

# **"Let's Automate"**

## **- Renewing FREE SSL certificates on your FileMaker Server**

TonicNote, Inc.  
Koji Takeuchi

# Who am I ?

Koji Takeuchi / 竹内 康二  TonicNote, Inc. FileMaker Database Development, System Consulting.

```
{  
  "Work for": "FileMaker Developer, Trainer, System Administrator",  
  "Community": "FileMaker Pro Tokyo Users Meeting (FM-Tokyo) Chairman, Snack/Beverage Server",  
  "Community": "FileMaker Community MVP", 🏆  
  "Qualification": "FileMaker 7 - 18, 2020 Certified Developer",  
  "Qualification?": "Apple Certified Trainer (used to be...)",  
  "Award": "FileMaker Excellence Award 2006 winner",  
  "Book": "Technical Reviewer of FileMaker Pro 14: The Missing Manual (O'Reilly Media)",  
  "Book": "Technical Reviewer of FileMaker Pro 13: The Missing Manual (O'Reilly Media)",  
  "Book": "Co-Translator and Technical Reviewer of FileMaker Pro 8: The Missing Manual (Japanese)",  
  "Book": "Co-Translator and Technical Reviewer of FileMaker Pro 9: The Missing Manual (Japanese)",  
  "Book": "Co-Author of Apple Certified Technical Coordinator Guide Book"  
}
```

# Agenda

- Let's Encrypt
- Get the certificate
- Put the certificate
- Automate the process
- Run it periodically

# Let's Encrypt

- Certification Authority provided by Internet Security Research Group (ISRG)
- Free, Open Standard
- DV (Domain Validation) only
  - Otherwise it cannot be automated
  - No OV (Organization Validation), or EV (Extended Validation)
- Supports multiple domains / wildcard
- Expires in 90 days
  - Have to renew within (every) 90 days
  - Want to automate?

# How it works



We



Let's Encrypt Server



# Get the certificate (challenge types)

- HTTP
  - Easier
  - Host must be reached from the Internet
    - "Host" means the host which has the exact same FQDN (ex: fms.example.com) which about to getting certificate
- DNS
  - Little complex (depends on your DNS server)
  - Host could stay inside of the local network

# Get the certificate (challenge types)

- DNS
  - Little complex (depends on your DNS server)
    - Not really,
    - If your DNS Service provider supports API and use the right tool
  - Host could stay inside of the local network

# Get the certificate (tools)

- Certbot
  - <https://certbot.eff.org>
  - Python script
  - Seems most popular
- dehydrated
  - <https://github.com/dehydrated-io/dehydrated>
  - Shell script
  - Bit easier to setup...(?)
- And many...

# Get the certificate (tools)

- Certbot
  - There are number of plugins for the common DNS services
  - <https://certbot.eff.org/docs/using.html#dns-plugins>
- dehydrated
  - We can find lots of hook scripts for the common DNS services, too
  - <https://github.com/dehydrated-io/dehydrated/wiki>

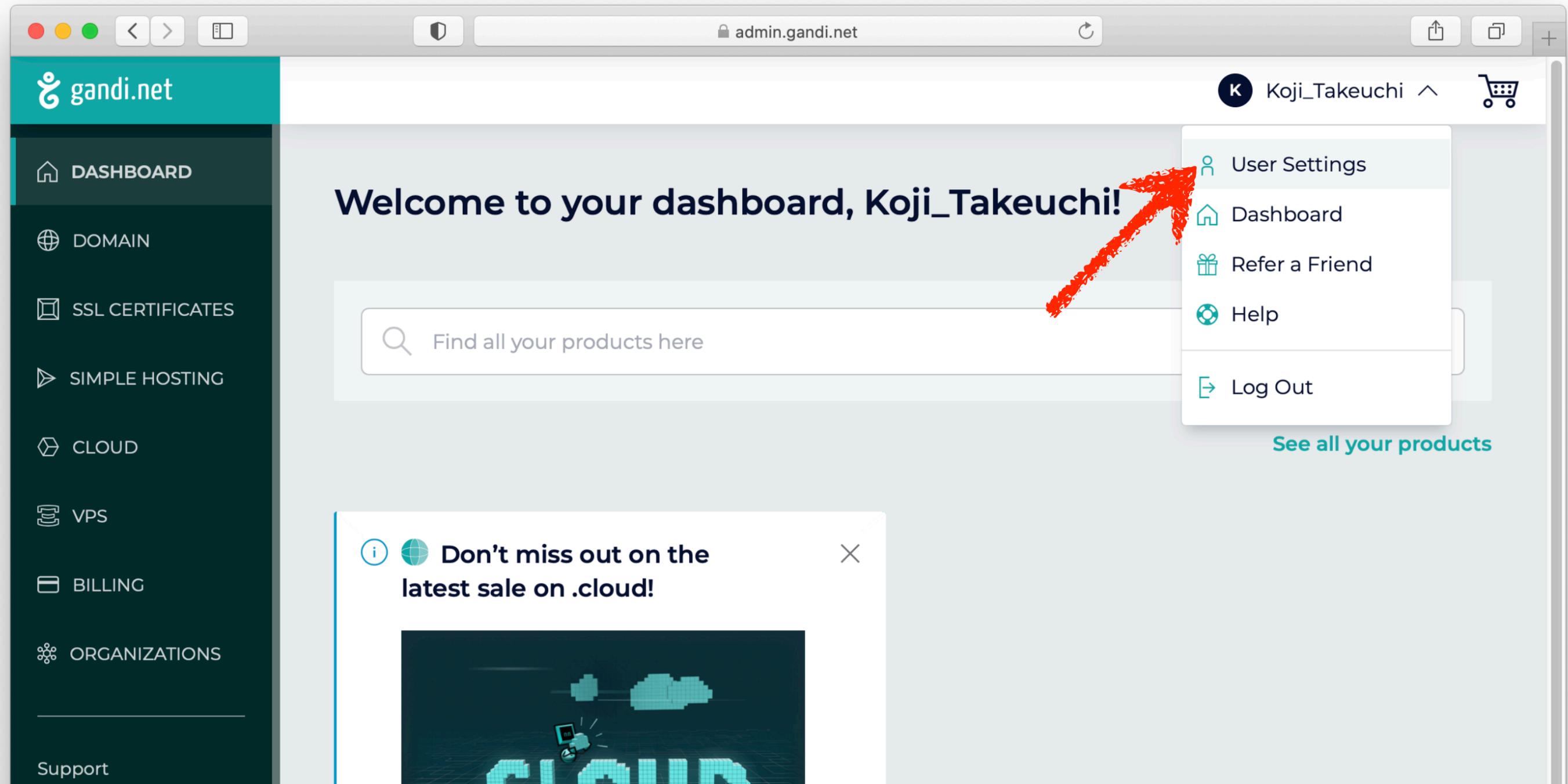
# Let's do it!

- Demo 1
  - Tool: Certbot
  - DNS service: gandi.net
- Demo 2
  - Tool: dehydrated
  - DNS service: AWS Route 53
- Both basically the same
  1. Send challenge request to Let's Encrypt server
  2. Edit DNS record via API

# Let's do it!

- Demo 1
  - Tool: Certbot
  - DNS service: gandi.net

# Getting API key of gandi.net



## User Settings

**Note:**

These settings affect your personal account's profile (Koji\_Takeuchi). If you want to edit one of your organizations' profiles, use the Organizations entry in the menu.

Language preference English

Newsletter subscription No

**Edit preferences**



Manage login and security options

**Manage the user account and security settings**



**Change password & configure access restrictions**



**Manage authorized apps**



# Security

Edit your account and security settings, as well as third-party applications and authorizations.

[Settings](#)[Security](#)[Authorized apps](#)[My apps](#)

## Account security

Password

Last updated January 3, 2021. [Change password](#)

Two-factor authentication

[Enable TOTP](#)

Security key

[Manage your security key authentication](#)

Production API key

[Generate the API key](#)

Our RESTful API for use with our new website is currently available in BETA testing. For more information please consult [our online documentation](#).

Restrict Login IP Addresses

[Add an IP restriction](#)

# Let's do it!

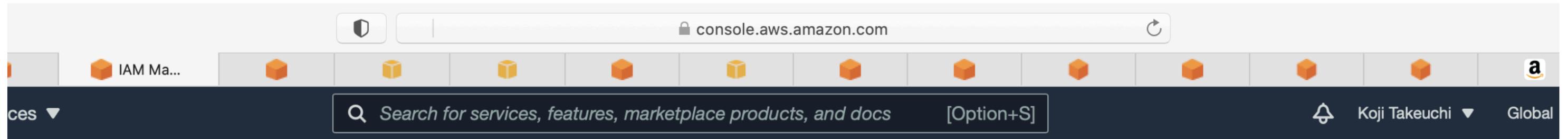
- Demo 2
  - Tool: dehydrated
  - DNS service: AWS Route 53

# Getting API key of Route 53

The screenshot shows the AWS IAM console interface. At the top, there's a navigation bar with the AWS logo, a search bar, and user information for 'Koji Takeuchi'. The main content area is titled 'Identity and Access Management (IAM)'. On the left, there's a sidebar menu with options like 'Dashboard', 'Access management', 'Users', 'Roles', 'Policies', etc. The 'Users' section is highlighted. At the top of the main area, there are 'Add user' and 'Delete user' buttons. A red arrow points to the 'Add user' button. Below this is a search bar and a table of users. The table has columns for 'User name', 'Groups', 'Access key age', 'Password age', 'Last activity', and 'MFA'. Five users are listed: fmpcontainer, ladmin, ses-smtp-user-virginia, ses-smtp-user.ap-northeast-1, and takeuchi.

<input type="checkbox"/>	User name	Groups	Access key age	Password age	Last activity	MFA
<input type="checkbox"/>	fmpcontainer	None	⚠️ 97 days	None	Today	Not enabled
<input type="checkbox"/>	ladmin	admin	❗ 2172 days	1838 days	88 days	Virtual
<input type="checkbox"/>	ses-smtp-user-virginia	None	❗ 647 days	None	Today	Not enabled
<input type="checkbox"/>	ses-smtp-user.ap-northeast-1	None	⚠️ 300 days	None	300 days	Not enabled
<input type="checkbox"/>	takeuchi	None	❗ 2172 days	2172 days	None	Not enabled

# Getting API key of Route 53



## Add user



## Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

**User name\***

[+ Add another user](#)

## Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

- Access type\***
- Programmatic access**  
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
  - AWS Management Console access**  
Enables a **password** that allows users to sign-in to the AWS Management Console.

## Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name\*

[+ Add another user](#)

## Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type\*



**Programmatic access**

Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.



**AWS Management Console access**

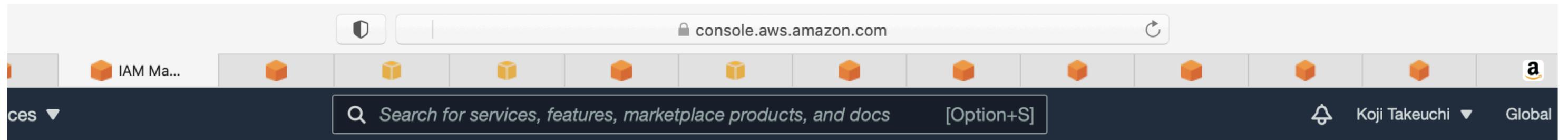
Enables a **password** that allows users to sign-in to the AWS Management Console.

\* Required

Cancel

Next: Permissions

# Getting API key of Route 53



## Add user



### Set permissions

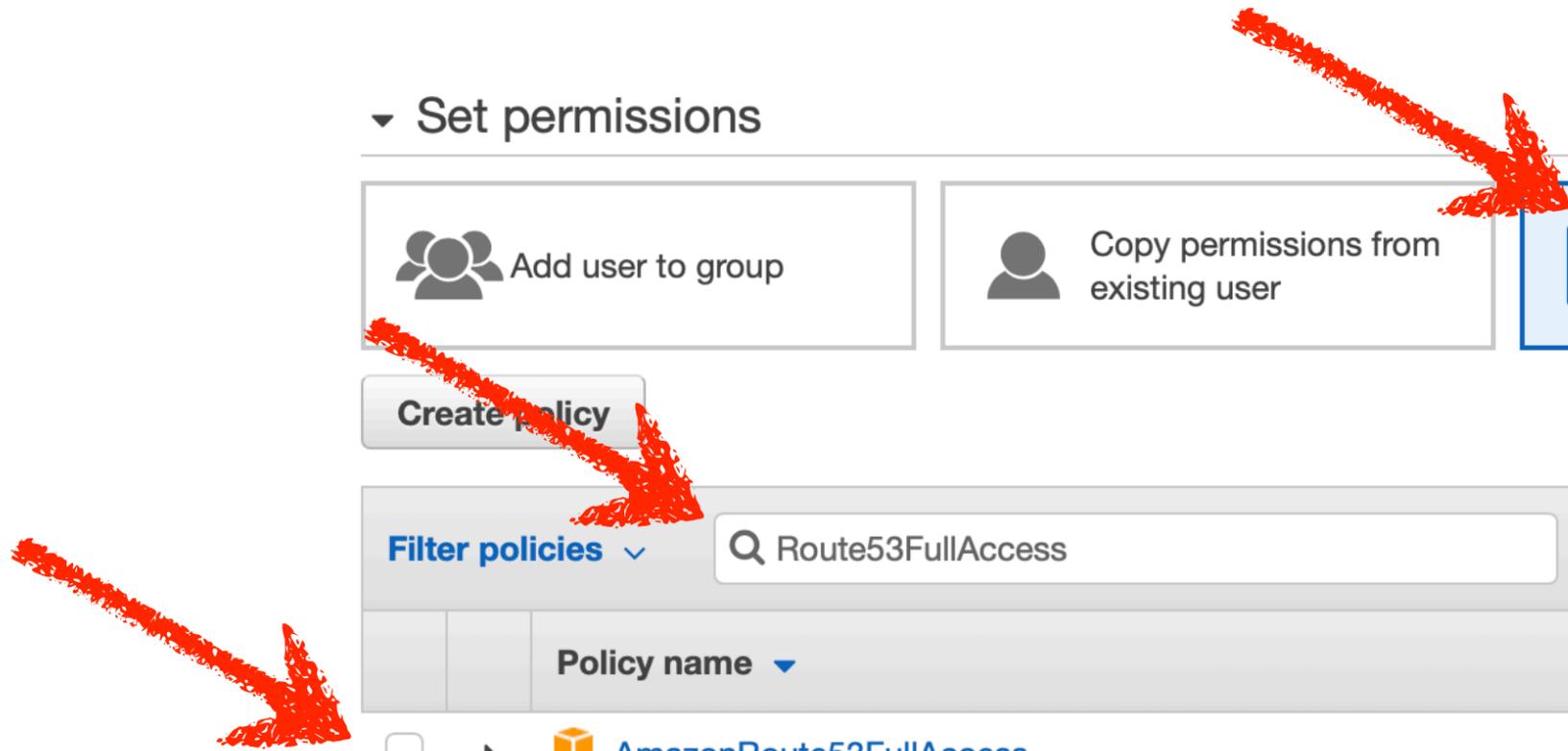
Three options for setting permissions are shown in a row:

- Add user to group**: Represented by an icon of three people.
- Copy permissions from existing user**: Represented by a single person icon.
- Attach existing policies directly**: Represented by a document icon with a list. This option is highlighted with a blue border and a red arrow pointing to it.

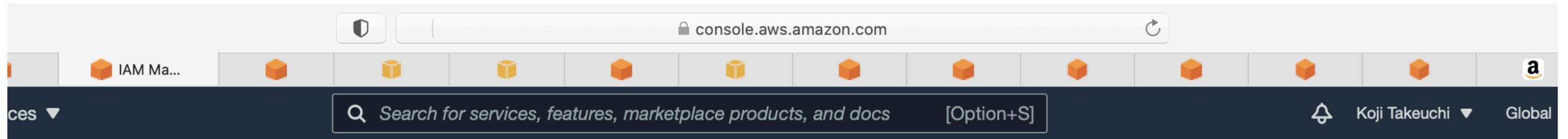
A 'Create policy' button is on the left, and a refresh icon is on the right.

A search bar with the text 'Route53FullAccess' and a magnifying glass icon. To the right, it says 'Showing 1 result'.

	Policy name	Type	Used as
<input type="checkbox"/>	AmazonRoute53FullAccess	AWS managed	None



# Getting API key of Route 53



## Add user



### Set permissions

Three buttons are displayed in a row:

- Add user to group**: Represented by an icon of three people.
- Copy permissions from existing user**: Represented by a single person icon.
- Attach existing policies directly**: Represented by a document icon with a blue border around it.

Below these buttons is a 'Create policy' button on the left and a refresh icon on the right.

Filter policies  Showing 1 result

	Policy name	Type	Used as
<input checked="" type="checkbox"/>	AmazonRoute53FullAccess	AWS managed	None

▼ Set permissions

 Add user to group

 Copy permissions from existing user

 Attach existing policies directly

Create policy



Filter policies ▾  Showing 1 result

	Policy name ▾	Type	Used as
<input checked="" type="checkbox"/>	 AmazonRoute53FullAccess	AWS managed	None

► Set permissions boundary

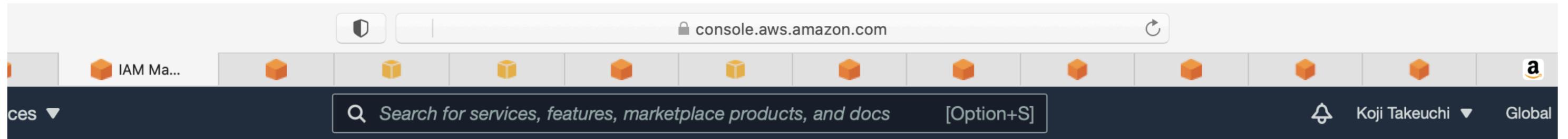
Cancel

Previous

Next: Tags



# Getting API key of Route 53



## Add user



## Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. [Learn more](#)

Key	Value (optional)	Remove
<input type="text" value="Name"/>	<input type="text" value="For Route53 demo on dotfmp"/>	<input type="button" value="x"/>
<input type="text" value="Add new key"/>	<input type="text"/>	

You can add 49 more tags.

## Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. [Learn more](#)

Key	Value (optional)	Remove
<input type="text" value="Name"/>	<input type="text" value="For Route53 demo on dotfmp"/>	<input type="button" value="✕"/>
<input type="text" value="Add new key"/>	<input type="text"/>	

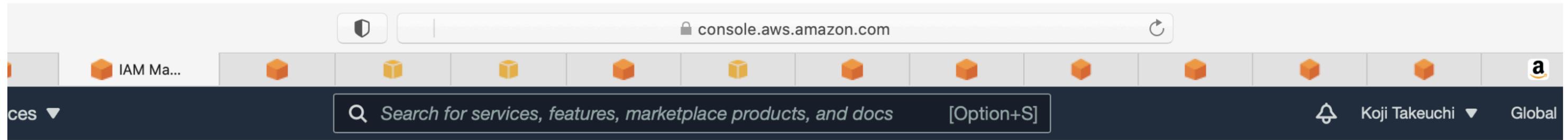
You can add 49 more tags.

[Cancel](#)

[Previous](#)

[Next: Review](#)

# Getting API key of Route 53



## Add user



## Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

## User details

<b>User name</b>	route53_dotfmp
<b>AWS access type</b>	Programmatic access - with an access key
<b>Permissions boundary</b>	Permissions boundary is not set

## Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	<a href="#">AmazonRoute53FullAccess</a>

## Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

### User details

<b>User name</b>	route53_dotfmp
<b>AWS access type</b>	Programmatic access - with an access key
<b>Permissions boundary</b>	Permissions boundary is not set

### Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	<a href="#">AmazonRoute53FullAccess</a>

### Tags

The new user will receive the following tag

Key	Value
Name	For Route53 demo on dotfmp

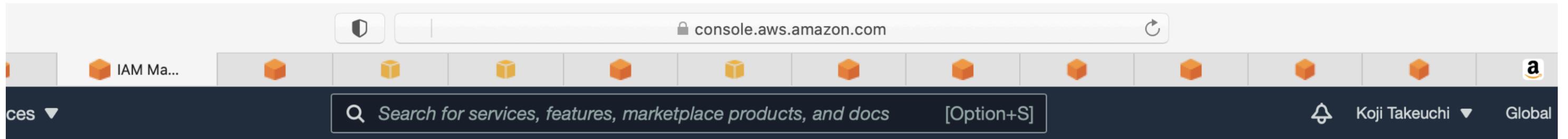
Cancel

Previous

Create user



# Getting API key of Route 53



## Add user



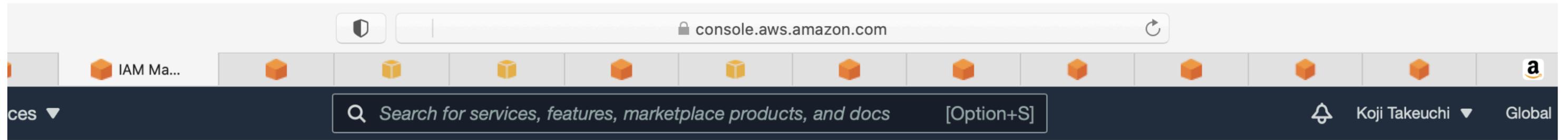
 **Success**  
You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://614535025694.signin.aws.amazon.com/console>

 **Download .csv**

	User	Access key ID	Secret access key
▶ 	route53_dotfmp	 	***** <a href="#">Show</a>

# Getting API key of Route 53



## Add user



✔ **Success**  
You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

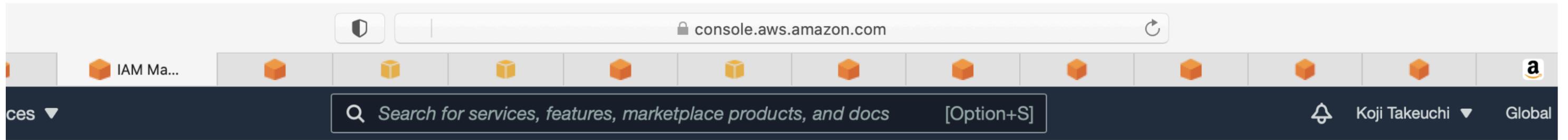
Users with AWS Management Console access can sign-in at: <https://614535025694.signin.aws.amazon.com/console>

Download .csv

	User	Access key ID	Secret access key
▶	✔ route53_dotfmp	AKIAI44QH8D8DFK1L536U	***** Show



# Getting API key of Route 53



## Add user



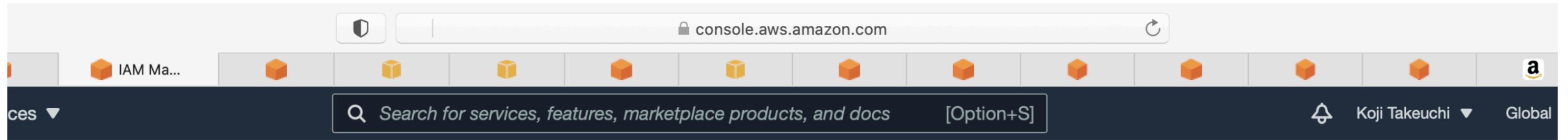
 **Success**  
You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://614535025694.signin.aws.amazon.com/console>

 **Download .csv**

	User	Access key ID	Secret access key
▶ 	route53_dotfmp		 Hide

# Getting API key of Route 53



## Add user



### Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

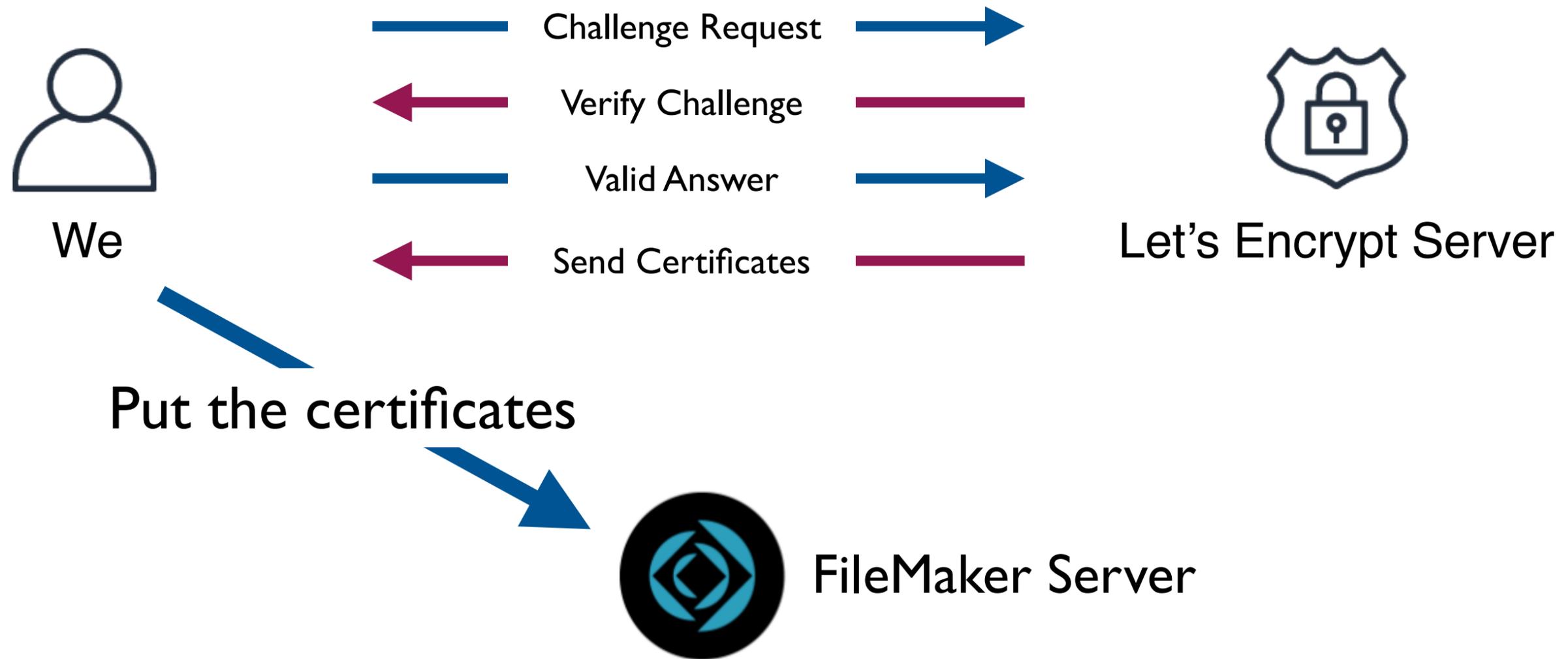
Users with AWS Management Console access can sign-in at: <https://614535025694.signin.aws.amazon.com/console>



 Download .csv

	User	Access key ID	Secret access key
▶	✔ route53_dotfmp	 	  <a href="#">Hide</a>

# Put the certificate



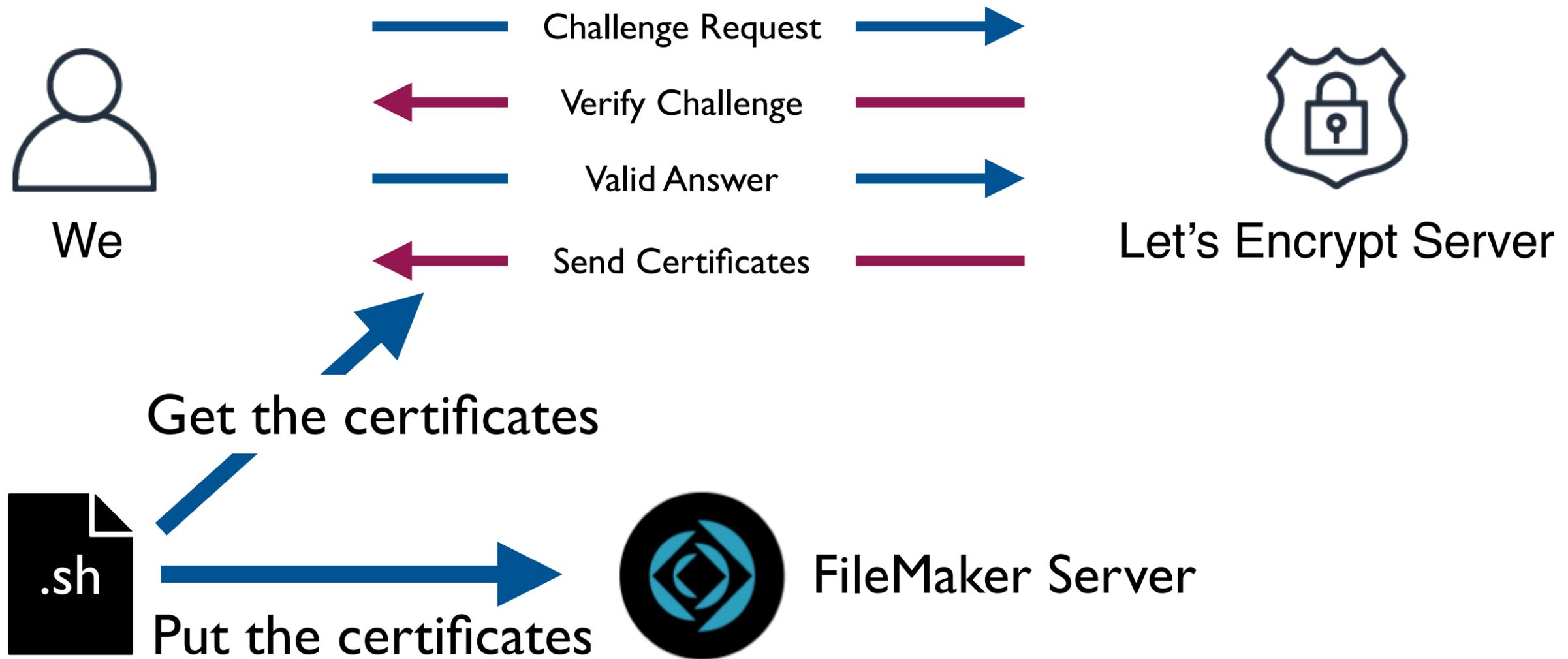
# Put the certificate

- Delete existing certificates
  - Restart FileMaker Server
- Import new certificates
  - Restart FileMaker Server
- Done.

# Put the certificate

- Demo

# Automate the process



# Automate the process

- Put them into "wrapper" script
  - Get the certificate,  
Then
  - Put the certificate

```
$ vi /usr/local/bin/wrapper.sh
#!/bin/sh
/usr/local/bin/certbot certonly \
  --authenticator dns-gandi \
  --dns-gandi-credentials /etc/letsencrypt/gandi/gandi.ini \
  -d fms.example.com
/usr/local/bin/sslUpdateOnFMS.sh
```

# Run it periodically

- Run the wrapper by crontab
- ex: Run on 4:30 of 1st day of every odd months.

```
$ sudo crontab -e  
# 2021.06.04, Koji Takeuchi  
# fms.example.com SSL update  
30 4 | 1,3,5,7,9,11 * /usr/local/bin/wrapper.sh >> /PATH_TO_LOGS/sslupdate.log 2>&1
```

(PATH\_TO\_LOGS may like /opt/FileMaker/FileMaker\ Server/Logs/)

# Hurry!

- Everything I did today was on CentOS 7
- But CentOS 7 will be discontinued, soon...
  
- ...Don't worry, it will be the same on Ubuntu
  - (Basically the same)
  - (Roughly, Substitute ( Commands ; "yum" ; "apt" ))

# Thank you!

- You can download everything on:
- <https://dotfmp.berlin/sessions/311>

# Q&A

- Any Questions...?