Mac in a Hurry

Cloud Macs for Development and Beyond

2023 MACADMINS CONFERENCE

Presented by:

Roger Herling (he/him)
Apple/Jamf End User Computing Engineer
McGraw Hill

&

Dave Siederer (he/him)
Specialist Solutions Architect, EC2 Mac
Amazon Web Services

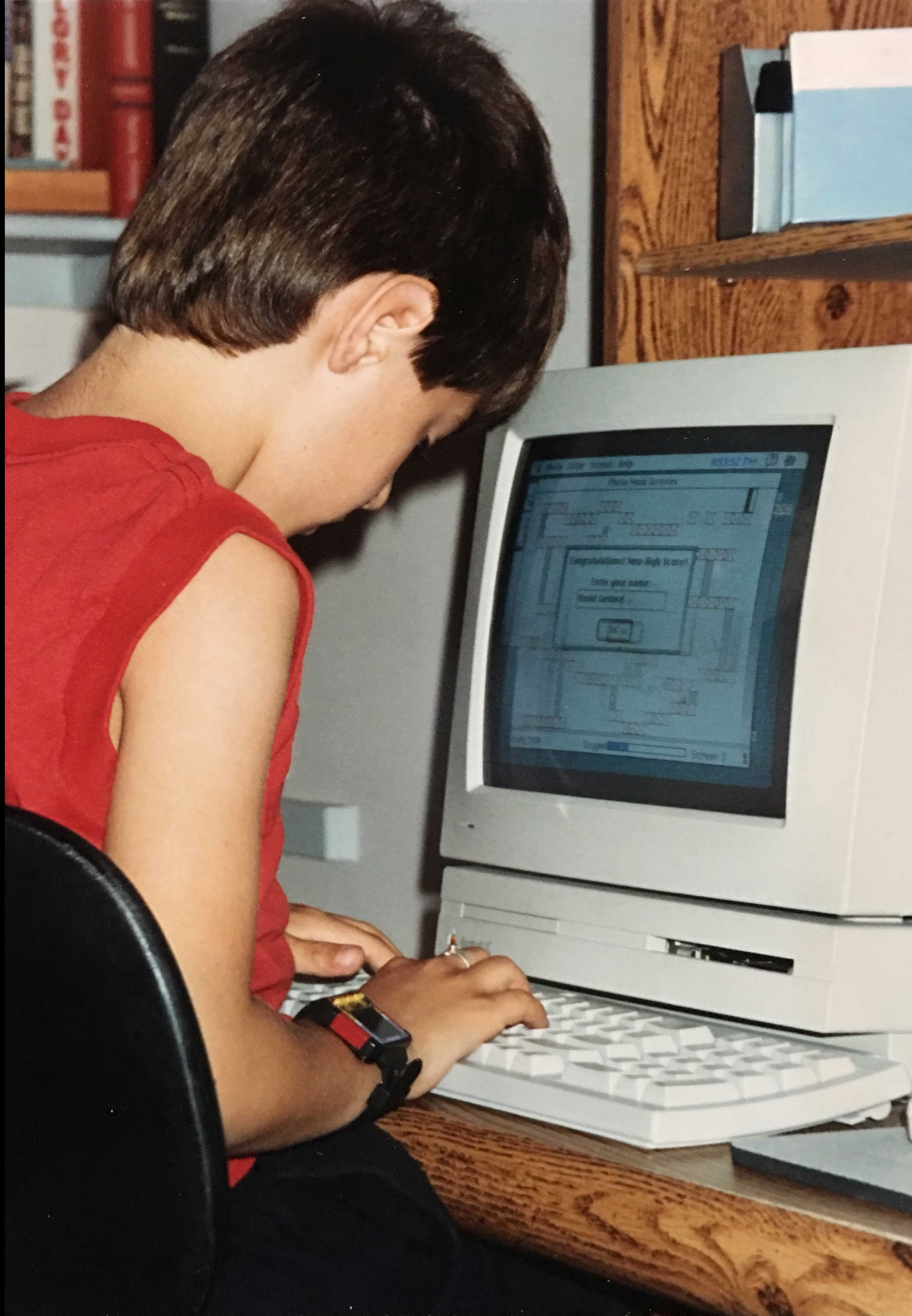
A Little About Us

Roger Herling (@rogerH)

- Work for McGraw Hill
- Reformed Windows Guy
- 20+ years in IT
- Over 10 in the macOS world
- Manage over 4000 devices currently
- Married w/2Kids and 2 dogs
- Doctor Who and Lego nerd

Dave Siederer
(@ds)

- Specialist Solutions Architect for EC2 Mac @ AWS
- Long-time fixation on Mac automation (`on mouseUp`)
- Created ZeroTouch & FirstAID in AppleScript in 2011
- Apple-obsessed since 1986 (1990 pictured)
- @ds0x GitHub/GitLab
- @ds0 most other places
- First time at MacAdmins Conference (finally!)



Agenda:

- Use Cases & What is EC2 Mac?
- Evolution of Solutions
- What Does the Future Hold?
- Q & A

Use Case
#1
Application Development

Key challenges with building Apple applications

Infrastructure overhead

Operating an on-premises fleet consumes time and resources

Disparate build environment

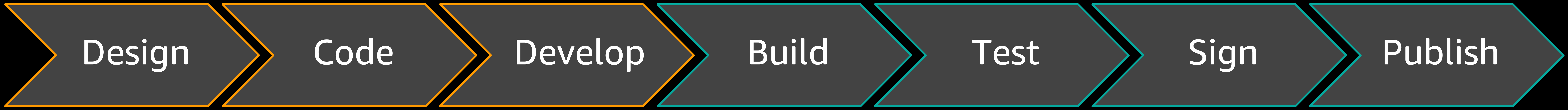
Managing cross-platform builds adds complexity and creates security risks

Inability to scale

Working with limited Mac resources delays time to market

Overhead of managing Apple hardware infrastructure slows down innovation

Application development lifecycle



Design

Code

Develop

Build

Test

Sign

Publish

Requires **Xcode**, which runs only on macOS

34+ million developers

1+ million apps

2+ billion active devices

Xcode

iOS macOS iPadOS

tvOS Safari watchOS

visionOS

macOS on Amazon EC2 empowers Apple development on AWS

Amazon Elastic Compute Cloud (Amazon EC2)

BROADEST AND DEEPEST COMPUTE PLATFORM CHOICE

CATEGORIES

General purpose

Compute optimized

Memory optimized

Storage optimized

Burstable

High Performance Computing

Dense storage

Machine Learning

Video Encoding

+

CAPABILITIES

Choice of processor
(AWS, Intel, AMD, Apple silicon)

Fast processors
(up to 4.5 GHz)

High memory footprint
(up to 16 TiB)

Instance storage
(HDD, SSD, NVMe)

Accelerated computing
(GPU, FPGA, VT1, DL1)

Networking
(up to 400 Gbps)

Bare Metal

Size
(.nano to .32xlarge)

+

OPTIONS

Amazon EBS

Amazon EFS

Amazon FSx

Amazon Elastic Inference

Amazon Elastic GPU

=

650+

INSTANCE TYPES

for virtually every workload and business need

AWS Nitro System

PUSHING THE LIMITS

Security

Enhanced security that continuously monitors, protects, and verifies instance hardware and firmware

Performance

Better performance across CPU, networking, and storage

Innovation

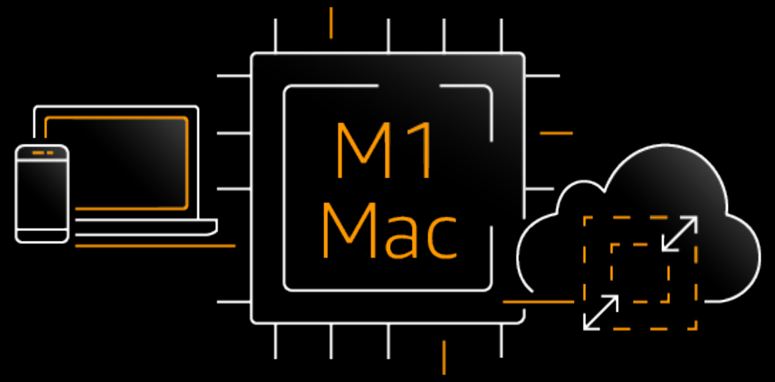
Building blocks can be assembled in many different ways

Modular building blocks for rapid delivery of Amazon EC2 instances and features

EC2 Mac:

Mac mini and the AWS Nitro System

Amazon EC2 Mac details



Available as Amazon EC2 bare metal instances

General Purpose instance family
- EC2 x86 Mac: mac1; instance type – mac1.metal
- EC2 M1 Mac: mac2; instance type – mac2.metal

Support for dedicated host tenancy with 24-hour minimum allocation

EC2 Mac instances provide multiple macOS versions via Amazon Machine Images (AMIs)

SSH for command line, VNC for GUI, and PCoIP agent for enhanced GUI connectivity

Customize instance launches via ec2-macOS-init:
https://github.com/aws/ec2-macos-init

Amazon EC2 Mac instance customers & partners

Customers

Goldman Sachs

The Pokémon Company INTERNATIONAL

intuit

PAPAYA GAMING

RIOT GAMES

FLIPBOARD

Electronic Arts

NBCUniversal

circleci

MPL

DeNA

STRABAG

INCOGNIA™

aspyr®

twitch

JAMCITY

DNB

EastSide Games

ring

Star Stable

applitools

Dimps DIGITAL INNOVATOR

Partners

jamf

Veertu

CIS® Center for Internet Security®

Anyware

Buildkite

To view all EC2 Mac Customer and Partner references, please visit our [EC2 Mac customer page](#).
To view all AWS Partners, please visit [AWS Partner Solutions Finder](#).

> “We were seeking an infrastructure capable of hyper-growth and scale so were thrilled when we heard that AWS is now offering macOS-based EC2 instances. We are delighted with the performance of our new, native-mobile, visual AI-powered test cloud running on Amazon’s EC2 Mac instances.”

Adam Carmi

CTO and co-founder

applitools

https://aws.amazon.com/ec2/instance-types/mac/; section ‘Customers’

> “We recently started using Amazon EC2 instances for our iOS build machines for tasks such as daily betas, App Store builds and submissions, and UI testing. **Build times have reduced from 20 minutes to 5 minutes. UI automation tests that used to take 3 hours now take less than 1 hour.** Download speeds are amazing, and the VNC sessions are as smooth as butter. We are super happy with the finished results.”

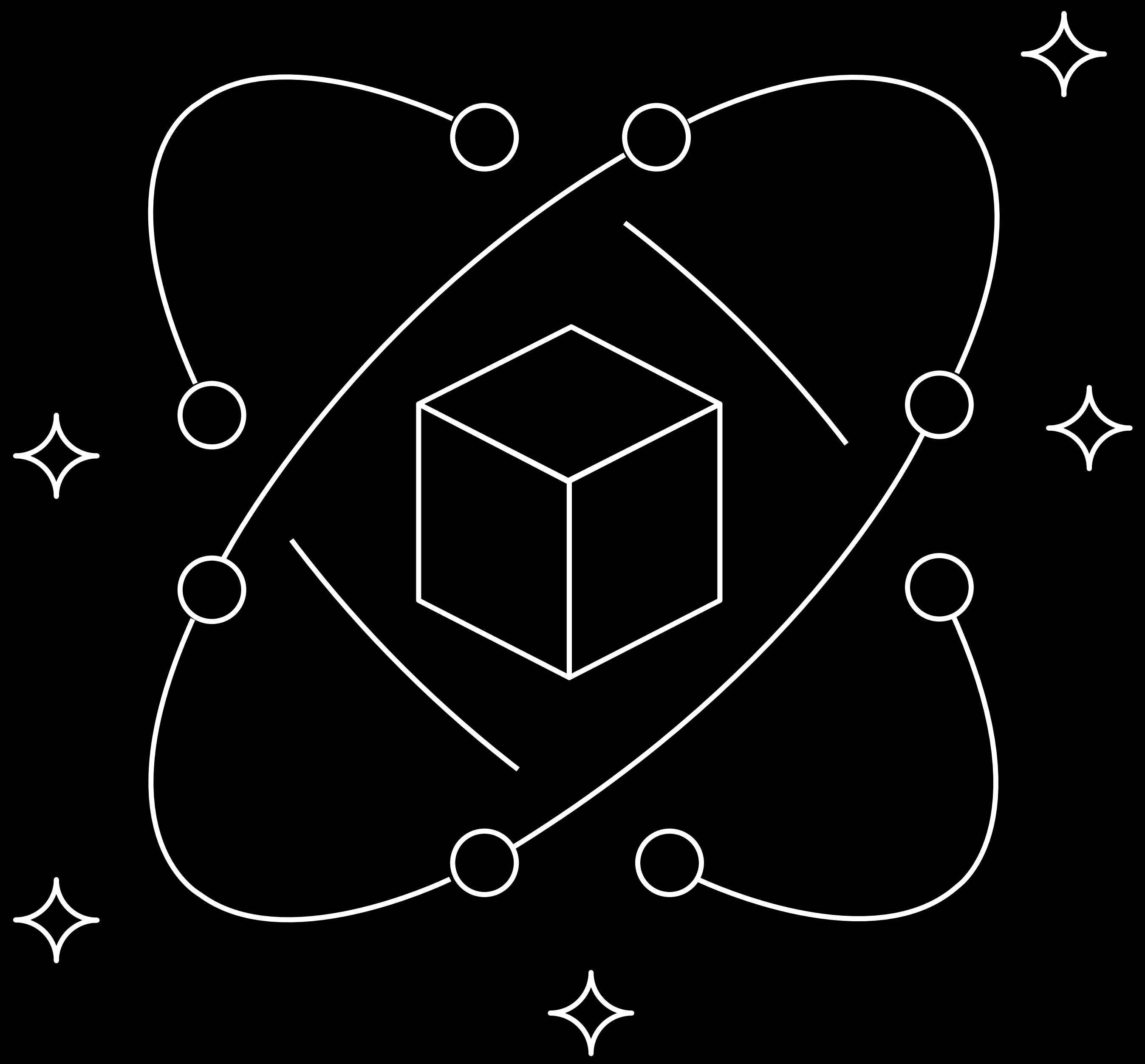
Colin Caufield

Lead iOS Engineer

FLIPBOARD

https://aws.amazon.com/ec2/instance-types/mac/; section ‘Customers’

AWS & Jamf Partnership



- Introduced a workflow for Jamf **agent-based** EC2 Mac enrollment at JNUC 2022
- Automation to assist **profile** enrollment with EC2 Mac (**LastMile**) in late 2022
- Integration between **Jamf Private Access** and **Amazon Verified Access**

Key benefits – Apple fleet management with Jamf

Automated, scalable Mac fleet deployment

Secured, scalable Apple environments

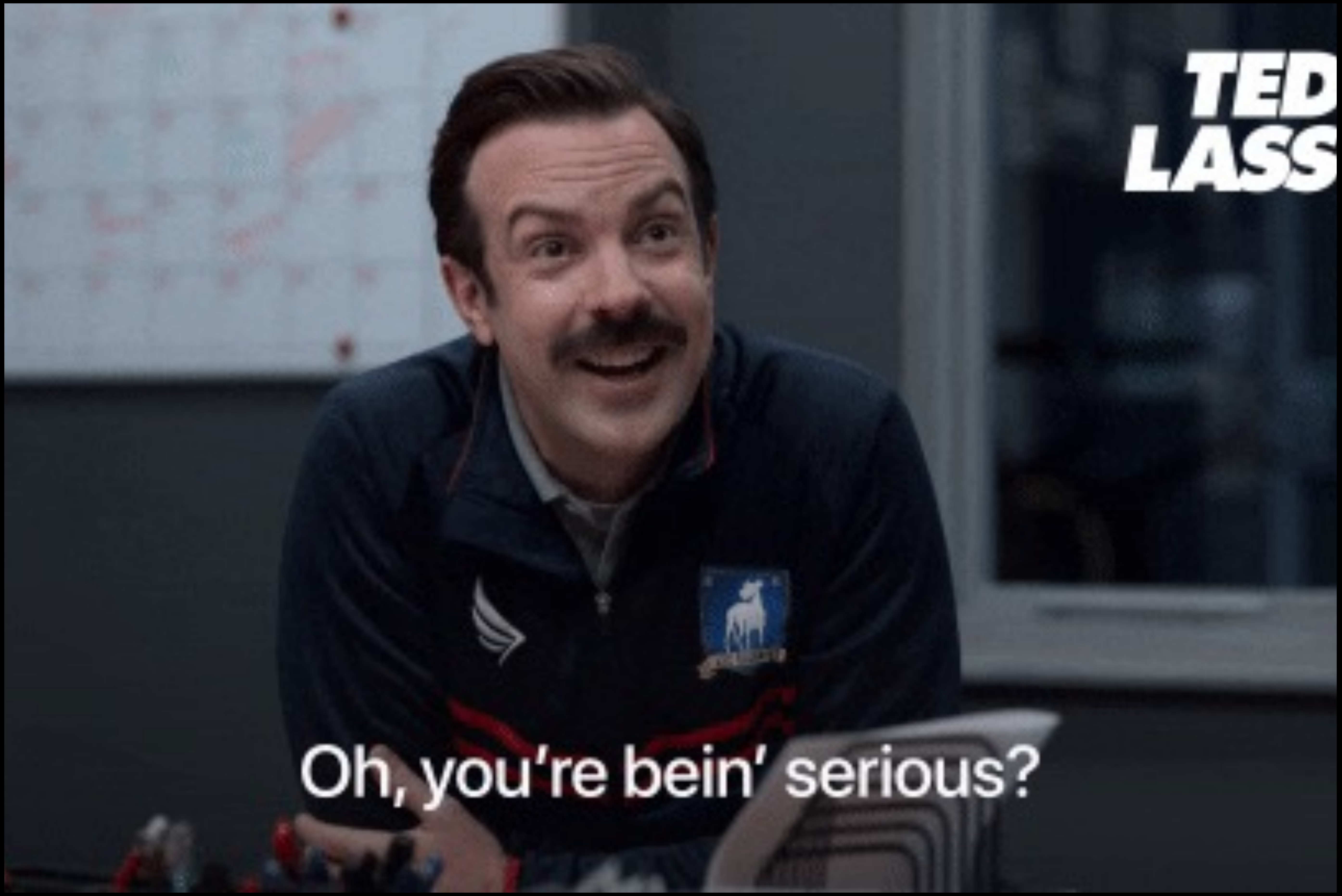
Amplify admin, dev, and user productivity

Access, develop, and test from anywhere

Amazon EC2 Mac instances accelerate your Mac admin workflows

- Test scripts and apps across multiple, non-virtualized macOS versions effortlessly—*on the same Mac*
- Integrate with device management to enroll and test complex workflows—*before they reach your users*
- Build, test, sign, and publish your Apple apps in the cloud—*not under someone's desk*

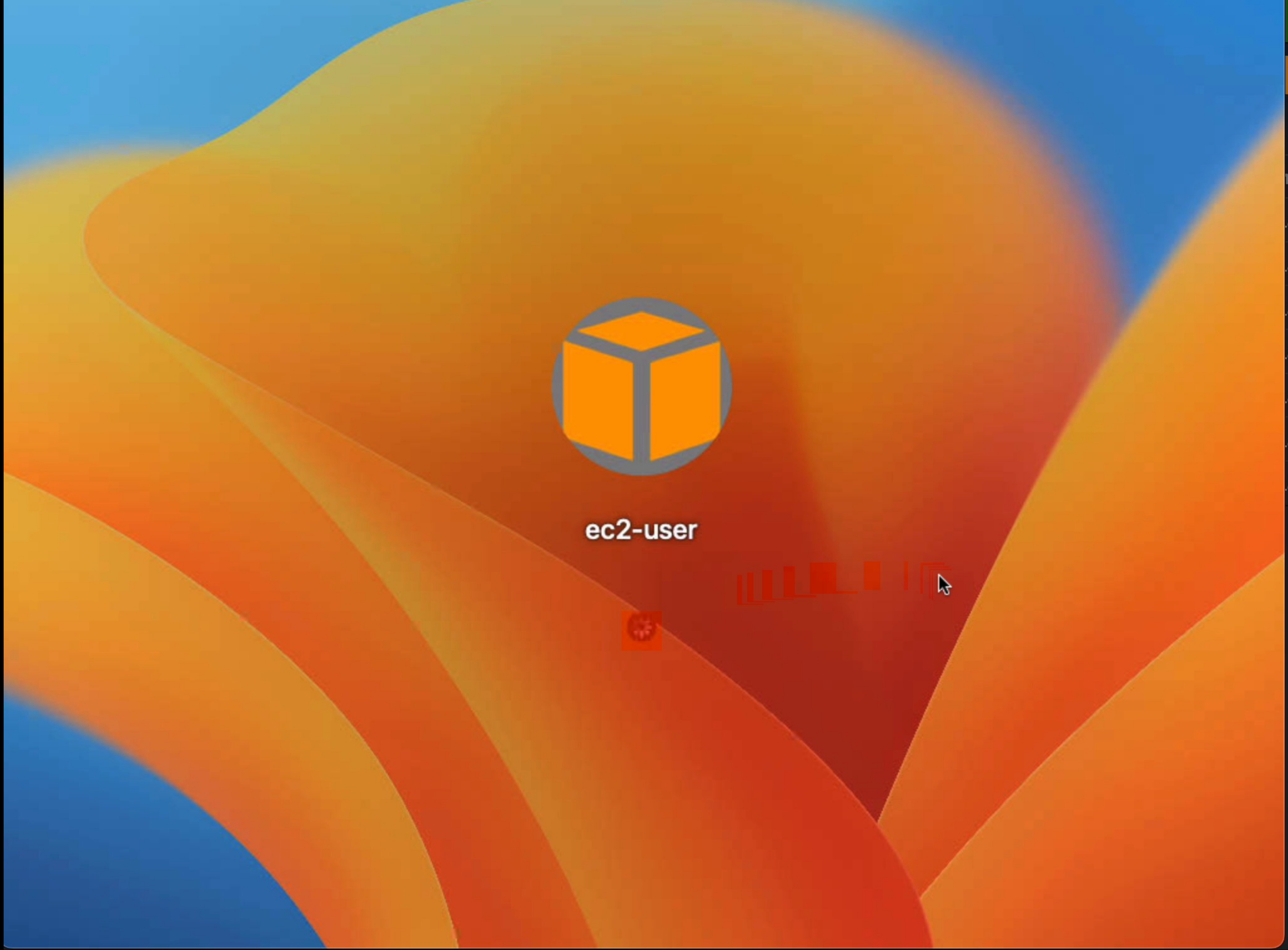
Use Case
#2
Temporary Workstations

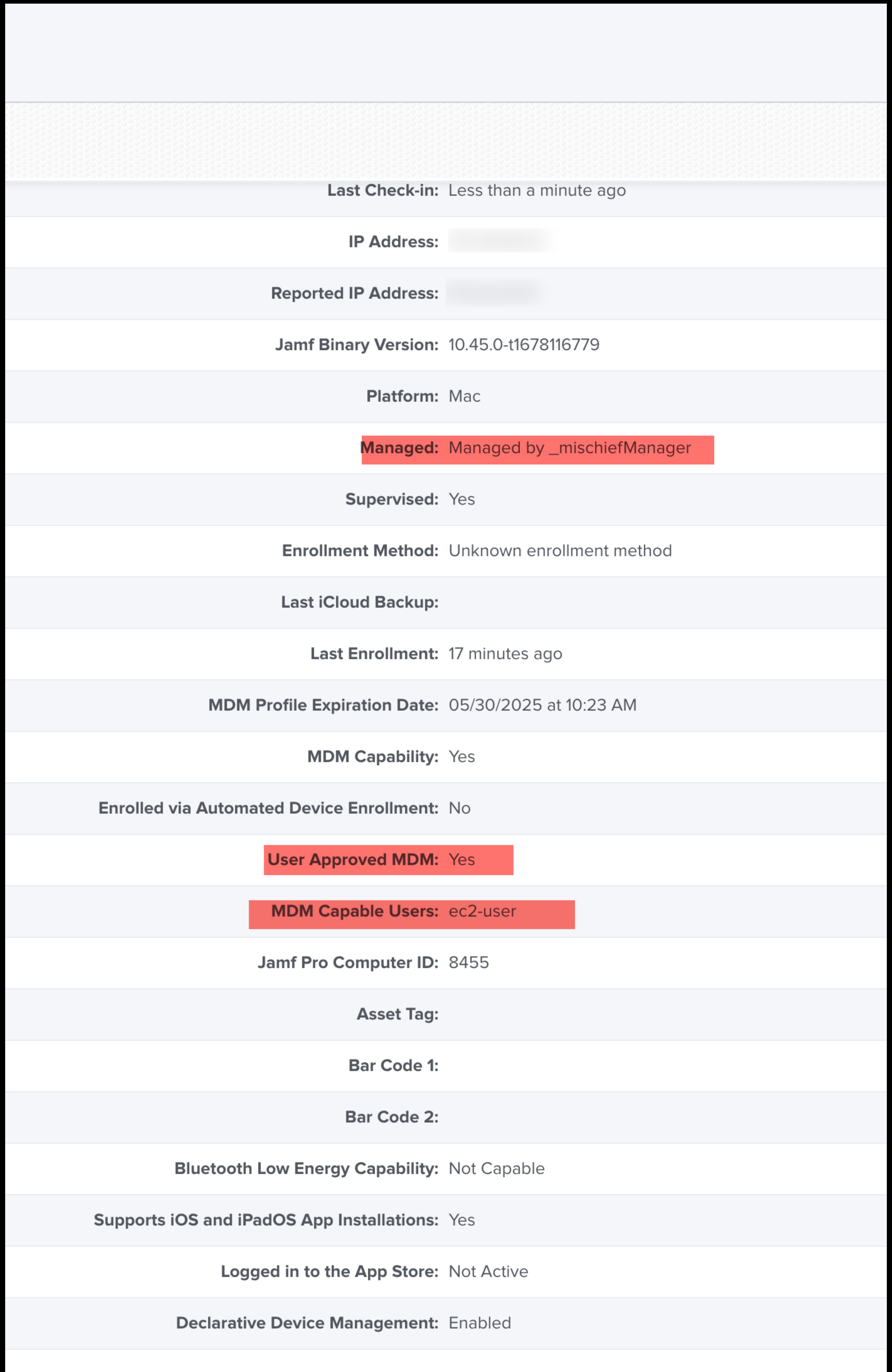

TED LASSO
Oh, you're bein' serious?

FEDERAL
EXPRESS
FEDERAL
EXPRESS
When it absolutely, positively
has to be there overnight.

Remote Workstation Challenges

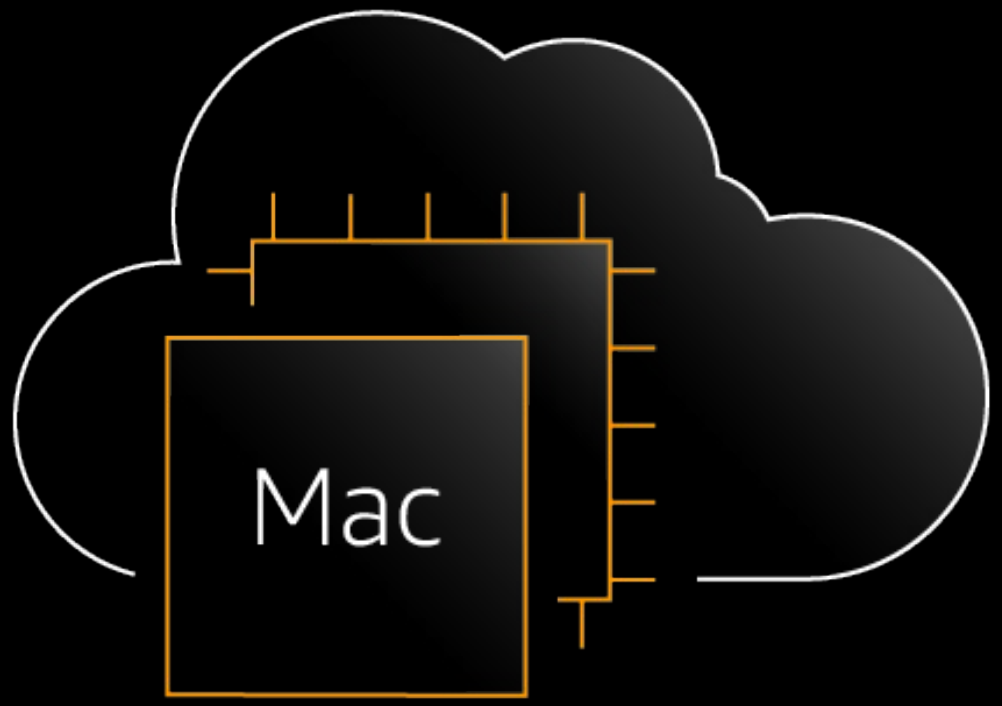
- Shipping will take weeks
  - Customs delays and fees
- Must be fully managed
- Must be secure
- Access to company assets and software
- User friendly
- Preferably without having to install software on non company assets


ec2-user



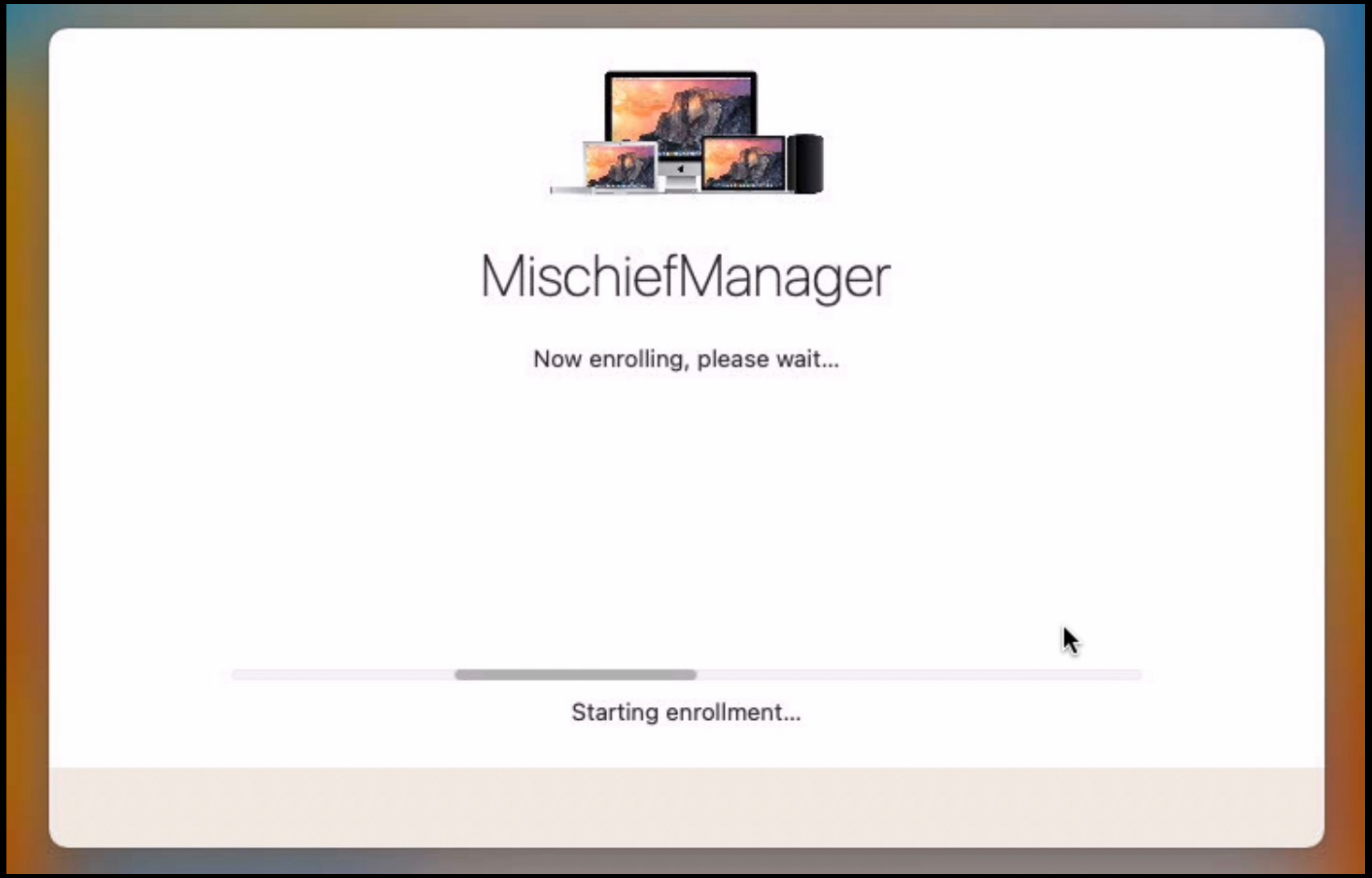
Last Check-in:	Less than a minute ago
IP Address:	[redacted]
Reported IP Address:	[redacted]
Jamf Binary Version:	10.45.0-t1678116779
Platform:	Mac
Managed:	Managed by _mischiefManager
Supervised:	Yes
Enrollment Method:	Unknown enrollment method
Last iCloud Backup:	
Last Enrollment:	17 minutes ago
MDM Profile Expiration Date:	05/30/2025 at 10:23 AM
MDM Capability:	Yes
Enrolled via Automated Device Enrollment:	No
User Approved MDM:	Yes
MDM Capable Users:	ec2-user
Jamf Pro Computer ID:	8455
Asset Tag:	
Bar Code 1:	
Bar Code 2:	
Bluetooth Low Energy Capability:	Not Capable
Supports iOS and iPadOS App Installations:	Yes
Logged in to the App Store:	Not Active
Declarative Device Management:	Enabled

Imaging (is undead)



- The "i" word lives again (in the cloud)!
- Amazon Machine Images (AMIs) are used to launch EC2 Mac instances
- AMI Catalog offers images directly from AWS, third-parties through AWS Marketplace, and public community images
- Snapshot to create your own derivative image, and launch new instances with your customized AMIs
- Launching instances from an MDM-enrolled AMI invalidates APNs communication

MischiefManager (code name)



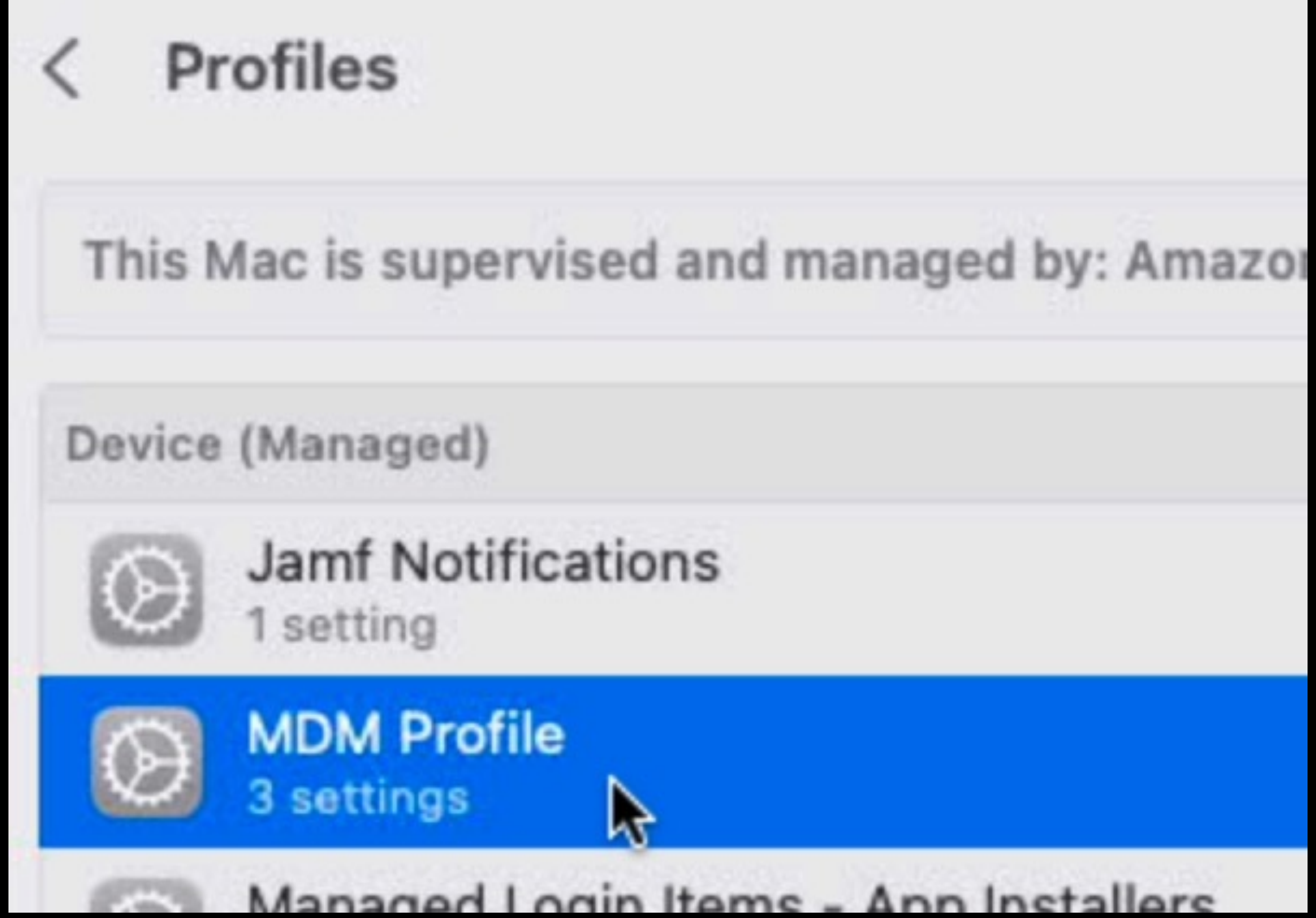
MischiefManager

Now enrolling, please wait...

Starting enrollment...

- Started **private preview** in **Q2’23**
- Example AppleScript designed to **automate** the process of **MDM enrollment** for **Amazon EC2 Mac instances**
- **Invisible** to user, can occur before instance is available for connection
- Tested on latest versions of macOS **Catalina** through **Ventura+**, **mac1** and **mac2** instances
- **Light AMI preparation** required (instructions available)

EC2 Mac MDM Enrollment (continued)



Profiles

This Mac is supervised and managed by: Amazo

Device (Managed)

Jamf Notifications
1 setting

MDM Profile
3 settings

Managed Login Items - App Installers

- MDM enrollment is **fully automated** for any EC2 Mac instances launched from a prepared (permissions-accepted) AMI
- Enrolled as **supervised** to Jamf/MDM
- **Integrated** with Jamf API to generate enrollment profiles
- **CloudFormation** and **Terraform** templates are available for both **AWS Secrets Manager** and **Parameter Store** for credentials

Jamf Extension Attribute for EC2 Metadata

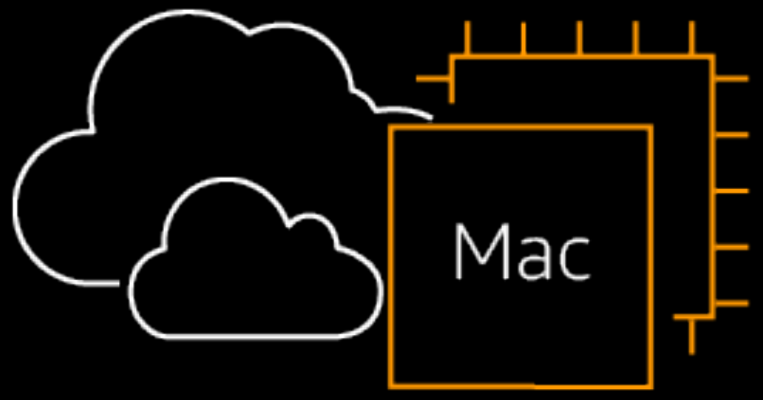
```
#!/bin/sh
dataPoint="placement/region"
PATH=/usr/local/bin:/usr/bin:/bin:/usr/sbin:/sbin:/opt/homebrew/bin:/opt/homebrew/sbin
MDToken=$(curl -X PUT "http://169.254.169.254/latest/api/token" -s -H "X-aws-ec2-metadata-token-ttl-seconds: 21600")
EC2Return=$(curl -H "X-aws-ec2-metadata-token: $MDToken" -s http://169.254.169.254/latest/meta-data/$dataPoint && echo || echo "Not an EC2 host.")
EC2Return="<result>"$EC2ID"</result>"
echo $EC2Return
exit 0;
```

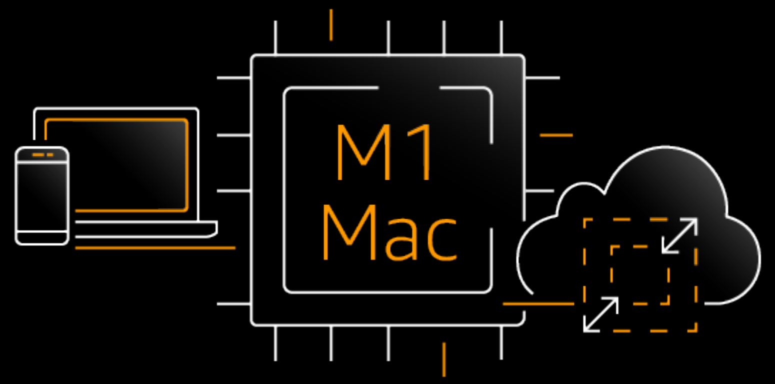
MischiefManager EC2 Metadata

```
on awsMD(MDPath)
	set sessionToken to (do shell script "curl -X PUT 
	http://169.254.169.254/latest/api/token -s 				-H 'X-aws-ec2-
metadata-token-ttl-seconds: 21600’”)
	set MDReturn to (do shell script "curl -H 'X-aws-ec2-metadata-token: " 	&
sessionToken & "' -s http://169.254.169.254/latest/meta-data/" & 	MDPath)
return MDReturn
end awsMD

set currentRegion to (my awsMD("placement/region"))
```

How It Was Done: MischiefManager





- **AppleScript**, with heavy use of **shell**
- **LaunchAgent** to manage setup and automation
- **DEPNotify (optional)** to shield UI during enrollment
- Minor **setup** required to create AMI and grant permissions for MischiefManager's access to:
  - System Events
  - Accessibility
  - App Management (only for mac2 instances using DEPNotify)
- Detection of **MDM contact issues** with **`profiles`** command
- Helper app **`cliclick`** for enrollment on Ventura or greater

Get an AWS EC2 Mac instance in a snap: InstaMac!

```
#!/bin/sh

# InstaMac.sh
# Fill in the variables below with your settings.

EC2InstanceType="mac2.metal"
EC2AMIID="ami-0a1b2c3d4e5a6b7c"
EC2KeyPairName="my-ssh-key"

EC2Region="us-east-1"
EC2AZ="d"

PATH=/usr/local/bin:/usr/bin:/bin:/usr/sbin:/sbin:/opt/homebrew/bin:/opt/homebrew/sbin
```

Allocate an EC2 Mac Dedicated Host

```
EC2HostID=$(aws ec2 allocate-hosts --availability-zone $EC2Region$EC2AZ \
    --auto-placement 'on’ \
    --host-recovery 'off’ \
    --quantity 1 \
    --instance-type $EC2InstanceType \
    --output text | awk {'print $NF'})

echo "$EC2HostID allocated!"
```

Start an EC2 Mac Instance

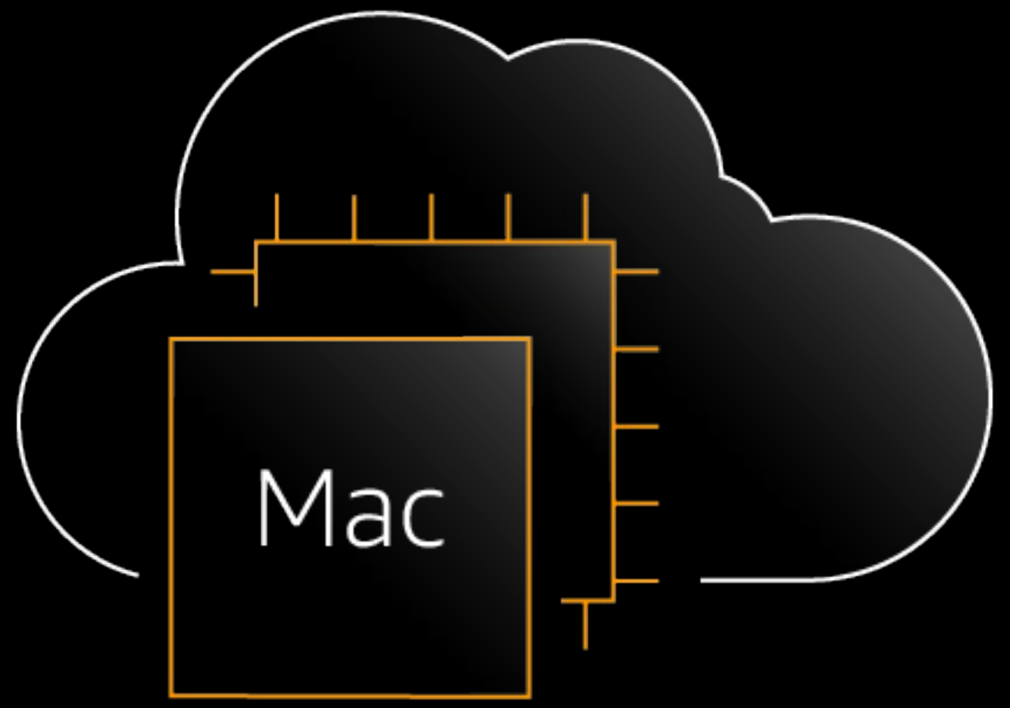
```
EC2InstanceID=$(aws ec2 run-instances --region $EC2Region \
    --instance-type $EC2InstanceType \
    --image-id $EC2AMIID \
    --key-name $EC2KeyPairName \
    --associate-public-ip-address \
    --placement 'Tenancy'='host','Affinity'='host','HostId'=$EC2HostID \
    | grep 'InstanceId' | awk {'print $NF'} | tr -d '\",')
```

Verify & Connect to an EC2 Mac Instance

```
EC2InstanceDNS=$(aws ec2 describe-instances --instance-id $EC2InstanceID --query
'Reservations[].Instances[].PublicDnsName' --output text)
EC2HostState=$(aws ec2 describe-hosts --host-id $EC2HostID --query 'Hosts[].State' --
output text)

if [ $EC2InstanceID ]; then
    echo "$EC2InstanceID launched successfully!"
    echo "You can access it at $EC2InstanceDNS."
else
    echo "Error starting instance."
fi
```

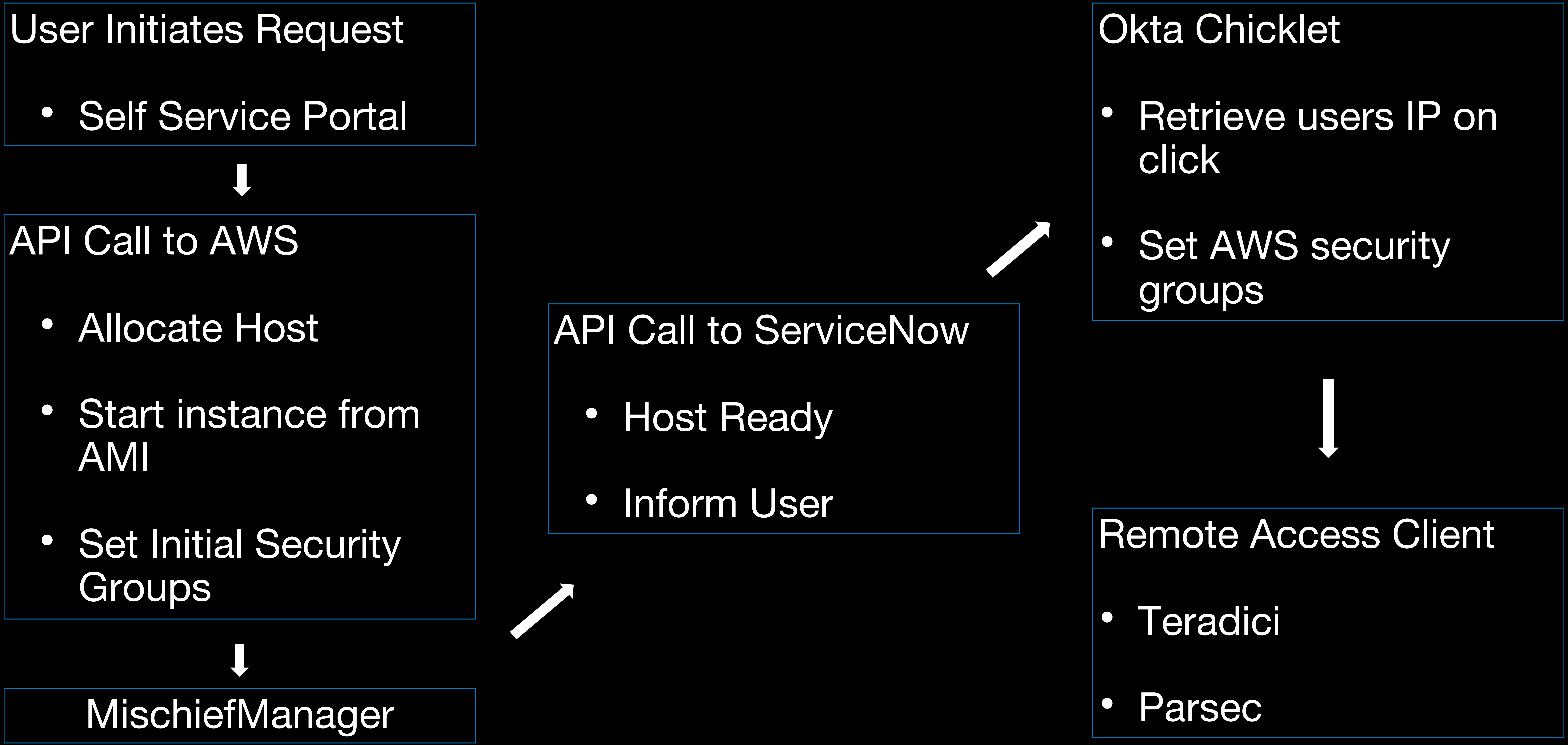
EC2 Mac instances: What's New



- Mac2 instances (Apple silicon) can perform **in-place macOS updates** for macOS **Monterey** and greater
- **Replace Root Volume** allows faster reversion to a snapshot or AMI on a running instance
- Instance start time improvements

Solution

Temp Dev Environment Workflow



User Initiates Request

- Self Service Portal

API Call to AWS

- Allocate Host
- Start instance from AMI
- Set Initial Security Groups

MischiefManager

API Call to ServiceNow

- Host Ready
- Inform User

Okta Chicklet

- Retrieve users IP on click
- Set AWS security groups

Remote Access Client

- Teradici
- Parsec

Things to Consider

- Existing profiles that will not work in the cloud
  - FileVault 2
    - EBS encryption is as secure
  - Wi-Fi
  - Bluetooth
  - Update settings*
- Anything else you don’t want to run VPN etc…

2023
MACADMINS
CONFERENCE

Q&A

Additional Resources

Mac Admins Intro to EC2 Mac & LastMile GitHub Repository

Auto Scaling for EC2 Mac Instances

Building AMIs for EC2 Mac instances with Packer

How to Use a CIS Hardened AMI for EC2 Mac

2023
MACADMINS
CONFERENCE

Thank you!

Feedback: https://bit.ly/psumac2023-114