MAIPU

Maipu AAS

Installation Manual

V1.0

迈普通信技术股份有限公司
www.maipu.com

Copyright

Security Statement

Important! Before powering on and starting the product, please read the security and compatibility information of the product.

Environmental protection

This product has been designed to comply with the environmental protection requirements. The storage, use, and disposal of this product must meet the applicable national laws and regulations.

Preface

Manual Introduction

This manual mainly describes how to install Maipu AAS system. Before installation, perform the environment preparation according to Chapter 1; it is suggested to use the U-disk to install; when using the virtual machine, you can use the ios file to install, and the installation process is the same as the U-disk; when you have installed the desired operation system, install according to the installation mode of the installation package.

Product Version

The product version of the manual is as follows

Product Name	Software Version
Maipu AAS(V4)	AAS-V3R2C03

Audience

This documentation is intended for:

- Commissioning engineers
- Field maintenance engineers
- System maintenance engineers

Conventions

Symbol conventions:

Format	Description
Note	An alert that contains additional or supplementary information.
Caution	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
Warning	An alert that calls attention to important information that if not understood or followed can result in personal injury or router damage.

Command conventions:

Convention	Description
Boldface	Bold text represents commands and keywords that you enter literally as shown.
Italic	Italic text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

Matching Manuals

The manuals matching with the product:

Manual Name	Manual Introduction
Maipu AAS Troubleshooting V1.0	This manual mainly describes the solutions or workaround of the common problems when installing and using Maipu AAS.
Maipu AAS User manual V1.0	This manual mainly describes the using methods and functions of Maipu AAS.

Obtaining Documentation

You can access the most up-to-date Maipu product documentation on the World Wide Web at www.maipu.cn.

Technical Support

- Technical supporting hotline: 400-886-8669
- Fax: (+8628)85148948

Documentation Feedback

You can feed back your opinions and suggestions by:

- Email: techsupport@maipu.com

- Technical hotline: 400-886-8669

Content

1.Maipu AAS Installation Preparations

1.1Installation Environment Requirements

Lowest Requirements of Hardware	Operation System Version	Remarks
Intel/AMD 3.0G Hz 4-core processor, memory 16G, hard disk 1T, 64-bit operation system	SLES-11-SP3(x86_64)	used to install the user authentication platform, marketing platform of the standalone Maipu AAS
Intel/AMD 3.0G Hz 4-core processor, memory 32G, hard disk 1T, 64-bit operation system	SLES-11-SP3(x86_64)	used to install the user authentication platform, marketing platform of the dual-machine Maipu AAS

1.2 Preparations before Installation

Before installing Maipu AAS, you need to prepare the server and do network topology plan. If you choose to install via the software package, please configure the firewall and the server time (for the server time, refer to the description in chapter 2 “ISO Package Installation”), and prepare the Maipu AAS software package.

1.2.1 Prepare the Server

1. Standalone Mode

Before installing Maipu AAS standalone mode, you just need to prepare one server.

2. HA Dual-Machine Hot Backup Mode

Before installing Maipu AAS HA dual-machine hot backup mode, prepare two servers.

Active/standby server: two

For each server, you need to configure two Gigabit Ethernet ports. One serves as the service Ethernet port, and the other serves as the heartbeat Ethernet port of the

communication between the active and standby servers (as shown in the following figure, eth0 serves as the service Ethernet port, eth1 serves as the heartbeat Ethernet port):

Server 1:

```
linux-sft3:~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:33:F3:B9
          inet addr:128.255.40.29  Bcast:128.255.43.255  Mask:255.255.252.0
          inet6 addr: fe80::20c:29ff:fe33:f3b9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1530 errors:0 dropped:30 overruns:0 frame:0
          TX packets:127 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:126615 (123.6 Kb)  TX bytes:12608 (12.3 Kb)

eth1      Link encap:Ethernet  HWaddr 00:0C:29:33:F3:C3
          inet6 addr: fe80::20c:29ff:fe33:f3c3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3219 errors:0 dropped:69 overruns:0 frame:0
          TX packets:648 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:267803 (261.5 Kb)  TX bytes:106065 (103.5 Kb)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:26 errors:0 dropped:0 overruns:0 frame:0
          TX packets:26 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1940 (1.8 Kb)  TX bytes:1940 (1.8 Kb)
```

Server 2:

```
linux-25eu:~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:C9:80:D2
          inet addr:128.255.40.26  Bcast:128.255.43.255  Mask:255.255.252.0
          inet6 addr: fe80::20c:29ff:fec9:80d2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:385 errors:0 dropped:9 overruns:0 frame:0
          TX packets:269 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:32566 (31.8 Kb)  TX bytes:22363 (21.8 Kb)

eth1      Link encap:Ethernet  HWaddr 00:0C:29:C9:80:DC
          inet6 addr: fe80::20c:29ff:fec9:80dc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2790 errors:0 dropped:68 overruns:0 frame:0
          TX packets:304 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:228716 (223.3 Kb)  TX bytes:47745 (46.6 Kb)
          Interrupt:16 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:147 errors:0 dropped:0 overruns:0 frame:0
          TX packets:147 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:62332 (60.8 Kb)  TX bytes:62332 (60.8 Kb)
```

3. Check the Server Time

Check whether the server time, timezone, and time are correct. If no, change the date

and time setting.

1.2.2 Network Plan

1. Standalone Mode

Before installing the standalone mode of Maipu AAS, you need to plan the IP address, that is, one service IP address and one domain name. The domain name needs to map the service IP address of the server.

IP address/domain name	Quantity	Remarks
IP address	1	**One service IP address** One service IP address for the server of the user authentication platform, marketing platform
Domain name	1	**One domain name:** Map to the service IP address of the user authentication platform, marketing platform, used by the terminal user to access the portal page via Internet domain name

Standalone mode

2. HA Dual-Machine Hot Backup Mode

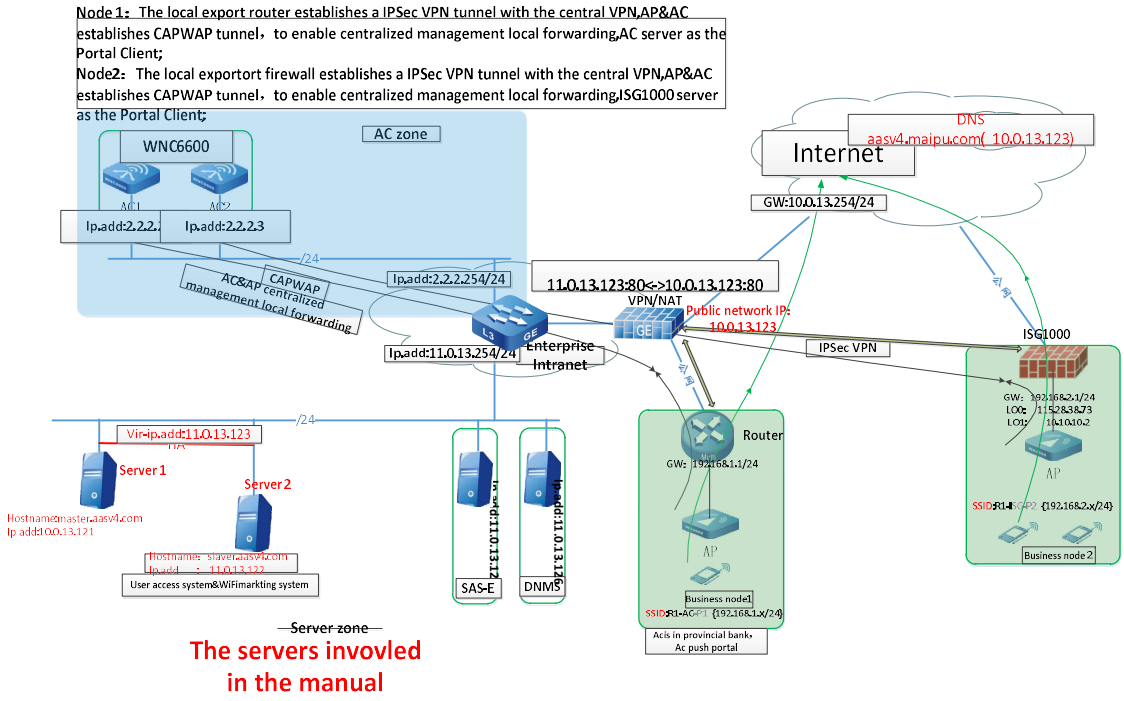
Before installing the HA dual-machine hot backup mode of Maipu AAS, you need to plan IP address. To install the active and standby servers of the user authentication platform and marketing platform, you need to plan one service IP address and one heartbeat IP address respectively, and plan one floating IP address between the active and standby servers. Besides, plan one domain name, which needs to map to the floating IP address between the active and standby servers of the user authentication platform and marketing platform.

IP address/domain name	Quantity	Remarks
IP address	5	**Three service IP addresses:** One IP address for the active server of the user authentication platform,

		marketing platform; One IP address for the standby server of the user authentication platform, marketing platform; The active and standby servers of the user authentication platform, marketing platform share one floating IP address. **Two heartbeat IP addresses:** One heartbeat IP address for the active server of the user authentication platform, marketing platform; One heartbeat IP address for the standby server of the user authentication platform, marketing platform.
Domain name	1	**One domain name:** Map to the floating IP address of the user authentication platform and marketing platform, used by the terminal user to access the portal page via the Internet domain name

HA dual-machine hot backup mode

1.2.3 Network Topology



Note: In the figure, the planed instance IP is the HA mode. If it is the deployment of the standalone mode, use the address 11.0.13.123 as the standalone IP to demonstrate.

1.2.4 Firewall Configuration

Source Address	Destination Address	Type	Port
NAS device address and all user terminal device address	Maipu AAS server address	TCP	80 1. Used by the user terminal to access portal re-direction address 2. Used by the phone terminal user to access the portal page of the marketing platform
NAS device	Maipu AAS server address	UDP	1812 Used for the RADIUS

Source Address	Destination Address	Type	Port
			authentication 1813 Used for the RADIUS accounting 2000 Used for the Portal authentication
Maipu AAS server address	NAS device	UDP	2000 Used for the Portal authentication
Marketing platform	SMS gateway server	Configure by the actuality	Configure by the actuality
All user terminal device addresses	Authentication platform address	TCP	80 Used by the user terminal to scan the QR code for authentication
Administrator client address	Maipu AAS server address	TCP	8443 Used by the user to access Maipu AAS

2.Maipu AAS ISO Package Installation

When using the new physical machine or virtual machine to install, you can use the ISO package to complete the system installation. This chapter describes the installation of the user authentication platform, and the installation and fast configuration of the marketing platform. The configuration in the installation deployment of this document takes the topology in the environment preparation as an example to describe. In actuality, be subject to the deployment.

If choosing to use the ISO package to install, you can make the ISO package as the boot disk of the U-disk. The following is the making mode of the U-disk.

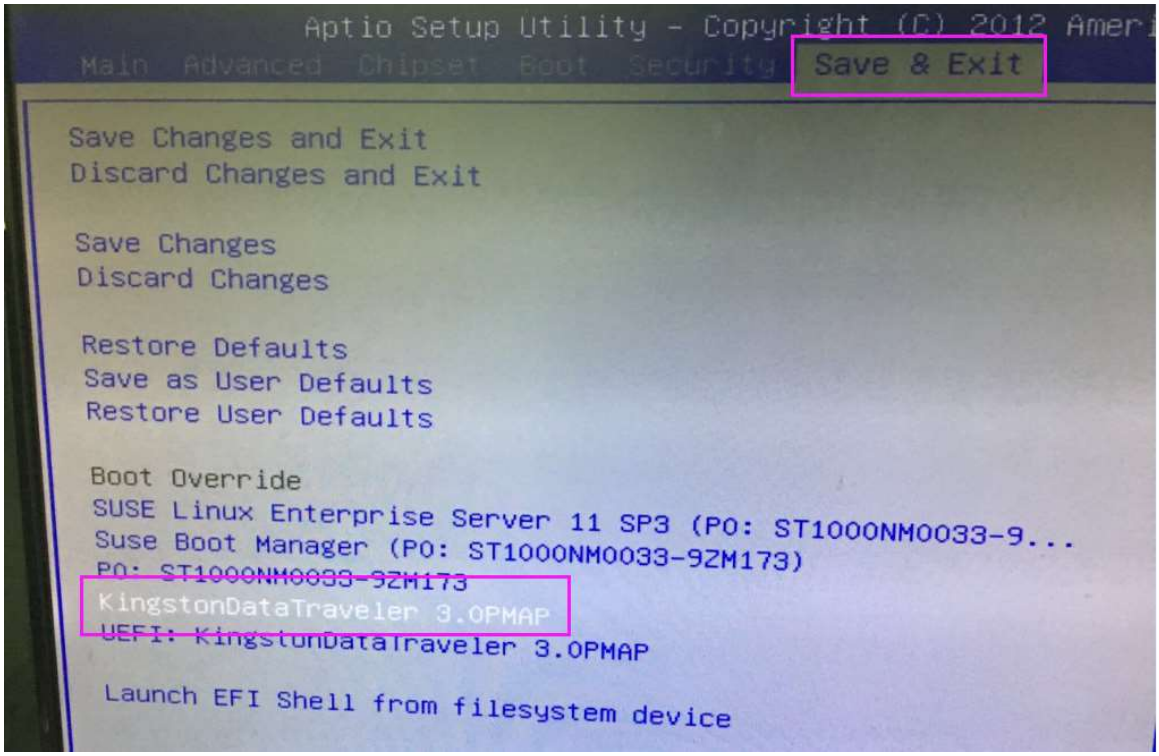
U盘烧写、检验说明v1 0.docx

2.1 Description of Booting U-disk via Hardware V3 Server BIOS

Step 1: Insert the made D-disk to the server and enable the server.

Step 2: Press **Delete** continuously to enter the BIOS setting interface of the server.

Step 3: Enter the “Save&Exit” menu, select the U-disk, and press **Enter**.



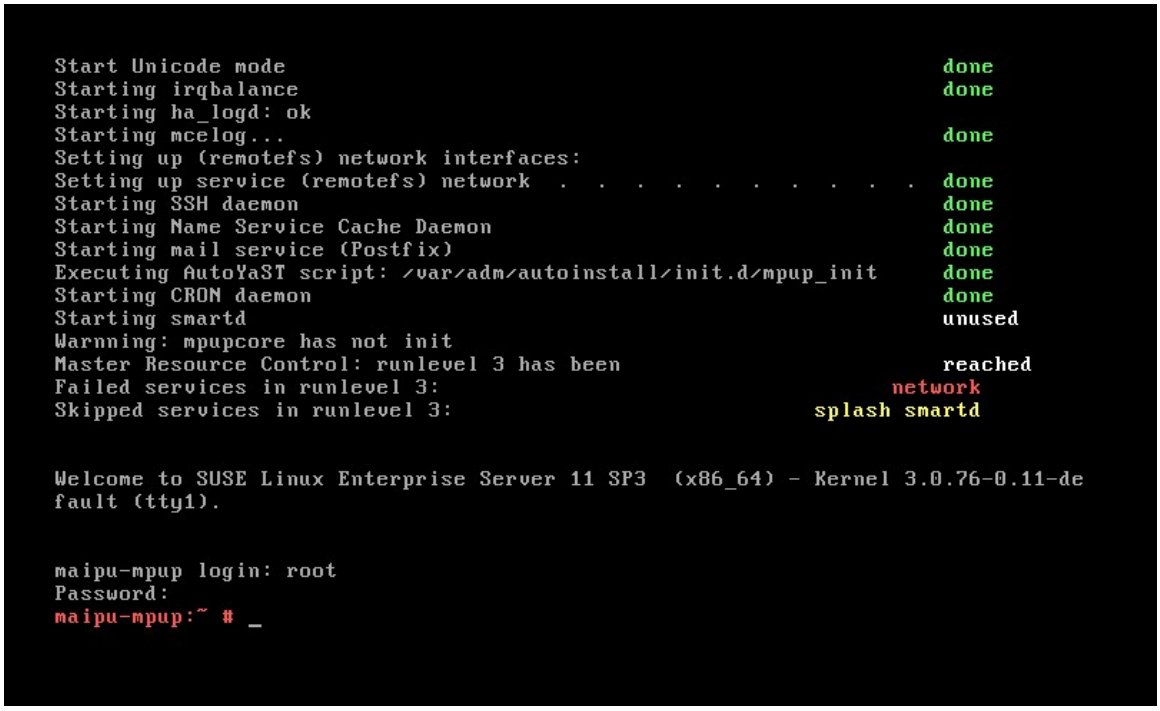
2.2 Install Standalone Mode

Before installing the standalone mode of Maipu AAS, you need to prepare one server: used to install the user authentication platform, marketing platform.

2.3.1 Install User Authentication Platform, Marketing Platform

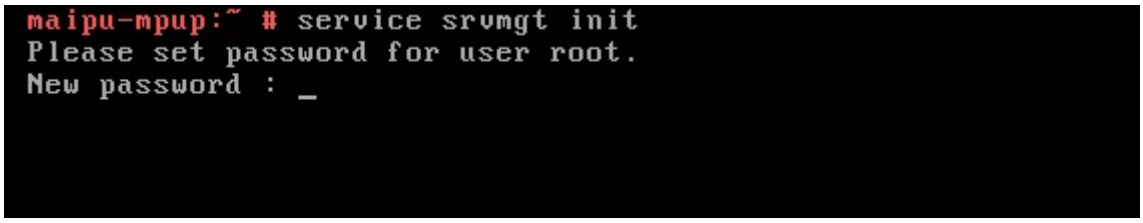
Step 1: After booting the U-disk via BIOS correctly, enter the following interface, and select “1 Setup Maipu AAS(V4) (CMP-Portal)(en)” to install the user authentication platform, marketing platform.

Step 2: After the system is installed automatically, input the user name and password to enter the operation system (the user name is root, and the default password is mproot).



2.3.2 Initialize User Authentication Platform, Marketing Platform

1. After installing, execute the **service srvmgt init** command to initialize the configuration. Before initializing, the user needs to re-set one password with higher security (the password should be more than six characters, and contain the upper case letter, lowercase letter, number, and special characters).



Initialize the basic service configuration:

[MPUP] Stop srvmgt service . . . [MPUP] done

[MPUP] ########################## Network config ##########################

IP Address : **[]:11.0.13.121** (Configure the IP address, input the planned server IP address)

IP Mask : **[]:255.255.255.0** (Configure the mask, input according to the actual network segment of the planned IP address)

Defalut Gateway: **[]:11.0.13.254** (Configure the default gateway of the server, input the network management address according to the actual network topology)

Host Domain : **[maipu-mpup]:aasv4** (Configure the host name, press Enter, that is, use the default value; if it is necessary to configure again, input directly, and then, press Enter)

2. Configure the mpsecsrv service, as follows:

Start mpsecsrv? (y/n) **[y]:** (the service is the security service; by default, it is enabled. Press Enter.)

3. Enable the HA configuration. Configure the HA and other information according to the actuality, as follows:

Configure HA? (y/n) **[n]:** (In the standalone mode, do not need to enable. By default, it is not enabled. Press Enter.)

4. Configure the ftp service.

Configure FTP Server? (y/n)**[n]:** (In the standalone mode, do not need to configure the ftp service. Press Enter.)

5. Configure the component service

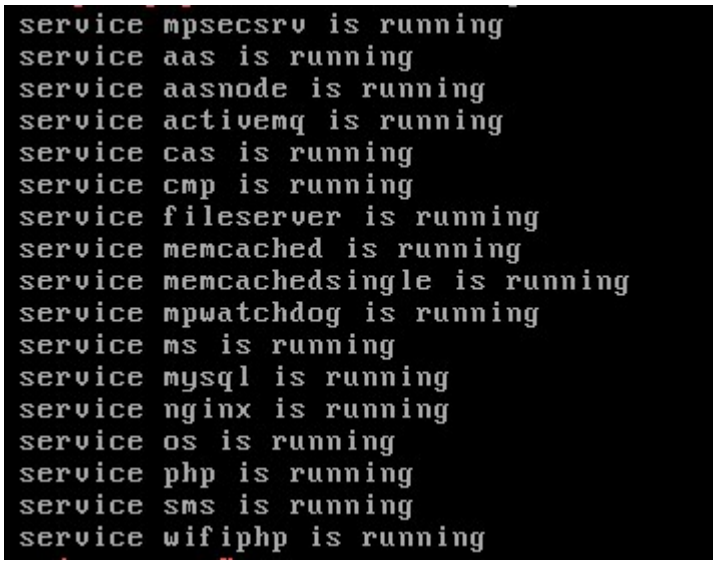
Configure application servers? (y/n) **[y]:** (Configure the component services? By default, it is y. Press Enter.)

6. For the other configuration items without special description, directly use the default values, and then, wait for initializing.

7. Execute the **service srvmgt start** command to start the system service.

2.3.3 Check Service Status of Standalone Mode

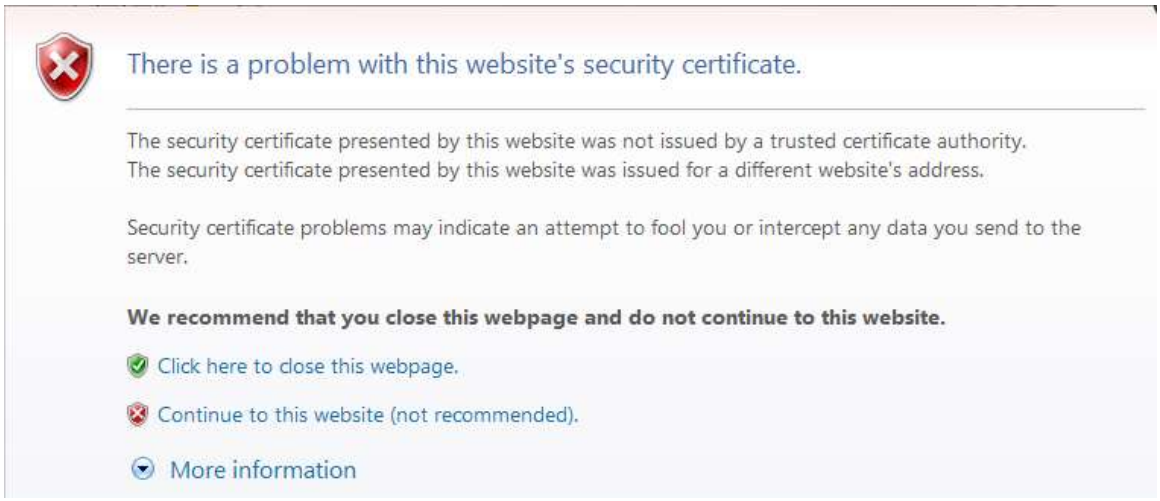
1. Execute the **service srvmgt status** command to view the boot status of the service.



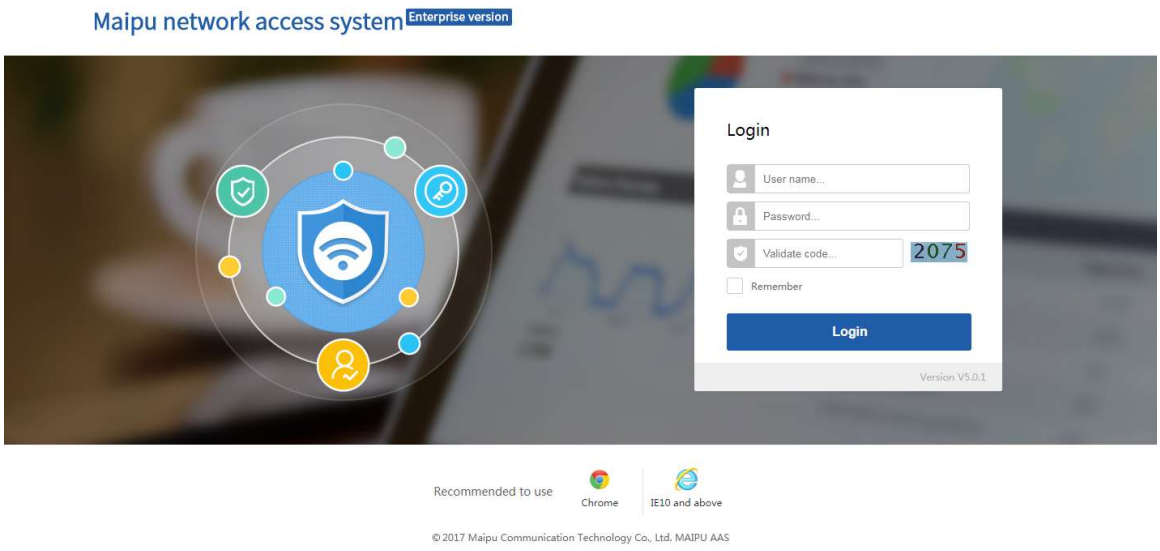
2. Access Maipu AAS via https://IP:8443, such as https://11.0.13.121:8443, as shown in the following figure:

(IP: the IP address of the installed server)

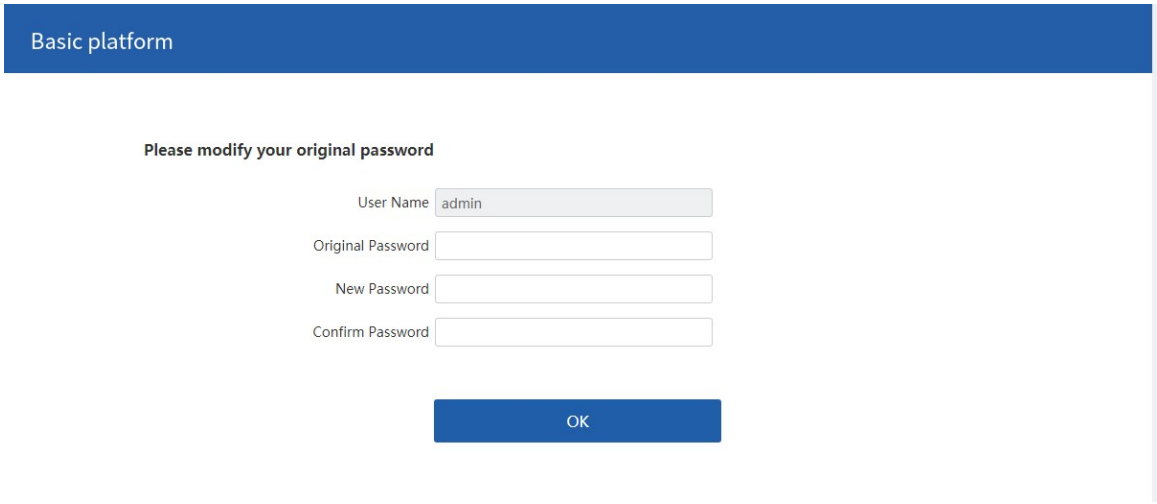
After installing, the certificate may not be trusted when accessing Maipu AAS for the first time, and the following interface appears:



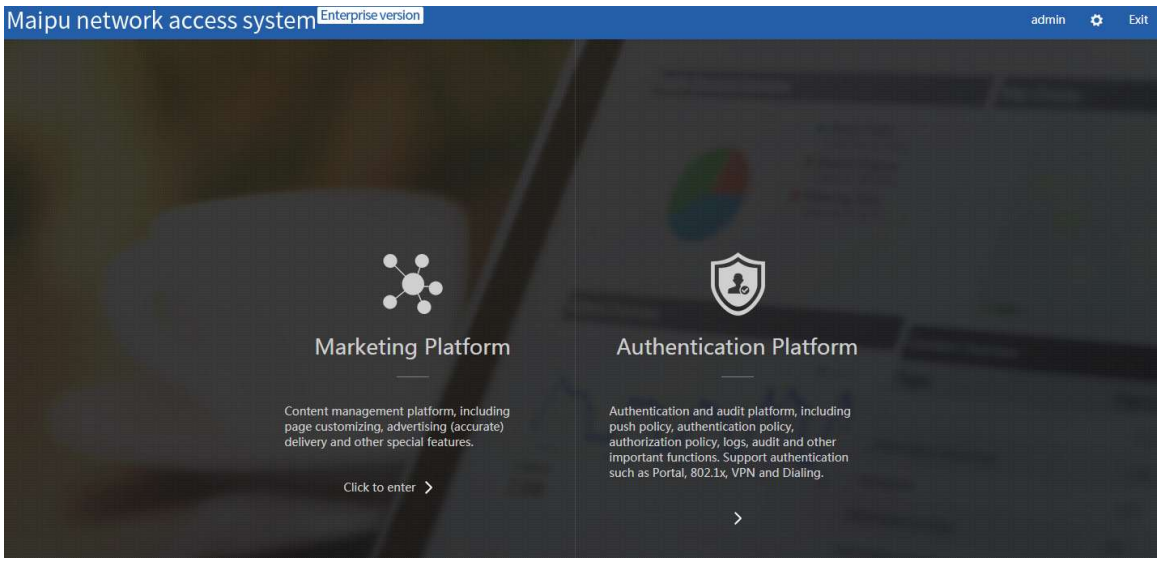
Click **Continue to this websit e(not recommended)**, and you can enter the login interface correctly:



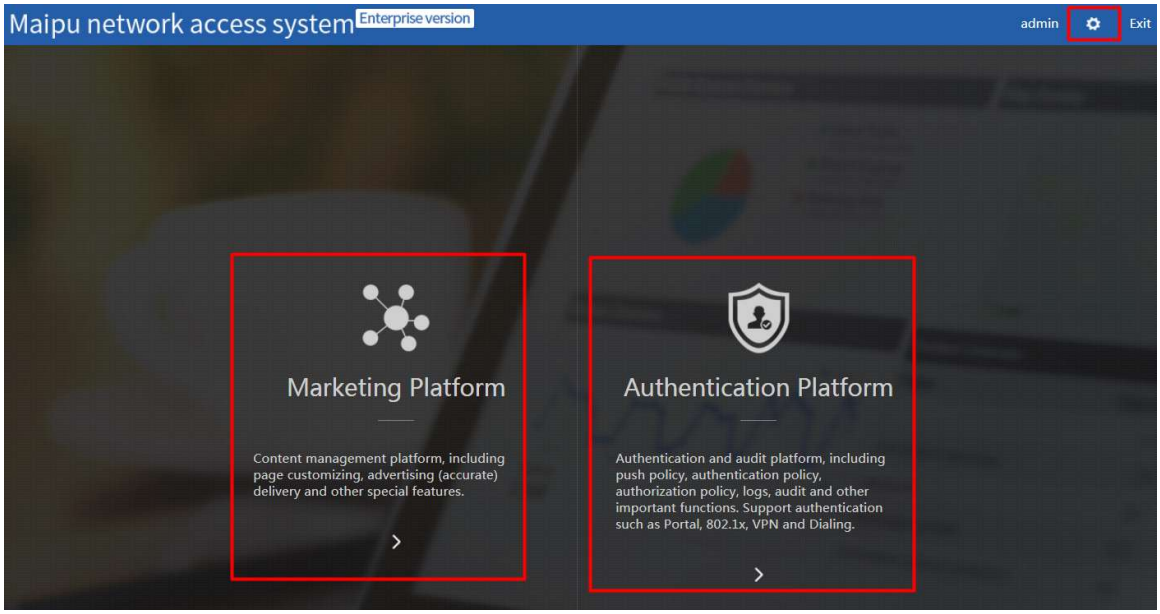
3. Input the default user name and password (admin/admin) and verification code to log in. After logging in successfully, the administrator modifies the initial password (the password should be more than six characters, and contain the uppercase letter, lowercase letter, number and special characters), as shown in the following figure:



4. After modifying the initial password, the user adopts the new password to log in again and enter the platform entrance interface, as shown in the following figure:



5. The user can click “Marketing Platform, Authentication Platform” to enter the component platform. Click the gear shape icon at the top right corner of the interface to enter the “Basic Platform”, as shown in the following figure:



6. If you can enter all platforms correctly and the menus can be loaded normally, it indicates that the installation is complete.

2.3 Install HA Dual-machine Hot Backup Mode

Before installing the system, prepare two servers according to the requirement for the server in the last chapter. One server serves as the active server, and install the user authentication platform and marketing platform. The other server serves as the standby server, and install the user authentication platform and marketing platform. The following describes how to install the system.

2.4.1 Install User Authentication Platform and Marketing Platform

Step 1: On the active server that needs to install the user authentication platform and marketing platform, boot the U-disk via BIOS correctly, and then, enter the following interface. Select “2 Setup Maipu AAS(V4) (CMP-Portal)”, and install the user authentication platform and marketing platform server.

Step 2: After installing the system, input the user name and password to enter the operation system (the user name is root, and the default password is mproot).

```
maipu-mpup login: root
Password:
maipu-mpup:~ # _
```

Step 3: Install the standby server. For the installation of the standby server, refer to the installation of the active server.

Caution

ISO version file contains all services of the system and AAS, so the installation may be slow. Please wait patiently.

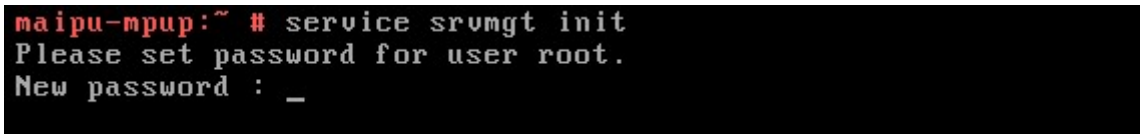
The server time should be consistent with the current time.

The hostnames of the active and standby servers cannot be the same.

2.4.2 Initialize User Authentication Platform and Marketing Platform on Active Server

1. After installing, execute the **service srvmgt init** command to initialize the configuration.

Before initializing the configuration, you need to re-set one password with higher security for the root user (the password should be more than six characters and contain the uppercase letter, lowercase letter, number and special characters).



2. Initialize the basic service configuration:

[MPUP] Stop srvmgt service . . . [MPUP] done

[MPUP] ########################## Network config ##########################

IP Address : **[]:11.0.13.121** (Configure the IP address of the service Ethernet port. Input the corresponding service IP address, and press Enter)

IP Mask : **[]:255.255.255.0** (Configure the mask of the service Ethernet port IP address. Input the mask of the service IP address, and press Enter)

Defalut Gateway: **[]:11.0.13.254** (Configure the gateway of the service Ethernet port IP address. Input the gateway of the service IP address, and press Enter)

Host Domain : [Linux]: **AASV4_MASTER** (Configure the host name. Input the host name, and press Enter)

3. Configure the mpsecsrv service, as follows:

Start mpsecsrv? (y/n) **[y]:** (The service is security service. By default, it is enabled. Press Enter)

4. Enable the HA configuration. Configure HA and other information according to the actuality, as follows:

Configure HA? (y/n) [n]: **y** (Whether to enable the HA active and standby mode? Input y to enable, and then, press Enter)

Please choose ha role(master/slave) : **master** (Input the role of the current server. Input master and press Enter)

Please choose extern interface(eth0/eth1) : **[eth0]** (Select the external

service Ethernet port. By default, use the first Ethernet port (that is eth0) as the service Ethernet port)

`Please choose HA heartbeat interface(eth0/eth1) : [eth1]` (Select the heartbeat Ethernet port. By default, use the second Ethernet port (that is eth1) as the service Ethernet port)

`Please input local host's ip address on HA interface 'eth1' : 2.2.2.1` (Input the IP address of the heartbeat Ethernet port. Here, you just need to ensure that the IP address and the heartbeat IP address of the standby server are in the same network segment)

`Please input local host's ip netmask on HA interface 'eth1' : [255.255.255.0]` (Input the subnet mask of the heartbeat Ethernet port)

`Please input peer ip address on HA interface : 2.2.2.2` (Input the IP address of the heartbeat Ethernet port of the standby server. Here, you need to ensure that the IP address is the same as the heartbeat IP address of the standby server)

`Please input peer full hostname : AASV4_SLAVE` (Input the host name of the standby server. It needs to be consistent with the configured host name of the standby server)

`Please input virtual ip address on eth0 : 11.0.13.123` (Input the virtual address. The external access is performed via the virtual address)

`Please input virtual netmask : [255.255.255.0]` (Input the subnet mask of the virtual address. The external access is performed via the virtual address)

`Enter advance config(y/n)? : [n] y` (Enter the advanced configuration, used by the serial port heartbeat and so on)

`Please input serial interface(none ttyS0 ttyS1) : [none]` (Configure the heartbeat address of the serial port as desired. If not configured, use the default value)

`Please input heartbeat deadtime : [20]` (Configure the heartbeat dead time according to the actual demand. Usually, adopt the default value)

`Please input ping node's ip address(input 0.0.0.0 means not config) : [0.0.0.0] [11.0.13.254]` (Configure the PingNode address. Configure the IP address in the same network segment as the service network card. Usually, configure the gateway address)

5. Wait for the script to install automatically, and prompt installing FTP, as follows:

`Configure FTP Server? ( y/n )[n]:` (Whether to configure the ftp server. Here, do not need to configure, but press Enter to adopt the default value)

6. Configure the component service

`Configure application servers? (y/n)` **`[y]:`** (Configure the component services? By default, it is y. Press Enter.)

7. Configure the external actual IP address of the node server. If there are multiple, separate by the space, as follows:

`Please input node address list(if more than one, please use the space division) : [127.0.0.1]` (Configure the external actual IP. Here, do not need to configure, but press Enter to adopt the default)

8. For the other configuration items without special description, directly use the default values, and then, wait for initializing.

Caution

The heartbeat addresses of the HA active and standby servers should be in the same segment. Otherwise, it may affect the HA communication of the active and standby servers.

If no special requirements for the HA advanced configuration, adopt the default values, and do not configure.

2.4.3 Initialize User Authentication Platform and Marketing Platform on Standby Server

1. After installing, execute the **service srvmgt init** command to initialize the configuration.

Set the security password for the root user of the standby server (the password should be more than six characters and contain the uppercase letter, lowercase letter, number and special characters).

2. Initialize the basic service configuration:

`[MPUP] Stop srvmgt service . . . [MPUP] done`

`[MPUP] ########################## Network config ##########################`

`Please input the index of the eth interface for service (0 - 1):` **`[0]:`** (Select the service Ethernet port. By default, use the first Ethernet port (eht0) as the service Ethernet port, and press Enter. If it is necessary to modify, input the corresponding network card ID, and press Enter)

IP Address : **[]:11.0.13.122** (Configure the IP address of the service Ethernet port. Input the corresponding service IP address, and press Enter)

IP Mask : **[]:255.255.255.0** (Configure the mask of the service Ethernet port IP address. Input the mask of the service IP address, and press Enter)

Defalut Gateway: **[]:11.0.13.254** (Configure the gateway of the service Ethernet port IP address. Input the gateway of the service IP address, and press Enter)

Host Domain : [Linux]: **AASV4_SLAVE** (Configure the host name. Input the host name, and press Enter)

3. Configure the mpsecsrv service, as follows:

Start mpsecsrv? (y/n) **[y]:** (The service is security service. By default, it is enabled. Press Enter)

4. Enable the HA configuration. Configure HA and other information according to the actuality, as follows:

Configure HA? (y/n) [n]: **y** (Whether to enable the HA active and standby mode? Input y to enable, and then, press Enter)

Please choose ha role(master/slave) : **slave** (Input the role of the current server. Input master and press Enter)

Please choose extern interface(eth0/eth1) : **[eth0]** (Select the external service Ethernet port. By default, use the first Ethernet port (eth0) as the service Ethernet port)

Please choose HA heartbeat interface(eth0/eth1) : **[eth1]** (Select the heartbeat Ethernet port. By default, use the second Ethernet port (that is eth1) as the service Ethernet port)

Please input local host's ip address on HA interface 'eth1' : **2.2.2.2** (Input the IP address of the heartbeat Ethernet port. Here, you just need to ensure that the IP address and the heartbeat IP address of the active server are in the same network segment)

Please input local host's ip netmask on HA interface 'eth1' : **[255.255.255.0]** (Input the subnet mask of the heartbeat Ethernet port)

Please input peer ip address on HA interface : **2.2.2.1** (Input the IP address of the heartbeat Ethernet port of the active server. Here, you need to ensure that the IP address is the same as the heartbeat IP address of the active server)

Please input peer full hostname : **AASV4_MASTER** (Input the host name of the active server. It needs to be consistent with the configured host name of the active server)

`Please input virtual ip address on eth0 :` **`11.0.13.123`** (Input the virtual address, the same as the active server. The external access is performed via the virtual address)

`Please input virtual netmask :` **`255.255.255.0`** (Input the subnet mask of the virtual address, the same as the active server. The external access is performed via the virtual address)

`Enter advance config(y/n)? : [n]` **`y`** (Enter the advanced configuration, used by the serial port heartbeat and so on)

`Please input serial interface(none ttyS0 ttyS1) :` **`[none]`** (Configure the heartbeat address of the serial port as desired. If not configured, use the default value)

`Please input heartbeat deadtime :` **`[20]`** (Configure the heartbeat dead time according to the actual demand. Usually, adopt the default value)

`Please input ping node's ip address(input 0.0.0.0 means not config) : [0.0.0.0]` **`[11.0.13.254]`** (Configure the PingNode address. Configure the IP address in the same network segment as the service network card. Usually, configure the gateway address)

5. Wait for the script to install automatically, and prompt installing FTP, as follows:

`Configure FTP Server? ( y/n )` **`[n] :`** (Whether to configure the ftp server. Here, input n.)

6. Configure the component service.

`Configure application servers? (y/n)` **`[y] :`** (Configure the component services? By default, it is y. Press Enter.)

Configure the external actual IP address of the node server. If there are multiple, separate by the space, as follows:

`Please input node address list(if more than one, please use the space division) : [127.0.0.1]` (Configure the external actual IP. Here, do not need to configure, but press Enter to adopt the default)

7. For the other configuration items without special description, directly use the default values, and then, wait for initializing.

Caution

- When starting the server of the HA mode, you need to start the active server first. After the active server is started, start the standby server.

- After the active and standby servers are re-started and if the active and standby synchronization status is not consistent with the status in 2.4.8 of the section, execute the command of synchronizing data: service srvmgt config db dbload-frompeer.

2.4.4 Start System Services of Active and Standby Servers

After initializing the system, start the service:

1. Enter the active server, and execute the **service srvmgt start** command to start the active server.
2. After starting the active server, enter the standby server and execute the **service srvmgt start** command to start the system service of the standby server.

2.4.5 Synchronize Active and Standby Data of HA Dual-machine Hot Backup Mode

For the first installation, you need to synchronize the active and standby data on the standby server manually. Before synchronizing data, please check the time of the active and standby servers. You can synchronize the data only when the time of the active server is synchronous with the time of the standby server. If the time of the active server is not consistent with the time of the standby server, please set.

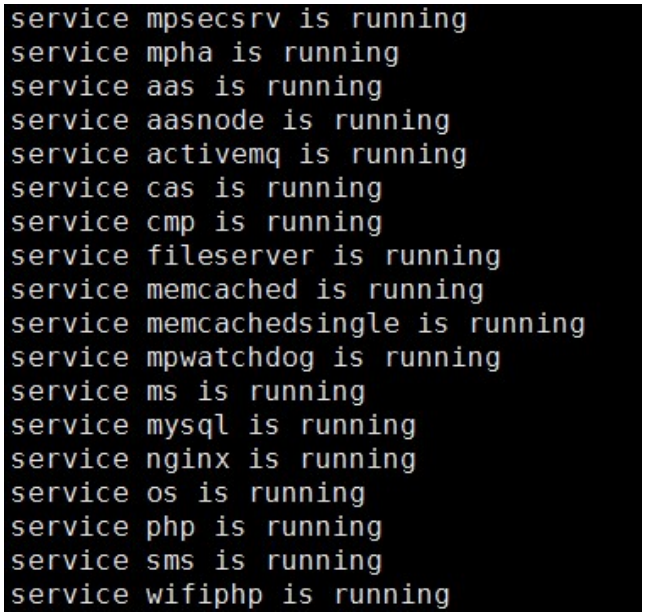
In the standby server, synchronize the data in the active server:

```
AASV4_Slave:~ # service srvmgt config db dbload-frompeer
  Warning:
        The program will drop local mysql data, and sync from
peer!!!!!!
  Confirm(y/n)? : [n] y
  * Start 'mysql' service...
  * Stop local slave
  * Dump remote database to local , this can take a long time ...
  * Set remote slave pos
  * Start local slave
  * mysql: Wait sync-from-peer...
```

```
* mysql: Wait sync-from-peer finishd
* Load memcache from peer...
* Stop memcache
* memcache: Wait sync from peer...
* memcache: Wait a few...
* memcache: Wait sync-from-peer finished
```

2.4.6 Check Service Status of HA Dual-machine Hot Backup Mode

1. In the active server, execute the **service srvmgt status** command, and the result is as follows:



2. In the active server, execute the **service mpha status** command and the result is as follows:

```
NodeList
   Master: master (Current - Active)
   Slave : slave
Heartbeat interface Status
   [eth1] UP
VIP Status
   [10.10.8.153] - UP
Services Status
   [mysql] UP HealthOK
   [memcached] UP HealthOK
   [memcachedsingle] UP HealthOK
   [nginx] UP HealthOK
   [php] UP HealthOK
   [activemq] UP HealthOK
   [cas] UP HealthOK
   [ms] UP HealthOK
   [os] UP HealthOK
   [aas] UP HealthOK
   [aasnode] UP HealthOK
   [sms] UP HealthOK
   [wifiphp] UP HealthOK
   [cmp] UP HealthOK
   [fileserver] UP HealthOK
MySQL replication Status
   [IO Thread] DOWN
   [Slave Thread] DOWN
Memcached Status
   [Total] 33
DB2MC status
   not load
```

3. In the standby server, execute the **service srvmgt status** command and the result is as follows:

```
service mpsecsrv is running
service mpha is running
service aas is stoped
service aasnode is stoped
service activemq is running
service cas is running
service cmp is stoped
service fileserver is running
service memcached is running
service memcachedsingle is running
service mpwatchdog is running
service ms is stoped
service mysql is running
service nginx is running
service os is running
service php is running
service sms is stoped
service wifiphp is stoped
```

4. In the standby server, execute the **service mpha status** command and the result is as follows:

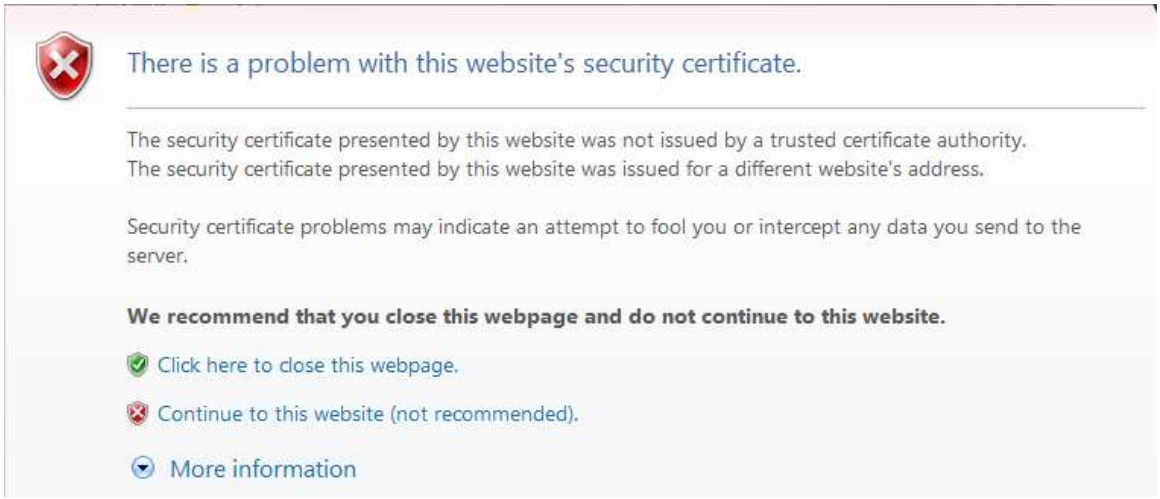
Caution

- On the standby server installed with the user authentication platform and marketing platform, only enable the mpsecsrv, mpha, mysql, memerched, memcachedsingle, activemq, cas, fileserver, mpwatchdog, nginx, php, and os services. When the active and standby server switch, the standby server enables the other services.

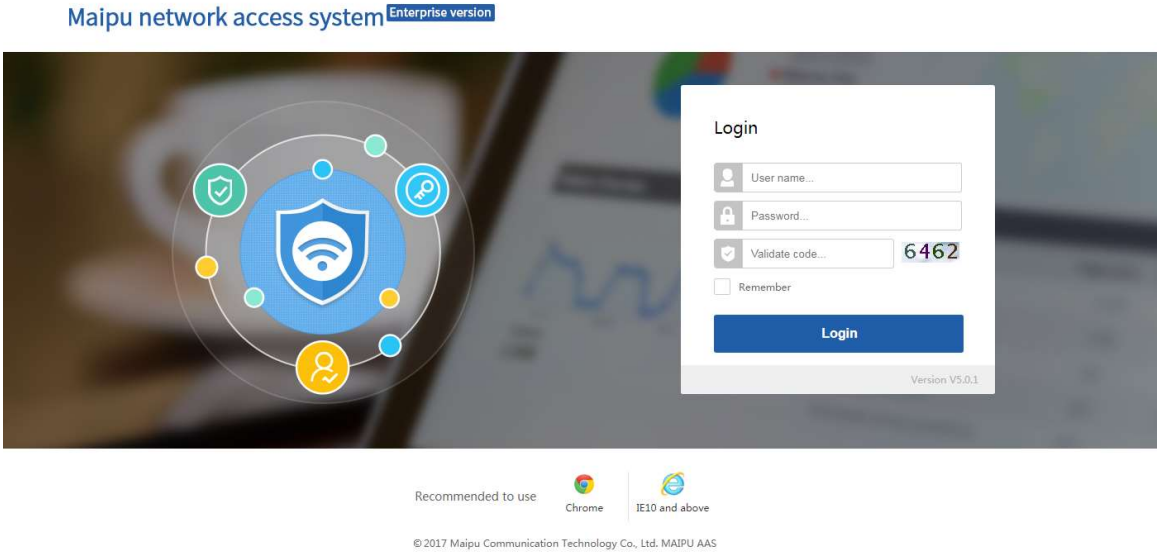
5. Access Maipu AAS via https://IP:8443, such as https://11.0.13.123:8443.

(HA dual-machine hot backup mode, the accessed IP address is the virtual IP address filled for the active and standby servers.)

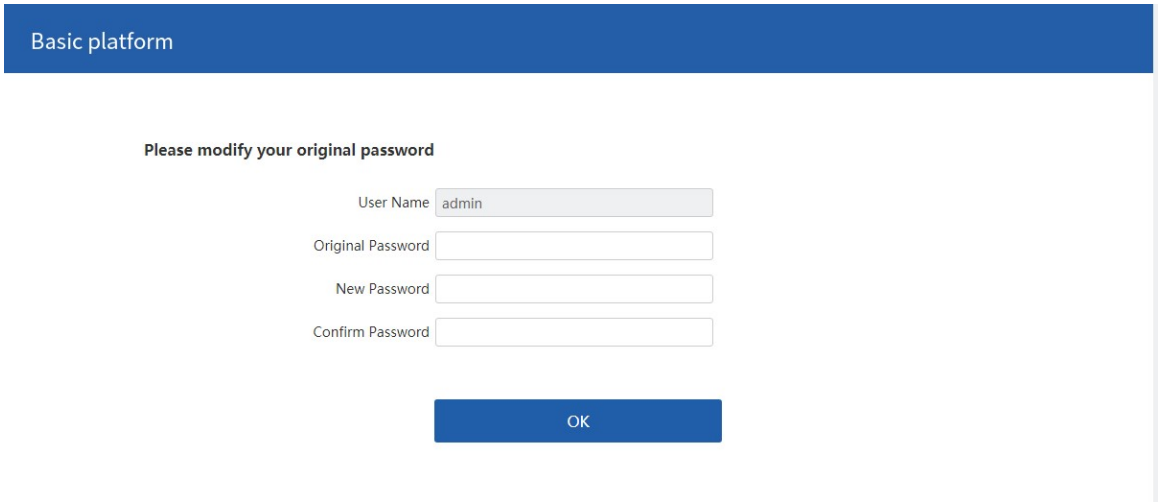
After installing, the certificate may not be trusted when accessing Maipu AAS for the first time, and the following interface is displayed:



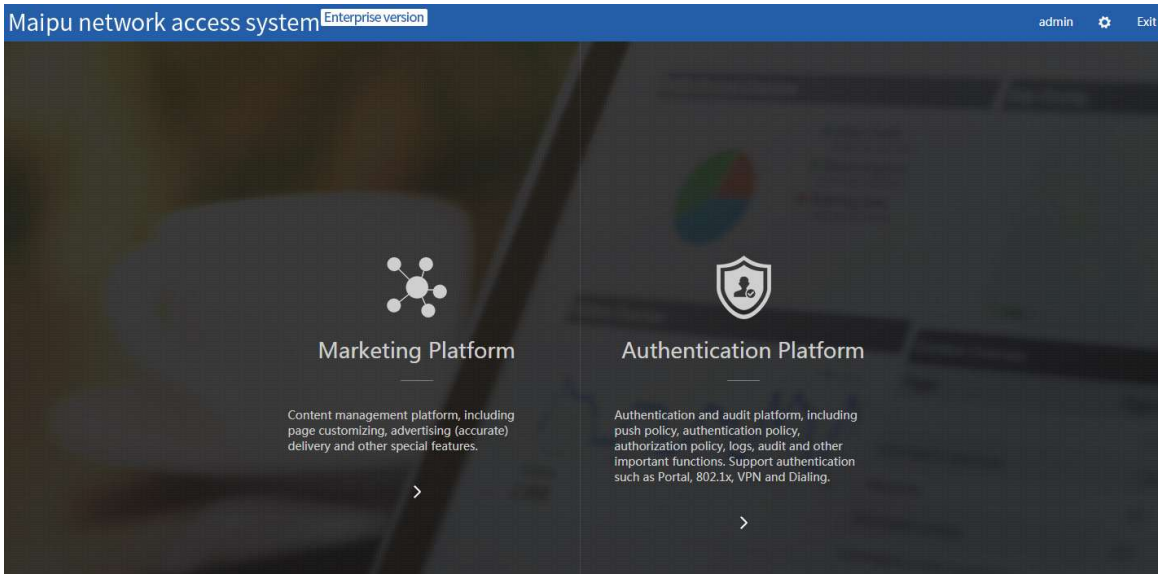
Click **Continue to this websit e(not recommended)** and you can enter the login interface correctly:



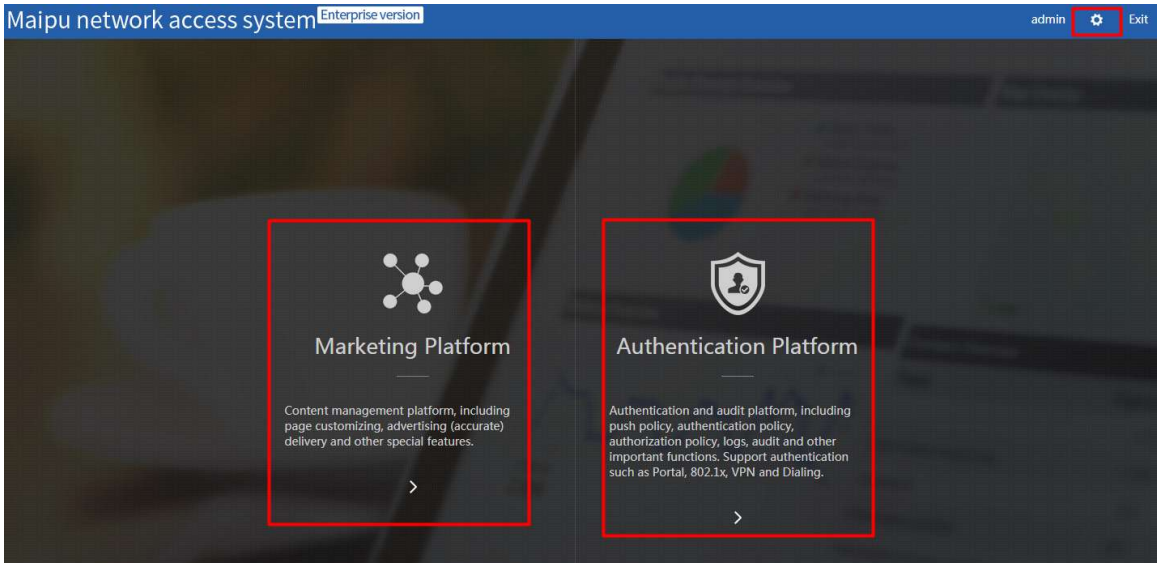
6. Input the default user name and password (admin/admin) and verification code to log in. After logging in successfully, the administrator modifies the initial password (the password should be more than six characters, and contain the uppercase letter, lowercase letter, number and special characters), as shown in the following figure:



7. After the administrator modifies the password, the user adopts the new password to log in again and enter the platform entrance interface, as shown in the following figure:



8. The user can click “Marketing Platform, Authentication Platform” to enter the component platform. Click the gear shape icon at the top right corner of the interface to enter the “Basic Platform”, as shown in the following figure:



9. If you can enter all platforms correctly and the menus can be loaded normally, it indicates that the installation is complete.

3.Maipu AAS Software Package Installation

This chapter describes the installation of the user authentication platform and marketing platform, and fast configuration via the SH software package on the operating system. The configuration in the installation deployment of this document takes the figure in section 1.2.3 “Network Topology” to describe. In the actuality. In the actual use, follow the deployment.

3.1Install Standalone Mode

3.1.1 Install All Services

Copy the installation package to the desired server. For example, in the /home/ directory, need to install the basic platform, authentication platform, and marketing platform on the server. The installation is as follows:

1. Linux:~ # **sh /home/ Maipu-AASV4-CMPPortal-SUSE-EN-V3R2C03BXXXX.sh install** (install the script)

(Maipu-AASV4-CMPPortal-SUSE-EN-V3R2C03BXXXX.sh is the installation package of containing the basic platform, wifi user authentication platform, and marketing platform.)

2. Wait for the script to install, and display the following interface: Input the installation path, press Enter, and the script is installed in /home/mpup/mpup by default.

```
[enterprisescene-cmpportal] Verifying archive integrity... All good.
[enterprisescene-cmpportal] Uncompressing enterprisescene-cmpportal  installer-
Done
[enterprisescene-cmpportal] Input setup dest path: [/home/mpup/mpup]
```

3. Wait for the script to install, and display the following interface: Press Enter, and confirm the installation.

```
--------------------------------------------------------------------------------
Setup Maipu AAS(V4) (CMP-Portal)(en)
--------------------------------------------------------------------------------
The setup program will install files
[enterprisescene-cmpportal] Confirm install [y/n]? : [y] _
```

4. Display the following interface, indicating that the installation is complete:

```
[enterprisescene-cmpportal] [INFO] Call scene ./_callbackscript/cbkscene.sh (pos
tinstall)
[enterprisescene-cmpportal] [INFO] [INSTALL] Backup setup files ...
[enterprisescene-cmpportal] [INFO] [INSTALL] Finished
[enterprisescene-cmpportal] INFO all packages has been installed successfully!
```

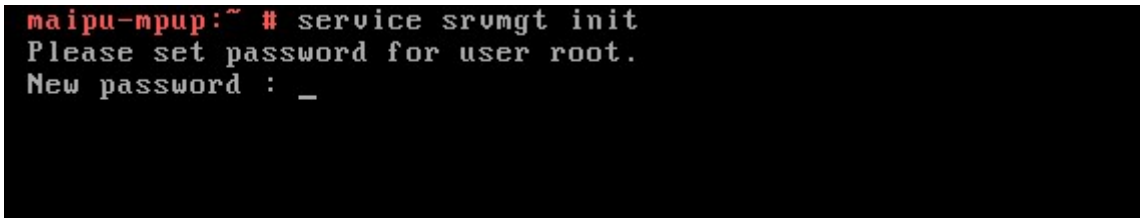
Caution

- If the version is installed wrongly, you can uninstall the program according to the uninstalling mode in chapter 5, and then, select the correct installation package to install the system again.

3.1.2 Initializing Service

After installation, you need to perform the initialization operation, initializing the database and component system configuration.

1. After installation, execute the **service srvmgt init** command to initialize the configuration. Before initializing, you need to set one password with higher security for the root user (the password should be larger than six characters, and contain uppercase letter, lowercase letter, number and special characters).



2. Initialize the basic service configuration:

[MPUP] Stop srvmgt service . . . [MPUP] done

[MPUP] ########################## Network config ##########################

Please input the index of the eth interface for service (0 - 1): **[0]**

(Select the service Ethernet port. By default, use the first Ethernet port (eht0) as the service Ethernet port, and press Enter. If it is necessary to modify, input the corresponding network card ID, and press Enter. If there is only one network card, the option is not available)

IP Address : **[11.0.13.121]:** (Configure the IP address. Press Enter to adopt the default IPv4 address of the local device. To re-configure, directly input and press Enter.)

IP Mask : **[255.255.255.0]:** (Configure the mask. Press Enter to adopt the default mask of the local device. To re-configure, directly input and press Enter.)

Defalut Gateway: **[11.0.13.254]:** (Configure the default gateway of the server. Press Enter to adopt the default gateway of the local device. To re-configure, directly input and press Enter.)

Host Domain : [maipu-mpup]**:aasv4** (Configure the host name. Press Enter to adopt

the default value. To re-configure, directly input and press Enter.)

3. Configure the mpsecsrv service, as follows:

`Start mpsecsrv? (y/n)` **`[y]:`** (The service is the security service. By default, it is enabled. Press Enter)

4. Enable the HA configuration. Configure HA and other information according to the actuality, as follows:

`Configure HA? (y/n) [n]:` **`n`** (In the standalone mode, do not need to enable. By default, it is disabled. Press Enter)

5. Install the ftp service.

`Configure FTP Server? ( y/n )[n]:` (In the standalone deployment mode, do not need to configure the ftp service, but just need to press Enter)

6. Configure the component service.

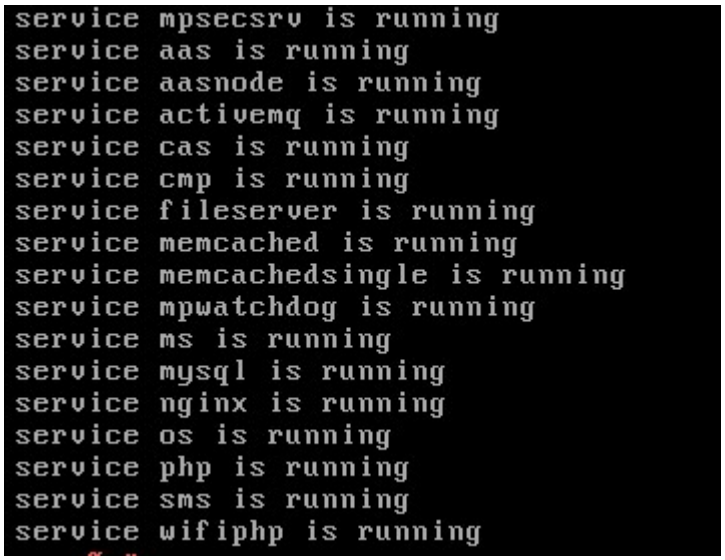
`Configure application servers? (y/n)` **`[y]:`** (Configure the component service to take effect. By default, it is y. Press Enter)

7. For the other configuration items without special description, directly use the default values, and then, wait for initializing.

8. Execute the **service srvmgt start** command to start the system service.

3.1.3 Check Service Status of Standalone Mode

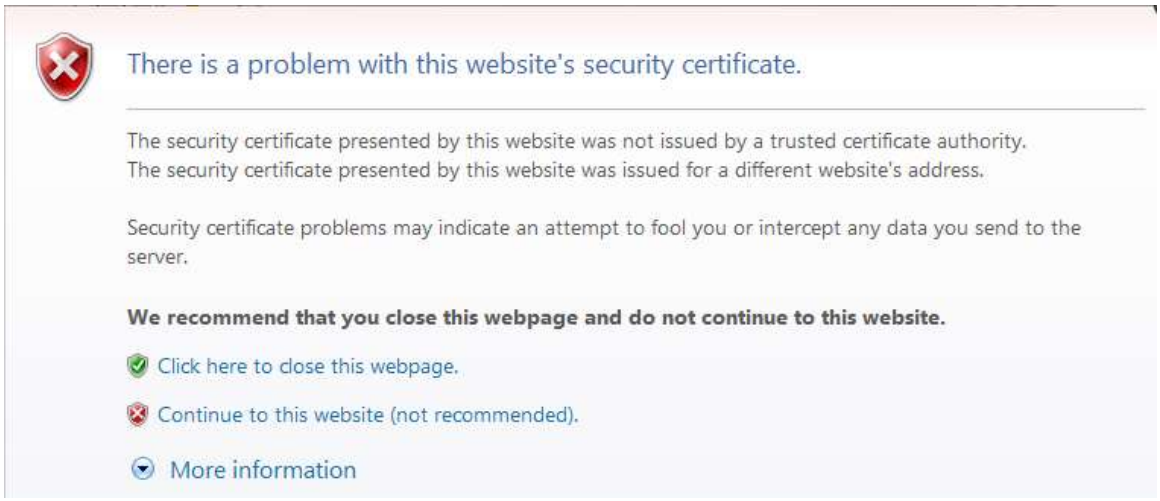
1. After enabling the user authentication platform and marketing platform, execute the **service srvmgt status** command, and the result is as follows:



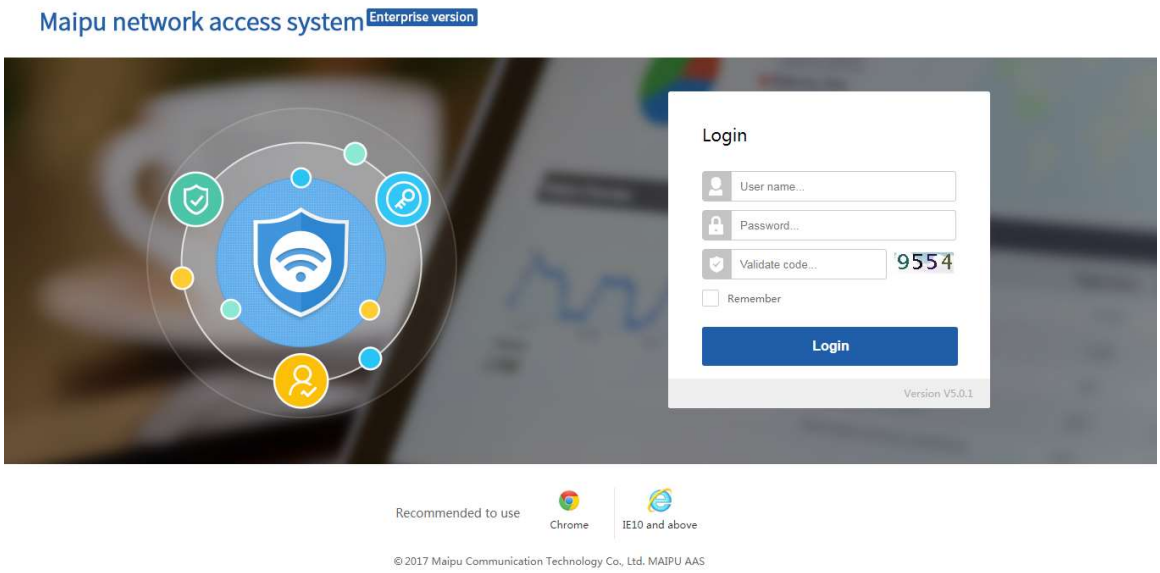
2. Access Maipu AAS via https://IP:8443, such as https://11.0.13.121:8443.

   (IP: the IP address of the server of installing the scenario package Maipu-AASV4-CMPPortal-SUSE-EN-V3R2C03BXXXX.sh)

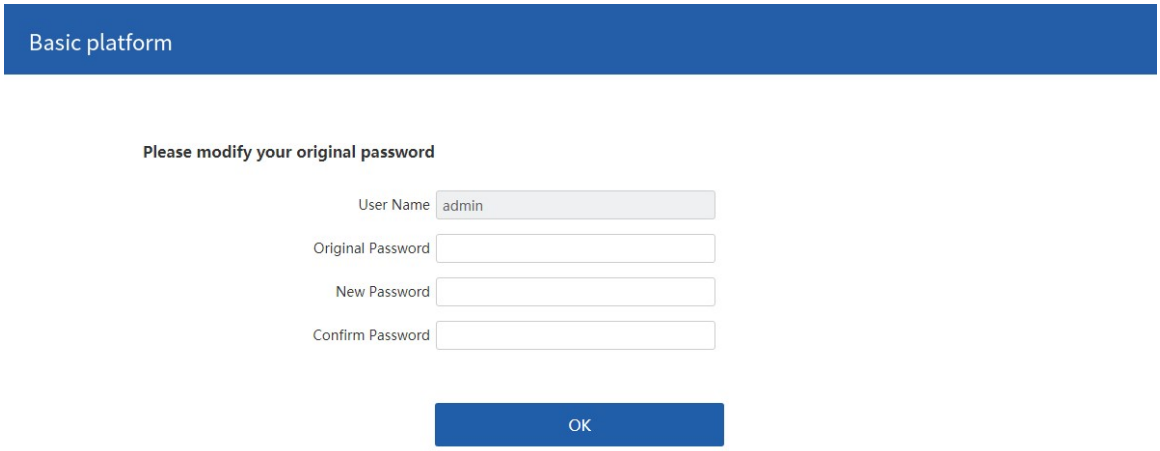
   After installing, the certificate may not be trusted when accessing Maipu AAS for the first time, and the following interface is displayed:



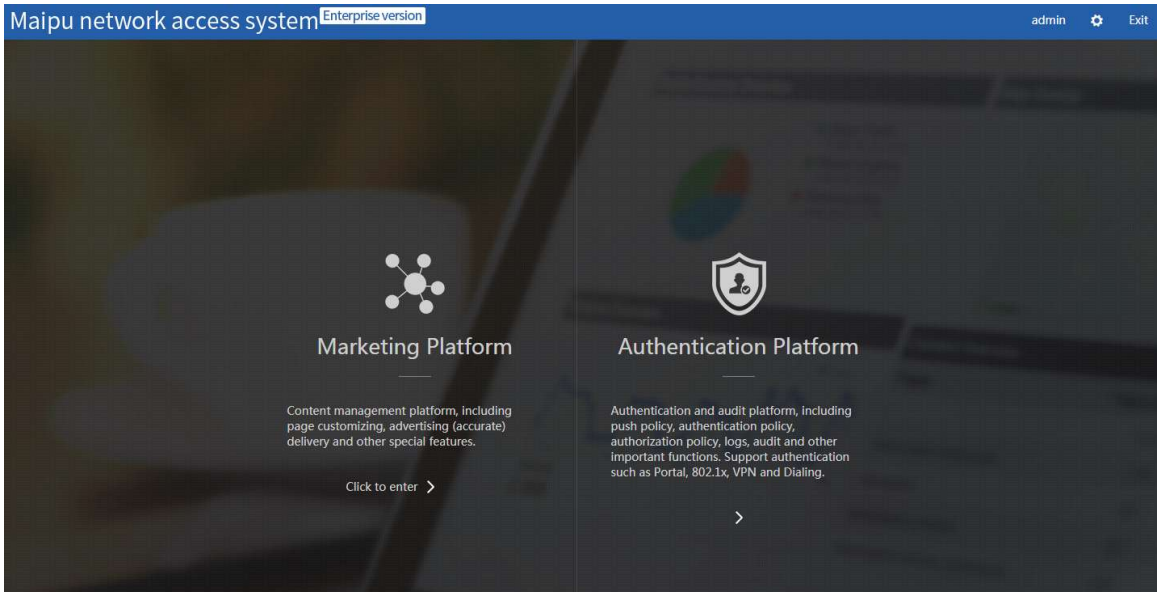
   Click **Continue to this website(not recommended)** and you can enter the login interface correctly:



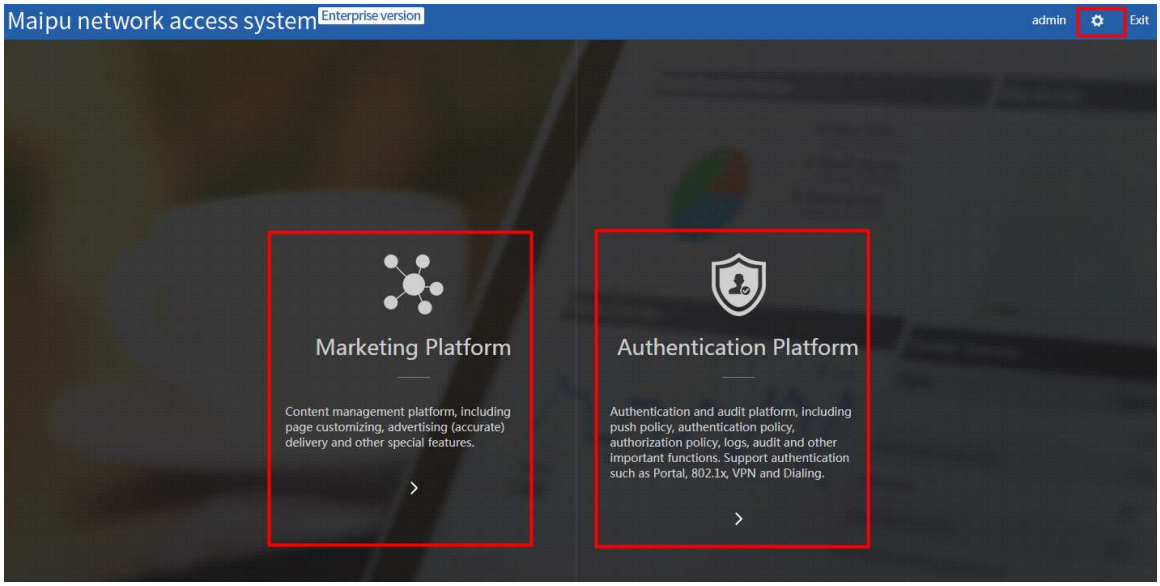
3. Input the default user name and password (admin/admin) and verification code to log in. After logging in successfully, the administrator modify the initial password (the password should be more than six characters, and contain the uppercase letter, lowercase letter, number and special characters), as shown in the following figure:



4. After modifying the password successfully, the user adopts the new password to log in again:



5. The user can click “Marketing Platform, Authentication Platform” to enter the component platform. Click the gear shape icon at the top right corner of the interface to enter the “Basic Platform”, as shown in the following figure:



6. If you can enter all platforms correctly and the menus can be loaded normally, it indicates that the installation is complete.

3.2 Install HA Dual-machine Hot Backup Mode

3.2.1 Install the Active Server of User Authentication Platform and Marketing Platform

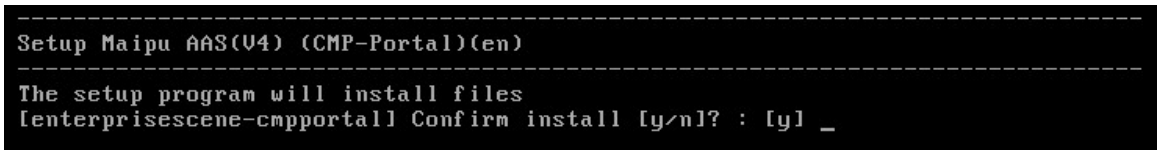
Copy the installation package to the desired server. For example, in the /home/ directory, need to install the platform, Wifi authentication platform and marketing platform on the server. The installation is as follows:

1. Linux:~ # sh /home/Maipu-AASV4-CMPPortal-SUSE-EN-V3R2C03BXXXX.sh install (Execute the installation script) (Maipu-AASV4-CMPPortal-SUSE-EN-V3R2C03BXXXX.sh is the installation package of containing the basic platform, user authentication platform, marketing platform)
2. Wait for the script to install automatically until displaying the following interface: Input the installation path, press Enter, and the script is installed in /home/mpup/mpup by default.

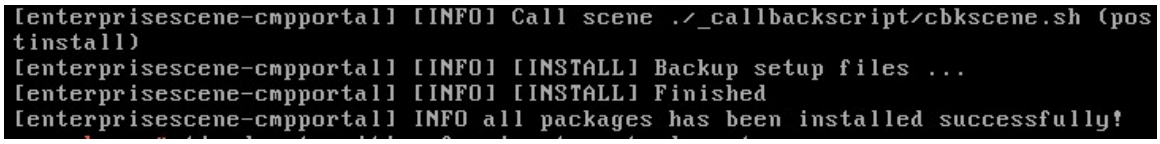
```
[enterprisescene-cmpportal] Verifying archive integrity... All good.
[enterprisescene-cmpportal] Uncompressing enterprisescene-cmpportal  installer-
Done
[enterprisescene-cmpportal] Input setup dest path: [/home/mpup/mpup]
```

3. Wait for the script to install automatically until displaying the following interface: Confirm

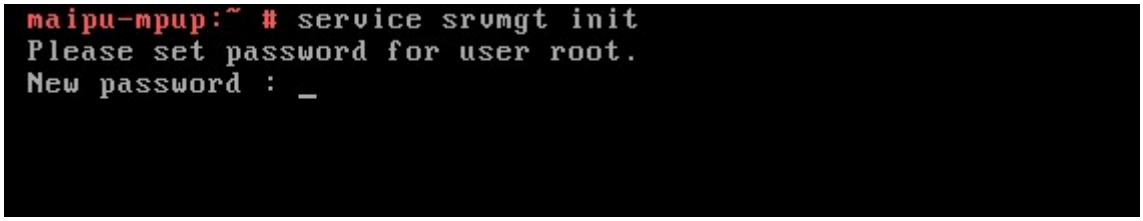
installing the cmpportal component. Input y, and press Enter.



4. Display the following interface, indicating that the installation is complete:



5. After installing, execute the **service srvmgt init** command to initialize the configuration. Before initializing, the user needs to set one password with higher security for the root user (the password should be more than six characters, and contain the upper case letter, lowercase letter, number, and special characters).



6. Initialize the basic service configuration:

[MPUP] Stop srvmgt service . . . [MPUP] done

[MPUP] ########################## Network config ##########################

Please input the index of the eth interface for service (0 - 1): **[0]**

(Select the service Ethernet port. By default, use the first Ethernet port (eht0) as the service Ethernet port, and press Enter. If it is necessary to modify, input the corresponding network card ID, and press Enter. If there is only one network card, the option is not available)

IP Address : **[11.0.13.121]:** (Configure the IP address of the service Ethernet port. By default, adopt the configured IP of eth0, and press Enter; to modify, input the corresponding service IP address, and press Enter)

IP Mask : **[255.255.255.0]:** (Configure the mask of the service Ethernet port IP address. By default, adopt the configured mask of eth0, and press Enter; to modify, input the mask of the corresponding service IP address, and press Enter)

Defalut Gateway: **[11.0.13.254]:** (Configure the gateway of the service Ethernet port IP address. By default, adopt the configured gateway of eth0, and press Enter; to modify, input the gateway of the corresponding service IP address, and press Enter)

Host Domain : [Linux]: **AASV4_MASTER.site** (Configure the host name. By default, adopt the current host name, and press Enter; to modify, input the host name and press Enter)

7. Configure the mpsecsrv service, as follows:

Start mpsecsrv? (y/n) **[y]:** (The service is the security service. By default, it is enabled. Press Enter)

8. Enable the HA configuration. Configure HA and other information according to the actuality, as follows:

Configure HA? (y/n) [n]: **y** (whether to enable the HA master/slave mode; by default, do not enable; input y and press Enter)

Please choose ha role(master/slave) : **master** (Input the role of the current server; input master and directly press Enter)

Please choose extern interface(eth0/eth1) : **[eth0]** (Select the external service Ethernet port. By default, use the first Ethernet port (that is eth0) as the service Ethernet port)

Please choose HA heartbeat interface(eth0/eth1) : **[eth1]** (Select the heartbeat Ethernet port. By default, use the second Ethernet port (that is eth1) as the service Ethernet port)

Please input local host's ip address on HA interface 'eth1' : **2.2.2.1**

(Input the IP address of the heartbeat Ethernet port. Here, you just need to ensure that the IP address and the heartbeat IP address of the standby server are in the same network segment)

Please input local host's ip netmask on HA interface 'eth1' : **[255.255.255.0]** (Input the subnet mask of the heartbeat Ethernet port)

Please input peer ip address on HA interface : **2.2.2.2** (Input the IP address of the heartbeat Ethernet port of the standby server. Here, you need to ensure that the IP address is the same as the heartbeat IP address of the standby server)

Please input peer full hostname : **AASV4_SLAVE.Site** (Input the host name of the standby server. It needs to be consistent with the configured host name of the standby server)

Please input virtual ip address on eth0 : **11.0.13.123** (Input the virtual address. The external access is performed via the virtual address)

Please input virtual netmask : **[255.255.255.0]** (Input the subnet mask of the virtual address. The external access is performed via the virtual address)

`Enter advance config(y/n)? :` **`[n]`** (Enter the advanced configuration; by default, select n, used by the serial port heartbeat and so on. Usually, it is not configured)

used by the serial port heartbeat and so on)

9. Wait for the script to install automatically, and prompt installing FTP, as follows:

`Configure FTP Server? (y/n)` **`[n]:`** (Whether to configure the ftp server. Here, input n, and do not configure the ftp server)

10. Configure the component service

`Configure application servers? (y/n)` **`[y]:`** (Configure the component services? By default, it is y. Press Enter.)

11. Configure the external actual IP address of the node server. If there are multiple, separate by the space, as follows:

`Please input node address list(if more than one, please use the space division) : [127.0.0.1]` (Configure the external actual IP. Here, do not need to configure, but press Enter to adopt the default)

12. For the other configuration items without special description, directly use the default values, and then, wait for initializing

13. After installation, execute the **service srvmgt start** command to start all services.

3.2.2 Install the Standby Server of User Authentication Platform and Marketing Platform

Copy the installation package to the desired server. For example, in the /home/ directory, need to install the platform, Wifi authentication platform and marketing platform on the server. The installation is as follows:

1. Linux:~ # sh /home/Maipu-AASV4-CMPPortal-SUSE-EN-V3R2C03BXXXX.sh install (Execute the installation script) (Maipu-AASV4-CMPPortal-SUSE-EN-V3R2C03BXXXX.sh is the installation package of containing the basic platform, user authentication platform, marketing platform)

2. Wait for the script to install automatically until displaying the following interface: Input the installation path, press Enter, and the script is installed in /home/mpup/mpup by default.

```
[enterprisescene-cmpportal] Verifying archive integrity... All good.
[enterprisescene-cmpportal] Uncompressing enterprisescene-cmpportal  installer-
Done
[enterprisescene-cmpportal] Input setup dest path: [/home/mpup/mpup]
```

3. Wait for the script to install automatically until displaying the following interface: Confirm installing the cmpportal component. Input y, and press Enter.

```
--------------------------------------------------------------------------------
Setup Maipu AAS(V4) (CMP-Portal)(en)
--------------------------------------------------------------------------------
The setup program will install files
[enterprisescene-cmpportal] Confirm install [y/n]? : [y] _
```

4. Display the following interface, indicating that the installation is complete:

```
[enterprisescene-cmpportal] [INFO] Call scene ./_callbackscript/cbkscene.sh (pos
tinstall)
[enterprisescene-cmpportal] [INFO] [INSTALL] Backup setup files ...
[enterprisescene-cmpportal] [INFO] [INSTALL] Finished
[enterprisescene-cmpportal] INFO all packages has been installed successfully!
```

5. After installing, execute the **service srvmgt init** command to initialize the configuration. Before initializing, the user needs to set one password with higher security for the root user (the password should be more than six characters, and contain the upper case letter, lowercase letter, number, and special characters).

```
maipu-mpup:~ # service srvmgt init
Please set password for user root.
New password : _
```

6. Initialize the basic service configuration:

```
[MPUP] Stop srvmgt service . . . [MPUP] done

[MPUP] ########################## Network config ##########################

Found Multi-Ethernet Interfaces:

Index   IfName    MAC               IP                Linked

[0]     eth0     00:0C:29:33:F3:B9    11.0.13.122         yes
[1]     eth1     00:0C:29:33:F3:C3                        no
Please input the index of the eth interface for service (0 - 1): [0]:
```

(Select the service Ethernet port. By default, use the first Ethernet port (eht0) as the service Ethernet port, and press Enter. If it is necessary to modify, input the corresponding network card ID, and press Enter.)

```
IP Address : [11.0.13.122]:
```
(Configure the IP address of the service Ethernet port. By default, adopt the configured IP of eth0, and press Enter; to modify, input the

corresponding service IP address, and press Enter)

IP Mask : **[255.255.255.0]:** (Configure the mask of the service Ethernet port IP address. By default, adopt the configured mask of eth0, and press Enter; to modify, input the mask of the corresponding service IP address, and press Enter)

Defalut Gateway: **[11.0.13.254]:** (Configure the gateway of the service Ethernet port IP address. By default, adopt the configured gateway of eth0, and press Enter; to modify, input the gateway of the corresponding service IP address, and press Enter)

Host Domain : [Linux]: **AASV4_SLAVE.site** (Configure the host name. By default, adopt the current host name, and press Enter; to modify, input the host name and press Enter)

7. Configure the mpsecsrv service, as follows:

Start mpsecsrv? (y/n) **[y]:** (The service is the security service. By default, it is enabled. Press Enter)

8. Enable the HA configuration. Configure HA and other information according to the actuality, as follows:

Configure HA? (y/n) [n]: **y** (whether to enable the HA master/slave mode; by default, do not enable; input y and press Enter)

Please choose ha role(master/slave) : **slave** (Input the role of the current server; input master and directly press Enter)

Please choose extern interface(eth0/eth1) : **[eth0]** (Select the external service Ethernet port. By default, use the first Ethernet port (that is eth0) as the service Ethernet port)

Please choose HA heartbeat interface(eth0/eth1) : **[eth1]** (Select the heartbeat Ethernet port. By default, use the second Ethernet port (that is eth1) as the service Ethernet port)

Please input local host's ip address on HA interface 'eth1' : **2.2.2.2**

(Input the IP address of the heartbeat Ethernet port. Here, you just need to ensure that the IP address and the heartbeat IP address of the active server are in the same network segment)

Please input local host's ip netmask on HA interface 'eth1' : **[255.255.255.0]** (Input the subnet mask of the heartbeat Ethernet port)

Please input peer ip address on HA interface : **2.2.2.1** (Input the IP address of the heartbeat Ethernet port of the active server. Here, you need to ensure that the IP address is the same as the heartbeat IP address of the active server)

Please input peer full hostname : **AASV4_MASTER.Site** (Input the host name

of the active server. It needs to be consistent with the configured host name of the active server)

`Please input virtual ip address on eth0 : 11.0.13.123` (Input the virtual address, the same as the active server. The external access is performed via the virtual address)

`Please input virtual netmask : [255.255.255.0]` (Input the subnet mask of the virtual address, the same as the active server. The external access is performed via the virtual address)

`Enter advance config(y/n)? : [n]` (Enter the advanced configuration; by default, select n, used by the serial port heartbeat and so on. Usually, it is not configured)

used by the serial port heartbeat and so on)

9. Wait for the script to install automatically, and prompt installing FTP, as follows:

   `Configure FTP Server? ( y/n ) [n] :` (Whether to configure the ftp server. Here, input n, and do not configure the ftp server)

10. Configure the component service.

    `Configure application servers? (y/n) [y] :` (Configure the component services? By default, it is y. Press Enter.)

11. Configure the external actual IP address of the node server. If there are multiple, separate by the space, as follows:

    `Please input node address list(if more than one, please use the space division) : [127.0.0.1] ()`

12. For the other configuration items without special description, directly use the default values, and then, wait for initializing

13. After installation, execute the **service srvmgt start** command to start all services.

3.2.3 Synchronize Active and Standby Data of HA Dual-machine Hot Backup Mode

For the first installation, you need to synchronize the active and standby data on the standby server manually. The steps are as follows:

In the standby server, synchronize the data in the active server:

```
AASV4_Slave:~ # service srvmgt config db dbload-frompeer
```

```
Warning:

        The program will drop local mysql data, and sync from
peer!!!!!!

Confirm(y/n)? : [n] y

* Start 'mysql' service...

* Stop local slave

* Dump remote database to local , this can take a long time ...

* Set remote slave pos

* Start local slave

* mysql: Wait sync-from-peer...

* mysql: Wait sync-from-peer finishd

* Load memcache from peer...

* Stop memcache

* memcache: Wait sync from peer...

* memcache: Wait a few...

* memcache: Wait sync-from-peer finished
```

3.2.4 Check Service Status of HA Dual-machine Hot Backup Mode

1. In the active server, execute the **service srvmgt status** command, and the result is as follows:

```
service mpsecsrv is running
service mpha is running
service aas is running
service aasnode is running
service activemq is running
service cas is running
service cmp is running
service fileserver is running
service memcached is running
service memcachedsingle is running
service mpwatchdog is running
service ms is running
service mysql is running
service nginx is running
service os is running
service php is running
service sms is running
service wifiphp is running
```

2. In the active server, execute the **service mpha status** command and the result is as follows:

```
NodeList
   Master: master (Current - Active)
   Slave : slave
Heartbeat interface Status
   [eth1] UP
VIP Status
   [10.10.8.153] - UP
Services Status
   [mysql] UP HealthOK
   [memcached] UP HealthOK
   [memcachedsingle] UP HealthOK
   [nginx] UP HealthOK
   [php] UP HealthOK
   [activemq] UP HealthOK
   [cas] UP HealthOK
   [ms] UP HealthOK
   [os] UP HealthOK
   [aas] UP HealthOK
   [aasnode] UP HealthOK
   [sms] UP HealthOK
   [wifiphp] UP HealthOK
   [cmp] UP HealthOK
   [fileserver] UP HealthOK
MySQL replication Status
   [IO Thread] DOWN
   [Slave Thread] DOWN
Memcached Status
   [Total] 33
DB2MC status
   not load
```

3. In the standby server, execute the **service srvmgt status** command and the result is as follows:

```
service mpsecsrv is running
service mpha is running
service aas is stoped
service aasnode is stoped
service activemq is running
service cas is running
service cmp is stoped
service fileserver is running
service memcached is running
service memcachedsingle is running
service mpwatchdog is running
service ms is stoped
service mysql is running
service nginx is running
service os is running
service php is running
service sms is stoped
service wifiphp is stoped
```

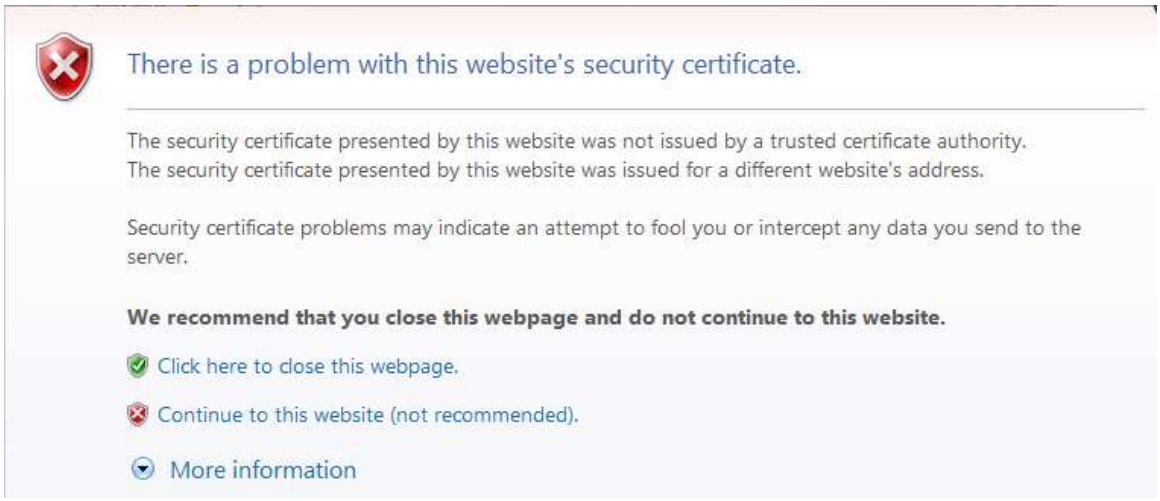
4. In the standby server, execute the **service mpha status** command and the result is as follows:

```
NodeList
   Master: master
   Slave : slave (Current - Passive)
Heartbeat interface Status
   [eth1] UP
VIP Status
   [10.10.8.153] - DOWN
Services Status
   [mysql] UP HealthOK
   [memcached] UP HealthOK
   [memcachedsingle] UP HealthOK
   [nginx] UP HealthOK
   [php] UP HealthOK
   [activemq] UP HealthOK
   [cas] UP HealthOK
   [ms] DOWN
   [os] UP HealthOK
   [aas] DOWN
   [aasnode] DOWN
   [sms] DOWN
   [wifiphp] DOWN
   [cmp] DOWN
   [fileserver] UP HealthOK
MySQL replication Status
   [IO Thread] UP
   [Slave Thread] UP
Memcached Status
   [Total] 33
DB2MC status
   not load
```

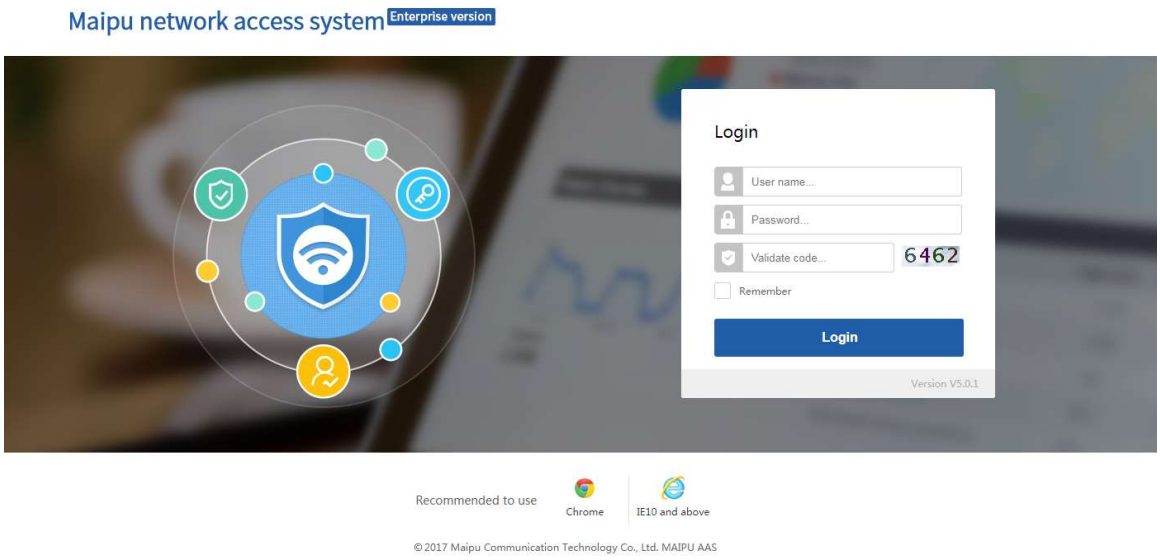
5. Access Maipu AAS via https://IP:8443, such as https://11.0.13.123:8443.

   (HA dual-machine hot backup mode, the accessed IP address is the virtual IP address filled for the active and standby servers.)

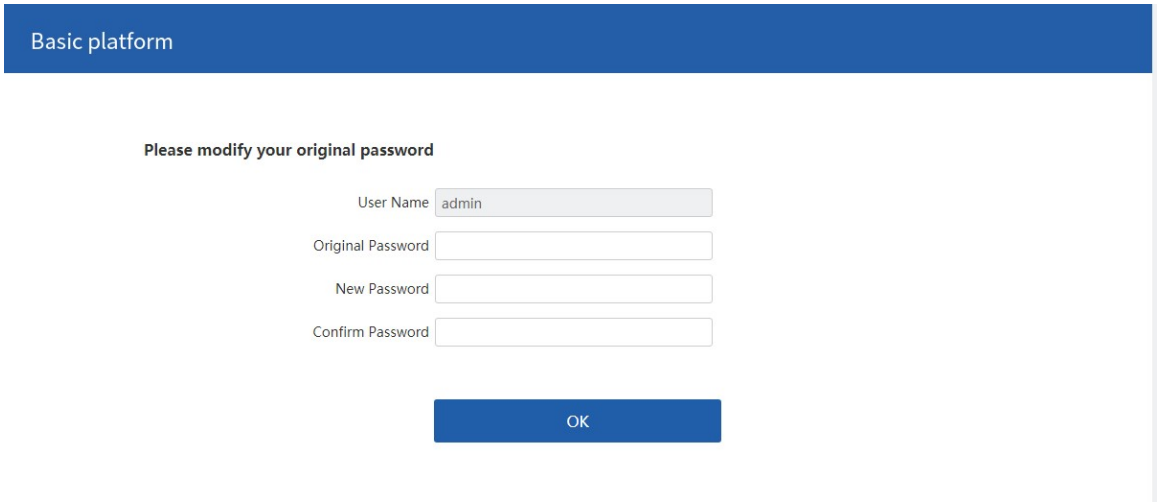
   After installing, the certificate may not be trusted when accessing Maipu AAS for the first time, and the following interface is displayed:



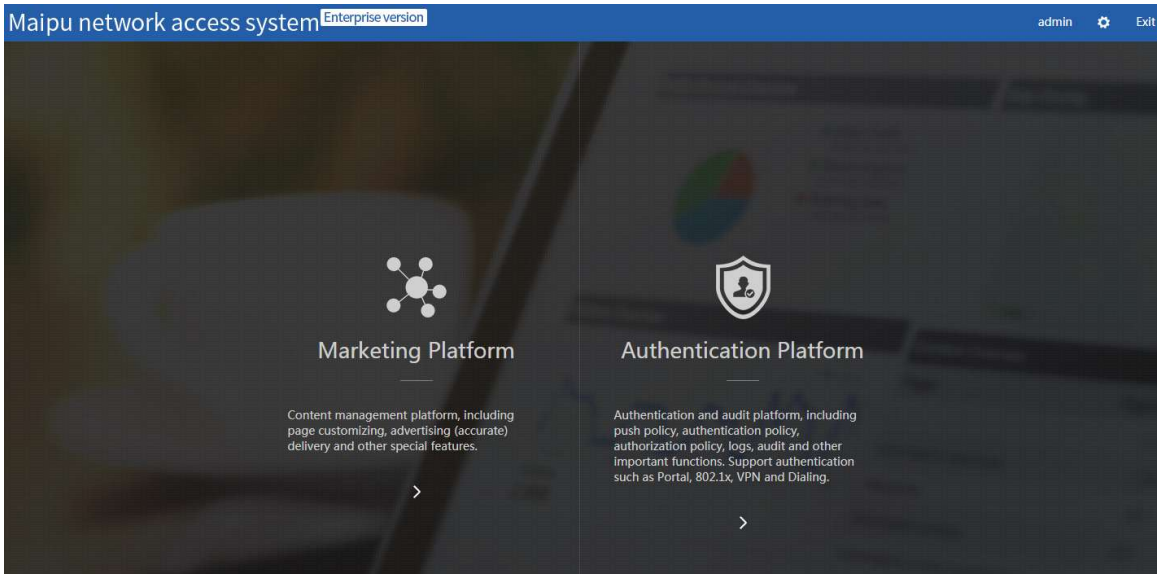
   Click **Continue to this websit e(not recommended)** and you can enter the login interface correctly:



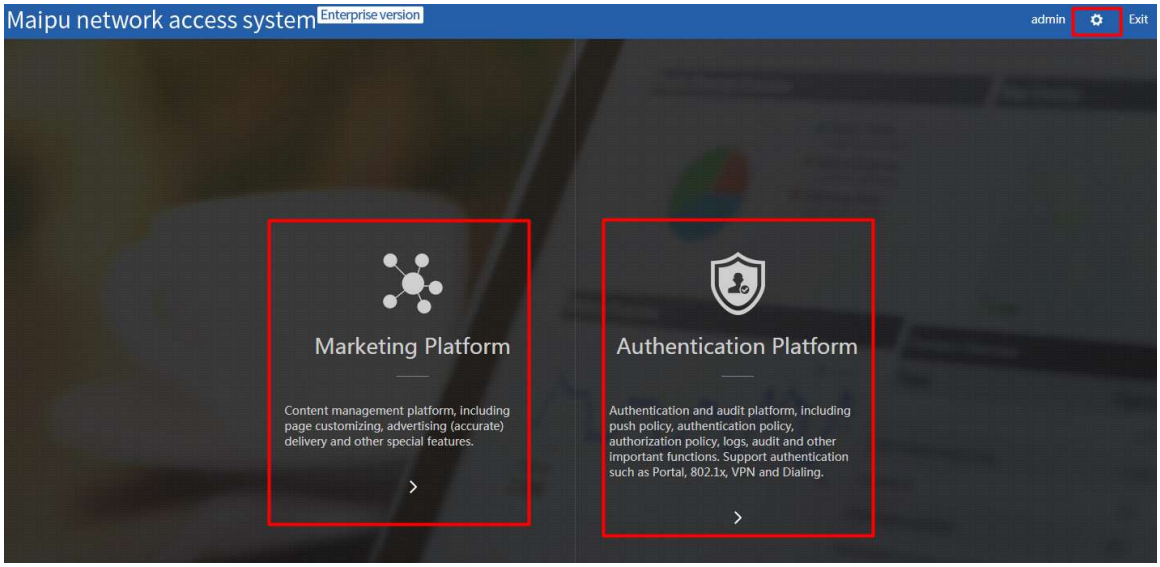
6. Input the default user name and password (admin/admin) and verification code to log in. After logging in successfully, the administrator modifies the initial password (the password should be more than six characters, and contain the uppercase letter, lowercase letter, number and special characters), as shown in the following figure:



7. After the administrator modifies the password, the user adopts the new password to log in again and enter the platform entrance interface, as shown in the following figure:



8. The user can click “Marketing Platform, Authentication Platform” to enter the component platform. Click the gear shape icon at the top right corner of the interface to enter the “Basic Platform”, as shown in the following figure:



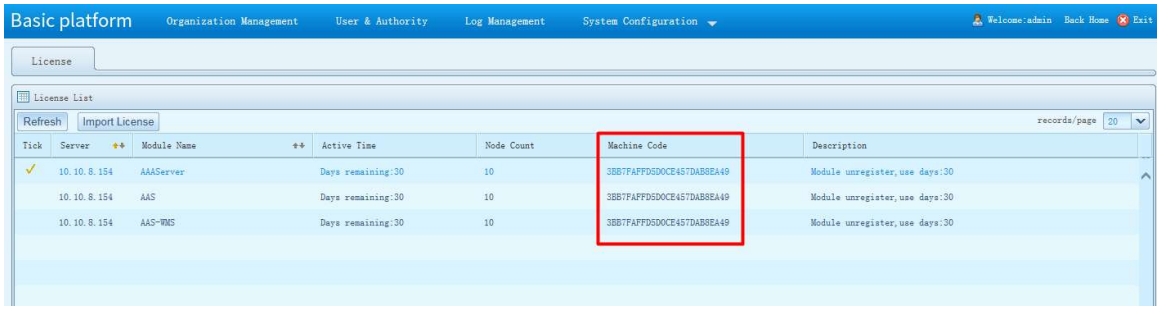
9. If you can enter all platforms correctly and the menus can be loaded normally, it indicates that the installation is complete.

4.License Installation

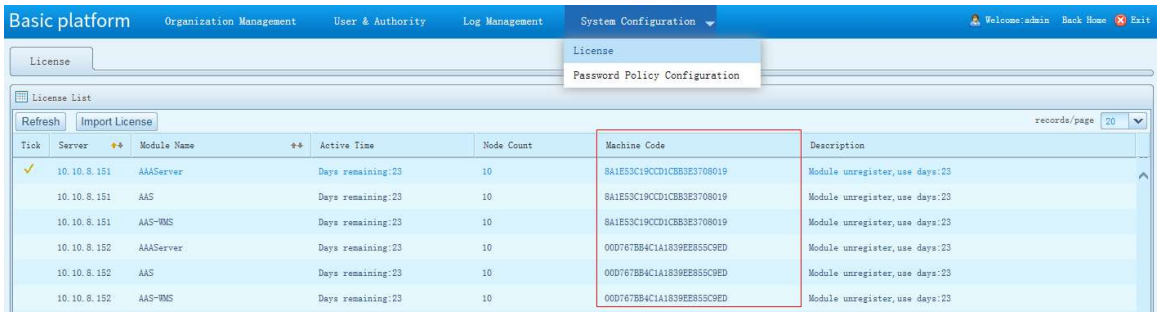
Install the front-end interface license:

Step 1: Log into the system, enter **Basic Platform** > **System Configuration** > **License**, view the license information, and get the server machine code;

The machine code of the standalone server:



The machine code of the active/standby server of the dual-machine hot backup mode:



Step 2: Send the got machine code and module name to Maipu staff, and apply for the License file.

Step 3: On the License management interface, click **Import License**, select the applied License file, and import the License.

Install the background interface license:

Step 1: Get the server machine code:

In the standalone mode, view the License information, and get the machine code:

```
aasv4 :~ # /home/mpup/mpupdefault/bin/mpup license show
Module Name          Days          Node Count          Machine Code
Plugin Name

AAAServer            24            10                  3BB7FAFFD5D0CE457DAB8EA49
aasnode
```

```
AAS                 24              10              3BB7FAFFD5D0CE457DAB8EA49
aasnode

AAS-WMS             24              10              3BB7FAFFD5D0CE457DAB8EA49
cmp
```

In the dual-machine hot backup mode, view the License information, and get the machine code:

1. View the license information of the master server:

```
AASV4_MASTER.Site:~ # /home/mpup/mpupdefault/bin/mpup license show

Module Name         Days            Node Count          Machine Code
Plugin Name

AAS                 30              10              3D1AC94445713FC1992B19015
  aasnode

AAAServer           30              10              3D1AC94445713FC1992B19015
  aasnode

AAS-WMS         30          10          3D1AC94445713FC1992B19015   cmp
```

2. View the license information of the standby server:

```
AASV4_SLAVE.Site:~ # /home/mpup/mpupdefault/bin/mpup license show

Module Name         Days            Node Count          Machine Code
Plugin Name

AAS                 30              10              3D1AC94445713FC1992B19016
aasnode

AAAServer           30              10              3D1AC94445713FC1992B19016
aasnode

AAS-WMS         30          10          3D1AC94445713FC1992B19016
cmp
```

Step 2: Send the got machine code and module name to Maipu staff, and apply for the License file.

Step 3: Copy the license file applied in Step 2 to the /home directory of the standby server, and execute the following command to install:

```
aasv4:~ # /home/mpup/mpupdefault/bin/mpup license install xxxx.lic (License file
```

name)

Module Name	Days	Node Count	Machine Code
AAS	90		10,000
3BB7FAFFD5D0CE457DAB8EA49			
AAAServer	90		10,000
3BB7FAFFD5D0CE457DAB8EA49			
AAS-WMS	90		10,000
3BB7FAFFD5D0CE457DAB8EA49			

The steps of installing the License file in the standalone mode are the same as the dual-machine hot backup mode. For the dual-machine hot backup mode, first install the License file of the active server, and then, install the license of the standby server.

5.System Uninstallation

5.1 mpsetup uninstall

The systems installed by using the ISO package and SH package all can use the **mpsetup uninstall** command to uninstall the system programs, and the steps are as follows:

5.1.1Standalone Mode Uninstallation

Step 1: Log into the system, and execute the command **mpsetup uninstall**.

```
aasv4 :~ # mpsetup uninstall
Warning: setup will uninstall all the follow packages
 * AAS-CMP-enterprise
 * AASPORTAL
 * FileServer
 * Resources
 * SMS
 * MPUPCore
 * MPUP
Confirm uninstall these packages (y/n)?[n] y (Input y, press Enter, and execute uninstallation)
```

Step 2: Wait for the program to uninstall automatically until displaying the following interface, indicating that the system is uninstalled:

```
[MPUP] Uninstall mpsecsrv success!
[MPUP] Uninstall completed!
[MPUP] [INFO]  * Remove mphb ...
[MPUP] [INFO] remove files /opt/mpup/pkginfo/MPUP-setup/filelist/MPUP-V2R1C02 ...
[MPUP] [INFO] [UNINSTALL] Run Unpostscript '_syssetuppatch.sh' ...
[MPUP] [INFO] Call ./_callbackscript/setup.sh (postuninstall)
[MPUP] [INFO] [UNINSTALL] Finished
[MPUP] INFO uninstall success MPUP V2R1C02B2698
```

5.1.2 Dual-Machine Hot Backup Mode Uninstallation

Step 1: Stop the service of the standby server:

```
AASV4_SLAVE.Site:~ # service srvmgt stop
* Stop HA...
Check heartbeat process ...
Stop watchdog for 'fileserver'...done
* HA-Stop 'fileserver' ...
* Service 'cmp' is stoped
* Service 'wifiphp' is stoped
* Service 'sms' is stoped
* Service 'aasnode' is stoped
* Service 'aas' is stoped
Stop watchdog for 'os'...done
* HA-Stop 'os' ...
* Service 'ms' is stoped
Stop watchdog for 'cas'...done
* HA-Stop 'cas' ...
Stop watchdog for 'activemq'...done
* HA-Stop 'activemq' ...
Stop watchdog for 'php'...done
* HA-Stop 'php' ...
Stop watchdog for 'nginx'...done
* HA-Stop 'nginx' ...
Stop watchdog for 'memcachedsingle'...done
* HA-Stop 'memcachedsingle' ...
Stop watchdog for 'memcached'...done
```

```
* HA-Stop 'memcached' ...
Stop watchdog for 'mysql'...done
* HA-Stop 'mysql' ...
* Finished!
* Stop 'mpsecsrv' service...
```

Step 2: Stop the service of the active server:

```
AASV4_MASTER.Site:~ # service srvmgt stop
* Stop HA...
Check heartbeat process ...
Stop watchdog for 'fileserver'...done
* HA-Stop 'fileserver' ...
* HA-Stop 'cmp' ...
* Service 'wifiphp' is stoped
* HA-Stop 'sms' ...
* Service 'aasnode' is stoped
* HA-Stop 'aas' ...
Stop watchdog for 'os'...done
* HA-Stop 'os' ...
* Service 'ms' is stoped
Stop watchdog for 'cas'...done
* HA-Stop 'cas' ...
Stop watchdog for 'activemq'...done
* HA-Stop 'activemq' ...
Stop watchdog for 'php'...done
* HA-Stop 'php' ...
```

```
Stop watchdog for 'nginx'...done
* HA-Stop 'nginx' ...
Stop watchdog for 'memcachedsingle'...done
* HA-Stop 'memcachedsingle' ...
Stop watchdog for 'memcached'...done
* HA-Stop 'memcached' ...
Stop watchdog for 'mysql'...done
* HA-Stop 'mysql' ...
* Finished!
* Stop 'mpsecsrv' service...
```

Step 3: Execute uninstallation in the active/standby server. Refer to the steps in section 5.1.1.

5.2 SH Installation Package Uninstallation

The system installed by using the SH package also can be uninstalled by the command **sh Maipu-AASV4-CMPPortal-SUSE-EN-V3R2C03BXXXX.sh uninstall**, and the steps are as follows:

Step 1: Enter the path of saving the installation package, and execute the uninstallation command:

```
aasv4:~ # sh /home/Maipu-AASV4-CMPPortal-SUSE-EN-V3R2C03BXXXX.sh uninstall
[enterprisescene-cmpportal] Verifying archive integrity... All good.
[enterprisescene-cmpportal] Uncompressing enterprisescene-cmpportal  installer - Done
[enterprisescene-cmpportal]
--------------------------------------------------------------------------------
--
[enterprisescene-cmpportal] Warning :
[enterprisescene-cmpportal] The setup program will uninstall all installed files and datas!!!
[enterprisescene-cmpportal]
--------------------------------------------------------------------------------
--
```

[enterprisescene-cmpportal] Confirm uninstall all installed files and datas [y/n]? : [n] **y** (Input y, press Enter, and execute uninstallation)

Step 2: Wait for the program to uninstall automatically until displaying the following interface, indicating that the system is uninstalled:

```
[enterprisescene-cmpportal] [INFO] [UNINSTALL] Run Unpostscript '_syssetupscene.sh' ...
[enterprisescene-cmpportal] [INFO] Call scene ./_callbackscript/cbkscene.sh (postuninstall)
 * Remove /home/mpup/mpup ...
 * Remove /opt/mpup ...
[enterprisescene-cmpportal] [INFO] [UNINSTALL] Finished
```

Caution

- If using the command mpsetup uninstall to uninstall the program, reserve the data of the basic platform and authentication platform; if using the SH package to uninstall the program, clear all related files and data of the program.

6.Command Commands

Shell Commands	Remarks
/home/mpup/mpupdefault/bin/mpup license show	View the machine code and license
/home/mpup/mpupdefault/bin/mpup license install xxxx.lic	Install the license
service srvmgt status	View all service status Running indicates that the service is normal stopped indicates that the service is stopped
service srvmgt start	Enable all services
service srvmgt stop	Stop all services
service srvmgt restart	Restart all services
service mpha status	View the HA status
service srvmgt config db dbload-frompeer	Synchronize the peer database file (it can only be executed at the standby server)

7.Module Name Explanation

Module Name	Usage
mysql	Mysql database
memcached	Memcached high-speed cache
memcachedsingle	High-speed cache of memcached temporary data
activemq	JMS message server
cas	Unified login
ms	Management service
os	Maintenance service
mpwatchdog	Service monitoring
aas	Web service of user authentication platform
aasnode	Business service of user authentication platform
wifiphp	Operation management client
nginx	Reverse proxy server
php	Hypertext preprocessor
cmp	Business service of WiFi marketing platform
fileserver	File server
sms	SMS docking server