Nodeum Security Guide
Version : 2022-12-02

Revision : 1.3

NODEUM®

Copyright

Notice

Trademarks

Table of Contents

Copyright 2

Summary 4

Chapter 1: Security Basics 5

- Security Health Check 5
- Auditing 5

Chapter 2: Authenticate Users 5

- Elements of User Authentication 5
- Configure User Authentication Services 5
- Connected Applications 5

Chapter 3: Give Users Access to Data and Management Interface 5

- Control Who Sees What 5
- User Permissions 6
- Profiles 6

Chapter 4: Strengthen Your Security with Encryption 6

- Connection’s encryption 6
- Data’s encryption 6

Chapter 5: Monitoring Your Organization’s Security 7

- Monitor Login History 7
- Monitor Setup Changes with Data Management Audit Trail 7
- Monitor Data Changes with Data Access Audit Trail 7

CHAPTER 6 - Security Best Practices for Service Management 7

- Network Interface Service Mapping 9

Contact Us 10

Summary

Nodeum is built with security to manage your data.

You can also implement your own security scheme to reflect the structure and needs of your organization. Managing your data is a joint responsibility between you and Nodeum. The Nodeum security enable you to empower your users to do their jobs safely and efficiently.

Security Basics

Nodeum limits exposure of data to the users and limit the access to the data management platform. Implement security controls that are appropriated for the sensitivity of your data management. We'll work together to manage.

Authenticate Users

Authentication means preventing unauthorized access to Nodeum and your organization data.

Give Users Access to Data

Choosing the user or group privileges who can see the data stored into the container.

Strengthen Your Security with Encryption

Encryption refers to protecting data or connection while in transit and at rest (while it is about data storage on a storage media). You can protect the connection or data in transit using Secure Socket Layer/Transport Layer Security (SSL/TLS) or client-side encryption.

Monitoring Your Organization’s Security

Track login and field history, monitor setup changes, and take actions based on events.

Security Best Practices for Service Management

Allows administrators to configure many interfaces with varied security policies. When discussing the networks topology, the different connected interface can expose different type of services. Networks interfaces are typically defined in regard to security protection and management purpose. Firewall rules implementation provide additional security layer to protect network to sensible services.

Chapter 1: Security Basics

Security Health Check

At each installation of a new product version, all packages are upgraded to the last stable and verified version to fix any potential known vulnerabilities.

Auditing

It provides information about the use of the system, which can be critical in diagnosing potential or real security issues. The auditing features don't secure your organization by themselves; someone in your organization should do regular verification and control to detect potential abuse.

Chapter 2: Authenticate Users

Authentication means preventing unauthorized access to your organization or its data by ensuring each logged-in user is whom they say they are.

Elements of User Authentication

Nodeum provides several methods to authenticate users. Some methods are automatically enabled, and some require that you enable and configure them. Using this user authentication spectrum, you can build authentication to fit your organization's needs and your users' use patterns.

Configure User Authentication Services

In the User Management settings, you can define the Authentication Services you need.

Connected Applications

A connected application enables integration with Nodeum using APIs and standard SDKs. Connected applications use an API Security mechanism to manage the authentication, and authorization to Nodeum.

Chapter 3: Give Users Access to Data and Management Interface

Choosing the user or group privileges who can see the data stored in the container and what functions they can use in the management interface.

Control Who Sees What

Nodeum data sharing lets you expose specific data sets to individuals and groups of users. Permission sets, permission set groups. User roles and sharing rules control the individual records that users can view and edit.

User Permissions

User permissions specify what users can perform.

Profiles

Profiles define what functions the users can access in the Management interface. Two different roles are available: administrator and end-user. When you create users, you assign a profile to each one.

- **Administrator:** allows each user to access all functions of the Management Interface without limitation.
- **End-User:** limited access to only the content catalog where the user has the rights and privileges on the data.

Chapter 4: Strengthen Your Security with Encryption

Encryption refers to protecting data or connection while in transit and at rest (while it is about data storage on a storage media). You can protect the connection or data in transit using Secure Socket Layer/Transport Layer Security (SSL/TLS) or client-side encryption.

Connection’s encryption

The best practice to encrypt communication protocol is to use Transport Layer Security (TLS) or, formerly, Secure Sockets Layer (SSL). The protocol is therefore also referred to as HTTP over TLS or HTTP over SSL.

Out-of-the-box Nodeum is configured for HTTP; however, Nodeum is prepared to support HTTPS with the idea that minimal steps are required for you to implement HTTPS.

The instructions are automated in the Ansible deployment to apply the keys and certificates.

These will be used by Web UI and API to answer on the HTTPS port instead of HTTP port.

Once HTTPS is activated, Nodeum do not listen anymore to HTTP request.

Data’s encryption

You have the following options for protecting data at rest when stored in secondary storage:

- Object Storage
- Tape Storage
- NAS Storage

For Object Storage, Nodeum supports the three S3 SSE standard encryption methods:

- SSE-S3
- SSE-C
- SSE-KMS

For Tape and Disk Storage, Nodeum supports hardware-based encryption technologies from vendors.

Chapter 5: Monitoring Your Organization’s Security

Track login and usage history, monitor configuration changes, and take actions based on facts.

Monitor Login History

As an administrator, you can monitor all login attempts to Nodeum. The Audit section shows records of user logins for the past months.

Monitor Setup Changes with Data Management Audit Trail

Data Management Audit Trail tracks the recent configuration changes that you and other administrators make. Audit history is especially useful when there are multiple administrators.

Monitor Data Changes with Data Access Audit Trail

Data Access Audit Trail tracks the recent file changes (read, write, remove) that you, other administrators, and users make.

CHAPTER 6 - Security Best Practices for Service Management

The solution deployment allows a different form of security hardening in terms of firewall and network interface segregations. The solution deployment allows to configure services binding to dedicated network interfaces.

External or Internal Firewalls can be configured to filter and protect network flows between different network security layers. Nodeum does not make any changes you’re your own internal firewall configuration.

The following information helps to configure and determine the different security components parts of your network security settings.

Service Name	Interface	Port	Protocol
NODEUM SUPERV	Internal	1301	TCP
NODEUM WORKFLOW MANAGER	Internal	1501	TCP
NODEUM WATCHDOG	Internal	1502	TCP
NODEUM LIBRARY MANAGER	Internal	1503	TCP
NODEUM DATA MINING	Internal	1504	TCP
NODEUM WORKFLOW MANAGER COMMAND	Internal	1518	TCP
NODEUM LIBRARY MANAGER COMMAND	Internal	1519	TCP
NODEUM SCHEDULER	Internal	8081	TCP
NODEUM_FILE_LIST_PROCESSING	Internal	8082	TCP
NODEUM_CATALOG_INDEXER	Internal	8083	TCP
NODEUM REFPARSER	Internal	8084	TCP
NGNIX	External	80-443	TCP
SOLR	Internal	8983	TCP
MONGODB	Internal	27017	TCP
SSH	Internal External	22	TCP
NFS	External	111-2049	TCP/UDP
SMB	External	139-445	TCP
MinIO	External	9000	TCP
LDAP	Internal	389-636	TCP/UDP
MariaDB Client	Internal	3306	TCP
MariaDB Galera Traffic	Internal	4567-4568	TCP

MariaDB Galera SST	Internal	4444	TCP

Network Interface Service Mapping

Service can be bind to specific network interface, for doing that, the Nodeum Ansible Installation playbook needs to be reapplied once the inventory files have been modified accordingly to the mapping you need.

The following different parameters are available to definition the listening interface.

Service Name	Parameter
DEFAULT	iface_name
SAMBA	smb_iface_name
NFS	nfs_iface_name
RAILS	rails_iface_name
SOLR	solr_iface_name
CATALOG INDEXER	catalog_iface_name

Contact Us

Do you need help with your huge & complex data? Do you need to move, secure, process, share, or manage it in some other way that you can’t right now? Contact Nodeum to learn more how you can do it.

info@nodeum.io | www.nodeum.io

Follow us

https://twitter.com/nodeum_io

https://www.linkedin.com/company/nodeum/

https://www.youtube.com/channel/UCl4Mt9wm8fXI8W33lvV1fEw