian or OSS? Is there a specific need for either REST or SOAP?) to open up NonStop applications as Web services, the following items should be considered as part of a secure Web services strategy:

- Network isolation
- Protection of sensitive data in transit and at rest
- Authentication
- Authorization
- Access control
- Auditing

This article will elaborate on each of these areas of security, with a goal of assisting those interested in deploying secure REST services. Not all of these security points will be required in every instance, but all should be considered. Specific organizations may have additional requirements that should be discussed with the organization's security team.

Network Isolation

Network isolation typically involves using an HTTP proxy, or similar, to create a firewall. In most environments, the NonStop Server will already be protected by a firewall, however consideration will need to be given to the new Web services and their impact on the firewall. Do new ports need to be opened? Should additional examination of the Web service payload be considered? These issues should be discussed with the networking team.

Protection of Sensitive Data

In most cases, the new Web services will likely be carrying some sort of sensitive data, be it card holder data (CHD), health care information, or other types of personally identifiable information (PII). This data will now be carried over an HTTP connection and could potentially be picked up by a user with access to a network trace facility, either inside the enterprise, or even externally. This data needs to be protected using SSL/TLS. TLS 1.1 is now required by PCI DSS, with strong encouragement from the PCI security council to move to TLS 1.2. TLS 1.3 has just been finalized (as of Aug 2018) and should be kept in mind for future deployments. NonStop SSL can be deployed to address this need, or the Web service middleware vendor may have SSL built-in to provide end-to-end encryption of Web service traffic.

Sensitive data should also be considered when it is written to disk. PCI DSS req 3.4 requires that any PAN data be rendered unreadable when stored on disk. Many middleware solutions, including those from NuWave, allow sensitive data to be masked. Alternatively, this requirement may be met using an encryption or tokenization solution from companies such as MicroFocus or Comforte.

Authentication

At its simplest, the process of authentication is validating that a user is who they say they are. In the case of Web services, authentication is the first step in determining whether access should be allowed to a particular service. Authentication can be achieved in a variety of ways, including with certificates or tokens, but in most cases the tried and true method of username and password is often sufficient. Some middleware solutions will support HTTP Basic and Digest Authentication to allow username and password to be safely carried and used for authentication.

Authorization

Once the user is authenticated, the next important step is to determine whether they should be allowed to access the specific service they're trying to invoke. In the case of Web services, the resource they are accessing is the API or the service. The Web service middleware solution needs to be able to link the authenticated user to the service being accessed to determine if access should be allowed.

Access Control

The previous steps outlined will not be a lot of use if the management or administrative environment used by the Web service middleware is not itself secured. Without adequate Access Control in place rogue users could reconfigure the solution allowing unauthorized access to the services. The solution needs to provide Access Control to ensure that only authorized users are allowed access to the administrative environment.

Auditing

Auditing provides a historical record of what actions were performed within the Web service environment, and by whom. This record is important if ever a breach occurs, but it can also be used proactively by security incident event management (SIEM) solutions like Microfocus ArcSight and RSA Secure Analytics. These solutions piece together security information from across the enterprise to determine if a security incident might be occurring. The middleware solution should support auditing of both the administrative and run-time (i.e APIs and REST services) environments.

The LightWave product set from NuWave addresses all applicable requirements listed in this article. SSL/TLS is fully supported, to ensure data is protected over the wire. HTTP Authentication can be used in both Server and Client mode. Authorization is supported based on a number of different criteria, including user, group and client IP address. The administrative console used by LightWave products allows users to be configured with access to the console, ensuring that only authorized personnel access this critical environment. And finally, the next version of the products, due out by the end of 2018, will have comprehensive auditing support included, allowing auditing of both the Web services operations being invoked, and also the administrative functions being performed through the console.

Web services are a powerful tool for integrating the NonStop Server with other parts of the enterprise, and with external customers, partners, and services, boosting the value of our NonStop platform and its applications. With a carefully considered approach to security, you can ensure that your organization gets all the benefits of those Web services without risking its valuable data.

Andrew Price has over 28 years of experience in the NonStop space. After working at Insession and ACI in numerous positions, including Director of Solutions Consulting and Sales Support, he moved on to XYPRO, where he was initially Director of Product Management and then VP Technology. Today, he is Director of Sales and Business Operations in Asia Pacific for NuWave; focusing on sales, business development, and first-level support in the region.