



Advanced Authentication 6.3

Server Installation and Upgrade Guide

December 2019

Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <http://www.microfocus.com/about/legal/>.

© Copyright 2019 Micro Focus or one of its affiliates.

Contents

About this Book	5
1 System Requirements	7
2 Installing Advanced Authentication	9
Obtaining Advanced Authentication	9
Downloading the Purchased Version	9
Downloading the Trial Version	9
Installing Advanced Authentication	10
Deploying Advanced Authentication on Amazon Web Services	11
Prerequisites	11
Deployment Procedure	11
Deploying Advanced Authentication on Azure Kubernetes Services	13
Prerequisites	13
Deployment Procedure	13
3 Getting the Latest Online and Offline Updates	17
Registering To and Performing the Online Updates	17
Managing the Updates	18
Performing the Offline Updates	18
Updating Advanced Authentication and Product Repositories on the Local SMT	19
Registering the Offline Updates on Advanced Authentication	20
Updating Advanced Authentication to a Field Patch	20
4 Upgrading Advanced Authentication	23
Upgrading Advanced Authentication Appliance 6.1 to 6.2	23
Migrating Advanced Authentication from Version 5.x	24
Upgrading Advanced Authentication on Public Cloud Using Kubernetes	25
5 Troubleshooting	27
Viewing the Logs for Debugging	27
Managing Systemd Services	27
Enabling SSH for Appliance	27
The Advanced Authentication Portals are Inaccessible After Upgrade	28
The Dashboard Displays Empty Widgets and Error After Deploying Advanced Authentication on Kubernetes Cluster	29

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 client components and plug-ins, see the related documentation.

The following table lists the system requirements for Advanced Authentication appliance:

Requirement	Detail
Virtual Systems	<ul style="list-style-type: none">♦ Hyper-V Server 2016 or later♦ VMware ESX 5.5 or later♦ Citrix XenServer 7.5♦ Citrix Hypervisor 8.0
Memory	Minimum requirement: 6 GB of RAM Recommended requirement: 12 GB of RAM
Hard disk space	Minimum requirement: 40 GB Recommended requirement: 60 GB
CPU	Minimum requirement: 4 Cores CPU Recommended requirement: 8 Cores CPU Processor must support SSE 4.2 instructions. For more information about how to check whether the CPU supports SSE 4.2 instructions, see Verifying SSE 4.2 Instructions on CPU .
Browsers	Any one of the following browsers: <ul style="list-style-type: none">♦ Microsoft Internet Explorer 11♦ Microsoft Edge 20.0 and later♦ Google Chrome 65 and later♦ Mozilla Firefox 58 and later♦ Safari 11 and later
IP Ports	Ensure that the default ports for the Advanced Authentication appliance are open in your firewall. For more information, see Configuring the Firewall (https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/firewall.html) .

Requirement	Detail
LDAP Repositories	<p>Any one of the following repositories:</p> <ul style="list-style-type: none"> ♦ Microsoft Active Directory Services ♦ Microsoft Active Directory Lightweight Directory Services ♦ NetIQ eDirectory ♦ OpenLDAP ♦ OpenDJ ♦ Microsoft SQL Server 2016

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” on page 9
- ♦ “Installing Advanced Authentication” on page 10
- ♦ “Deploying Advanced Authentication on Amazon Web Services” on page 11
- ♦ “Deploying Advanced Authentication on Azure Kubernetes Services” on page 13

Obtaining Advanced Authentication

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

- ♦ “Downloading the Purchased Version” on page 9
- ♦ “Downloading the Trial Version” on page 9

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 [Customer Center](#).
- 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 <https://dl.netiq.com>.
- 2 Click the **Free Trials** link.
- 3 Scroll down to find Advanced Authentication, then click **Download**.
- 4 Specify your information to receive an email with the download link.

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 Unpack the file `AdvancedAuthAppliance-x.x-xxx.zip`, and use the `AdvancedAuthAppliance-x.x-xxx.iso` file.
- 3 Mount 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.
 - ♦ **Region and Time Zone:** Select a region and time zone.
 - ♦ **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.

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 \(https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/time.html\)](https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/time.html).

NOTE: For information about migrating Advanced Authentication appliance from version 5.x to 6.1, see [“Migrating Advanced Authentication from Version 5.x”](#).

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

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 11](#)

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 \(https://docs.aws.amazon.com/eks/latest/userguide/getting-started.html\)](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 \(https://docs.aws.amazon.com/eks/latest/userguide/install-kubectl.html\)](https://docs.aws.amazon.com/eks/latest/userguide/install-kubectl.html) and [configure kubectl \(https://docs.aws.amazon.com/eks/latest/userguide/configure-kubectl.html\)](https://docs.aws.amazon.com/eks/latest/userguide/configure-kubectl.html).

Deployment Procedure

- 1 Download the `aaf-<version>-helm-chart.zip` file from [NetIQ Downloads \(https://dl.netiq.com\)](https://dl.netiq.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 the following command to deploy three Advanced Authentication instances into the cluster:

```
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/
```

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 \(https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/ch-appliance-config.html\)](https://www.netiq.com/documentation/advanced-authentication-61/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 \(https://docs.aws.amazon.com/eks/latest/userguide/install-aws-iam-authenticator.html\)](https://docs.aws.amazon.com/eks/latest/userguide/install-aws-iam-authenticator.html).
2. Install AWS CLI. For more information see, [Installing AWS CLI \(https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-install.html\)](https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-install.html).
3. Configure AWS CLI Credentials. For more information see, [Configuring AWS CLI \(https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-configure.html\)](https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-configure.html).
4. Install eksctl. For more information see, [Install eksctl section in Getting Started with eksctl \(https://docs.aws.amazon.com/eks/latest/userguide/getting-started-eksctl.html\)](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 Run the following command to install tiller on your cluster:

```
helm init
```

- 3 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 \(https://kubernetes.io/docs/reference/access-authn-authz/rbac/\)](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
```

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

```
helm install --namespace aaf-test --name=aaf-test-1 --set  
lb.enabled=true ./aaf_62/
```

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.

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 \(https://docs.microsoft.com/en-us/azure/aks/kubernetes-walkthrough\)](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 [NetIQ Downloads \(https://dl.netiq.com\)](https://dl.netiq.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 the following command to deploy three Advanced Authentication instances into the cluster:

```
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/
```

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 \(https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/ch-appliance-config.html\)](https://www.netiq.com/documentation/advanced-authentication-61/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 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 Run the following command to install tiller on your cluster:

```
helm init
```

- 3 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 \(https://kubernetes.io/docs/reference/access-authn-authz/rbac/\)](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
```

- 4** Run the following command to deploy Advanced Authentication instance into your cluster:

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


3 Getting the Latest Online and Offline Updates

Use the **Online Update** option to register for the online update service from the [Customer Center](https://www.netiq.com/customercenter) (<https://www.netiq.com/customercenter>). You can install updates automatically or manually. For more information about the OpenSUSE online updates, see [OpenSUSE patch vs update](https://lukerawlings.com/opensuse-patch-vs-update/) (<https://lukerawlings.com/opensuse-patch-vs-update/>).

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-61/server-administrator-guide/data/firewall.html) (<https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/firewall.html>).

This section contains the following sections:

- ♦ “[Registering To and Performing the Online Updates](#)” on page 17
- ♦ “[Performing the Offline Updates](#)” on page 18
- ♦ “[Updating Advanced Authentication to a Field Patch](#)” on page 20

Registering To and Performing the Online Updates

To register for the Online Update Service:

- 1 [Log in](#) to the Configuration console as the `root` user.
- 2 Click **Online Update**.
- 3 If the Registration dialog does not open automatically, click the **Register** tab.
- 4 Select the **Service Type** as:
 - ♦ **Micro Focus Customer Center**
- 5 Specify the following information about the [Customer Center](https://www.netiq.com/customercenter) (<https://www.netiq.com/customercenter>) 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 [Micro Focus Customer Center](https://www.netiq.com/customercenter) (<https://www.netiq.com/customercenter>).
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**.

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: It is not recommended to schedule the update due to complexity of the update procedure in a clustered environment.

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.

Perform the following to install and configure the SMT server:

- ♦ “Installing and Configuring the Local SMT Server” on page 19
- ♦ “Mirroring of Repositories” on page 19

Installing and Configuring the Local SMT Server

- 1 To install the organizational level SMT server:
 - 1a Run **YaST > Software > Software Management**.
 - 1b Select **View > Patterns**.
 - 1c Select the SMT pattern and install SMT software.
- 2 To configure the local SMT server:
 - 2a Run **YaST > Network Services > SMT Configuration Wizard**.
 - 2b Select **Enable Subscription Management Tool Service (SMT)**.
 - 2c Open the port in Firewall.
 - 2d Specify the following in NCC Mirroring Credentials:
 - ♦ **For Novell Customer Center:**
Registration Server URL: <https://secure-www.novell.com/center/regsvc/> (<https://secure-www.novell.com/center/regsvc/>)
Download Server URL: <https://nu.novell.com/> (<https://nu.novell.com/>)
 - ♦ **For Suse Customer Center:**
Registration Server URL: <https://scc.suse.com/connect> (<https://scc.suse.com/connect>)
Download Server URL: [:https://updates.suse.com](https://updates.suse.com) (<https://updates.suse.com>)
Provide a valid username and password. You can get them from (<https://scc.suse.com/organization>) or the Novell Customer Center.
Test the credentials and save.
 - 2e Click **Database and Reporting** and provide a valid password for the **smt** user.
 - 2f Click **OK**.

Mirroring of Repositories

- 1 Create a local mirror or repos of the SUSE repositories.
- 2 Run **Yast >> SMT Server Management**.
- 3 In the **Repositories** section, all repositories which are hosted on SCC are displayed.
- 4 Select **Aauth-Appliance-6.2-OS** and click **Mirror Now**.

- 5 Repeat the same for `Aauth-Appliance-6.2-Product` and click **Mirror Now**.
- 6 Click **OK**.

For more information, see the [SUSE documentation on Mirroring Repositories on the SMT Server](https://www.suse.com/documentation/sles-12/book_smt/data/smt_mirroring.html). (https://www.suse.com/documentation/sles-12/book_smt/data/smt_mirroring.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 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. You can use manual or automatic options 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 [Patch Finder \(https://dl.netiq.com/patch/finder/\)](https://dl.netiq.com/patch/finder/) website.
 - 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 \(https://lukerawlins.com/opensuse-patch-vs-update/\)](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 6.1 to 6.2” on page 23](#)
- [“Migrating Advanced Authentication from Version 5.x” on page 24](#)
- [“Upgrading Advanced Authentication on Public Cloud Using Kubernetes” on page 25](#)

Upgrading Advanced Authentication Appliance 6.1 to 6.2

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

For migrating from Advanced Authentication 5.x to 6.1, see [“Migrating Advanced Authentication from Version 5.x”](#) section.

For upgrading from Advanced Authentication 6.0 to 6.1, see [Upgrading Advanced Authentication Appliance 6.0 to 6.1 \(https://www.netiq.com/documentation/advanced-authentication-61/install-upgrade-guide/data/productupgrade.html\)](https://www.netiq.com/documentation/advanced-authentication-61/install-upgrade-guide/data/productupgrade.html).

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

To upgrade Advanced Authentication Appliance 6.1 to 6.2, 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 Repeat steps [Step 3](#) to [Step 6](#) for database servers and [Step 3](#) to [Step 5](#) for web servers.

NOTE: You cannot upgrade directly from 6.0 to 6.2. You must first upgrade from 6.0 to 6.1 and then upgrade from 6.1 to 6.2.

Migrating Advanced Authentication from Version 5.x

You cannot upgrade from Advanced Authentication 5.0 to 6.1. However, you can export the configurations of the database from Advanced Authentication 5.6 to 6.1. After you install Advanced Authentication 6.1, you can import all configuration details from 5.6.

For example, to upgrade from Advanced Authentication 5.5 to 6.1, you must first upgrade from Advanced Authentication 5.5 to 5.6. Then, install Advanced Authentication 6.1 and import the configuration details from 5.6.

For information about how to export and import the configurations, see “[Exporting and Importing the Database](#)” in the *Advanced Authentication - Administration* guide.

To migrate 5.0 to Advanced Authentication 6.1, perform the following steps:

- 1 Deploy the Advanced Authentication Global Master 6.1 server. For more information about deploying the Global Master, see [Configuring Global Master Server \(https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/configuringglobalmaster.html\)](https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/configuringglobalmaster.html).
- 2 Export the database of Advanced Authentication 5.6 and import it to the database of Advanced Authentication 6.1.

For information about how to export and import the configurations, see “[Exporting and Importing the Database](#)” in the *Advanced Authentication - Administration* guide.

NOTE: The first 6.1 server where the database is imported becomes the new Global Master server of the cluster by default.

- 3 Deploy other Advanced Authentication servers in the cluster.
For more information about clustering, see [Configuring a Cluster](#) in the *Advanced Authentication - Administration* guide.
- 4 Reconfigure the third-party integrations to point them to the new server address.
For example, Advanced Authentication integrates with ADFS through the SAML or OAuth event. After you migrate Advanced Authentication from 5.6 to 6.1, you must redirect all these third-party integrations to the new 6.1 server.
- 5 Create the `_aav6` DNS service location records for the new servers of the 6.1 cluster.

For more information about how to set the DNS records in Windows Client, see [“Setting a DNS for Advanced Authentication Server Discovery”](#) in the *Advanced Authentication - Windows Client* guide.

6 Upgrade the client packages on the endpoints.

NOTE

- ♦ It is recommended to not migrate all clients together. Instead, first migrate a few clients and complete the testing for these. Then upgrade the other set of clients and perform the testing. After that, complete the migration of the remaining clients.
 - ♦ Do not delete the `_aaa` service location records from DNS for the servers available in the Advanced Authentication 5.6 cluster until all endpoints are migrated to Advanced Authentication 6.1.
-

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 --namespace <name_of_kubernetes_namespace> --  
name=<helm_chart_release_name> <path_of_helm_chart> --recreate-pods;
```

For example, `helm upgrade --namespace aaf-test --name=aaf-test --set lb.enabled=true /6.2_Pu2/aaf --recreate-pods;`

NOTE

- ♦ During the upgrade process, existing pods are re-created so you can expect downtime.
 - ♦ Re-creating pods do not affect existing data, and pods persist post the upgrade.
-

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” on page 27](#)
- ♦ [“Managing Systemd Services” on page 27](#)
- ♦ [“The Advanced Authentication Portals are Inaccessible After Upgrade” on page 28](#)
- ♦ [“The Dashboard Displays Empty Widgets and Error After Deploying Advanced Authentication on Kubernetes Cluster” on page 29](#)

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 \(https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/services.html\)](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/aaauth/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 \(https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/firewall.html\)](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 \(https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/network.html#t46ltypycv7a\)](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-auth
```

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
```

