NetBrain® Integrated Edition 8.0

Security Brief

Version 8.01 | Last Updated 2019-10-31

Contents

Overview

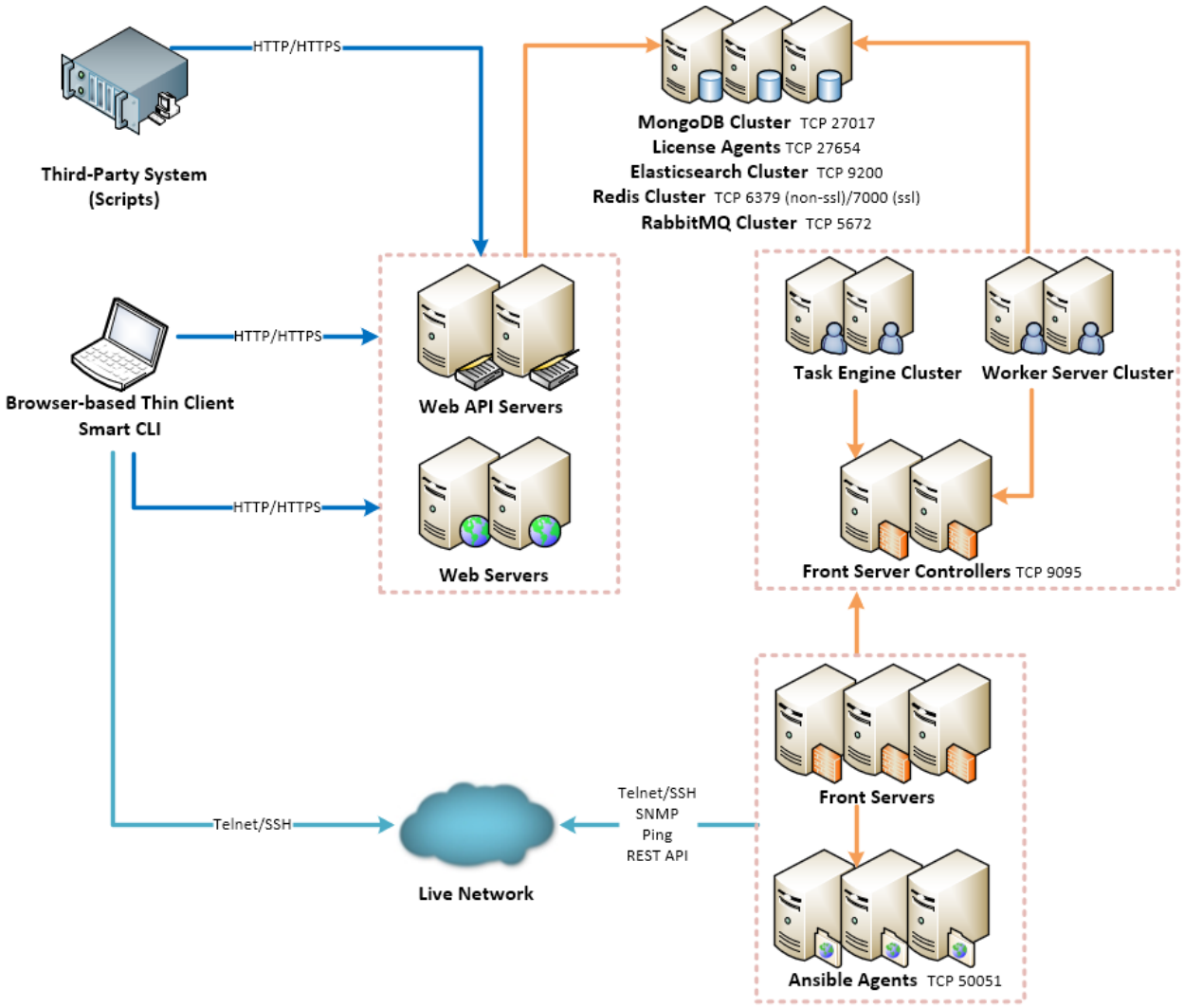
NetBrain Integrated Edition is a browser-based interface backed by a full-stack architecture, adopting advanced distributed technologies to support large-scale networks with more expansion possibilities. Its security solution consumes industry-standard best practices, with a strong focus on outbound data isolation, communication channel encryption, and customer access management.

This document introduces the primary security features and best practices, including:

1. Server Communication
2. User Account Management
3. Data
4. APIs for Third-Party Authentication and Integration
5. Best Practices

1. Server Communication

The connectivity and communications between external and system components are illustrated as follows:



Protocol and Port Number [1)]	Source	Destination
HTTP/HTTPS (80/443)	Thin Client	Web Server Web API Server
HTTP/HTTPS (80/443)	Service Monitor Agent	Web API Server
HTTPS (443)	Web API Server	Knowledge Cloud Domain (https://knowledgecloud.netbraintech.com/)

Protocol and Port Number [1)]	Source	Destination
ICMP (TCP 7) SSH (TCP 22) Telnet (TCP 23) SNMP (TCP 161/162) REST API	Front Server	Live Network
TCP 4369/25672 (for HA only)	RabbitMQ	RabbitMQ
TCP 5672	Web API Server Worker Server Task Engine Front Server Controller	RabbitMQ
TCP 6379 (non-ssl) TCP 7000 (ssl)	Web API Server Worker Server Front Server Controller	Redis
TCP 9095	Worker Server Task Engine Front Server	Front Server Controller
TCP 9200	Web API Server Worker Server	Elasticsearch
TCP 9300 (for HA only)	Elasticsearch	Elasticsearch
TCP 16379/26379 (for HA only)	Redis	Redis
TCP 27017	Web API Server Worker Server Task Engine Front Server Controller MongoDB	MongoDB
TCP 27654	Web API Server Worker Server	License Agent
TCP 50051	Front Server	Ansible Agent

Note: [1)] The port numbers listed are defaults only. The actual port numbers used during installation can be different.

TLS 1.2 is utilized to secure TCP communication links. Using HTTPS to establish secure encrypted communication between the Thin Client and Web Server is considered a best practice and the most secure choice (refer to Setting Up an SSL Secure NetBrain Webpage).

Note: As a fallback, for configurations where TLS is not applicable, the system can also be configured to establish communications via HTTP. However, this approach lacks any inherent security.

2. User Account Management

NetBrain Integrated Edition provides a set of policies to enable users to protect their accounts and data security. Areas addressed by these policies include Accounts, Authentication, and Authorization.

2.1. Account

NetBrain Integrated Edition stores user credentials in MongoDB (Database Server). User account passwords are stored using cryptographically secure hashes.

Several account control mechanisms are present in the system to allow the Administrator to better secure user accounts. These mechanisms are described in detail below.

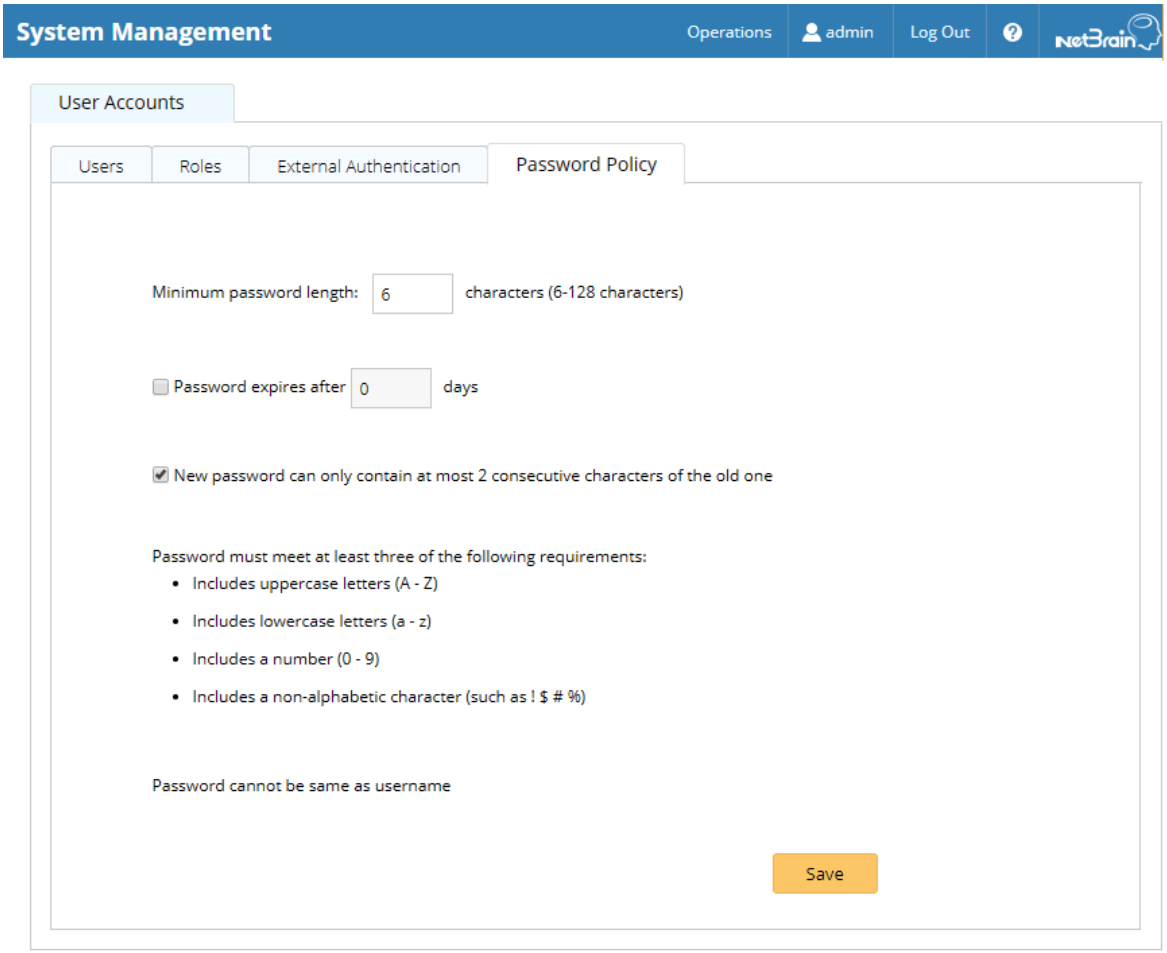
2.1.1.Password Complexity

The system allows the administrator to configure the policy governing the minimum complexity of user account passwords, including:

- Enforce “Require Password Change at First Login” for users whose accounts are created by admin.
- Minimum password length (6 - 128 characters)
- Password Expiry in days (1-9998)
- New password can only contain at most 2 consecutive characters of the old one
  For example, if the previous password was ‘**My**D0g$Gr8’, then the one ‘**My**C4tRul3$’ will be invalid.
- Enforce “Password must meet at least three requirements”:
  - Includes upper letters (A - Z)
  - Includes lowercase letters (a - z)
  - Includes a number (0 - 9)
  - Includes a non-alphabetic character (! @ # $ % ^ & *)

- Enforce “Password cannot be the same as username”

To configure these settings, go to **System Management > User Accounts > Password Policy**.



2.1.2.Session

Once a user completes a successful login, a unique session for that user will be created, and a token for that session will be issued to the user.

The default session expiry is 4 hours and configurable globally (go to **System Management > Advanced Settings**).

2.1.3.Accounts Lockout Policy

By default, the system automatically locks user accounts after 5 unsuccessful login attempts to protect user-information confidentiality. Locked user accounts will be available in 1 hour.

This policy also applies to the Password Reset function. When users are attempting to reset their passwords via GUI or API calls, entering incorrect passwords for too many times will lock their user accounts.

2.1.4.Audit Log

NetBrain recommends configuring to record user operations in the product audit log as a best practice.

The retention period of the log is configurable (go to **System Management > Advanced Settings**).

2.1.5.Access Controls

The access privileges of user accounts can be managed via one or more of the following controls:

- Start services with restricted privileges – the system enforces to launch NetBrain related services with restricted privileges to reduce the risk of elevated privileges when interacting with both Windows and Linux. Startup accounts with restricted privileges will be either created or configured during the system installation, rather than using privileged accounts of operating systems
- Management of user account authentication (if enabled).
- Domain-based user access – users can be limited to visit specific domains and tenants.
- Role-based privileged operations – users with different roles can have different privileges to perform operations or use features in a domain.

2.1.6.Built-in Admin Account

Privileged accounts may pose potential security risks if not managed. They usually have broad access to underlying customer information that resides in applications and databases. And passwords for these accounts

are often embedded and stored in unencrypted text files, a vulnerability that is replicated across multiple servers to provide greater fault tolerance for applications.

To eliminate this risk, IEv8.0 allows deleting the default administrator account.

Note: Before the deletion of the admin account, make sure there is at least one active user account with user management privilege in the system.

2.2. Authentication

The authentication aspect deals with validating user credentials and establishing the identity of the user. Every user must log in to the system with his or her username and password. User accounts can be created by the Administrator in the System Management page.

Alternatively, the following third-party authentication methods can be used:

- LDAP/AD Authentication

  NetBrain Integrated Edition supports integration with an LDAP/AD server to provide centralized control and management of user authentication. The Administrator can import user groups from your LDAP/AD servers and then define the corresponding roles for each group. Once configured, users can use their LDAP/AD accounts to log into the system. This solution simplifies user management for enterprise customers.

- TACACS Authentication

  NetBrain Integrated Edition supports integration with a TACACS+ server as an authentication center to manage domain logins. After configuring TACACS+ settings, adding users to the TACACS+ server and finishing the corresponding configurations in the System Management page, users can use their accounts on the TACACS+ server to log into the system.

- SSO (Single Sign-On) Authentication

  NetBrain Integrated Edition supports Security Assertion Markup Language (SAML) 2.0 based SSO and integrates with federation servers or individual identity providers to share session information across different security domains. SAML SSO works by transferring the user's identity through an exchange of digitally signed XML documents. There are two mechanisms of implementation:

- **Service Provider Initiated** — Users log into the NetBrain system by logging into other identity providers first.
- **Identity Provider Initiated** — Users who are already logged-in at other identity providers can directly view embedded NetBrain applications, such as map, path and data view.

2.3. Authorization

NetBrain Integrated Edition uses roles and privileges to define which operations each user can perform at the domain level. Each user account can be associated with one or more roles and privileges.

- Privileges reflect individual permissions to system operations or visibility.
- Roles are based on the types of tasks that a user is expected to perform while interacting with the system and is a collection of privileges.
  - System Admin
  - Domain-Level Roles

2.3.1.Privileges of System Administrator

The privileges of a system administrator are separated into two types: System Management and User Management. The corresponding privileges between the two types are described in the following table:

Management Category	Featured Management Module	System Management	User Management
System Management Page	System Home Page, including Usage Report		√
	License	√	
	Tenant Manager	√	
	User Accounts		√
	Front Server Controller Manager	√	

	Email Settings		√
	Advanced Settings - Global Session Timeout		√
	Advanced Settings - Audit Log + Login Logo	√	
	Resource Update	√	
	Task Manager	√	
	API Adapter Manager	√	
	Script Manager	√	
	Deployment Status [1)]	√	√
	Service Monitor	√	√
Tenant Management Page	User Authorization		√
	Domain List	√	
	MVS Configuration	√	
	Misc Configuration	√	
	GDR Data Configuration	√	
	API Manager	√	
	Interface Type	√	
	Platform Management	√	
	Topology Link Style	√	
	Advanced Settings	√	

Note: [1)] Only if you install multiple DC, the Deployment Status is displayed in the list.

2.3.2.Privileges of Domain-Level Roles

By default, the privileges of domain-level roles are listed as follows:

Privileges	Explanation	Domain Admin	Power User	Engineer	Guest	Network Change Creator	Network Change Executor	Network Change Approver
Domain Management	Log into the Domain Management page and do the following domain management tasks: ▪ View, export, and delete discovery report in the Fine Tune ▪ Add network definition ▪ View, add, modify, delete, and disable topology links in the Topology Link Manager ▪ Resolve duplicated IPs and subnets in the Duplicated IP and Subnet Manager ▪ Add checkpoint OPSEC tasks in the Checkpoint OPSEC Manager ▪ Configure network security settings and minimum subnet mask in L2 topology building ▪ Configure a desktop profile for all users under a domain	√	√			√	√	√
Share Policy Management	▪ Configure share policy (assign domain access and privileges to other users in this domain)	√						
Device Management	▪ Add, modify, and remove MPLS cloud	√	√			√	√	√

Privileges	Explanation	Domain Admin	Power User	Engineer	Guest	Network Change Creator	Network Change Executor	Network Change Approver
	▪ Remove devices from a domain							
Shared Resource Management	Only system/tenant administrator can edit built-in files in the shared folder of Device Group, Qapp, Gapp, Parser, Dashboard Widget and Template, and Runbook Template	√	√	√		√	√	√
Site Management	▪ Add MPLS clouds and unclassified network devices from the Fine Tune to a site ▪ Open the Site Manager to do site management, such as creating, editing, deleting, importing, committing, and rebuilding sites	√	√			√	√	√
Discover/Tune Network Device	▪ Create a do-not-scan list ▪ Add discovery tasks from the Start Page or the Schedule Task page ▪ Rediscover selected IPs and devices in the Fine Tune ▪ Tune live access ▪ Run on-demand discoveries	√	√			√	√	√
Schedule Benchmark	▪ Add benchmark tasks from the Start Page or the Schedule Task page	√	√			√	√	√
Manage Network Settings	▪ Configure and manage shared network settings	√	√			√	√	√
Manage Device Settings	▪ Configure and manage shared device settings for	√	√	√		√	√	√

Privileges	Explanation	Domain Admin	Power User	Engineer	Guest	Network Change Creator	Network Change Executor	Network Change Approver
	each device in a domain from the following entries: ○ Site pane ○ Map ○ Fine Tune ○ Discover ○ Tune Live Access							
Access to Live Network	Download the shared network settings or device settings data from the server and use these data to retrieve live device data from the network, which includes: ▪ Run CLI commands and Qapps on a map page or in a runbook ▪ Run monitor (Qapp-based) widgets and retrieve live data in static widgets in a dashboard ▪ Retrieve variables once or monitor variables periodically from the live network in Instant Qapp ▪ Calculate live paths (use the live network as the data source) ▪ Configure SNMP, CLI timeout, SNMP hostname trim rules, management interface selection order, and live access method polling order (SNMP/Telnet/SSH/Jumpbox) ▪ Browse live access logs in the Fine Tune	√	√	√	√	√	√	√

Privileges	Explanation	Domain Admin	Power User	Engineer	Guest	Network Change Creator	Network Change Executor	Network Change Approver
Create Network Change	Create network change tasks	√	√			√		
Execute Network Change	Execute network change tasks	√	√				√	
Approve Network Change	Approve network change tasks	√	√					√
View Network Change	View network change tasks	√	√			√	√	√
Map Layout Management	Associate layout styles with site maps and shared device group maps	√	√			√	√	√
Variable Mapping Management	View and manage variable mappings	√	√			√	√	√
Run Qapp	Run and schedule Qapp tasks	√	√	√		√	√	√
Golden Baseline Manual Definition	Define golden baseline manually	√	√	√		√	√	√
Golden Baseline Dynamic Calculation Management	Enable or disable dynamic calculation to set golden baseline	√	√					
Manage SPOG URL	View and define SPOG URL	√	√					

2.3.3.Prevention of Vertical Privilege Escalation

Vertical Privilege Escalation, also known as privilege elevation, is where a lower privilege user accesses functions or content that is reserved for higher privilege users.

The system is protected from Vertical Privilege Escalation in API calls by implementing the following measures:

- Username and user ID parameters have been removed to avoid malicious data updates.
- Enhanced inspection of the request parameter of a user ID for anonymous access.

3. Data

NetBrain Integrated Edition provides a series of measures to protect data security.

1. Data Encryption
2. Data Backup
3. User Data Input
4. Third-Party Dependencies

3.1. Data Encryption

The proper management of cryptographic keys is essential to the effective use of cryptography for security. Securely storing and retrieving these keys as needed is a major security enhancement.

To address a significant FIPS requirement and to enhance the solution's security, IEv8.0 builds a new keystore in the database, as a repository to store cryptographic keys, and also adopts enhanced hashing and encryption algorithms.

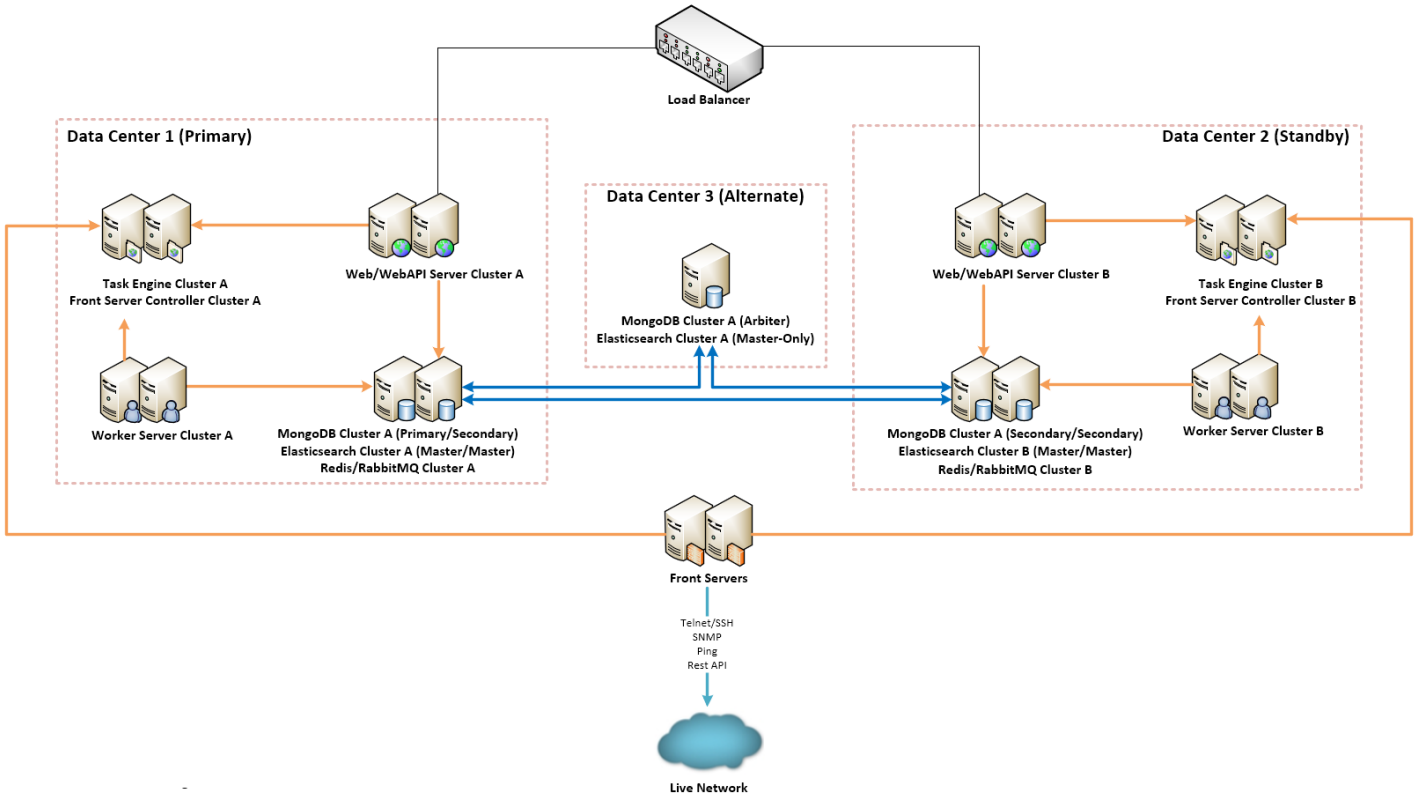
Algorithm	Used in IEv7.x	Adopted in IEv8.0
Non-Cryptographic Hashing	MD5	SHA256 Spooky 128
Password Hashing	MD5/SHA256	PBKDF2
Encryption/Decryption	DES	AES-256-CBC

Note: This upgrade of hashing and encryption algorithms has backward compatibility with user data in IEv7.x, except for Network Settings. A convert tool can be used to adapt existing Network Settings to IEv8.0.

3.2. Data Backup

The system data is stored in MongoDB, and there are two methods to deploy MongoDB.

- A standalone MongoDB instance. For the detailed data backup procedures, see Backing Up MongoDB Data for more details.
- A MongoDB replica set to provide data availability and prevent single-point-of-failure (SPOF) or system failover, which can be even across data centers. Here is a sample figure for multi-DC deployment, with one active system and one standby system.



For multiple separate large networks managed by MSP (managed service providers), the system supports multi-tenant data storage in separate MongoDB instances, to enhance both security and performance.

3.3. User Data Input

The system performs the following checks and validations to prevent malicious attacks.

- Validation of Uploaded Files
- Prevention of Cross-Site Scripting (XSS) Injection
- Prevention of Formula Injection

3.3.1.Validation of Uploaded Files

The system validates uploaded files across four key factors, including the file extension, mime-type, size, and upload frequency. The following validations are included:

- Enforce an upper limit on file size on a case-by-case basis.
- Enforce a default whitelist or blacklist of file extensions on a case-by-case basis. For example, define forbidden file extensions for generic cases, including **exe** and **bat**; define allowed file extensions for PDF, text and Word document, including **pdf**, **txt**, and **doc**.
- Validate the frequency of file uploads in API calls, by defining the minimum interval, the maximum concurrency count, and more parameters. When the system detects a high frequency of file uploads from a single user, he or she will be prohibited from uploading. The interval for his or her next allowed attempt can be configured.
- Validate a few bytes in the header of a file, which is known as the “Magic Number” of the file format and will uniquely identify the file type. For example, all PDF files start with the byte-sequence “%PDF”.

3.3.2.Prevention of Cross-Site Scripting (XSS) Injection

The system prevents Cross-site scripting (XSS) by validating and sanitizing user input. Each character of the data is encoded using the HTML Text Element scheme, and the result string is then inserted into the generated web page. For example, the characters `<`, `>`, `"`, `'` are encoded as `&#60;`, `&#62;`, `&#34;`, `&#39;` before being inserted into an HTML Text Element.

3.3.3.Prevention of Formula Injection

A Formula Injection vulnerability refers to the exported spreadsheet files that are dynamically constructed from inadequately validated input data. Once injected, it affects application end-users that access the exported spreadsheet files. For example, if the spreadsheet contains untrusted user-supplied data, the cell-level syntax consisting of an equal sign followed by a function name or an expression could be interpreted as formulas by a recipient's spreadsheet program, such as Microsoft Excel, and execute on the recipient's system.

The system validates user input to prevent formula injection before any input is inserted into spreadsheet data fields:

- Escape all untrusted input by placing a single-quote (`'`) before the content. For example, `=HYPERLINK(…)` will be processed as `'=HYPERLINK(…)`.
- Add a pair of double quotation marks (`" "`) to include an input containing a comma (`,`). For example, `a,b,c` will be processed as `"a,b,c"`.
- Avoid the use of scientific notation in CSV output. For example, `123456052535` will be processed as `="123456052535"`.

3.4. Third-Party Dependencies

To ensure the longevity of support and the most up-to-date code from a security standpoint, many components have been upgraded to the latest version in IEv8.0.

Component	Version NO. in IEv7.1x	Version NO. in IEv8.0
MongoDB	3.6.4	4.0.6
Elasticsearch	6.0.0 6.5.2 (v7.1a2)	6.7.2
Redis	3.0.504	5.0.4
RabbitMQ	3.7.7	3.7.14

The third-party dependencies of the system have been upgraded to the latest versions at the time of development completion, to ensure the most up-to-date code from a security standpoint.

4. APIs for Third-Party Authentication and Integration

NetBrain provides dozens of RESTful APIs for users to read (Get) and write (Post/Put/Delete) system data. To protect the data, NetBrain APIs use strict authentications based on OAuth2 framework.

Before using the APIs, users need to log in to the system with their usernames and passwords to obtain a token and then use the token for subsequent API calls. When there is no user activity until the session timeout, the token will expire.

5. Best Practices

The following best practices are recommended to enhance system security:

- Configuring Live Network Settings
- Masking Sensitive Data from Device Configuration File
- Setting Up an SSL Secure NetBrain Webpage
- Hardening Data Server

5.1. Configuring Live Network Settings

Many NetBrain features require access to live networks, such as discovery, benchmarking, path calculation and monitoring. To enable these features, go to **Domain Management > Discovery Settings > Network Settings** to complete the live-related settings, including:

- Non-privilege and privilege passwords, used to access devices via Telnet/SSH and retrieve live data by issuing CLI commands.
- SNMP RO strings, used to access devices via SNMP.
- SSH Private Key, used to log into network devices.
- Front Server settings, used to access and collect data from the live network.
- Server Jumpbox (secure administrative host), used as a hop-through system that the Front Server can access by using Telnet/SSH before accessing live devices.

5.2. Removing Sensitive Data from Device Configuration File

To remove the following sensitive data from both device configurations and user interface, go to **Domain Management > Operations > Domain Settings > Advanced Settings** and select the checkbox under the **Network Security** area.

1. Line and console passwords

2. Local user passwords
3. Enable passwords
4. Enable Secret
5. SNMP community string
6. TACACS and Radius keys
7. VPN Keys and Certs
8. SSH Private keys (these may show up on CSS devices)

5.3. Setting Up an SSL Secure NetBrain Webpage

To protect the data transfer between the web browser and Web Servers, enabling HTTPS is recommended to encrypt the communication.

1. Import the certificate into the IIS Manager of the machine where the Web Server is installed.
    1) Click the start menu and click **Administrative Tools** on the machine where the Web API Server is installed.
    2) Double-click **Internet Information Services (IIS) Manager** to open the IIS Manager.
    3) Double-click the machine name in the **Connections** pane and then double-click **Server Certificates** on the **Features View** tab page.
    4) Click **Import** in the **Actions** pane.
    5) Click the ... icon to select the certificate file and enter the password.
    6) Select **Web Hosting** from the **Select Certificate Store** list.
    7) Click **OK** to import the file.
2. Bind the certificate with the NetBrain web site.
    1) Double-click the NetBrain website in the **Connections** pane and click **Bindings** in the **Actions** pane.
    2) In the **Site Bindings** dialog, click **Add**.
    3) Select **https** from the **Type** list.

4) Click **Select** to select the certificate and click **OK**.

5) Click **OK**.

6) Click **SSL Settings** on the **Features View** tab page and select the **Require SSL** check box.

5.4. Hardening Data Server

HDD Encryption

While NetBrain does not configure HDD encryption by default, it is recommended to prevent outsiders from gaining easy access to data stored in the hard disk drive of MongoDB (Database Server), that you configure encryption of the entire hard disk drive via third-party applications, for example, MS BitLocker.

Linux Server Hardening

The system database has a dependency on Linux. It is recommended to harden your Linux server by following your company's security policies, such as:

- Install anti-virus software
- Apply corporate security policy
- Backup VM server image if the servers are VM-based