NMSaaS

Guide to Security – Authentication, Authorization and Encryption in NMSaaS and the Amazon AWS Service

v2.03 NMSaaS - 2012

1 Scope

This document covers all aspects of NMSaaS related to application and data security. It covers

- Authentication
- Authorization
- Encryption
- Amazon AWS Platform Security

1. In all of NMSaaS's components:
2. Graphical User Interface (GUI)
3. Web Interface and Reporting
4. Database
5. NMSaaS® Agent

As NMSaaS® is a distributed Hybrid-Cloud system there are various places where security is of concern. The default encryption used if not otherwise stated is AES with a key length of 128 bit. The AES variant used is AES CBC mode with IV. This block cipher mode with initialization vectors is the most secure variant.

2 Authentication

The NMSaaS® Cloud Server is based on JBoss 4.0.5 and uses the standard JAAS (Java Authentication and Authorization Service) to securely identify a user. When a client connects to the NMSaaS® Cloud Server, no matter which way, a username and a password must be submitted in order to verify a user's identity.

2.1 Towards NMSaaS® Server

The NMSaaS® Cloud Server, also called the middleware, is the central component in NMSaaS®. It includes a user database where every NMSaaS® user must be registered, first. The initial configuration is done with a default administrative user. In order to work with NMSaaS, every user must connect to and log in to the server. Therefor a user name and a non-empty password will be be provided by NMSaaS for each customer.

2.1.1 Password Transmission

There are several ways for a user to authenticate to the server:

- When logging in from NMSaaS® GUI, the password sent to the server is encrypted.
- When logging in to the NMSaaS® web interface via HTTP the password is sent in clear text format
- When logging in to the NMSaaS® web interface via HTTPS the password is sent encrypted

2.1.2 Local Authentication

Authentication is performed directly by the NMSaaS® cloud server. The password provided by the client is compared to the password stored in the user database. If the passwords match, the user is granted access.

2.2 User Access in Reporting

All data in NMSaaS is protected and not available without logging in to the server. In order to build custom interfaces, like umbrella web interfaces, charts and statistics and various other data need to be accessed. This is implemented via URL, passing required data to the server. Besides functional data, a user name and a password must be contained in the URL, which is used to log in to the server. This password is different from the user's normal password and will only work for the access to the web resources.

2.3 Authentication towards NMSaaS Agent

Access to the NMSaaS (onsite) agent is also password protected. The user is usually not going to talk directly to the NMSaaS agent, it is the NMSaaS server who needs to authenticate towards the agent. During installation of the agent, a username and password is defined. These credentials must be provided when the agent is registered to the NMSaaS server. The password check is implemented with a challenge response mechanism, using a variable salt to prevent replay attacks.

3 Authorization

After authentication is successfully finished, NMSaaS® checks what objects the user is allowed to access and which operations can be performed. This is implemented by a role based access control mechanism. There are users which can be assigned to groups and are granted access to elements based on the groups' roles.

Every element in NMSaaS® can be assigned to a set of groups. The elements include

- Measurements
- Device Data
- Reports
- Jobs
- Device Configurations
- Weather Maps

Besides the role based access model, it is possible to hide menu entries in web interface on a per user basis. But this is just a way of user interface customization rather than access control.

4 Encryption

Another important topic when dealing with critical data is encryption. This helps to prevent unauthorized access to secret data. As stated in the introduction above, the standard is AES 128Bit.

4.1 Communication between NMSaaS Server and Agent

The communication between the agent and the cloud server can be completely encrypted using the standard encryption mechanism if there is a danger of exposing secrets. The full encryption is available as a separate license module.

Critical data like passwords and SNMP communities will always be encrypted. They will also be encrypted in the agent's local configuration files.

Another way to protect the communication between agent and server is to set up a VPN tunnel between them.

4.2 Communication between NMSaaS Server and GUI

Once the client is authenticated to the cloud server the security relevant data is encrypted. All traffic is encoded in the Java RMI format. The following Java APIs are used:

- Java RMI – Remote Method Invocation
- JNDI – Java Naming and Directory Interface
- JMS – Java Messaging System

4.3 Encryption in the Web Interface

The web interface can be accessed via HTTP or HTTPs. When accessing via HTTP all data is transferred in clear text format, otherwise everything is encrypted using SSL.
When setting up an encrypted SSL connection one of the first steps is the server's authentication towards the client. NMSaaS ships with a default, self-signed certificate by default.

4.4 Database Access and Storage

All of NMSaaS's data is stored in a single, central relational database. It is accessed using JDBC which does not provide encryption. This means, most of the data will be transferred unencrypted between the server and the database except secrets like passwords and SNMP communities.

4.5 Accessing Network Devices

NMSaaS communicates with network devices permanently for different reasons and in different ways:

- Discovery
- Monitoring
- Configuration and Backup

4.5.1 SNMP

Discovery uses SNMP to query information from the devices. There are different versions of SNMP in use:

1. SNMP v1 deprecated, weak authorization via plain text community string, slow
2. SNMP v2, most common today, similar to SNMP v1 regarding security
3. SNMP v3 supports strong encryption and authentication. The encryption supported in the standard is DES. The authentication is SHA1 or MD5 which can be chosen in NMSaaS®.

NMSaaS® supports all current versions of SNMP. The network discovery must be configured to use the desired version and the network elements must be configured accordingly.

4.5.2 Monitoring

Network monitoring is mostly based on ICMP and SNMP protocol. Like for the discovery, the security and encryption provided is dependent on the chosen SNMP version. This is the case for polling measurements and for the analysis of SNMP traps and notifications.
NMSaaS also supports custom extension of the monitoring capabilities. Custom measurement scripts might use additional protocols and expose data to the network. Please consult the NMSaaS® User Script documentation for more information about this.

4.5.3 Configuration and Backup

NMSaaS® comprises a configuration management engine which is available as a separate license module. In order to communicate with a network device, NMSaaS® sets up a connection to the device. This is done via secure shell (SSH). The use of telnet is discouraged as passwords and data will be exposed in clear text to the network. It can be configured if really needed.

During a session with a device additional traffic might be generated and data might be exposed which NMSaaS® is not responsible for, e.g.:

- The login to a network device might cause network traffic to a central authentication server, if the device is configured to use a central TACACS(+) server.
- Configuration commands issued on the device might trigger additional actions like copying files to or from an FTP server, which are not encrypted

5 **AWS Security and Compliance Center**

Amazon Web Services (AWS) delivers a highly scalable cloud computing platform with high availability and reliability, and the flexibility to enable customers to build a wide range of applications. In order to provide end-to-end security and end-to-end privacy, AWS builds services in accordance with security best practices, provides appropriate security features in those services, and documents how to use those features. In addition, AWS customers must use those features and best practices to architect an appropriately secure application environment. Enabling customers to ensure the confidentiality, integrity, and availability of their data is of the utmost importance to AWS, as is maintaining trust and confidence.

AWS provides a wide range of information regarding its IT control environment to customers through white papers, reports, certifications, and other third-party attestations. This information assists customers in understanding the controls in place relevant to the AWS services they use and how those controls have been validated by independent auditors. This information also assists customers in their efforts to account for and to validate that controls are operating effectively in their extended IT environment.

Overview

At a high level, we’ve taken the following approach to secure the AWS infrastructure:

5.1 Reports, Certifications, and Independent Attestations. AWS has in the past successfully completed multiple SAS70 Type II audits, and now publishes a Service Organization Controls 1 (SOC 1), Type 2 report, published under both the SSAE 16 and the ISAE 3402 professional standards as well as a Service Organization Controls 2 (SOC 2) report. In addition, AWS has achieved ISO 27001 certification, and has been successfully validated as a Level 1 service provider under the Payment

Card Industry (PCI) Data Security Standard (DSS). In the realm of public sector certifications, AWS has received authorization from the U.S. General Services Administration to operate at the FISMA Moderate level, and is also the platform for applications with Authorities to Operate (ATOs) under the Defense Information Assurance Certification and Accreditation Program (DIACAP). We will continue to obtain the appropriate security certifications and conduct audits to demonstrate the security of our infrastructure and services. For more information on risk and compliance activities in the AWS cloud, consult the Amazon Web Services: Risk and Compliance whitepaper.

5.2 Physical Security. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. AWS infrastructure is housed in Amazon-controlled data centers throughout the world. Only those within Amazon who have a legitimate business need to have such information know the actual location of these data centers, and the data centers themselves are secured with a variety of physical controls to prevent unauthorized access.

5.3 Secure Services. Each of the services within the AWS cloud is architected to be secure and contains a number of capabilities that restrict unauthorized access or usage without sacrificing the flexibility that customers demand. For more information about the security capabilities of each service in the AWS cloud, consult the Amazon Web Services: Overview of Security Processes whitepaper.

5.4 Data Privacy. AWS enables users to encrypt their personal or business data within the AWS cloud and publishes backup and redundancy procedures for services so that customers can gain greater understanding of how their data flows throughout AWS. For more information on the data privacy and backup procedures for each service in the AWS cloud, consult the Amazon Web Services: Overview of Security Processes whitepaper referenced above.

The AWS Security Center provides links to technical information, tools, and prescriptive guidance designed to help you build and manage secure applications in the AWS cloud. Our goal is to use this forum to proactively notify developers about security bulletins. Such transparency is the backbone of trust between AWS and our customers.

6 Certifications and Accreditations

6.1 SOC 1/SSAE 16/ISAE 3402

Amazon Web Services now publishes a Service Organization Controls 1 (SOC 1), Type 2 report. The audit for this report is conducted in accordance with the Statement on Standards for Attestation Engagements

No. 16 (SSAE 16) and the International Standards for Assurance Engagements No. 3402 (ISAE 3402) professional standards. This dual-standard report can meet a broad range of auditing requirements for U.S. and international auditing bodies. The SOC 1 report audit attests that AWS' control objectives are appropriately designed and that the individual controls defined to safeguard customer data are operating effectively. Our commitment to the SOC 1 report is on-going and we plan to continue our process of periodic audits. This audit is the replacement of the Statement on Auditing Standards No. 70 (SAS 70) Type II report.

6.2 SOC 2

In addition to the SOC 1 report, AWS publishes a Service Organization Controls 2 (SOC 2), Type 2 report. Similar to the SOC 1 in the evaluation of controls, the SOC 2 report is an attestation report that expands the evaluation of controls to the criteria set forth by the American Institute of Certified Public Accountants (AICPA) Trust Services Principles. These principles define leading practice controls relevant to security, availability, processing integrity, confidentiality, and privacy applicable to service organizations such as AWS. The AWS SOC 2 is an evaluation of the design and operating effectiveness of controls that meet the criteria for the security principle set forth in the AICPA's Trust Services Principles criteria. This report provides additional transparency into AWS security based on a pre-defined industry standard of leading practices and further demonstrates AWS' commitment to protecting customer data.

6.3 FISMA Moderate

AWS enables U.S. government agency customers to achieve and sustain compliance with the Federal Information Security Management Act (FISMA). FISMA requires federal agencies to develop, document, and implement an information security system for its data and infrastructure based on the National Institute of Standards and Technology Special Publication 800-53, Revision 3 standard. FISMA Moderate Authorization and Accreditation requires AWS to implement and operate an extensive set of security configurations and controls. This includes documenting the management, operational, and technical processes used to secure the physical and virtual infrastructure, as well as the third-party audit of the established processes and controls. AWS has received a three-year FISMA Moderate authorization for Infrastructure as a Service from the General Services Administration. AWS has also successfully achieved other ATOs at the FISMA Moderate level by working with government agencies to certify their applications and workloads.

6.4 PCI DSS Level 1

AWS has achieved Level 1 PCI compliance. We have been successfully validated as a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS). Merchants and other service providers can now run their applications on our PCI-compliant technology infrastructure for storing, processing, and transmitting credit card information in the cloud. Other enterprises can also benefit by running their applications on other PCI-compliant technology infrastructure. PCI validated services include Amazon Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3), Amazon Elastic Block Storage (EBS) and Amazon Virtual Private Cloud (VPC), Amazon Relational Database Service (RDS), Amazon Elastic Load Balancing (ELB), Amazon Identity and Access Management (IAM), and the underlying physical infrastructure and the AWS Management Environment.

For more information please visit our PCI DSS Level 1 FAQs.

ISO 27001

AWS has achieved ISO 27001 certification of our Information Security Management System (ISMS) covering our infrastructure, data centers, and services including Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3) and Amazon Virtual Private Cloud (Amazon VPC). ISO 27001/27002 is a widely-adopted global security standard that sets out requirements and best practices for a systematic approach to managing company and customer information that's based on periodic risk assessments. In order to achieve the certification, a company must show it has a systematic and ongoing approach to managing information security risks that affect the confidentiality, integrity, and availability of company and customer information. This certification reinforces Amazon's commitment to providing transparency into our security controls and practices. AWS's ISO 27001 certification includes all AWS data centers in all regions worldwide and AWS has established a formal program to maintain the certification. A copy of our ISO certificate, available to AWS customers, describes the ISMS services and geographic scope.

6.5 International Traffic In Arms Compliance

The AWS GovCloud (US) region supports US International Traffic in Arms Regulations (ITAR) compliance. As a part of managing a comprehensive ITAR compliance program, companies subject to ITAR export regulations must control unintended exports by restricting access to protected data to US Persons and restricting physical location of that data to US land. AWS GovCloud (US) provides an environment physically located in the US and where access by AWS Personnel is limited to US Persons, thereby allowing qualified companies to transmit, process, and store protected articles and data under ITAR. The AWS GovCloud (US) environment has been audited by an independent third party to validate the proper controls are in place to support customer export compliance programs for this requirement.

6.6 FIPS 140-2

The Federal Information Processing Standard (FIPS) Publication 140-2 is a US government security standard that specifies the security requirements for cryptographic modules protecting sensitive information. To support customers with FIPS 140-2 requirements, the Amazon Virtual Private Cloud VPN endpoints and SSL terminations in AWS GovCloud (US) operate using FIPS 140-2 validated hardware. AWS works with AWS GovCloud (US) customers to provide the information they need to help manage compliance when using the AWS GovCloud (US) environment.

6.7 Other Compliance Initiatives

The flexibility and customer control that the AWS platform provides permits the deployment of solutions that meet industry-specific compliance requirements.

6.7.1 HIPAA: Customers have built healthcare applications compliant with HIPAA's Security and Privacy Rules on AWS. AWS provides the security controls customers can use to help to secure electronic health records. Please see the related whitepaper (link below).
CSA:AWS has completed the Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire. This questionnaire published by the CSA provides a way to reference and document what security controls exist in AWS's Infrastructure as a Service offerings. The questionnaire (CAIQ) provides a set of over 140 questions a cloud consumer and cloud auditor may wish to ask of a cloud provider. Customers can find the completed questionnaire in Appendix A of the AWS Risk and Compliance whitepaper
6.7.2 MPAA: The Motion Picture Association of America (MPAA) has established a set of best practices for securely storing, processing and delivering protected media and content. Media companies use these best practices as a way to assess risk and audit their content and infrastructure. AWS commissioned an independent assessment of AWS's compliance with the MPAA best practices and has achieved the highest maturity rating possible, indicating that the AWS infrastructure is compliant with all applicable MPAA infrastructure controls across all the AWS services under review. While the MPAA does not offer a "certification", media companies can use this report to complete their own risk assessment and audit of MPAA-type content on AWS.

7 Background Information

Delivering a secure cloud computing platform involves implementing numerous best practices for on-premise infrastructure as well as a host of additional considerations unique to a hosted infrastructure environment. The *Amazon Web Services: Overview of Security Processes* whitepaper will provide background information and an overview of the AWS philosophy in offering a secure cloud computing platform.

Amazon Web Services Overview of Security Processes whitepaper (pdf)

Security Best Practices (pdf)

Creating HIPAA-Compliant Medical Data Applications with AWS whitepaper (pdf)

AWS Risk and Compliance whitepaper (pdf)