Advanced Authentication 6.4

Server Installation and Upgrade Guide

July 2022

Legal Notices

Contents

About this Book

This Installation guide is intended for system administrators and describes the procedure of installing, configuring, and upgrading the Advanced Authentication appliance.

Intended Audience

This book provides information for audience responsible for understanding administration concepts and implementing a secure, distributed administration model.

Advanced Authentication Overview

For an overview about Advanced Authentication, see “Introduction to Advanced Authentication”.

1 System Requirements

IMPORTANT: The Advanced Authentication appliance is based on the SUSE Linux Enterprise Server 12 Service Pack 4 operating system.

For system requirements of Advanced Authentication appliance, see Server Requirements.

For system requirements of client components, see Client Components Requirements.

Verifying SSE 4.2 Instructions on CPU

Ensure that CPU supports SSE 4.2 instructions.

To check whether your CPU supports the SSE 4.2 instructions, run the following command:

```
grep -q sse4_2 /proc/cpuinfo && echo "SSE 4.2 supported" || echo "SSE 4.2
not supported"
```

If your CPU supports SSE 4.2, the command returns a message SSE `4.2 supported`.

2 Installing Advanced Authentication

This chapter includes the following topics:

Obtaining Advanced Authentication

Advanced Authentication is available in two versions: trial and purchased.

Downloading the Purchased Version

You must have purchased Advanced Authentication to access the full version of the product. To buy a full version of Advanced Authentication, see How to Buy. The activation code is in the Customer Center where you download the software. For more information, see Customer Center Frequently Asked Questions.

To access a full version of Advanced Authentication:

1. Log in to the Software Licenses and Downloads (https://sld.microfocus.com/)portal.
2. Click **Software**.
3. In the **Entitled Software** tab, click the appropriate version of Advanced Authentication to download.

Downloading the Trial Version

You can download and install the trial version of Advanced Authentication to see how the product works.

To download the trial version:

1. Access the Download page at Software Licenses and Downloads (https://sld.microfocus.com/) portal.
2. Click the **Free Trials** link.
3. Scroll down to find NetIQ Advanced Authentication, then click **Free Trial**.

4 Specify your information to receive an email with the download link, then click **Start free trial**.

   You must specify a valid email address or you will not receive the email that contains the link to download the trial version.

5 After you receive the email, click the link and download the appropriate version for your environment.

Installing Advanced Authentication

To install the Advanced Authentication appliance, perform the following steps:

1 Ensure that your environment complies with the System Requirements.

2 Extract the file `AdvancedAuthAppliance-x.x-xxx.zip`, and use the `AdvancedAuthAppliance-x.x-xxx.iso` file.

3 Select the Advanced Authentication installation ISO file and boot the machine.

4 Select the **Install advancedauthappliance** option from the list.

5 Select **Yes** to delete all data in the SDA drive.

6 Select the appropriate language, read the license, and click **Accept**.

7 Use the following information to configure the appliance:

- **root Password**: Specify a password for the root user on the appliance.
- **NTP Server**: Specify a primary and secondary NTP server used to keep time on the appliance.
- **Hostname and Networking options**: Specify a hostname for the appliance, then select whether to use a **Static IP address** or **DHCP**. If you use a static IP address, you must specify the IP address, subnet mask, the gateway, and DNS servers.

8 Click **Finish** and wait for the appliance initialization to complete.

9 After a prompt to login is displayed on the console, you must wait for 15 minutes. Even after the wait, if you are unable to access the Advanced Authentication portals then reboot the appliance.

NOTE:

- It is not recommended to install any third-party software on the Advanced Authentication Appliance.
- While installing the Advanced Authentication appliance on some hypervisors if a black screen is displayed, it is recommended to remove the `nomodeset` parameter. For more information, see Removing the nomodeset Parameter for Better Boot Screen Performance.

IMPORTANT: The time on Advanced Authentication servers must be synchronized with NTP servers. Ensure that the NTP port 123 (UDP) is open on your corporate firewalls to allow Advanced Authentication servers to sync time on the predefined NTP servers or specify your internal NTP servers. For more information about time setting, see Configuring Time Settings (https://www.netiq.com/documentation/advanced-authentication-63/server-administrator-guide/data/time.html).

WARNING: When you log in to the console as **root** and run **yast novell-vainit**, it is recommended to not select the **Reboot** or **Shutdown** option. Otherwise, you will not be able to access the web user interface when you reboot the appliance or start the appliance after shut down.

Deploying Advanced Authentication on Amazon Web Services

NOTE: We officially support only the Amazon EKS cluster to deploy Advanced Authentication on AWS. The EC2, Fargate, or ECS methods of deployment is not supported. EKS manages high availability, data replication, and auto-scalability. Also, it reduces manual intervention, unlike the other case of deployment.

This section contains details about how to deploy Advanced Authentication on Amazon Web Services (AWS) using Kubernetes. You can deploy Advanced Authentication containers into Kubernetes clusters by using the Helm charts.

- "Prerequisites" on page 11
- "Deployment Procedure" on page 12

NOTE: The procedure in this section are based on the assumption that you know basics of how containers work.

NOTE: The Risk Service is not supported on the Advanced Authentication server that is deployed on the public cloud.

Prerequisites

In addition to the system requirements of Advanced Authentication appliance, ensure that you have completed following tasks:

- Created an administrative account on Amazon Elastic Container Service for Kubernetes (Amazon EKS).
- Configured an Amazon EKS cluster.

  For more information about how to configure an Amazon EKS cluster, see Getting Started with Amazon EKS (https://docs.aws.amazon.com/eks/latest/userguide/getting-started.html).
- Set the Node Type as T3 large and Node Volume Size as 60 GB.
- Installed `kubectl` and configured it to work with the Amazon EKS.

  For more information about installing and configuring kubectl, see install kubectl (https://docs.aws.amazon.com/eks/latest/userguide/install-kubectl.html) and configure kubectl (https://docs.aws.amazon.com/eks/latest/userguide/configure-kubectl.html).

Deployment Procedure

1. Download the `aaf-<version>-helm-chart.zip` file from Software Licenses and Downloads (https://sld.microfocus.com/) portal.
2. Unpack the zip file. You can view the `aaf-<version>.tgz` tar file.
3. Run the following command to unpack the tar file:

   ```
   tar zxvf aaf-<version>.tgz
   ```

4. Run one of the following commands to deploy three Advanced Authentication instances into the cluster:

   - For helm v3.0.0, and kubectl v1.19.6 or prior versions:

     ```
     helm install --namespace <name_of_kubernetes namespace> --
     name=<helm_chart_release_name> --set lb.enabled=true <path_of
     _helm_chart>
     ```

     For example,

     ```
     helm install --namespace aaf-test --name=aaf-test-1 --set
     lb.enabled=true ./aaf/
     ```

   - For helm v3.4.0 and kubectl v1.20.1 or later versions:

     ```
     helm install --create-namespace --namespace <name_of_kubernetes
     namespace> <helm_chart_release_name> --set lb.enabled=true
     <path_of_helm_chart>
     ```

     where, `lb` represents load balancer.

     For example,

     ```
     helm install --create-namespace --namespace aaf-test aaf-test-1 --
     set lb.enabled=true ./aaf/
     ```

   NOTE: You can deploy one instance for testing purpose. But it is highly recommended to create a cluster with multiple instances of the server for the production environment.

5. Run the following command to get the IP addresses that are assigned to each Advanced Authentication instance in the cluster:

   ```
   kubectl -n aaf-test get svc | grep LoadBalancer
   ```

NOTE: The Configuration Portal (port 9443) is not available for the Kubernetes environment. The Managing the Appliance (https://www.netiq.com/documentation/advanced-authentication-63/server-administrator-guide/data/ch-appliance-config.html) is only relevant for the appliance.

Sample Deployment

This sample explains the prerequisites and step-by-step procedure to deploy Advanced Authentication instance on AWS with minimum configuration.

Before deployment, ensure to perform the following tasks:

1. Install AWS IAM authentication. For more information see, Installing AWS IAM Authenticator (https://docs.aws.amazon.com/eks/latest/userguide/install-aws-iam-authenticator.html).

2. Install AWS CLI. For more information see, Installing AWS CLI (https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-install.html).
3. Configure AWS CLI Credentials. For more information see, Configuring AWS CLI (https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-configure.html).
4. Install eksctl. For more information see, **Install ekstcl** section in Getting Started with ekstcl (https://docs.aws.amazon.com/eks/latest/userguide/getting-started-eksctl.html).

Perform the following steps to deploy Advanced Authentication on AWS with basic configuration:

1 Run the following command to create a cluster:

```
eksctl create cluster --name prod --version 1.13 --nodegroup-name
standard-workers --node-type t3.large --node-volume-size 80 --nodes 2 -
-nodes-min 2 --nodes-max 2 --node-ami auto --zones us-east-1a,us-east-
1b
```

2 Configure cluster role binding for particular group to grant access to Advanced Authentication instance on AWS for users with the specific role.

For more information, see Role-based access control (https://kubernetes.io/docs/reference/access-authn-authz/rbac/).

WARNING: The following policy allows ALL service accounts to act as cluster administrators. Any application running in a container receives service account credentials automatically, and could perform any action against the API, including viewing secrets and modifying permissions. However, this is not a recommended policy for production environment.

```
kubectl create clusterrolebinding cluster-admin-default --
clusterrole=cluster-admin --user=system:serviceaccount:kube-
system:default
```

---

3 Run the following command to deploy Advanced Authentication instance into the cluster:

```
helm install --create namespace --namespace aaf-test aaf-test-1 --set
lb.enabled=true ./aaf_63/
```

Deploying Advanced Authentication on Azure Kubernetes Services

This section contains details about how to deploy Advanced Authentication on Azure Kubernetes Service. You can deploy Advanced Authentication containers into Kubernetes clusters by using the Helm charts.

This section includes the following:

NOTE: The procedures in this section are based on the assumption that you know basics of how containers work.

NOTE: The Risk Service is not supported on the Advanced Authentication server that is deployed on the public cloud.

Prerequisites

In addition to the system requirements of Advanced Authentication appliance, ensure that you have completed following tasks:

- Created an administrative account on Azure Kubernetes Services (AKS).
- Configured a Microsoft AKS cluster.

  For more information about how to configure a Microsoft AKS cluster, see Get started tutorial (https://docs.microsoft.com/en-us/azure/aks/kubernetes-walkthrough).
- Set the Node Size as DS3_V2 Standard.
- Installed `kubectl` and configured it to work with Microsoft AKS.

Deployment Procedure

1. Download the `aaf-<version>-helm-chart.zip` file from Software Licenses and Downloads (https://sld.microfocus.com/).
2. Unpack the zip file. You can view the `aaf-<version>.tgz` tar file.
3. Run the following command to unpack the tar file:

   ```
   tar zxvf aaf-<version>.tgz
   ```
4. Run one of the following commands to deploy three Advanced Authentication instances into the cluster:
   - For helm v3.0.0, and kubectl v1.19.6 or prior versions:

     ```
     helm install --namespace <name_of_kubernetes namespace> --
     name=<helm_chart_release_name> --set lb.enabled=true <path_of
     _helm_chart>
     ```

     where, lb represents load balancer.

     For example,

     ```
     helm install --namespace aaf-test --name=aaf-test-1 --set
     lb.enabled=true ./aaf/
     ```
   - For helm v3.4.0 and kubectl v1.20.1 or later versions:

     ```
     helm install --create-namespace --namespace <name_of_kubernetes
     namespace> <helm_chart_release_name> --set lb.enabled=true
     <path_of_helm_chart>
     ```

     where, `lb` represents load balancer.

     For example,

     ```
     helm install --create-namespace --namespace aaf-test aaf-test-1 --
     set lb.enabled=true ./aaf/
     ```

NOTE: You can deploy one instance for testing purpose. But it is highly recommended to create a cluster with multiple instances of the server for the production environment.

5 Run the following command to get the IP addresses that are assigned to each Advanced Authentication instance in the cluster:

```
kubectl -n aaf-test get svc | grep LoadBalancer
```

NOTE: The Configuration Portal (port 9443) is not available for the Kubernetes environment. The Managing the Appliance (https://www.netiq.com/documentation/advanced-authentication-63/server-administrator-guide/data/ch-appliance-config.html) is only relevant for the appliance.

NOTE: After the deployment, if you get the error message, `1 node(s) exceeds maximum volume count` then set the scaling method for the nodepool to autoscale.

For more information, see Custom Autoscale (https://portal.microfocus.com/s/article/KM000003739).

Sample Deployment

This sample explains the prerequisites and step-by-step procedure to deploy Advanced Authentication instance on Azure with minimum configuration.

Before deployment, ensure to perform the following tasks:

1. Install kubectl.
2. Configure AKS cluster.
3. Set the Node Size as DS3_V2 Standard.

Perform the following steps to deploy Advanced Authentication on Azure with basic configuration:

1 Run the following command to configure kubectl with the credentials for your AKS cluster:

```
az aks get-credentials --resource-group myResourceGroup --name myAKSCluster
```

2 Configure cluster role binding for particular group to grant access to Advanced Authentication instance on Azure for users with the specific role.

For more information, see Role-based access control (https://kubernetes.io/docs/reference/access-authn-authz/rbac/).

WARNING: The following policy allows ALL service accounts to act as cluster administrators. Any application running in a container receives service account credentials automatically, and could perform any action against the API, including viewing secrets and modifying permissions. However, this is not a recommended policy for production environment.

```
kubectl create clusterrolebinding cluster-admin-default --clusterrole=cluster-admin --user=system:serviceaccount:kube-system:default
```

---

3 Run the following command to deploy Advanced Authentication instance into your cluster:

```
helm install --create-namespace --namespace aaf-test aaf-test-1 --set lb.enabled=true ./aaf_63/
```

Post Deployment

After deploying Advanced Authentication on Azure Kubernetes Service, perform the following:

- Add an external repository (https://www.netiq.com/documentation/advanced-authentication-64/server-administrator-guide/data/add_an_extr_repo.html)
- Install Repo Agent

Deploying Advanced Authentication on Azure Kubernetes Services in an Air Gap Environment

This section contains details on the deployment of Advanced Authentication in an air gap environment on Azure Kubernetes Service. You can deploy Advanced Authentication containers into Kubernetes clusters using the docker images and Helm charts.

An air gap environment indicates a server or cluster disconnected from a public network for security. To install Advanced Authentication on an air gap environment, an administrator must download the required installation files to a server that is connected to the Internet. Then transfer them to an installation server that is not connected to the Public Internet but connected to a private intranet.

Prerequisites

In addition to the system requirements of Advanced Authentication appliance, ensure that you have completed following tasks:

- Created an administrative account on Azure Kubernetes Services (AKS).
- Configured a Microsoft AKS cluster.

  For more information about how to configure a Microsoft AKS cluster, see Get started tutorial (https://docs.microsoft.com/en-us/azure/aks/kubernetes-walkthrough).
- Set the Node Size as DS3_V2 Standard.
- Installed `kubectl` and configured it to work with Microsoft AKS.
- Perform Pre-Deployment Procedure.

Pre-Deployment Procedure

1. Download the `AdvancedAuthDocker-<version>.zip` file from Software Licenses and Downloads (https://sld.microfocus.com/).
2. Unzip the `AdvancedAuthDocker-<version>.zip` file and navigate to the `dockerimages` directory.
3. Run the following command to load the images from the docker images tgz file on your server:

   ```
   docker load -i aauth-images.tgz
   ```
4. Run the following command and verify that the images are loaded:

   ```
   docker images
   ```

   - `mfsecurity/aaf-webauth:<version>`
   - `mfsecurity/aaf-aucore:<version>`

- `mfsecurity/aaf-redis:<version>`
- `mfsecurity/aaf-repldb:<version>`
- `mfsecurity/aaf-fipsd:<version>`
- `mfsecurity/aaf-afisd:<version>`
- `mfsecurity/aaf-radiusd:<version>`
- `mfsecurity/aaf-searchd:<version>`
- `mfsecurity/aaf-webd:<version>`
- `mfsecurity/aaf-audb:<version>`
- `gliderlabs/logspout:<version>`

5 Run the following commands to retag the docker images per specifications from your internal docker repository:

```
docker tag mfsecurity/<name>:<version> <internalDocker>/
<name>:<version>
```

```
docker tag gliderlabs/<name>:<version> <internalDocker>/
<name>:<version>
```

6 Run the following command to push the newly tagged images to your internal docker repository:

```
docker push <internalDocker>/<name>:<version>
```

Deployment Procedure

1 Download the `aaf-<version>-helm-chart.zip` file from Software Licenses and Downloads (https://sld.microfocus.com/).

2 Unpack the zip file. You can view the `aaf-<version>.tgz` file.

3 Run the following command to unpack the tar file:

```
tar zxvf aaf-<version>.tgz
```

4 Modify the `values.yaml` file by replacing the default value `mfsecurity` with the value for the internal repository `internalDocker`.

5 Run one of the following commands to deploy three Advanced Authentication instances into the cluster:

- For helm v3.0.0, and kubectl v1.19.6 or prior versions:

  ```
  helm install --namespace <name_of_kubernetes namespace> --
  name=<helm_chart_release_name> --set lb.enabled=true <path_of
  _helm_chart>
  ```

  where, lb represents load balancer.

  For example,

  ```
  helm install --namespace aaf-test --name=aaf-test-1 --set
  lb.enabled=true ./aaf/
  ```

- For helm v3.4.0 and kubectl v1.20.1 or later versions:

  ```
  helm install --create-namespace --namespace <name_of_kubernetes
  namespace> <helm_chart_release_name> --set lb.enabled=true
  <path_of_helm_chart>
  ```

where, `lb` represents load balancer.

For example,

```
helm install --create-namespace --namespace aaf-test aaf-test-1 --
set lb.enabled=true ./aaf/
```

NOTE: You can deploy one instance for testing purpose. But it is highly recommended to create a cluster with multiple instances of the server for the production environment.

6 Run the following command to get the IP addresses that are assigned to each Advanced Authentication instance in the cluster:

```
kubectl -n aaf-test get svc | grep LoadBalancer
```

NOTE: The Configuration Portal (port 9443) is not available for the Kubernetes environment. The Managing the Appliance (https://www.netiq.com/documentation/advanced-authentication-63/server-administrator-guide/data/ch-appliance-config.html) is only relevant for the appliance.

3 Getting the Latest Online and Offline Updates

WARNING: All updates and upgrades must be initiated from the Appliance Configuration console (:9443/vaconfig/update or :9443/vaconfig/upgrade).

Use the **Online Update** option to register for the online update service from the Software Licenses and Downloads portal (https://sld.microfocus.com/).

To activate the Update Channel, you must obtain the key from the Customer Center. If the key is not available, contact the Customer Center through an email.

WARNING: Before performing the online update, ensure to add rules in the firewall to allow https traffic to the URLs, such as docker.io, nu.novell.com and secure-www.novell.com.

For more information about configuring the firewall, see Configuring the Firewall (https://www.netiq.com/documentation/advanced-authentication-64/server-administrator-guide/data/firewall.html).

NOTE: The recommended upgrade sequence is the upgrade of Advanced Authentication servers, followed by plug-ins and Client components. Any change in the upgrade sequence is not supported.

This section contains the following sections:

Registering To and Performing the Online Updates

NOTE: When SUSE releases the fix, updates including vulnerability fixes are available in the Update channel automatically.

To register for the Online Update Service:

1. Log in to the Appliance Configuration console as the `root` user.
2. Click **Online Update**.
3. If the Registration dialog does not open automatically, click **Register**.
4. Select the **Service Type** as **Micro Focus Customer Center**.
5. Specify the following information about the account for this appliance:
   - **Email address** of the account in Customer Center.

- **Activation key** (the same Full License key that you used to activate the product).

  Perform the following steps to obtain the activation key:

  1. Log in to Software Licenses and Downloads (https://sld.microfocus.com/) portal.
  2. Click **Software > Entitled Software > NetIQ Advanced Authentication > Keys**.
  3. Make a note of the applicable key.

- Select any of the following options to **Allow data send**:
  - **Hardware Profile**
  - **Optional information**

6 Click **Register**.

  Wait while the appliance registers with the service.

7 Click **OK**.

NOTE: If you are unable to register the appliance for Online update, see Unable to Register the Appliance for Online Update in the Configuration Portal to register manually.

After you register the appliance, you can view a list of the needed updates, or view a list of installed updates. You can use manual or automatic options to update the appliance. For more information, see Managing the Updates.

Managing the Updates

You can perform the following actions after registration:

- **Update Now:** Perform the following steps to install the downloaded updates:

  WARNING: You must start the upgrade process first from the Global Master server (GMS), then upgrade the database servers, and finally upgrade the web servers.

  ---

  1. Create snapshots for all Advanced Authentication servers.
  2. Click **Update Now** to install the downloaded updates.
  3. Restart the server to complete the update. It may take up to 10 minutes to get the required services started.
  4. Log in to the Advanced Authentication Administration portal on the upgraded server.
  5. Click **Cluster > Conflicts** to resolve the conflicts.
  6. Repeat steps Step 2 to Step 5 for database servers and Step 2 to Step 4 for web servers.

- **View Info:** Click **View Info** to display a list of installed and downloaded software updates.
- **Refresh:** Click **Refresh** to reload the status of updates on the appliance.

WARNING: Use the manual update only. Do not attempt to schedule updates for the frequency: daily, weekly, or monthly.

Performing the Offline Updates

You can perform the offline updates in a three step process:

1. Update Advanced Authentication and product repositories on the Subscription Management Tool (SMT) server installed locally.
2. Register the Advanced Authentication appliance to the local SMT server.
3. Perform the operating system and product updates.

Updating Advanced Authentication and Product Repositories on the Local SMT

Before you update the Advanced Authentication appliance, you must ensure that the SMT server is installed and the Advanced Authentication repositories are mirrored.

Prerequisite:

Ensure you have SLES 12 SP5 server to install the SMT server.

Perform the following to install and configure the SMT server:

- “Installing and Configuring the Local SMT Server” on page 21
- “Mirroring of Repositories” on page 22

Installing and Configuring the Local SMT Server

1 Download the Micro Focus Subscription Management Tool (https://marketplace.microfocus.com/appdelivery/content/micro-focus-subscription-management-tool).

2 Extract the downloaded file `Micro Focus Subscription Management Tool.zip`.

3 Open **YaST > Software > Add-On Products**.

4 Click **Add** in **Installed Add-on Products**.

5 Select **Local ISO Image** from the list and click **Next**.

6 Specify the **Repository Name** and click **Browse** then select the `MF-SMT-<version>-GM-CD1.iso` file from the extracted zip file.

7 Click **Next**.

8 Click **Trust**.

9 Click **Accept** and click **Continue**.

10 Click **Finish**.

11 Check whether the tool is installed successfully then click **OK**.

To verify the installation, open YaST and check for the following under Network Services:

- Micro Focus SMT Configuration Wizard
- Micro Focus SMT Server Configuration
- Micro Focus SMT Server Management

12 Launch the Micro Focus SMT Configuration Wizard.

13 Specify the following details for registration:

- **User**: The user name from the Micro Focus Customer Portal.
- **Password**: Password associated with the above mentioned user name.
- **NCC E-mail**: The email associated with your user account for the Micro Focus Customer Portal.

14 Click **Test** to check whether the specified details are valid.

15 Click **Next**.

16 Select the database password for SMT user and confirm it.

You need to remember this password to change configuration in future.

17 Click **Next**.

A prompt to create CA management certificate is displayed if you have not created a CA certificate on the SLES server.

18 Click **Run CA management**.

A prompt to set the CA password is displayed.

19 Specify **Password** and confirm it then click **OK**.

20 Click **Next**.

The Installation Overview is displayed.

For more information, see Micro Focus SMT Installation (https://www.microfocus.com/documentation/subscription-management-tool/smt-1.0/mfsmt/install.html) and Micro Focus SMT Server Configuration (https://www.microfocus.com/documentation/subscription-management-tool/smt-1.0/mfsmt/configure.html).

Mirroring of Repositories

1 Run **Micro Focus SMT Server Management** in YaST.

In **Repositories** tab all repositories that are hosted on SCC are displayed.

2 Select AAuth-Appliance-6.4-OS and click **Toggle Mirroring**.

3 Repeat the toggle for Aauth-Appliance-6.4-Product.

After toggle, a check mark appears against AA-Appliance-6.4-OS and AA-Appliance-6.4-Product.

4 Select the toggled files and click **Mirror Now**.

5 Click **OK**.

For more information, see the Mirroring Repositories on the Micro Focus SMT Server. (https://www.microfocus.com/documentation/subscription-management-tool/smt-1.0/mfsmt/mirror_repos.html).

Registering the Offline Updates on Advanced Authentication

After you configure the SMT server, you must register the service on Advanced Authentication and specify the following:

1. Select **Local SMT** in the **Online Update Service**.
2. Specify the **Hostname** such as **smt.example.com**.
3. (Opitonal) Specify the **SSL certificate URL** that communicates with the SMT server in the `http://<SMT_server>/smt.crt` format.
4. (Optional) specify the **Namespace path** of the file or directory.
5. Click **Register**.

   After you register the appliance, you can view a list of the needed updates, or view a list of installed updates. Use the manual option to update the appliance. For more information, see Managing the Updates.

Updating Advanced Authentication to a Field Patch

You can add patches provided by the product team in the **Field Patch** tab. A field patch is not a complete patch and you must use it only until a complete patch is released.

Perform the following steps to apply a field patch:

1. Disable all other updates for the appliance. Else, the field patch might be overwritten.
2. Create snapshots for all Advanced Authentication servers.
3. Log in to the Configuration console as the `vaadmin` user.
4. Click **Field Patch**, then follow the prompts to install the patch update.
5. (Conditional) Install a downloaded patch update:
   - **5a** Download the Advanced Authentication patch update file from the Software Licenses and Downloads (https://sld.microfocus.com/) portal.
   - **5b** In the **Install a Downloaded Patch** section, click **Browse**.
6. (Conditional) Uninstall a patch update:

   You might not be able to uninstall some patch updates.
   - **6a** In the **Patch Name** column of the **Field Patch** list, select the patch update that you want to uninstall.
   - **6b** Click **Uninstall Latest Patch**.
7. (Conditional) Click **Download Log File** for the appropriate patch update.

   NOTE: Ensure that you disable online updates and automatic updates until you apply a complete patch that contains the fix.

   ---
8. Restart the server to complete the update. It may take up to 10 minutes to get the required services started.
9. Log in to the Advanced Authentication Administration portal on the upgraded server.

10 Click **Cluster > Conflicts** to resolve the conflicts.

11 Repeat steps Step 3 to Step 10 for database servers and Step 3 to Step 9 for web servers.

The Patches are intended for specific bug fixes and security fixes for software that comes packaged by OpenSUSE and is maintained in the Main Updates repository. For more information, see OpenSUSE patch vs update (https://lukerawlins.com/opensuse-patch-vs-update/).

4 Upgrading Advanced Authentication

This section describes how to upgrade Advanced Authentication to the latest version through the Configuration console.

To access the Configuration console, perform the following steps:

1. In a web browser, specify the DNS name or the IP address of the appliance with the port number 9443. For example:

   `https://10.10.10.1:9443`

   or

   `https://mycompany.example.com:9443`

2. Specify **root** or **vaadmin** as the user name and specify the password for the appliance, then click **Sign in**.

IMPORTANT: It is recommended to upgrade when users' activities are less. The period of upgrade must be reduced as the replication of databases that do not synchronize can break the database servers.

This section includes the following topics:

Upgrading Advanced Authentication Appliance

You can upgrade your appliance using the **Product Upgrade** option.

The **Product Upgrade** option is displayed only when you can use it to upgrade the service hosted on your appliance.

NOTE: The recommended upgrade sequence is the upgrade of Advanced Authentication servers, followed by plug-ins and Client components. Any change in the upgrade sequence is not supported.

To upgrade Advanced Authentication Appliance, perform the following steps:

1. Create snapshots for all Advanced Authentication servers.
2. Click the **Online Update** tab and apply all updates.

   You can also apply the updates offline if there is no internet connection. For more information, see Performing the Offline Updates.
3. Click the **Product Upgrades** tab and upgrade the appliance.

4 Restart the server to complete the update.

   It may take up to 10 minutes to get the required services started.

5 Log in to the Advanced Authentication Administration portal on the upgraded server.

6 Click **Cluster > Conflicts** to resolve the conflicts.

7 In the minimal time frame, repeat steps Step 3 to Step 6 for the servers in the following order:

   7a DB Servers of the primary site.

   7b Master Servers of the other sites.

   7c DB Servers of the other sites.

8 Repeat steps Step 3 to Step 5 for web servers.

NOTE: You cannot upgrade directly from version 6.1 to 6.4. You must first upgrade from version 6.1 to 6.2 then upgrade from version 6.2 to 6.3 and then upgrade from version 6.3 to 6.4.

For upgrading from Advanced Authentication 6.1 to 6.2, see Upgrading Advanced Authentication Appliance 6.1 to 6.2 (https://www.netiq.com/documentation/advanced-authentication-62/install-upgrade-guide/data/upgrade.html).

Upgrading Advanced Authentication on Public Cloud Using Kubernetes

This section contains details about how to upgrade Advanced Authentication on public cloud - Amazon Web Services and Azure using Kubernetes. You can upgrade Advanced Authentication containers into Kubernetes clusters by using the Helm charts.

1 Download the `aaf-<version>-helm-chart.zip` file from NetIQ Downloads.

2 Unpack the zip file. You can view the `aaf-<version>.tgz` tar file.

3 Run the following command to unpack the tar file:

   ```
   tar zxvf aaf-<version>.tgz
   ```

4 Run the following command to upgrade the helm chart:

   ```
   helm upgrade <name_of_kubernetes_namespace>  --namespace
   <helm_chart_release_name>  <path_of_helm_chart>
   ```

   For example, `helm upgrade aaf-test1 --namespace aaf-test --set lb.enabled=true ./aaf_63sp3/`

NOTE: After upgrade, perform the following to monitor events, logs, and persistent volume claims of your namespace:

- Run the following command to view latest events:

  ```
  kubectl get events --namespace <name_of_kubernetes_namespace>
  ```

- Run the following command to get the logs of Advanced Authentication containers:

  ```
  kubectl logs $(kubectl get pods --no-headers -o custom-
  columns=":metadata.name" --namespace <name_of_kubernetes_namespace>) -c
  aucore --namespace <name_of_kubernetes_namespace>
  ```

- Run the following command to check persistent volume claims:

  `kubectl get pvc --namespace <name_of_kubernetes_namespace>`

Upgrading Advanced Authentication on Azure Kubernetes Services in an Air Gap Environment

This section contains details on the upgrade of Advanced Authentication in an air gap environment on Azure Kubernetes Service. You can upgrade Advanced Authentication containers into Kubernetes clusters using the docker images and Helm charts.

Pre-Upgrade Procedure

NOTE: Ensure to install the following packages on a Linux client machine (Windows OS is not supported):

Linux operating system, docker, docker-ce, docker-ce-cli, containerd.io, docker-compose-plugin, helm, kubectl, and Azure CLI.

1. Download the `AdvancedAuthDocker-<version>.zip` file from Patch Manager.
2. Unzip the `AdvancedAuthDocker-<version>.zip` file and go into the dockerimages directory.
3. Run the following command to start the docker:

   `systemctl start docker`
4. Run the following command to load the images from the docker images tgz file on your server:

   `docker load -i aauth-images.tgz`
5. Run the following command and verify that the images are loaded:

   `docker images`
   - `mfsecurity/aaf-webauth:<version>`
   - `mfsecurity/aaf-aucore:<version>`
   - `mfsecurity/aaf-redis:<version>`
   - `mfsecurity/aaf-repldb:<version>`
   - `mfsecurity/aaf-fipsd:<version>`
   - `mfsecurity/aaf-afisd:<version>`
   - `mfsecurity/aaf-radiusd:<version>`
   - `mfsecurity/aaf-searchd:<version>`
   - `mfsecurity/aaf-webd:<version>`
   - `mfsecurity/aaf-audb:<version>`
   - `gliderlabs/logspout:<version>`
6. Run the following commands to retag the docker images per specifications from your internal docker repository:

```
docker tag mfsecurity/<name>:<version> <internalDocker>/
<name>:<version>

docker tag gliderlabs/<name>:<version> <internalDocker>/
<name>:<version>
```

7 Provide the credentials to perform docker login to your internal or private registry.

8 Run the following command to push the newly tagged images to your internal docker repository:

```
docker push <internalDocker>/<name>:<version>
```

Upgrade Procedure

1 Download the `aaf-<version>-helm-chart.zip` file from Patch Manager.

2 Unpack the zip file. You can view the `aaf-<version>.tgz` tar file.

3 Run the following command to unpack the tar file:

```
tar zxvf aaf-<version>.tgz
```

4 Modify the `values.yaml` file by replacing the default value `mfsecurity` with the value for the internal repository `internalDocker`.

5 Log in to Azure.

6 Run the following command to upgrade the helm chart:

```
helm upgrade --namespace <name_of_kubernetes_namespace>
<helm_chart_release_name> <path_of_helm_chart>
```

For example,

```
helm upgrade --namespace aaf-test aaf-test1 --set lb.enabled=true ./
aaf_63sp3/
```

NOTE: After upgrade, perform the following to monitor events, logs, and persistent volume claims of your namespace:

- Run the following command to view latest events:

  ```
  kubectl get events --namespace <name_of_kubernetes_namespace>
  ```

- Run the following command to get the logs of Advanced Authentication containers:

  ```
  kubectl logs $(kubectl get pods --no-headers -o custom-
  columns=":metadata.name" --namespace
  <name_of_kubernetes_namespace>) -c aucore --namespace
  <name_of_kubernetes_namespace>
  ```

- Run the following command to check persistent volume claims:

  ```
  kubectl get pvc --namespace <name_of_kubernetes_namespace>
  ```

---

5 Troubleshooting

This chapter contains the following sections:

Viewing the Logs for Debugging

To view the logs of Advanced Authentication appliance docker, specify the following path:

```
/var/lib/docker/volumes/aaf_aucore-logs/_data
```

The `/var/lib/docker/volumes/aaf_aucore-logs/_data` contains logs related to aucore, replication, webauth, and so on.

To view the processes running on docker, run the following command:

```
$ docker ps --format "{{.Names}}"
```

Managing Systemd Services

You can reboot Advanced Authentication from the command prompt.

To start the Systemd services, run the following command:

```
systemctl start aauth
```

To stop the Systemd services, run the following command:

```
systemctl stop aauth
```

To view the status of Advanced Authentication services running on the appliance, run the following command:

```
systemctl status aauth
```

Enabling SSH for Appliance

To enable Advanced Authentication server to interact with the clients, you must enable the SSH option.

To enable SSH for appliance, run the following commands:

```
systemctl enable sshd.service
```

```
systemctl start sshd.service
```

`lsof -i :22` (to check that the port is listening)

NOTE: You can also perform these services in Accessing System Services (https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/services.html) of the Configuration console.

The Advanced Authentication Portals are Inaccessible After Upgrade

Issue: After updating Advanced Authentication, you are unable to open the Advanced Authentication portals except for the Configuration portal (:9443).

Reason: This issue occurs due to one of the following reasons:

- The docker bypasses the proxy settings.
- Insufficient disk space during the upgrade process. The minimum free space required for upgrading the appliance is 4 GB.

Workaround: Perform one of the following:

- Workaround 1
- Workaround 2

Workaround 1: Perform the following steps:

1. Execute the command `/opt/aauth/start` to start the Advanced Authentication services manually.

   If an error message `ERROR: Get https://registry-1.docker.io/v2/: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)` is displayed, then proceed to step 3.
2. Check the firewall settings. The Advanced Authentication server must be able to access `docker.io` through the port 443 (HTTPS).

   For more information about the firewall settings, see Configuring the Firewall (https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/firewall.html).
3. Ensure the proxy settings are configured in YaST.

   For more information about the proxy settings, see Configuring the Proxy Settings (https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/network.html#t46ltypycv7a)

4 Navigate to the path `/etc/systemd/system/docker.service.d`.

5 Create a file `http-proxy.conf` and specify the following parameters:

- `[Service]`
- `Environment="HTTP_PROXY=<proxy_URL>"`
- `Environment="NO_PROXY=<proxy_exception>"`
- `Environment="PROXY_USER=<username>:<password>"`

For example,

```
[Service]
Environment="HTTP_PROXY=http://proxy.local:8080/"
Environment="NO_PROXY=.local, .company.com"
Environment="PROXY_USER=proxuser:password"
```

6 Save the configuration file.

7 Restart the server.

Workaround 2: Perform the following steps:

1 Log in to the Linux console and run the following command to verify the available disk space:

```
df -h /dev/sda1
```

If the minimum free space of 4 GB is not available, then increase the disk space.

2 Run the following command to re-initiate the upgrade process:

```
zypper in -f web-aauth
```

The Dashboard Displays Empty Widgets and Error After Deploying Advanced Authentication on Kubernetes Cluster

Issue: After you deploy Advanced Authentication on Kubernetes local cluster, the Dashboard page on the Advanced Authentication Administration portal displays empty widgets and an error message, `Unknown server error`.

Reason: This issue might occur due to low `mmap` count in the docker host machine and this might result in out of memory exceptions.

Workaround: Run the following command as the `root` user to increase the `mmap` count limit:

```
sysctl -w vm.max_map_count=262144
```

To set the `mmap` count permanently, update the `vm.max_map_count` setting in `/etc/sysctl.conf`. Later run the following command to verify the count after reboot:

```
sysctl vm.max_map_count
```

Error when updating the Advance Authentication

Issue: Not able to perform the online update. While performing the online update, an error message `com.google.gwt.user.client.rpc.IncompatibleRemoteServiceException: Type 'com.google.gwt.user.client.rpc.XsrfToken' was not assignable to 'com.google.gwt.user.client.rpc.IsSerializable' and did not have a custom field serializer. For security purposes, this type will not be deserialized.` is displayed.

Workaround: Clear cookies in browser.

Removing the nomodeset Parameter for Better Boot Screen Performance

Issue: While installing Advanced Authentication appliance on some hypervisors, a black screen is displayed.

Reason: This might occur due to the pre-defined `nomodeset` parameter.

Workaround: Perform the following steps to remove the `nomodeset` parameter:

1. Press **Tab** on the boot screen after mounting Advanced Authentication ISO file.
2. Remove the `nomodeset` parameter from the line that starts with `linux initrd=initrd`.
3. Press **Enter**.

Unable to Register the Appliance for Online Update in the Configuration Portal

Issue: You are unable to register for Online update in the Configuration portal (:9443).

Workaround: Perform the following to register using commands:

1. Log in to the Advanced Authentication server command line as the root user.
2. Run the following command to register the appliance for Online update manually:

   ```
   suse_register -a regcode-aauth=xxxxx -a email=xxxxx -L /tmp/register.txt
   ```

   Before executing the command, ensure to replace xxxx with the valid activation key and email address respectively.