fuse
Management Central

Fuse Management Central

Installation and Administration Guide

Version 1.6.0

VILT

Contents

Fuse Management Central 1.6.0

08-05-2023

VILT Group, S.A.
Rua Ivone Silva, 6 - 7º Esq
1050-124 Lisboa
Portugal
Tel: +351 210 343 399
info@vilt-group.com

For more information, visit http://www.vilt-group.com

Disclaimer

1. Introduction

This guide walks you through the installation and administration of Fuse Management Central 1.6.0.

Fuse Management Central is a centralized web administration console for OpenText ™ solutions, providing to Self-Managed Customers or Managed Service Providers a Unified Management Experience. With Fuse Management Central intuitive user interface, as well as its simplified deployment, OpenText ™ system administrators can quickly and easily manage OpenText ™ solutions components, maintaining the context and understanding of them, always with the option to schedule any operation.

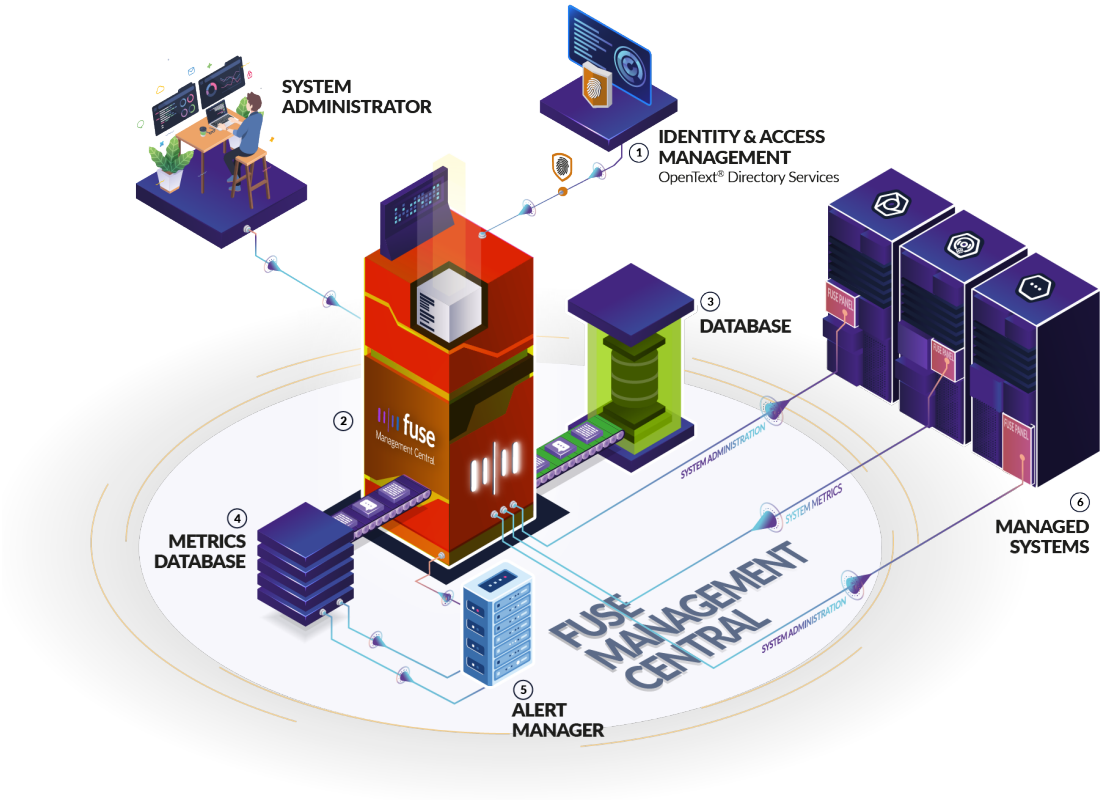
Fuse Management Central also separates system administration from content administration, introducing a new layer of security on top of the traditional OpenText ™ administration tools.

1.1. Document Revision History

Revision Number	Modification Date	Section Modified	Modifications
1.0	2023-05-08	All	Initial version

2. Overview of Fuse Management Central Architecture

The diagram below displays and briefly describes Fuse Management Central conceptual architecture, designed for high performance, scalability and security.



① Fuse Management Central integrates with OpenText ™ Directory Services to manage and authenticate its users.
OpenText ™ Directory Services provides a scalable identity management solution, by integrating multiple authentication services, such as Active Directory or Google.

② Fuse Management Central is the secret sauce centerpiece, responsible for orchestrating all system monitoring and management activities, regardless of its cluster type, whether productive or non-productive.

③ Fuse Management Central Database stores all application related data, such as administration settings, access roles, etc.

④ Fuse Management Central Metrics Database is used for long term metric storage, allowing system administrators to perform a temporal search on system metrics, combining them on aggregated system metric snapshots over time.

⑤ Fuse Management Central Alert Manager takes care of interpreting, deduplicating, grouping, and routing alerts to Fuse Management Central while allowing the option of silencing and inhibition of alerts.

⑥ All managed systems require Fuse Management Client installed and activated. Fuse

Management Client is responsible not only for collecting and dispatching all system components metric data but also to make the system management interface available while ensuring the data interchange security.

3. Install Fuse Management Central

3.1. Pre-Installation Tasks

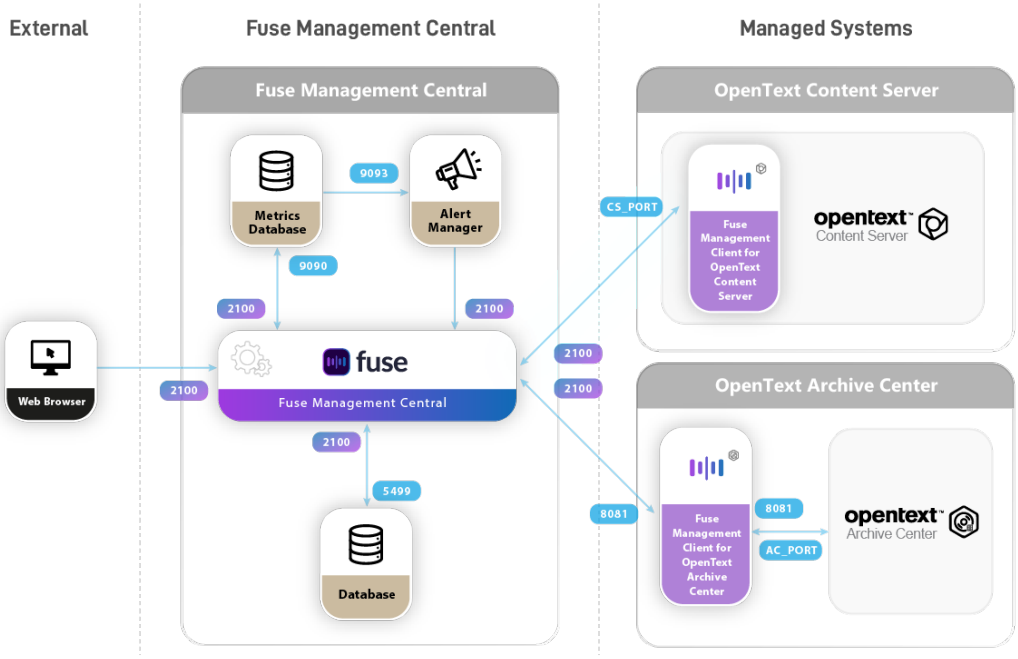
- Review Operating System Support
- Review Hardware Requirements
- Review Communication Ports Availability

> Please refer to the **Release Notes** document for a complete listing of supported systems and compatibility prior starting Fuse Management Central installation process.

3.1.1. Communication Ports Availability

Fuse Management Central uses designated ports for communication between its internal components. If a built-in firewall exists between any of these elements, you must manually open the required ports.

The following diagram should illustrate the communication ports availability and the relations between the several Fuse Management Central components.



Ports required for communication between components:

Port	Fuse Management Central Component
2100	Fuse Management Central port, used for both interface access and all APIs access.
5499	Fuse Database
9090	Fuse Metrics Database
9093	Fuse Alert Manager
8081	Default port for Fuse Management Client for OpenText Archive Center. This port can be changed on installation.
CS_PORT	Fuse Management Client for OpenText Content Server. This port entirely depends on your Content Server installation. Usually 80 or 8080.
AC_PORT	OpenText Archive Center port. This port entirely depends on your Archive Center installation. Usually 80 or 8080.

Fuse Management Client for OpenText Archive Center should be installed in the same system where Archive Center is running. Fuse Management Client for OpenText Content Server runs as a module inside Content Server, so no special port needs to be accessed, other than the actual Content Server port.

If any of the above ports are being used by other processes or applications, Fuse Management Central will not be able to properly operate.

3.1.2. Install Java

Before you start the Fuse Management Central installation, please check whether a supported JDK is already installed.

Please validate your current JDK version:

- *Option 1:* On Windows go to **Control Panel > Programs and Features** to see what JDK version is installed.
- *Option 2:* Check if JDK is already installed, by opening a command line and typing the following command:

```
java -version
```

1. Check Fuse Management Central **Release Notes** document to find out which JDK versions are supported for your Fuse Management Central version.
2. If no JDK is installed or the installed version is not supported:

- Download and install Java with the default option selected and make sure it is available in your `path`

Free long term support (LTS) versions of JDK are provided by Adoptium Eclipse Temurin and Oracle. We recommend you install a long term support version to use with Fuse Management Central.

3.1.3. Install NTP (recommended)

To avoid inconsistent metric data, and as a general good practice rule, it is highly advisable to keep the servers clocks synchronized.

For this purpose, installing Network Time Protocol (NTP) is strongly recommended in the Fuse Management Central server and all your configured Systems as well.

NTP helps ensure a consistent time of day across all the service nodes in the cloud. If you enable NTP in a network, configure the service nodes to obtain their time over the network.

3.1.4. Enabling SSL for HTTPS

In order to establish a secure communication channel between the user and Fuse Management Central, can be used HTTPS by enabling SSL.

To enable SSL the recommendation is to use a proxy web server, like NGINX, redirecting all traffic to HTTP 2100. With this approach there is no need to change any configuration in Fuse and everything should work as expected.

Optionally, it is possible to enable SSL security directly on Fuse, please refer to the **Configure SSL** section in the Spring Boot Reference Documentation. A key store for self-signed certificates can be configured and it is propagated as a trusted store for all internal SSL communications if needed.

```
server:
  # Fuse Management Central HTTPS Port
  port : 8443
  # If self-signed certificate is used, configure them in this block
  ssl:
    # path for SSL key store
    key-store: c:/path/keystore.jks
    # password for SSL key store
    key-store-password: secret
```

After this, it is necessary to change the Alert Manager and the Metrics Database configurations to correctly communicate with Fuse.

To configure the Alert Manger go to `<fuse_installation_folder>/alertManager/alertmanager.yml` and update the url with https and the new port.

```
receivers:
  - name: fuse
    webhook_configs:
      - url: 'https://127.0.0.1:443/api/alert'
```

And to configure the Metrics Database go to `<fuse_installation_folder>/metricsDatabase/prometheus.yml` and update each scrap configuration with the new URL and adding the property `scheme: https`.

```
scrape_configs:
  - job_name: 'prometheus'
    static_configs:
      - targets: ['127.0.0.1:9090']
  - job_name: 'fuse-spring-boot'
    metrics_path: '/actuator/prometheus'
    static_configs:
      - targets: ['127.0.0.1:443']
    scheme: https
  - job_name: 'fuse-metrics-5'
    metrics_path: '/api/metrics/5'
    scrape_interval: 5s
    static_configs:
      - targets: ['127.0.0.1:443']
    scheme: https
  - job_name: 'fuse-metrics-30'
    metrics_path: '/api/metrics/30'
    scrape_interval: 30s
    static_configs:
      - targets: ['127.0.0.1:443']
    scheme: https
  - job_name: 'fuse-metrics-60'
    metrics_path: '/api/metrics/60'
    scrape_interval: 60s
    static_configs:
      - targets: ['127.0.0.1:443']
    scheme: https
  - job_name: 'fuse-metrics-120'
    metrics_path: '/api/metrics/120'
    scrape_interval: 120s
    static_configs:
      - targets: ['127.0.0.1:443']
    scheme: https
```

3.2. Microsoft Windows

3.2.1. Installation

To run Fuse Management Central installer on Windows:

1. Log on to Windows as a user who is a member of the **Local Administrators** group.
2. **Start Fuse Management Central installation** wizard, by double-clicking the installation file (`/Fuse Management Central/Windows/`**`Fuse Management Central 1.6.0-Winx64.exe`**).
3. In the **Choose Components** dialog box, leave the default values selected and click **Next**.

4. In the **Choose Install Location** dialog box, accept the default **Destination Folder** or click Browse to select a different folder, and then click **Next**.
5. In the **Choose Data Location** dialog box, accept the default **Data Directory** folder or click Browse to select a different folder, and then click **Next**.

> To ensure business continuity, the **Data Directory** path should have a backup policy applied, enabling data recovery in the event of a disaster.

6. In the **Choose Start Menu Folder** dialog box, click **Install**.
7. When the installation process is complete, click **Close**.
8. Open Windows Services console and start **Fuse Management Central** service, once started all dependency services will start automatically.
   The following Windows services must be running:
   - **Fuse Management Central**
   - **Fuse Management Central (Alert Manager)**
   - **Fuse Management Central (Database)**
   - **Fuse Management Central (Metrics Database)**

3.2.2. Upgrade

> As the PostgreSQL version have been upgraded to 14.6, it is crucial to take proper precautions before upgrading Fuse Management Central. Failure to do so could result in the loss of all existing PostgreSQL data! To ensure the preservation of your data, before starting the Fuse Management Central upgrade you must first backup your PostgreSQL data, as described in this chapter. Once the upgrade is complete, you can then restore your data.

If you have a previous version of Fuse Management Central installed follow the following procedures:

1. Stop the following services:
   a. `Fuse Management Central`.
   b. `Fuse Management Central (Alert Manager)`.
   c. `Fuse Management Central (Metrics Database)`.

> Only the `Fuse Management Central (Database)` service should keep running.

2. Backup your **Fuse Data Directory**.
   a. Fuse Data Directory is setup accordingly to the installation instructions on chapter Installation on Microsoft Windows, for example `C:\ProgramData\Fuse Management Central`
3. Create a database backup by creating a dump of all the Postgres databases:
   a. Refer to the official `pg_dumpall` command documentation on how to create a

dump of all databases, for example:

```
cd "<fuse_installation_folder>\database\bin"
.\pg_dumpall -U postgres -p 5499 -f c:\\database_backup
```

The database dump can take several minutes, **please make sure it completes successfully**

4. Stop `Fuse Management Central (Database)` service.
5. Delete the `database` folder in **Fuse Data Directory**, For example, `C:\ProgramData\Fuse Management Central\database`

Ensure that you have previously made a proper backup of the folder

6. Uninstall Fuse Management Central following the instructions in the chapter Uninstall Fuse Management Central.
7. Install Fuse Management Central following the chapter Install Fuse Management Central configuring the same data directory used previously when prompted.
    a. **Do NOT start any service after installation**, only `Fuse Management Central (Database)`
8. Import the Postgres database dump, by running the script generated previously
    a. For example:

```
cd "<fuse_installation_folder>\database\bin"
.\psql.exe -p 5499 -U postgres -d postgres -f
c:\\database_backup
```

This can take several minutes, **please make sure it completes successfully**

9. Start `Fuse Management Central` service and make sure all the processes are running (`Fuse Management Central (Alert Manager)`, `Fuse Management Central (Metrics Database)` and `Fuse Management Central (Database)`).

3.3. Linux

Linux and manual installation resources are available in the `Linux` folder inside the Fuse Management Central package.

It is highly recommended that you check **Fuse Management Central architecture** chapter and understand the different pieces that are part of the product. Each one of those pieces should be installed manually.

3.3.1. Pre-requirements

- Install Java 8 or higher
- Install Prometheus 2.41.0 or any latest patch version (https://github.com/prometheus/prometheus/releases/tag/v2.41.0).
- Install AlertManager 0.25.0 or any latest patch version (https://github.com/prometheus/alertmanager/releases/tag/v0.25.0)
- Install PostgreSQL 14.6 or any latest minor version (https://www.postgresql.org/download/), including the **postgresql-contrib** subpackage (https://www.postgresql.org/docs/14.6/contrib.html)
- Install PostgreSQL **uuid-ossp** extension module (https://www.postgresql.org/docs/14.6/uuid-ossp.html)

Please refer to each third-party component documentation about procedures on how to install them. Alternatively, we provide general guides for third-party software installation in the **Appendix B - How-Tos**.

The next steps of the manual installation will assume that all the components are installed in the same machine and running with the default ports.

- All configuration is using 127.0.0.1 or localhost for communication
- All third-party software is using default ports:
  - PostgreSQL: `5432`
  - Prometheus: `9090`
  - AlertManager: `9093`

For different setup please review the configuration files supplied by Fuse Management Central package, as you go through each step of the installation:

- `config/application.yml`
- `prometheus_config/prometheus.yml`
- `alertmanager_config/alertmanager.yml`

3.3.2. Installation and Configuration

1. Unzip `Linux` folder from Fuse Management Central package to the folder where you want to install Fuse Management Central, for example `/opt/vilt/fuse/`.
2. Update `config/application.yml` to validate the datasource configuration to match your PostgreSQL installation, and add the username and password configuration. For example:

```
spring:
  datasource:
    driver-class-name: org.postgresql.Driver
    url: jdbc:postgresql://localhost:5432/postgres
    username: postgres
    password: myPassword
```

3. Redirect your Prometheus `--config.file` argument in your Prometheus startup script to `<fuse_installation_folder>/prometheus_config/prometheus.yml`
4. Change your Prometheus startup script to include the following arguments along with other arguments you might have:

```
--query.max-concurrency=32
```

5. Redirect your AlertManager `--config.file` argument in your AlertManager startup script to `<fuse_installation_folder>/alertmanager_config/alertmanager.yml`
6. Start Fuse Management Central as a standalone runnable jar

```
java -jar fuse.jar
```

7. It may take some time to complete the startup. After that you can open Fuse Management Central in your browser.
    - http://localhost:2100/
8. **Optional:** To integrate with **systemd** in *nix systems, Fuse Management Central integrates jsystemd. A sample service unit can be created like this:

   Sample `fuse.service`:

```
[Unit]
Description=Fuse Management Central
Requires=network.target
After=network.target
After=syslog.target
[Service]
Type=notify
WorkingDirectory=<fuse_installation_folder>
ExecStart=/usr/bin/java -jar <fuse_installation_folder>/fuse.jar
SuccessExitStatus=143
KillMode=mixed
TimeoutStopSec=10
TimeoutStartSec=120
[Install]
WantedBy=multi-user.target
```

3.3.3. Upgrade

If you have a previous version of Fuse Management Central installed follow the following procedure:

1. Stop all Fuse services: Fuse Management Central, Prometheus, AlertManager and PostgreSQL
2. Upgrade Prometheus to 2.41.0 version or any latest patch version
3. Upgrade AlertManager to 0.25.0 version or any latest patch version
4. Upgrade PostgreSQL to 14.6 version or any latest minor version

Please refer to each third-party component documentation about procedures on how to upgrade them. Always backup your data before making changes. Alternatively, we provide general guides for third-party software upgrade in the **Appendix B - How-Tos**.

With all third party services upgraded, please follow the next steps:

1. Update Fuse configuration file with the new one:
    a. Go to your Fuse installation folder
    b. Inside the `config` folder, backup your `application.yml` file
    c. If you have all default configurations (never modified this file manually), simply replace the old `application.yml` file by the new one
    d. If you have custom configurations, check for new configurations in the new `application.yml` file and merge them with your current file
2. Update Prometheus configurations:
    a. Go to your Fuse installation folder
    b. Inside the `prometheus_config` folder, backup all files and folders
    c. Replace current configuration files and folders by the new ones
3. Update AlertManager configurations:
    a. Go to your Fuse installation folder
    b. Inside the `alertmanager_config` folder, backup all files and folders
    c. Replace current configuration files and folders by the new ones

Please make sure that Prometheus and AlertManager startup scripts are loading configurations from your Fuse installation folder. Check the installation section for more information on this.

4. Update Fuse Management Central runnable jar with the new one:
    a. Go to your Fuse installation folder
    b. Backup your current `fuse.jar` file
    c. Replace your current `fuse.jar` file by the new one
5. Restart all Fuse services: Prometheus, AlertManager, PostgreSQL and Fuse Management Central

3.4. Docker

3.4.1. Pre-requirements

Before proceeding, please make sure you have installed the latest version of Docker and Docker Compose, as defined in the official documentation:

- Docker: https://docs.docker.com/install/
- Docker Compose: https://docs.docker.com/compose/install/

> **!** Please refer to the **Release Notes** for the required minimum versions.

3.4.2. Run with Docker Compose

1. Load the docker image with:

```
docker load < fuse-docker-image.tar
```

   This will create an image with the tag `vilt-group/fuse-server`

2. In the same directory as the `docker-compose.yml` provided, start all the services with:

```
docker-compose up -d
```

After start up open Fuse Management Central login page in your browser: http://localhost:2100

> **!** Make sure that port `2100` is available in your system. Otherwise change the exposed port in the `docker-compose.yml`file to one available.

3.4.3. Advanced Configuration

Data Persistence

Data is persisted in volumes, however backups are recommended for all the volumes. For backup recommendations please refer to Docker official documentation.

```
volumes:
  postgresql:
  prometheus:
  alertmanager:
```

Alternatively you can also map the data directories to filesystem mount points. Please follow the official documentation for the third-party containers.

JVM Options

To configure advanced JVM options in Fuse service use the `JAVA_TOOL_OPTIONS` environment variable:

```
    environment:
      - JAVA_TOOL_OPTIONS=
```

Third-Party Components

For more information regarding third-party configurations, please refer to the official third-party images documentation:

- Postgres
- Prometheus
- AlertManager

For information on running the docker image with kubernetes, please contact us by email product.support@vilt-group.com.

3.4.4. Upgrade

As the PostgreSQL version have been upgraded to 14.6, it is crucial to take proper precautions before upgrading Fuse Management Central. Failure to do so could result in the loss of all existing PostgreSQL data! To ensure the preservation of your data, before starting the Fuse Management Central upgrade you must first backup your PostgreSQL data, as described in this chapter. Once the upgrade is complete, you can then restore your data.

To upgrade your Docker installation, you first need to backup your database using `pg_dumpall`:

1. Stop all containers

```
docker compose stop
```

2. Backup the database data

```
# start the fuse-database, so you can dump it
docker compose start fuse-database

# dump the database (feel free to change the target file to a folder
with enough space available)
docker compose exec fuse-database pg_dumpall -U postgres -p 5432
--no-role-passwords | gzip > db_backup.sql.gz

# stop fuse-database and remove all containers
docker compose stop fuse-database
docker compose rm
```

3. Backup your existing `docker-compose.yml` file
4. Copy the new docker files from the release bundle (`docker-compose.yml` and `fuse-docker-image.tar`)
5. Optionally backup the data from all the named volumes, following Docker user guide **Docker User Guide**.
6. Copy the provided `docker-compose.yml` file and make any necessary adjustments
7. Delete existing `postgres` volume

```
# find and remove the postgres volume
docker volume ls | grep postgres

# that will output something like:
# local     fuse-server_postgresql

# use the volume name to remove it
docker volume rm fuse-server_postgresql
```

8. Load the docker image

```
docker load < fuse-docker-image.tar
```

9. Start the database and restore data from the backup

```
# starts the fuse-database to import the dumped file
docker compose up -d fuse-database

# import the dump (replace db_backup.sql.gz with your postgres
backup file)
gunzip -c db_backup.sql.gz | docker compose exec --no-TTY fuse-
database psql -U postgres -p 5432
```

10. Start all remaining services

```
docker-compose up -d
```

11. Make sure the new images were pulled correctly and the containers recreated

3.5. Validate Fuse Management Central Installation

To confirm if Fuse Management Central was successfully installed, open Fuse Management Central Administration page by using one of the following methods:

1. On Windows, click **Start**, point to **Programs**, point to the program folder name that was provided on the installation process (*default: Fuse Management Central*), and then click the **Fuse Management Central Administration** shortcut.
2. Open the following URL:

```
http://<fuse-management-central-host>:2100/
```

3. Login with your authentication credentials:
    - **Username**: `fuseadmin` *(default)*
    - **Password**: `fuseadmin` *(default)*
4. Navigate to ***Fuse Administration > Administration***
5. On Fuse Management Central Administration page, click **Status**

If Fuse Metrics Database, Fuse Database and Fuse Alert Manager components are green and healthy, Fuse Management Central was **successfully installed**! Otherwise please check Troubleshooting chapter.

3.6. Post-installation

After installing Fuse Management Central please check for possible hotfixes. Hotfixes are cumulative, so you only need to install the latest one. Available hotfixes can be found in Fuse Management Central repository (https://sw.vilt-group.com/), under the `Fuse Management Central/Hotfixes` folder of each Fuse Management Central version folder.

In order to download and apply the hotfix do the following:

- Download the zip file **fusemanagement-central-X.X.X.X-hotfix.zip**.
- Stop all Fuse services.
- Replace the **fuse.jar** from `<fuse_installation_folder>/` (e.g. `C:\Program Files (x86)\Fuse Management Central\` or `/opt/vilt/fuse/`) by the one provided in the downloaded zip file.
- Start all Fuse services.

3.7. Next Steps

Once Fuse Management Central is installed, it is **mandatory to perform a set of initial configurations, required for Fuse Management Central to properly and securely operate**.

Post-installation checklist:

- Review the **Security** settings
- Update **General** settings
- Request and apply a valid **License**

4. Install Fuse Management Client

4.1. Install Fuse Management Client for OpenText Content Server

1. Extract Fuse Management Client for OpenText Content Server ZIP file (`Clients/Fuse Management Client for OpenText Content Server 1.6.0/fuse-management-client-otcs-1.6.0.zip`) outside of the OpenText ™ Content Server® installation folder*.
2. Copy all the extracted `fuse-management-client-otcs-1.6.0` folder contents to the `<Content Server home>` directory, overriding the `staging` folder.

> ! If you are installing Fuse Management Client on a UNIX/Linux system, make sure that you are performing the setup actions with the user who installed OpenText ™ Content Server® and runs the Content Server service.

3. Open **Content Server Administration** page in a Web browser.
4. If prompted, enter the Administrator password, and then click **Log-in**.
5. Install or upgrade Fuse Management Client:
    a. If you already have a previous version of Fuse Management Client:
        i. Select:
            - *(OpenText ™ Content Server 16.2.5 and below)* **Module Administration > Upgrade Modules**
            - *(OpenText ™ Content Server 16.2.6 and above)* **Core System > Module Configuration > Upgrade Modules**
    b. For new installations:
        i. Select:
            - *(OpenText ™ Content Server 16.2.5 and below)* **Module Administration > Install Modules**
            - *(OpenText ™ Content Server 16.2.6 and above)* **Core System > Module Configuration > Install Modules**
6. From the **Installable Modules** list, install/upgrade **Fuse Management Client** module.
7. After the installation of **Fuse Management Client** module is completed, restart **Content Server**.

> ⚠ For some Content Server versions, especially earlier ones, we found out that the standard soft-restart is not enough to reload all the loaders required for Fuse Management Client, so we suggest you do a second hard-restart to make sure everything was updated. Please check the troubleshooting section.

4.1.1. User Requirements

Fuse Management Client for OpenText Content Server module needs a user with the following properties to be **installed** and **updated**:

- Be in the group *Web Administration*
- Having the privileges:
  - *Log-in enabled*
  - *Public Access enabled*
  - *System administration rights*

The Web Administration user is only used to install the Fuse Client module. Then, in order to **monitor** and **manage** OpenText Content Server, the Fuse Client just needs a **basic user** that can login in OpenText Content Server.

4.1.2. (Optional) Install Fuse Management Client for OpenText Content Server using Opentext System Center Manager

Alternatively, Fuse Management Client 1.6.0 module can also be deployed using OpenText System Center Manager (OTSCM):

1. Upload Fuse Management Client ZIP file:
   a. Open OTSCM, navigate to **Settings** and on the left menu choose **External Vendor Files**.
   b. On the top right there is a button named **Select external vendor files** that allows to upload a new file.
   c. Upload Fuse Management Client ZIP file (`Clients/Fuse Management Client 1.6.0/`**`fuse-management-client-otcs-1.6.0.zip`**).
2. Create an installation plan for Fuse Management Client:
   a. Navigate to the **Plans** tab and use the button **Add plan** to create a new plan for installing Fuse Management Client.
   b. Add each configured system where fuse-management-client-otcs-1.6.0 is to be installed, and for each one of them configure the required attributes:

Field	Description
Module Vendor	Third Party
Thirt party Module	Previously uploaded Fuse Client ZIP (e.g. *"fuse-management-client-otcs-1.6.0.zip"*)
Instance path	Path to OpenText Content Server installation
Admin username	OpenText Content Server Admin user

Field	Description
Host name	OpenText Content Server hostname
Site name	OpenText Content Server site name (configured in mappings.tbl)

c. Save the plan.

3. Execute plan:
    a. The plan can be executed by pressing the play button under actions.

4.1.3. Configure Fuse Management Client logs

Fuse Management Client module has its own log configurations. These configurations can be changed according to your needs.

In order to change Fuse Management Client log configurations, follow these steps:

1. Open **Content Server Administration** page in a Web browser.
2. If prompted, enter the Administrator password, and then click **Log-in**.
3. Access **Fuse System Administration > Log Settings**.
4. Change the settings accordingly to your needs

Field	Description
Log Level	Desired log level (OFF, ERROR, WARN, INFO, DEBUG, TRACE)
Location	Path where logs should be stored
Use rolling logs	Create a rotation mechanism for the log file
Number of log files	How many files should be stored after rotation
Size of each log file	Size of the log file to be rotated
Compress completed log files	If rotated log files should be compressed

5. Click on **Save Changes**

4.1.4. Patching Fuse Management Client for OpenText Content Server

To complete the installation of Fuse Management Client, or in order to fix known issues, you may need to apply one or more Content Server patch files.

Fuse Management Client patches are distributed as common OpenText Content Server patch files. Available patch files can be found in Fuse Management Central repository (https://sw.vilt-group.com/), under the `Clients/Fuse Management Client for OpenText Content Server x.x.x/Patches` folder of each Fuse Management Central version folder. Patches can also be sent directly to you in support cases.

To apply Fuse Management Client Patches follow the steps below:

1. **Download** Fuse Management Client patch files for OpenText Content Server, for example `pat140000001.txt`
2. **Stop** OpenText Content Server service.
3. **Copy** the patch file(s) to the OpenText ™ Content Server® patches folder (`<Content_Server_Home>/patch/`).
4. **Start** OpenText Content Server service.

> ! You don't need to apply patches if no patch files are available for your Fuse Management Client version.

4.2. Install Fuse Management Client for OpenText Archive Center

Before starting Fuse Management Client for OpenText Archive Center installation, please check if a supported Java version is already installed.

1. Check Fuse Management Central **Release Notes** document to find out which Java versions are supported for your Fuse Management Central version.
2. If Java is not installed or the installed version is not supported:
    - Download and install Java and make sure it is available in your `path` in the same host where OpenText Archive Center is installed.

> ! Fuse Management Client for OpenText Archive Center must be installed on the same host as OpenText Archive Center.

> Free long term support (LTS) versions of JDK are provided by Adoptium Eclipse Temurin and Oracle. We strongly recommend installing a long term support version to use with Fuse Management Central.

4.2.1. User Requirements

User permissions have an impact on OpenText Archive Center monitoring and on the management actions that can be performed in Fuse Management Central. These permissions directly depend on the OpenText Archive Center credentials that are used to connect Fuse Management Client with OpenText Archive Center.

Monitoring

In order to have full monitoring metrics, a user from the **aradmins** group should be used. Users from other groups might also work but have limited access to some data.

Management

In order to have full access to all actions available through Fuse Management Central, it requires the use of the **dsadmin** user, since Fuse Management Client uses both API and also `dsclient` and `spawncmd` calls to perform actions.

Users from **aradmins** can perform API actions but cannot execute `dsclient` calls, so actions performed by `dsclient` will not work. This is the current list of actions performed by Fuse Management Central using `dsclient` which require the use of **dsadmin** user specifically:

- Delete OpenText Archive Center Disk Volume

Users from other groups might work but have limited access to API actions that can be performed.

4.2.2. Installation on Microsoft Windows

1. Extract Fuse Management Client for OpenText Archive Center ZIP file (`Clients/Fuse Management Client for OpenText Archive Center 1.6.0/`**`fuse-management-client-otac-1.6.0-windows.zip`**) to the desired installation folder (e.g. C:\Program Files{oem-product} Management Client for OpenText Archive Center)
2. Inside the new folder location execute the batch file named `install.bat`: this will install the client in the current location and add it as a Windows service.
3. When the installation process is complete, if needed, close the console window.
4. Check the client settings in the `application.yml` file, according to the specification on Fuse Management Client for OpenText Archive Center Configuration Specification
5. Open Windows Services console and start the following Windows service:
    - **Fuse Management Client for OpenText Archive Center**

Optional: The path to the Java executable can be configured in the file `FuseClientArchiveCenter.xml` by editing the value of the tag `<executable>java</executable>`. This is optional and can be useful when you have multiple JREs installed and need to select a specific one.

4.2.3. Installation on Linux

Installation on Unix Systems supports both Init.d and Systemd to start the process as a service. Alternatively there is a script to start the process manually in the background, as a daemon.

Systemd

1. Extract Fuse Management Client for OpenText Archive Center ZIP file (`Clients/Fuse Management Client for OpenText Archive Center 1.6.0/fuse-management-client-otac-1.6.0-unix.zip`) to the folder `/opt/vilt/fuse-client-otac/` (The installation instructions assume this installation path).
2. Copy the script `/opt/vilt/fuse-client-otac/bin/fuse-client-otac.service` to the folder `/etc/systemd/system/` (If the path is different from the previous step this script needs to be changed to reflect the correct path)
3. Both the path of the application (default: /opt/vilt/fuse-client-otac/) and the user running the service (default: root) can be configured by editing this script.
4. Reload the available services with `sudo systemctl daemon-reload`
5. The application can then be started with the command: `sudo systemctl start fuse-client-otac`

To flag the application to start automatically on system boot, use the following command: `systemctl enable fuse-client-otac`

For additional configuration options please refer to **Spring Boot systemd Service documentation**.

Init.d

1. Extract Fuse Management Client for OpenText Archive Center ZIP file (`Clients/Fuse Management Client for OpenText Archive Center 1.6.0/fuse-management-client-otac-1.6.0-unix.zip`) to the folder `/opt/vilt/fuse-client-otac/`.
2. Create a symlink, as follows:

```
sudo ln -s /opt/vilt/fuse-client-otac/fuse-client-otac.jar
/etc/init.d/fuse-client-otac
```

3. The application can then be started with the command

```
service fuse-client-otac start
```

You can also flag the application to start automatically by using your standard operating system tools. For example, on Debian, you could use the following command: `update-rc.d fuse-client-otac defaults <priority>`

For additional configuration options please refer to **Spring Boot init.d Service documentation**.

Daemon

1. Extract Fuse Management Client for OpenText Archive Center ZIP file (`Clients/Fuse Management Client for OpenText Archive Center 1.6.0/fuse-management-client-otac-1.6.0-unix.zip`) to the folder `/opt/vilt/fuse-client-otac/`.
2. Change to the script directory:

```
cd /opt/vilt/fuse-client-otac/bin/
```

3. Execute the script to run the client in background:

```
./startup.sh
```

Fuse Management Client for OpenText Archive Center Configuration

Check the client settings in the `application.yml` file, according to the specification on Fuse Management Client for OpenText Archive Center Configuration Specification.

4.2.4. Upgrade Fuse Management Client for OpenText Archive Center

If you already have a version of Fuse Management Client for OpenText Archive Center, you can easily upgrade it following these steps:

1. Extract Fuse Management Client for OpenText Archive Center ZIP file (`Clients/Fuse Management Client for OpenText Archive Center 1.6.0/fuse-management-client-otac-1.6.0-[windows/unix].zip`) to a temporary folder
2. Inside you will find a new **fuse-client-otac.jar** file
    - For the Windows bundle, this file is located under the `lib` folder
3. **Stop** Fuse Management Client for OpenText Archive Center
4. In your Fuse Management Client for OpenText Archive Center installation folder, find the current **fuse-client-otac.jar** file
    - On Windows this file will be inside a `lib` folder
5. Replace your current **fuse-client-otac.jar** file by the new one
6. Locate your current configuration file
    - until version 1.5.x, it's named `config.yml`
    - from version 1.6.x forward, it's named `application.yml`
7. Check for new configurations that should be added, by comparing your current `config.yml` file with the new `application.yml` file of the new version, according to the specification on Fuse Management Client for OpenText Archive Center Configuration Specification.
8. **Start** Fuse Management Client for OpenText Archive Center again

4.2.5. Additional Settings

In this section you can find the available settings for Fuse Management Client for OpenText Archive Center and what each one of them does. These configurations can be changed in the `application.yml` file available in the client installation folder.

```
archive-center:
  # Archive Center Instance URL
  url: http://localhost:8080
  # Document Pipelines configuration
  document-pipelines:
    host: localhost
    port: 4032
    timeout: 15s

server:
  # Fuse Management Client HTTP Port
  port : 8081
```

SSL Support

To enable HTTPS communication between Fuse Management Client for OpenText Archive Center and Fuse Management Central, the following properties must be added to the `application.yml` file, under the `server` settings.

```
server:
  # Fuse Management Client HTTPS Port
  port : 8444
  ssl:
    # path for SSL key store
    key-store: /path/keystore.jks
    # password for SSL key store
    key-store-password: secret
```

For more SSL configuration options, please refer to the **Configure SSL** section in the Spring Boot Reference Documentation.

4.2.6. Post-installation steps

To validate if Fuse Management Client for OpenText Archive Center was successfully installed and is up and running, open the following URL and login using OpenText Archive Center credentials:

```
http://<otac.server.host>:8081
```

If Fuse Management Client for OpenText Archive Center is not running, check the **Appendix A - Troubleshooting** for possible known issues and workarounds.

4.2.7. Connect with OpenText Document Pipeline Server

To connect Fuse Management Client for OpenText Archive Center with OpenText Document Pipeline Server, the following properties must be added to the `application.yml` file, under `document-pipelines` settings:

- **host**: the hostname or ip from the server
- **port**: the port for the document pipelines, by default is 4032
- **timeout**: the timeout that will be used in the calls performed by the client

```
archive-center:
  # Archive Center Instance URL
  url: http://localhost:8080
  # Document Pipelines configuration
  document-pipelines:
    host: localhost
    port: 4032
    timeout: 15s
```

Please note that each Fuse Management Client for OpenText Archive Center instance can only be connected to one OpenText Document Pipeline Server.

5. Fuse Management Central Administration

This chapter explains how to configure Fuse Management Central interactively using its Administration pages, allowing Fuse administrators to adjust all of the application features.

To access **Fuse Management Central Administration** area:

1. **Open** Fuse Management Central:

```
http://<fuse-management-central-host>:2100
```

2. Login with your authentication credentials:
    - **Username**: `fuseadmin` *(default)*
    - **Password**: `fuseadmin` *(default)*
3. Click **Fuse Administration** on the navigation menu

5.1. Security

By default, Fuse Management Central has a built-in administrator user account named `fuseadmin`, which cannot be deleted.

This chapter describes how to change this user account password and email.

5.1.1. Change *fuseadmin* password

For security reasons, is highly recommended to change the `fuseadmin` user default password.

To change `fuseadmin` default password:

1. On Fuse Management Central Administration area, click **Security**
2. Fill the following fields and click **Change Password**:
    - **Current password** *(Default: `fuseadmin`)*
    - **New password**
    - **Confirm password**

5.1.2. Change *fuseadmin* email

To change `fuseadmin` email address:

1. On Fuse Management Central Administration area, click **Security**.
2. Insert or update the email address and click **Submit**.

5.2. General

To allow your systems to communicate with Fuse Management Central, the **API Endpoint** URL must be updated with its FQDN URL.

> To allow systems to dispatch their metrics to Fuse Management Central, the **API Endpoint** URL must be accessible by all managed systems.

To update the **API Endpoint** URL:

1. On Fuse Management Central Administration area, click **General**.
2. Under the **Fuse Management Central URL** section, update the **API Endpoint** URL and click **Update**:

> Please note that the **API Endpoint URL is built-in on your license key file, changing it will invalidate your current license and automatically deactivate all systems!**.
> Before changing Fuse Endpoint URL please request an updated license providing the new license data.

5.3. License

A valid license is required for Fuse Management Central to properly operate. By default, **when installed for the first time, Fuse Management Central has no license applied**.

Please note that **under the following license scenarios, Fuse Management Central will have limited functionality**:

- **Not Licensed** *(No license file found in the `license` folder)*
- **Invalid License** *(License data mismatch Fuse Management Central API Endpoint)*
- **Trial License Expired** *(The current trial license period has expired)*
- **Subscription License Expired** *(The current subscription license period has expired)*

Fuse Management Central can support multiple OpenText system types, currently OpenText Content Server and/or OpenText Archive Center, each one requiring its own license key file to enable its management functionalities.

5.3.1. Fuse Management Central for Content Server License

Fuse Management Central for Content Server has the following license models available:

Type	Description
Perpetual License - Per User	Limited to OpenText Content Server/Extended ECM total Standard Named Users.

Type	Description
Perpetual License - Per Managed System *(For MSP Only)*	Limited to a total of managed systems.
Subscription License - Per User	License issued monthly and limited to OpenText Content Server/Extended ECM total Standard Named Users.
Subscription License - Per Managed System *(For MSP Only)*	License issued monthly and limited to a total of managed systems.

5.3.2. Fuse Management Central for Archive Center Server License

Fuse Management Central for Archive Center has the following license models available:

Type	Description
Perpetual License - Per Managed System	Limited to a total of managed systems.
Subscription License - Per Managed System	License issued monthly and limited to a total of managed systems.

5.3.3. Request License

When requesting your license, either for OpenText Content Server and/or OpenText Archive Center, please provide the following information when contacting the software **Support** channel or your **Account Executive**:

- **System Type** *(OpenText Content Server or OpenText Archive Center)*
- **Trial Period** *(Trial License Only)*
- **Customer Name**
- **Fuse Management Central URL (API Endpoint)**
- **Total Managed Systems** *(For "Per Managed System" license models)*
- **Total System Named Users** *(Total OpenText Content Server/Extended ECM total Standard Named Users)*

Please note that each OpenText solution requires its own Fuse Management Central license key file in order to enable that solution functionalities. Once you receive your license file(s) you must ensure that each solution license file has the proper name:

- **OpenText Content Server** license file: `otcs-key.license`

- **OpenText Archive Center** license file: `otac-key.license`

Please be aware that when a license is issued all the above data will be hardcoded in it, meaning that any change on this data requires an updated license.

5.3.4. Apply License

To apply your license, please execute the following steps:

1. On Fuse Management Central main menu, navigate to **Fuse Administration > Administration**
2. Navigate to the **License** section
3. For each license file, accordingly with the license type (OTCS and/or OTAC), **upload** the license file in the corresponding area.
4. Validate on **License Information** if the license was updated successfully.

5.3.5. Validate License Status

To validate your license status:

1. On Fuse Management Central Administration area, click **License**.
2. Validate if your **License Information** data is correct and if Fuse Management Central license status is valid.

When Fuse Management Central is running using an invalid license (trial expired, Fuse Management Central URL mismatch, …), will cause all managed systems to automatically deactivate, limiting Fuse Management Central functionality.

5.4. OTDS Integration

Fuse Management Central has a built-in administrator user account (`fuseadmin`), which cannot be deleted.
In order to allow other users to access Fuse Management Central it must be integrated with OpenText ™ Directory Services (OTDS).

Fuse Management Central has a native OTDS integration, leveraging its authentication capabilities while allowing a centralized user management.

5.4.1. Create OTDS Resource

For Fuse Management Central to integrate with OTDS, a resource is required to be created on OTDS.

To create the OTDS resource:

1. Open OTDS Administration (e.g. `http(s)://otds.company.com:8080/otds-admin`)
2. From the web administration menu, click **Resources**.
3. On the button bar, click **Add**. The New Resource wizard will guide you through the steps to create a new resource.
4. On the **General** page:
    a. In the **Resource Name** box, type a descriptive name for this resource (e.g. *Fuse Management Central*).

    Please note that the name you type here cannot be edited later.

    b. *(Optional)* In the **Display Name** box, you can optionally type a different resource name.
    c. *(Optional)* In the **Description** box, you can optionally type a short resource description.
    d. Leave all other options with default values and click **Next**.
5. On the **Synchronization** page, make sure that **User and group synchronization** option is not checked, and click **Next**.
6. On the **Principal Attribute** page, leave all options with default values and click **Save**.
7. In the **Resource Activation** window, copy or write down the resource identifier.

Add users and/or groups to the created Resource

Once the OTDS Resource for Fuse Management Central is created, OTDS will automatically create an Access Role named "Access to <*ResourceName*>". Users and/or groups who will be able to login to Fuse Management Central must be added to this Access Role.

For more detailed information regarding OTDS functionality, please refer to OpenText ™ Directory Services documentation.

5.4.2. Activate OTDS Resource

To activate Fuse Management Central with OTDS:

1. On Fuse Management Central Administration area, click **OTDS Integration**
2. Fill the following fields and click **Activate**:
    - **OTDS URL**: *The FQDN address of the OTDS Server (e.g. `http(s)://otds.company.com:8080`)*
    - **OTDS Resource ID**: *The ID of the resource that has been created in OTDS*

Once activated, the OTDS resource activation status will only be displayed when authenticating in Fuse Management Central using an OTDS account with administrative privileges (e.g. `otadmin@otds.admin`).

5.4.3. Configuring Fuse Management Central Access Roles

To manage user privileges a set of access roles are available in Fuse Management Central, each one with specific privilege sets:

Access Role	Privilege Description
Fuse Admin	Permits access Fuse Administration area, allowing full control over Fuse Management Central. In addition to these privileges this role also has all privileges of **System Admin** role.
System Admin	Can manage all systems, allowing to perform actions on them e.g. Restart, Apply Configurations, etc…
Guest	Limited privileges role, for users with "read-only" access, meaning that no management actions can be performed allowing only to observe monitoring metrics.

To allow users to authenticate in Fuse Management Central using OTDS, these access roles **must be mapped with one or more OTDS groups** from both synchronized or unsynchronized partitions, depending on your OTDS partition scenarios.

To map an OTDS group with a Fuse Management Central access role:

1. Login to Fuse Management Central using the `otadmin@otds.admin` OTDS user account.
2. On Fuse Management Central Administration area, click **OTDS Integration**.
3. **Map** each role by selecting or inserting one or more OTDS groups to each role field.
4. click **Save roles**.

> ! Please note that **all OTDS groups mapped with Fuse Management Central access roles must be added to Fuse Management Central OTDS Access Role**.
> This access role is automatically created when the Fuse Management Central resource is created in OTDS.

5.5. Add New System

This section will guide you through the process of adding a new OpenText ™ system to Fuse Management Central.

Before starting, ensure that:

- ✅ You have the appropriate OpenText Content Server or OpenText Archive Center Fuse Management Client installed on your system
- ✅ Fuse Management Central can access your system:

- OpenText Content Server
  - Fuse Management Client for OpenText Content Server runs as a module installed inside OpenText Content Server, so you need to be able to access OpenText Content Server CGI URL *(e.g.* `http(s)://otcs.company.com/otcs/cs.exe`*)*

> Please note that the first time a OpenText ™ Content Server system is added to Fuse Management Central, it cannot be running under **Eclipse (CSIDE)**. If so, is mandatory to **close Eclipse (CSIDE)** and run OpenText Content Server service, then wait until Fuse Management Central scans all of your system's components.

- OpenText Archive Center
  - Fuse Management Client for OpenText Archive Center runs as a standalone application, so you need to be able to access Fuse Management Client for OpenText Archive Center URL: *(e.g.* `http(s)://otac.company.com:8081`*)*

Your system can access Fuse Management Central (e.g. `http://fuse.company.com:2100`)

5.5.1. Activation Request

1. Access Fuse Management Central:

```
http://<fuse-management-central-host>:2100
```

2. **Login** with your authentication credentials:
   - **Username**: `fuseadmin` *(default)*
   - **Password**: `fuseadmin` *(default)*
3. Click **Systems** on the navigation menu
4. Click **Add System**
5. Fill the following fields, following all wizard steps:

Field	Description
System Type	*OpenText Content Server* or *OpenText Archive Center*
System URL	* For OpenText Content Server: URL to Content Server CGI *(e.g.* `http(s)://otcs.company.com/otcs/cs.exe`*)* * For OpenText Archive Center: URL to Fuse Management Client for OpenText Archive Center *(e.g.* `http(s)://otac.company.com:8081`*)*

Field	Description
Username	User account with system login privileges (e.g. *"otadmin@otds.admin"*)
Password	User account password
Environment	Environment name (e.g. *"DEVELOPMENT"*) **Please note that only systems belonging to the same cluster can be added to the same environment. Mixing systems from different clusters on the same Fuse Management Central environment will cause system deactivation**!
System Name	System name or alias (e.g. *"LV181"*)
Advanced Options	
(Optional) **Description**	System description to help system identification (e.g. *"Partner sandbox"*)
(Optional) **Owners**	System owner(s) email(s) (e.g. *"john.doe@company.com"*), for event email notifications
(Optional) **Tags**	System tags (e.g. *"front-end"*)

System tags can be very useful when logically grouping systems, allowing you to filter them when, e.g. applying configurations, performing bulk actions, …

6. Click **Test Connection** to validate that your system fulfills all requirements

If connection test is not successful, please **review all system parameters** (System URL, credentials, …) and try again.

7. Click **Finish**
8. Next, copy **System ID** and send it to your system administrator to authorize Fuse Management Central activation request

5.5.2. Authorize Activation

For OpenText Content Server:

1. Open **Content Server Administration** page in a web browser.
2. If prompted, enter the Administrator password, and then click **Log-in**.
3. Select **Fuse System Administration > Fuse System Activation**.

4. Insert the provided **System ID** and click **Activate**
5. Your system is now **activated** and Fuse Management Central can start manage and monitoring it

For OpenText Archive Center:

1. Open **Fuse Management Client for OpenText Archive Center** web page in a web browser.
2. If prompted, login with OpenText Archive Center authentication.
3. You should see a pending activation request
4. Insert the provided **System ID** and click **Activate**
5. Your system is now **activated** and Fuse Management Central can start manage and monitoring it
6. **Next step:** Configure the log settings for OpenText Archive Center. You should indicate the ECM logs path and the Tomcat logs path.

The logs path configuration is **required** in order to be able to remotely open, view and download OpenText Archive Center logs directly from Fuse Management Central.

If the authorize activation process fails, please check if all requirements are fulfilled and review the procedure.

5.6. Integration Channels

Integration channels allow Fuse Management Central to integrate with SMTP and/or 3rd Party incident management or alert systems, to easily notify teams about OpenText performance or health issues.

Notifications Timezone

Communications made from Integration Channels have a specific timezone setting. This timezone is used to compose the messages sent to the configured Integration Channels, for example for the alert dates sent in email notifications or dates in ServiceNow incident comments.

The timezone used in these notifications can be changed in **Fuse Administration > Administration > Integration Channels**, in the **General Configurations** section.

5.6.1. SMTP

To enable email notifications for Fuse Management Central alerts, operations, etc… you must first configure the SMTP Settings.

1. On Fuse Management Central Administration area, click **Integration Channels**
2. On the **SMTP** panel, fill in the following information:

a. **Enabled**: *Enable or disable the SMTP integration.*

b. **Sender Email**: *Type the email address that will be used as the "From" address in all email notifications sent by Fuse Management Central.*

c. **SMTP Host**: *The FQDN hostname of the SMTP server to which Fuse Management Central will connect in order to send email.*

d. **SMTP Port**: *The port number used by the SMTP server.*

e. *(Optional)* **SMTP Username**: *If your SMTP server requires it, type the username to be used in the connection to the SMTP server.*

f. *(Optional)* **SMTP Password**: *If your SMTP server requires it, type the password for the username you typed in the previous step.*

g. **Enable StartTLS**: *Enable this option if your SMTP server requires TLS.*

h. **Enable SSL**: *Enable this option if your SMTP server requires SSL.*

3. Click **Send test email** and validate if you have received a test email notification.

> ! The test email notification will be sent to the email defined on your user account. If you are authenticated with the `fuseadmin` user account, this user account email must be properly set.

4. Click **Update** to save your SMTP configurations.

5.6.2. Checkmk Integration

Checkmk is one of the leading tools for Infrastructure and Application Monitoring, offering both Open Source and Enterprise license models.

Fuse Management Central offers a seamless integration with **Checkmk**, with an agent plug-in specifically designed to connect your Fuse Management Central instance to Checkmk.

Using the data provided by the Alerts API, the plug-in will add a complete list of Services to be monitored in Checkmk, from your OpenText Content Suite.

The shared information is related to **active alerts** and it is grouped by **System Type**, **System Name** and **Component**. It also offers alert monitoring for specific **Environment** scope alerts, as well as **Fuse Management Central** instance and administration alerts.

Checkmk Plug-in Download

To download the Fuse Management Central plug-in for Checkmk go to **Checkmk Exchange** and download the following package:

- **OpenText Fuse Management Central Plug-in**

Checkmk Plug-in Installation and Configuration

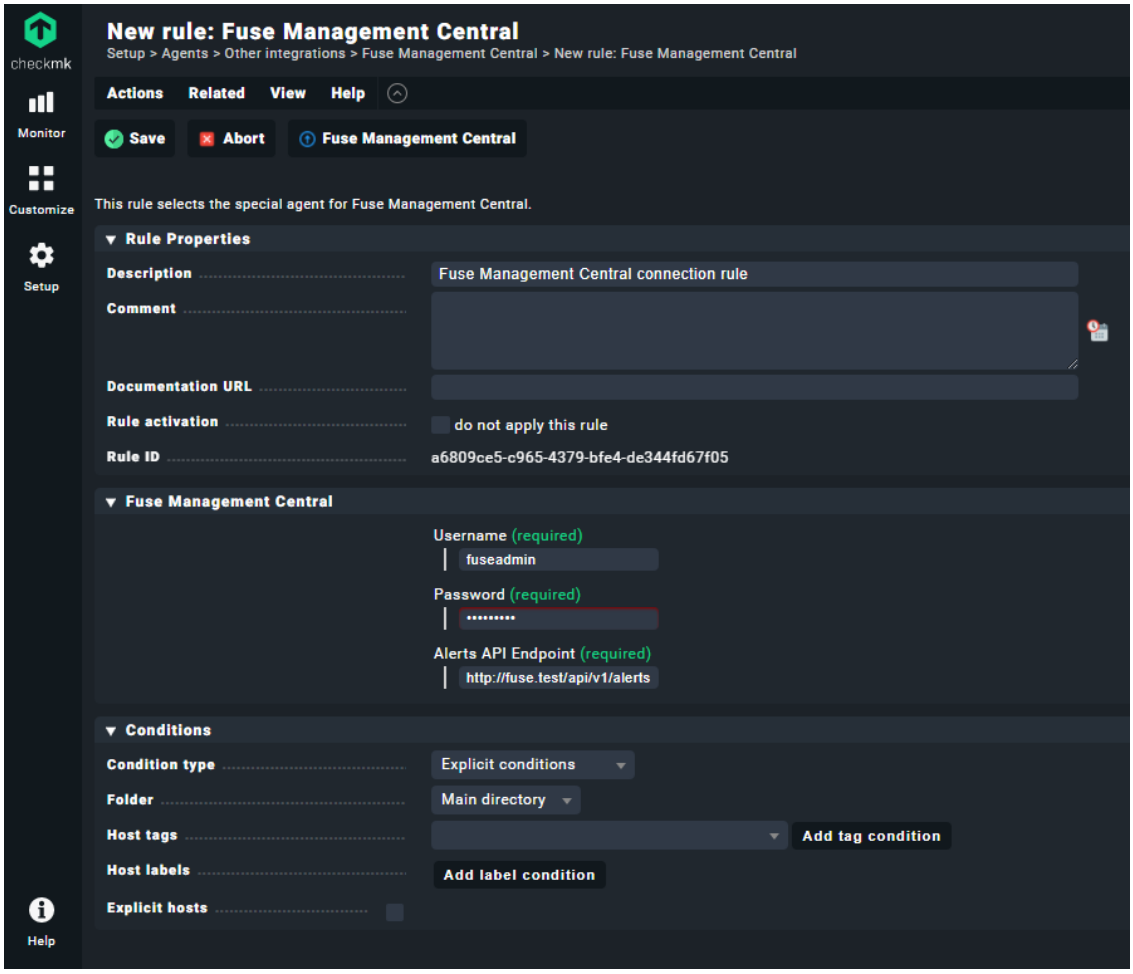
To install the Fuse Management Central plug-in in Checkmk follow these steps:

- Go to **Setup > Extension packages**.
- Click in **Upload package** and upload the recently downloaded Fuse Management Central package.
- Click in **Upload & Install**.

Configuration steps

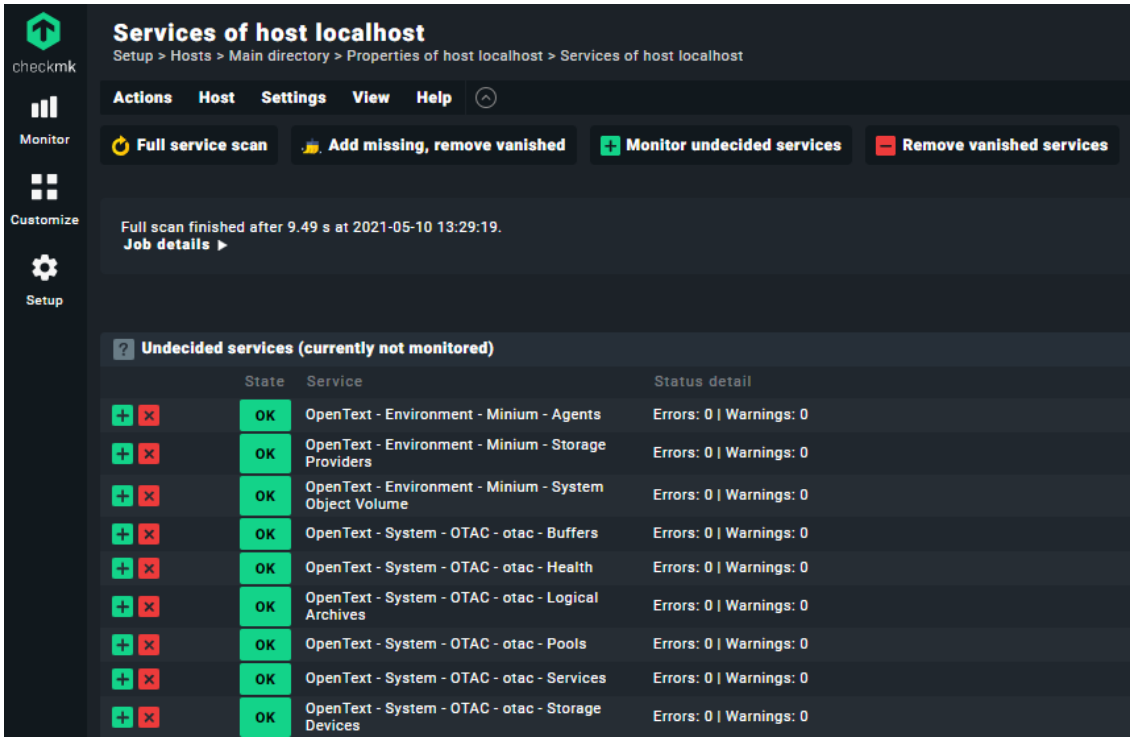
Now you have the Fuse Management Central plug-in in your Checkmk and you can configure it:

- Go to **Setup > Other integrations > Fuse Management Central**
- **Create a new rule** with the Fuse Administrator credentials (username and password) and the URL for the alerts API.
    - The Alerts API URL should be `http://[fuse-host]:[fuse-port]/api/v1/alerts/`.



After creating the rule for the Fuse Management Central plug-in, create a new host, and in the

Service Configuration page you can discover the Fuse services and add them to be monitored.



In order to correctly see the Fuse services summary, you need to go to **Setup > Services > Service monitoring rules > Escape HTML in service output** and create a rule for the host with the Fuse services to **don't escape html**.

Instance Service

The Fuse Management Central instance service has the name **Fuse Management Central - Instance**, this service will always appear.

If Checkmk can connect to the configured Fuse, it will have the state **OK**. If it can't connect to Fuse, it will have the state **CRIT** and the summary will have more information about why it could not connect to Fuse.

Other Services

For each pair **System - Component** type, you will have a service with the name **OpenText - System - [system type] - [system name] - [component type name]**.

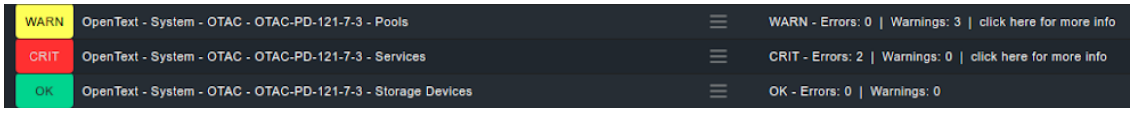
The same happens for the Environments, for each pair **Environment - Component** type, you will have a service named **OpenText - Environment - [environment name] - [component type name]**.

For the Admin component types, you will have one service for each, named **Fuse Management Central - [component type name]**.

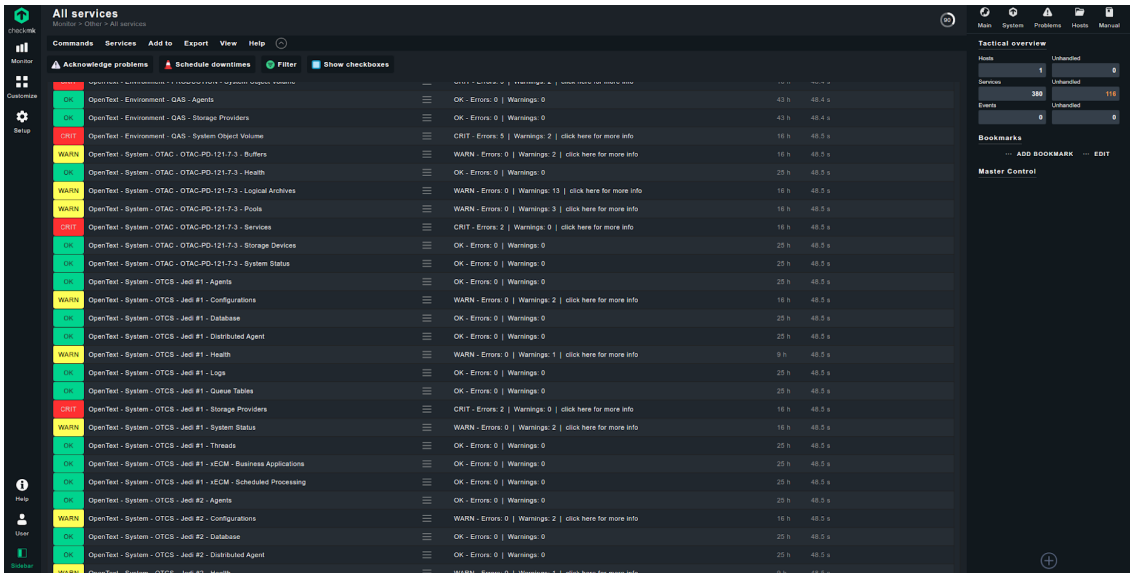
In these services you will be able to see the number of errors and warnings in their summary.

Regarding the state, they can have one of the following states:

- **OK** - there are no errors or warnings
- **WARN** - there are some warnings but no errors
- **CRIT** - there are errors



If a service is in the state **WARN** or **CRIT**, you will have a link to Fuse Management Central in its summary. The link will redirect you to the Fuse Management Central Alerts page with the correct filters selected, so you can see more details of the errors/warnings.



5.6.3. ServiceNow Integration

This integration allows Fuse Management Central to integrate with ServiceNow incident management to easily notify teams about OpenText performance, operation or health issues detected by Fuse Management Central.

ServiceNow Integration Setup

To enable ServiceNow notifications for Fuse Management Central alerts, you must first configure the ServiceNow Settings.

1. On Fuse Management Central Administration area, click **Integration Channels**
2. On the **ServiceNow** panel, fill the following information:
    a. **Enabled**: _Enable or disable the ServiceNow integration.
    b. **ServiceNow URL**: _Your ServiceNow instance URL, for example

https://dev115171.service-now.com.

c. **Username**: *Username to be used in the connection to the ServiceNow service.*

> ! User provided must have permissions to create and update incidents. Also, to be able to get all the possible configurations, the user needs to have permission to perform the following API calls listed in the end of the section.

d. **Password**: *Password for the username typed in the previous step.*

3. Click **Connect** to validate configuration provided. When settings are correct, the **Incident Settings** area is expanded.

> On this area you can configure some extra settings. None of those settings are required, but they will help ServiceNow incidents to be typified

a. Incident Status

i. *(Optional)* **New Incident**: *State selected will be used as default state when an incident is created.*

ii. *(Optional)* **Resolve Incident**: *State selected will be used as default state when an incident is resolved.*

b. Incident Severity

i. *(Optional)* **Warning Alert**: *Mapping between Fuse Alert severity type WARNING into ServiceNow severity optio.n*

ii. *(Optional)* **Error Alert**: *Mapping between Fuse Alert severity type ERROR into ServiceNow severity option.*

c. Additional Incident Fields *(depending on your ServiceNow configurations, settings below may or may not be displayed)*

i. *(Optional)* **Assignment Group**: *Group selected will be used as default assignment group when an incident is created.*

ii. *(Optional)* **Contact Type**: *Contact type selected will be used as default contact type when an incident is created.*

iii. *(Optional)* **Incident Area**: *Area selected will be used as default incident area when an incident is created.*

d. Static Settings *(these settings cannot be changed)*

i. **Caller**: *The Caller is a static field based on the user serviceNow account provided previously.*

ii. **Short Description**: *Incident title used when an incident is created.*

iii. **Description**: *Incident description used when an incident is created.*

4. Once all configurations are set according to your needs, press **Update** to save the configuration.

To work as expected, Fuse needs access to the following ServiceNow's endpoints:

HTTP method	API call
GET	{ServiceNow_URL}/api/now/table/sys_user?sysparm_query=user_name={username}&sysparm_fields=user_name,sys_id,roles
GET	{ServiceNow_URL}/api/now/table/sys_user_group?sysparm_fields=sys_id,name
GET	{ServiceNow_URL}/api/now/table/u_category?sysparm_fields=sys_id,u_incident_area
GET	{ServiceNow_URL}/api/now/table/sys_choice?name=incident&element={field}&language=EN&sysparm_fields=label,value
POST	{ServiceNow_URL}/api/now/table/incident
PUT	{ServiceNow_URL}/api/now/table/incident/{id}

5.7. Alert Manager

Fuse Management Central uses an Alert Manager to automatically detect system anomalies and consequently triggering real-time alerts. These alerts are used to report on warning or error situations, such as performance degradations, failing agent schedule, lack of resources, among others…

5.7.1. Integration Channels

The current supported integration channels are:

Channel	Description
User Interface *(Default)*	Notification events are displayed on Fuse Management Central user interface, being displayed on the events list and adjusting the failing component style, providing real-time feedback to users.
SMTP	If the SMTP Settings are properly set, alert notifications will be sent by email to system owners.
ServiceNow	If the ServiceNow Setup is properly set, alert notifications will be sent to ServiceNow.

To manage an alert integration channel:

1. On Fuse Management Central Administration area, click **Alert Manager**.
    a. **Click** on the ON/OFF toggle button to fully disable the alert for all integration channels.

b. **Click** on the specific integration channel (e.g. "SMTP") toggle button to disable it from being dispatched to that integration channel.

2. Click **Update** to save your new settings.

5.7.2. Metric Thresholds

Fuse Management Central system monitoring is based on numerous built-in, predefined metric thresholds. These default thresholds are set based on common usage scenarios but can be adjusted to fit your organization requirements.

To change the default metric thresholds:

1. On Fuse Management Central Administration area, click **Alert Manager**.
2. **Adjust** each alert threshold, to fit your requirements.
3. Click **Update** to save your new settings.

5.7.3. Dismissing Alerts

Fuse Management Central allows to dismiss alerts for specific components inside a specific system or environment.

On **Alert Manager** page, Fuse Administrators can check existent dismiss rules for any alert. These rules are listed inside each alert section and can be removed easily by **clicking** in the **Trash icon**.

It is possible to filter the alerts list by alerts which have any Dismiss Rules, by using the **Dismissed Alerts** filter on the top of the list, selecting the option **With Dismissed Rules**. This should facilitate searching for a Dismiss Rule.

5.8. Alerts API

Fuse Management Central provides a REST API to deliver a summary of all active alerts, allowing alerts integration with third-party centralized monitoring solutions.

Fuse Management Central Alert API is available in the following endpoints:

Endpoint	Description
`http://[host]:[port]/api/v1/alerts/layout`	**Layout Endpoint** - Layout and details of the existent Environments, Systems and Component Types
`http://[host]:[port]/api/v1/alerts/summary`	**Summary Endpoint** - Summary of all alerts, grouped by Environment, System and Component Type

5.8.1. Alerts API Endpoints

Layout Endpoint

The Layout API endpoint provides an overview on the existent Systems, Environments and Component Types, as well as the Component Types used to classify Fuse Administration alerts.

This information works as metadata to be cross-referenced by other endpoints of the API.

Summary Endpoint

The Summary API endpoint provides a summary list of current active alerts, grouped by Environment, System and Component Type.

The following attributes are provided for each entry:

Attribute	Description
`envId`	Unique identifier of the Environment
`systemId`	Unique identifier of the System
`componentType`	Unique identifier of the Component Type
`errors`	Total number of error alerts
`warnings`	Total number of warning alerts
`link`	Link to Fuse Management Central alert details page, with pre-configured filters for the alerts included in the summary entry

Summary entry use cases

Each summary entry can have one or multiple attributes missing, accordingly to which type of alerts is representing:

Attributes	Description
`systemId` is null but `envId` exists	These are Environment alerts, exclusive to the Environment scope.
`systemId` is null and `envId` is null	These are Administration alerts, exclusive to Fuse Administration scope.
`errors` is null	No error alerts to report.

Attributes	Description
`warnings` is null	No warning alerts to report.

Systems

List of all Systems in Fuse Management Central.

The following attributes are provided for each System:

Attribute	Description
`id`	Unique identifier of the System
`name`	Name of the System in Fuse Management Central
`type`	Type of the System (*OTCS* or *OTAC*)
`componentTypes`	List of Component Types existent in that System, identified by `id` and `displayName`.

Environments

List of all Environments in Fuse Management Central.

The following attributes are provided for each Environment:

Attribute	Description
`id`	Unique identifier of the Environment
`name`	Name of the Environment in Fuse Management Central
`componentTypes`	List of Component Types existent in that Environment, exclusive to the Environment scope, identified by `id` and `displayName`.

Admin

Fuse Administration alerts metadata.

The following attributes are provided:

Attribute	Description
`componentTypes`	List of Component Types existent to classify Admin alerts, identified by `id` and `displayName`.

5.9. Backup and Restore

Fuse Management Central deals with large amounts of data in different databases. It is highly recommended that you keep recurrent backups of the stored data, avoiding losing any data in case of unfortunate events.

5.9.1. Backup Fuse Management Central Data

All data stored by Fuse Management Central is saved into 2 different databases:

1. **Fuse Management Central Database** - A PostgreSQL database, used to store the application model and system metadata information.
2. **Fuse Management Central Metrics Database** - A Prometheus time series database, used to store system metrics and alerts data.

Both databases are located in the "Data Directory" that you selected during installation, usually `C:\ProgramData\Fuse Management Central`.

We strongly recommend to keep recurrent backups of this folder and its subfolders, since the databases can be later associated with a clean installation of Fuse Management Central if needed.

It is highly recommended that you stop all Fuse Management Central services before taking a backup of the folder. Backups during runtime can result in incomplete or corrupted data.

5.9.2. Restore a Backup

If you have a previous backup of the Data Directory folder being used by Fuse Management Central (usually `C:\ProgramData\Fuse Management Central`), you can use that folder as a restore point to a new installation of Fuse Management Central.

Restore to new installation

In order to restore Fuse Management Central with that data, simply make a new installation pointing the Data Directory to the existent restore folder that you have, instead of a new location. Bear in mind that this new installation will use this new folder as its Data Directory from now on, so choose a convenient location for that folder before the installation (we recommend `C:\Program Data\Fuse Management Central`).

Restore to current installation

If you don't want to do a new installation you can always replace the current Data Directory by your backup, just be sure to **stop all Fuse Management Central services** before replacing the current data with the backup.

Restore Considerations

After restoring a previous backup, some controlled errors may occur that may need your attention:

- Loss of data between the restore point and the current point will occur
- Licensing issues that may lead to deactivated systems
    - You may need to get and apply a new license and activate all systems again, if your license information is different now
    - New installation won't have license applied
- Fuse Management Central configurations, such as Hostname, API Endpoint and License may be different now
- OTDS Integration may need to be checked in case the hostname has changed

There are several possible problems that may have led to this situation, so any other kind of errors may occur and we are not able to prevent them all. If you find other problems or have difficulties restoring your data, please contact product.support@vilt-group.com for assistance.

6. Uninstall Fuse Management Central

This chapter describes how to remove Fuse Management Central from a host server.
If you are upgrading to a newer version of Fuse Management Central, it may be necessary to uninstall the older version.

6.1. Uninstall on Microsoft Windows

Fuse Management Central uses a Windows Installer to remove components from a Windows platform. The program is designed to remove all program files installed at the time of the Fuse Management Central installation.

> **!** The uninstall process **will not remove any configuration and long term metric data**. This is beneficial because you can retain these data files for use if you upgrade your Fuse Management Central software.
> To force the deletion of all Fuse Management Central data files, please contact product.support@vilt-group.com.

To uninstall Fuse Management Central on Windows:

1. Stop all Fuse Management Central services.
2. Using the Windows application for removing programs (for example, **Programs and Features**), select Fuse Management Central installer and then click **Uninstall**.
3. Use the uninstall wizard automatically to remove all Fuse Management Central installed components.

7. Appendix A - Troubleshooting

7.1. Known Issues and Workarounds

This section describes scenarios that users may run into and how to troubleshoot and workaround or fix them.

7.1.1. Metrics not available after installation or upgrade

In some Content Server installations, after installing/upgrading and activating a system, the metrics might not be available and your System will appear offline. In that case there are several things to check:

- If the installation / upgrade of the Fuse Management Central module does not complete the system restart correctly. Try restarting Content Server manually.
- Check if the firewall is blocking http requests between Fuse Management Central installation and the System being activated.
- Check Fuse Management Client logs to make sure metrics are being dispatched:
  - Change log level to 'DEBUG', using *<Content_Server_URL>?func=fuseclient.ConfigureLogging* or using Fuse Management Central logs widget configuration (please refer to the **Logs** section of Fuse Management Central User Guide)
  - Check the logs in the OTCS log directory with the name `fuseclient<date>.log`

7.1.2. Error when adding a new System with https

When adding a new system with https an error message similar to the following one might be displayed:

```
Failed to connect
Resource not reachable: I/O error on POST request ()...) unable to find
valid certification path to requested target
```

In this case, the public SSL certificate from the system must be imported to the JVM truststore used to run Fuse Management Central: example guide on how to import the certificate

7.1.3. Fuse Metrics Database corrupted files

Sometimes some data files in Fuse Metrics Database can get corrupted, preventing the Metrics service to start. We found that this commonly happens in these scenarios:

- Fuse Metrics Database service was not shutdown correctly
- Disk ran out of space

If this happens we suggest shutting down Fuse Management Central (all services) and then restart Fuse Management Central (all services).

At this point some errors may appear when restarting Fuse Metrics Database, in case there are corrupted data files. If an error appears when starting Fuse Metrics Database, please check the Fuse Metrics Database logs. Errors like these should be being logged:

```
err="opening storage failed: block dir:
\"data\\\\01E270EBZ1YPKF7BB2WZ38H5SV\": open
data\\01E270EBZ1YPKF7BB2WZ38H5SV\\meta.json: The system cannot find the
file specified."
```

or

```
err="opening storage failed: found unsequential head chunk files 23 and
25"
```

In order to fix this, the folder or file specified in the log message, for example *01E270EBZ1YPKF7BB2WZ38H5SV* or chunk files *23* and *25*, should be deleted. These folders can be found in the Fuse Metrics Database installation folder, inside the **data** or **data/chunks_head** folders.

This process should be repeated for each folder or file that appears on the logs until Fuse Metrics Database is able to start with no errors.

7.1.4. Uninstall Fuse Management Client for OpenText Content Server (16.2.2, 16.2.3, 16.2.4)

For the Content Server versions **16.2.2**, **16.2.3** and **16.2.4**, we found out that the standard soft-restart is not enough to reload all the loaders required for Fuse Management Client, so we suggest you to restart the processes/services of Content Server to make sure everything was updated.

7.1.5. Fuse Management Central unable to connect with ServiceNow

To configure ServiceNow in Fuse, the user provided must explicitly have one of the following roles: **admin**, **itil** or **itil_admin**.

If the user has one of the required roles, but you are still getting the error message informing that the user does not have permission to create or update incidents when trying to connect, please add the following configuration to **aplication.yml** located at `<fuse_installation_folder>/config/` (e.g. `C:\Program Files (x86)\Fuse Management Central\config\`).

```
service-now:
  roles:
    - admin
    - itil_admin
    - itil
```

7.1.6. CPU Usage not being displayed in Windows systems

Fuse Client needs permission to access the performance of the CPU in Windows systems. If the CPU usage chart is not displaying any data, maybe Fuse Client does not have the required permissions to retrieve it.

The Windows User running Fuse Client needs to belong to one of the following groups:

- Performance Log Users
- Performance Monitor Users

It is also possible that Windows system counters do not exist. You can check it by trying to open Windows Performance Monitor. For more information about system counters and how to rebuild them, please refer to official Microsoft documentation (Manually rebuild performance counters for Windows Server).

7.1.7. SELinux blocking Fuse Management Client for OTAC execution

If you have SELinux in your system, it might block the execution of the Fuse Client binary (`/path/to/fuse/client/fuse-client-otac.jar`).

If you try to run Fuse Client OTAC and it doesn't start, check your SELinux alerts and check if it's being blocked. If so, you'll need to change your SELinux policies and settings to allow the execution of `fuse-client-otac.jar`.

Sometimes a simple restore of the SELinux context is enough to unblock it:

```
/sbin/restorecon -v /path/to/fuse/client/fuse-client-otac.jar
```

By default, after extraction, the `fuse-client-otac.jar` might not be categorized as an executable. If that's the case, you might need to change the SELinux context of the file with:

```
chcon --type=java_exec_t /path/to/fuse/client/fuse-client-otac.jar
```

However, this is highly dependent on your own infrastructure and policies, so you might want to consult your System Administrator.

8. Appendix B - How-Tos

This section contains some quick and basic tutorials on general topics and tools related to Fuse Management Central.

Please have into consideration that these are general tutorials with general instructions, and the correct application of them highly depends on your specific scenario and systems.

These tutorials do not replace the official documentation available for each topic or tool. Please search the web for official documentation if you want more details on a certain topic or tool.

8.1. How to install and configure Prometheus on a Linux Server

This is a quick general guide, it does not work as official documentation and it does not exempt you from consulting it. The validity of this guide will depend on your specific scenario and system.

This guide explains how to install and configure Prometheus on a Linux Server.

8.1.1. Pre-requirements

- Superuser (sudo) access to the Linux machine
- Access to the internet to download Prometheus binaries

8.1.2. Setup Prometheus

1. Go to Prometheus downloads page (https://prometheus.io/download/#prometheus) and get the correct download link for the required version, for example https://github.com/prometheus/prometheus/releases/download/v2.41.0/prometheus-2.41.0.linux-amd64.tar.gz
2. Download and extract Prometheus binaries to a folder called `prometheus-files`

This guide uses `curl` to download the binaries, but you can download them on your own way, whichever is more convenient.

```
curl -LO
https://github.com/prometheus/prometheus/releases/download/v{prometh
eus-version}/prometheus-{prometheus-version}.linux-amd64.tar.gz
tar -xvf prometheus-{prometheus-version}.linux-amd64.tar.gz
mv prometheus-{prometheus-version}.linux-amd64 prometheus-files
```

3. Create a specific user for Prometheus

```
sudo useradd --no-create-home --shell /bin/false prometheus
```

4. Create required directories and make the **prometheus** user the owner of them

```
sudo mkdir /etc/prometheus
sudo mkdir /var/lib/prometheus
sudo chown prometheus:prometheus /etc/prometheus
sudo chown prometheus:prometheus /var/lib/prometheus
```

5. Copy `prometheus` and `promtool` binaries from `prometheus-files` to `/usr/local/bin` and make the **prometheus** user the owner of them

```
sudo cp prometheus-files/prometheus /usr/local/bin/
sudo cp prometheus-files/promtool /usr/local/bin/
sudo chown prometheus:prometheus /usr/local/bin/prometheus
sudo chown prometheus:prometheus /usr/local/bin/promtool
```

6. Copy the `consoles` and `console_libraries` directories from `prometheus-files` to `/etc/prometheus` and make the **prometheus** user the owner of them.

```
sudo cp -r prometheus-files/consoles /etc/prometheus
sudo cp -r prometheus-files/console_libraries /etc/prometheus
sudo chown -R prometheus:prometheus /etc/prometheus/consoles
sudo chown -R prometheus:prometheus
/etc/prometheus/console_libraries
```

8.1.3. Setup Prometheus Configuration

This guide will create a default Prometheus configuration in `/etc/prometheus/prometheus.yml`. During the Fuse Management Central installation, you'll be required to change this configuration to a file provided by Fuse Management Central.

1. Create the `prometheus.yml` file and add a default configuration for Prometheus to monitor itself.

```
sudo vi /etc/prometheus/prometheus.yml
```

```
global:
  scrape_interval: 10s
scrape_configs:
  - job_name: 'prometheus'
    scrape_interval: 5s
    static_configs:
      - targets: ['localhost:9090']
```

2. Make the **prometheus** user the owner of the config file.

```
sudo chown prometheus:prometheus /etc/prometheus/prometheus.yml
```

8.1.4. Setup Prometheus as a Service

1. Create a Prometheus service file

```
sudo vi /etc/systemd/system/prometheus.service
```

```
[Unit]
Description=Prometheus
Wants=network-online.target
After=network-online.target
[Service]
User=prometheus
Group=prometheus
Type=simple
ExecStart=/usr/local/bin/prometheus \
    --config.file=/etc/prometheus/prometheus.yml \
    --storage.tsdb.path=/var/lib/prometheus/ \
    --web.console.templates=/etc/prometheus/consoles \
    --web.console.libraries=/etc/prometheus/console_libraries
[Install]
WantedBy=multi-user.target
```

2. Reload the systemd service

```
sudo systemctl daemon-reload
```

3. Start the Prometheus service

```
sudo systemctl start prometheus
```

4. You can check the status of the service with:

```
sudo systemctl status prometheus
```

5. You can stop the Prometheus service with:

```
sudo systemctl stop prometheus
```

8.1.5. Validate Prometheus installation

With the Prometheus service running, you should be able to access Prometheus web console on `http://<prometheus-server>:9090/graph`.

8.1.6. Possible issues and workarounds

Running Prometheus in a different Port

The previous guide assumes that port `9090` is available and Prometheus will run there. If that's not the case, the following changes must be made to make Prometheus available in a different port.

1. Add the argument `--web.listen-address=0.0.0.0:<new-port>` to Prometheus startup script
2. Change `prometheus.yml` file default target to new port

```
scrape_configs:
  - job_name: 'prometheus'
    scrape_interval: 5s
    static_configs:
      - targets: ['localhost:<new-port>']
```

This configuration might already been replaced by Fuse Management Central own configuration and the default scrape target might not exist anymore, if you already proceeded with Fuse Management Central installation.

Firewall blocking external access to Prometheus

If you cannot access Prometheus web console from an external system, your Firewall might be blocking it.

External access to Prometheus **is not mandatory**, since all components that need access to Prometheus are in the same machine.

However, if you want to test the Prometheus installation by accessing it externally, please refer to your Firewall provider official documentation and allow external access to the Prometheus port.

SELinux blocking Prometheus binary execution

If you have SELinux in your system, it might block the execution of the Prometheus binary (`/usr/local/bin/prometheus`).

If you try to run Prometheus and it doesn't start, check your SELinux alerts and check if it's being blocked. If so, you'll need to change your SELinux policies and settings to allow the execution of Prometheus.

Sometimes a simple restore of the SELinux context is enough to unblock it:

```
/sbin/restorecon -v /usr/local/bin/prometheus
```

However, this is highly dependent on your own infrastructure and policies, so you might want to consult your System Administrator.

8.2. How to install and configure AlertManager on a Linux Server

This is a quick general guide, it does not work as official documentation and it does not exempt you from consulting it. The validity of this guide will depend on your specific scenario and system.

This guide explains how to install and configure AlertManager on a Linux Server.

8.2.1. Pre-requirements

- Superuser (sudo) access to the Linux machine
- Access to the internet to download AlertManager binaries

8.2.2. Setup AlertManager

1. Go to AlertManager downloads page (https://prometheus.io/download/#alertmanager) and get the correct download link for the required version, for example https://github.com/prometheus/alertmanager/releases/download/v0.25.0/alertmanager-0.25.0.linux-amd64.tar.gz
2. Download and extract AlertManager binaries to a folder called `alertmanager-files`

This guide uses `curl` to download the binaries, but you can download them on your own way, whichever is more convenient.

```
curl -LO
https://github.com/prometheus/alertmanager/releases/download/v{alert
manager-version}/alertmanager-{alertmanager-version}.linux-
amd64.tar.gz
tar -xvf alertmanager-{alertmanager-version}.linux-amd64.tar.gz
mv alertmanager-{alertmanager-version}.linux-amd64 alertmanager-
files
```

3. Create a specific user for AlertManager

```
sudo useradd --no-create-home --shell /bin/false alertmanager
```

4. Create required directories and make the **alertmanager** user the owner of them

```
sudo mkdir /etc/alertmanager
sudo mkdir /var/lib/alertmanager
sudo chown alertmanager:alertmanager /etc/alertmanager
sudo chown alertmanager:alertmanager /var/lib/alertmanager
```

5. Copy `alertmanager` and `amtool` binaries from `alertmanager-files` to `/usr/local/bin` and make the **alertmanager** user the owner of them

```
sudo cp alertmanager-files/alertmanager /usr/local/bin/
sudo cp alertmanager-files/amtool /usr/local/bin/
sudo chown alertmanager:alertmanager /usr/local/bin/alertmanager
sudo chown alertmanager:alertmanager /usr/local/bin/amtool
```

8.2.3. Setup AlertManager Configuration

This guide will create a default AlertManager configuration in `/etc/alertmanager/alertmanager.yml`. During the Fuse Management Central installation, you'll be required to change this configuration to a file provided by Fuse Management Central.

1. Copy the default `alertmanager.yml` file from `alertmanager-files` directory to `/etc/alertmanager/alertmanager.yml`.

```
sudo cp alertmanager-files/alertmanager.yml
/etc/alertmanager/alertmanager.yml
```

2. Make the **alertmanager** user the owner of the config file.

```
sudo chown alertmanager:alertmanager
/etc/alertmanager/alertmanager.yml
```

8.2.4. Setup AlertManager as a Service

1. Create an AlertManager service file

```
sudo vi /etc/systemd/system/alertmanager.service
```

```
[Unit]
Description=AlertManager
Wants=network-online.target
After=network-online.target
[Service]
User=alertmanager
Group=alertmanager
Type=simple
ExecStart=/usr/local/bin/alertmanager \
    --config.file=/etc/alertmanager/alertmanager.yml \
    --storage.path=/var/lib/alertmanager/
[Install]
WantedBy=multi-user.target
```

2. Reload the systemd service

```
sudo systemctl daemon-reload
```

3. Start the AlertManager service

```
sudo systemctl start alertmanager
```

4. You can check the status of the service with:

```
sudo systemctl status alertmanager
```

5. You can stop the AlertManager service with:

```
sudo systemctl stop alertmanager
```

8.2.5. Validate AlertManager installation

With the AlertManager service running, you should be able to access AlertManager web console on `http://<alertmanager-server>:9093/`.

8.2.6. Possible issues and workarounds

Running AlertManager in a different Port

The previous guide assumes that port `9093` is available and AlertManager will run there. If that's not the case, the following changes must be made to make AlertManager available in a different port.

1. Add the argument `--web.listen-address=0.0.0.0:<new-port>` to AlertManager startup script

Firewall blocking external access to AlertManager

If you cannot access AlertManager web console from an external system, your Firewall might be blocking it.

External access to AlertManager **is not mandatory**, since all components that need access to AlertManager are in the same machine.

However, if you want to test the AlertManager installation by accessing it externally, please refer to your Firewall provider official documentation and allow external access to the AlertManager port.

SELinux blocking AlertManager binary execution

If you have SELinux in your system, it might block the execution of the AlertManager binary (`/usr/local/bin/alertmanager`).

If you try to run AlertManager and it doesn't start, check your SELinux alerts and check if it's being blocked. If so, you'll need to change your SELinux policies and settings to allow the execution of AlertManager.

Sometimes a simple restore of the SELinux context is enough to unblock it:

```
/sbin/restorecon -v /usr/local/bin/alertmanager
```

However, this is highly dependent on your own infrastructure and policies, so you might want to consult your System Administrator.

8.3. How to upgrade Prometheus on a Linux Server

This is a quick general guide, it does not work as official documentation and it does not exempt you from consulting it. The validity of this guide will depend on your specific scenario and system.

This guide explains how to upgrade an existent installation of Prometheus on a Linux Server.

8.3.1. Requirements and Assumptions

This guide assumes that the Prometheus installation was done as described in **How to install and configure Prometheus on a Linux Server**.

You'll need **superuser (sudo)** access to the Linux machine.

8.3.2. Upgrade Prometheus

1. Stop Prometheus service

```
sudo systemctl stop prometheus
```

2. Create a backup of Prometheus data storage directory:
    - `/var/lib/prometheus`
3. Go to Prometheus downloads page (https://prometheus.io/download/#prometheus) and get the correct download link for the required version, for example https://github.com/prometheus/prometheus/releases/download/v2.41.0/prometheus-2.41.0.linux-amd64.tar.gz
4. Download and extract Prometheus binaries to a folder called `prometheus-upgrade-files`

This guide uses `curl` to download the binaries, but you can download them on your own way, whichever is more convenient.

```
curl -LO
https://github.com/prometheus/prometheus/releases/download/v{prometh
eus-version}/prometheus-{prometheus-version}.linux-amd64.tar.gz
tar -xvf prometheus-{prometheus-version}.linux-amd64.tar.gz
mv prometheus-{prometheus-version}.linux-amd64 prometheus-upgrade-
files
```

5. Replace current `prometheus` and `promtool` binaries with the new ones and make sure the **prometheus** user is the owner of them

```
sudo cp prometheus-upgrade-files/prometheus
/usr/local/bin/prometheus
sudo cp prometheus-upgrade-files/promtool /usr/local/bin/promtool
sudo chown prometheus:prometheus /usr/local/bin/prometheus
sudo chown prometheus:prometheus /usr/local/bin/promtool
```

6. Replace the current `consoles` and `console_libraries` directories with the new ones and make sure the **prometheus** user is the owner of them

```
sudo cp -r prometheus-upgrade-files/consoles /etc/prometheus
sudo cp -r prometheus-upgrade-files/console_libraries
/etc/prometheus
sudo chown -R prometheus:prometheus /etc/prometheus/consoles
sudo chown -R prometheus:prometheus
/etc/prometheus/console_libraries
```

7. Start Prometheus service again

```
sudo systemctl start prometheus
```

8.4. How to upgrade AlertManager on a Linux Server

This is a quick general guide, it does not work as official documentation and it does not exempt you from consulting it. The validity of this guide will depend on your specific scenario and system.

This guide explains how to upgrade an existent installation of AlertManager on a Linux Server.

8.4.1. Requirements and Assumptions

This guide assumes that the AlertManager installation was done as described in **How to install and configure AlertManager on a Linux Server**.

You'll need **superuser (sudo)** access to the Linux machine.

8.4.2. Upgrade AlertManager

1. Stop AlertManager service

```
sudo systemctl stop alertmanager
```

2. Create a backup of AlertManager data storage directory:
    - `/var/lib/alertmanager`
3. Go to AlertManager downloads page (https://prometheus.io/download/#alertmanager) and get the correct download link for the required version, for example https://github.com/prometheus/alertmanager/releases/download/v0.25.0/alertmanager-0.25.0.linux-amd64.tar.gz
4. Download and extract AlertManager binaries to a folder called `alertmanager-upgrade-files`

This guide uses `curl` to download the binaries, but you can download them on your own way, whichever is more convenient.

```
curl -LO
https://github.com/prometheus/alertmanager/releases/download/v{alert
manager-version}/alertmanager-{alertmanager-version}.linux-
amd64.tar.gz
tar -xvf alertmanager-{alertmanager-version}.linux-amd64.tar.gz
mv alertmanager-{alertmanager-version}.linux-amd64 alertmanager-
upgrade-files
```

5. Replace current `alertmanager` and `amtool` binaries with the new ones and make sure the **alertmanager** user is the owner of them

```
sudo cp alertmanager-upgrade-files/alertmanager
/usr/local/bin/alertmanager
sudo cp alertmanager-upgrade-files/amtool /usr/local/bin/amtool
sudo chown alertmanager:alertmanager /usr/local/bin/alertmanager
sudo chown alertmanager:alertmanager /usr/local/bin/amtool
```

6. Start AlertManager service again

```
sudo systemctl start alertmanager
```