What’s New in Apple Filesystems

Max Matveev, CoreOS
Jon Becker, CoreOS
Bill Stouder-Studenmund, CoreOS
Protecting system software on macOS

APFS volume replication

External files for iOS
APFS Refresher
Default filesystem on iOS since 10.3 and macOS since High Sierra
APFS Refresher
Default filesystem on iOS since 10.3 and macOS since High Sierra
APFS Refresher
Default filesystem on iOS since 10.3 and macOS since High Sierra
Protecting System Software

Max Matveev, CoreOS
Protecting System Software on macOS

System Integrity Protection is designed to help prevent potentially malicious software from modifying files and folders on your Mac.
Read-Only System Volume
Container Layout

Macintosh HD

Preboot  Recovery  VM
Delete Old System Content

Disk 1:
- Macintosh HD — Data
  - /
  - usr
    - bin
    - local
    - bin
  - Users
    - Jane S
    - lib
Delete Old System Content

Macintosh HD — Data

disk1

Macintosh HD — Data

/

usr

local

bin

lib

Users

Jane S

Preboot

Recovery

VM
Divide et Impera

Macintosh HD — Data

usr
local
bin
lib

Users

Jane S

Macintosh HD

Preboot
Recovery
VM
Firmlinks

Bi-directional wormhole in path traversal
Firmlinks

Bi-directional wormhole in path traversal

New filesystem object, similar to symlink
Firmlinks

Bi-directional wormhole in path traversal

New filesystem object, similar to symlink

- Consistent forward and backward traversal of the file name space
Firmlinks
Bi-directional wormhole in path traversal

New filesystem object, similar to symlink
• Consistent forward and backward traversal of the file name space
• Only for directories
Firmlinks
Bi-directional wormhole in path traversal

New filesystem object, similar to symlink
• Consistent forward and backward traversal of the file name space
• Only for directories
• Created on the system volume at installation time
FirmLinks
Bi-directional wormhole in path traversal

New filesystem object, similar to symlink
• Consistent forward and backward traversal of the file name space
• Only for directories
• Created on the system volume at installation time
• **Not** expected to be noticed by a user or an application
Stitch It Up

Macintosh HD — Data

Macintosh HD

Preboot

Recovery

VM
Stitch It Up

Macintosh HD — Data

- `/`
- `usr`
- `local`
- `lib`
- `Users`
- `Jane S`

Macintosh HD

- `/`
- `usr`
- `bin`
- `local`

Preboot  |  Recovery  |  VM
Stitch It Up
Stitch It Up
Stitch It Up
Take Home Message
Take Home Message

The volumes are split during the update, no way to opt-out
Take Home Message

The volumes are split during the update, no way to opt-out
• System volume is writable in the Developer Preview
Take Home Message

The volumes are split during the update, no way to opt-out
• System volume is writable in the Developer Preview
• Create a file named /.rootro to force read-only behavior
Take Home Message

The volumes are split during the update, no way to opt-out

- System volume is writable in the Developer Preview
- Create a file named /.rootro to force read-only behavior
- Will be made read-only in a future seed build
The volumes are split during the update, no way to opt-out

- System volume is writable in the Developer Preview
- Create a file named /.rootro to force read-only behavior
- Will be made read-only in a future seed build
- Read-only state of the system volume can be disabled but not persistently, will revert to read-only after a reboot
Take Home Message

The volumes are split during the update, no way to opt-out

• System volume is writable in the Developer Preview
• Create a file named /.rootro to force read-only behavior
• Will be made read-only in a future seed build
• Read-only state of the system volume can be disabled but not persistently, will revert to read-only after a reboot

Test your applications
ASR, Volume Replication, and Snapshots

Jon Becker, CoreOS
What is Volume Replication?
What is Volume Replication?

Copying volume content
What is Volume Replication?

Copying volume content
Superior to file copies
What is Volume Replication?

- Copying volume content
- Superior to file copies
- All volume data, metadata
What is Volume Replication?

- Copying volume content
- Superior to file copies
- All volume data, metadata
- Apple Software Restore (ASR)
Who Wants This?

Enterprise / Education IT, setting up labs

Backup utilities
Traditional Model (HFS Plus)
Partitions and volumes in one-to-one relationship
APFS

Great features
APFS

Great features
• Volume management, space sharing
APFS

Great features
• Volume management, space sharing
• Encryption
APFS

Great features
• Volume management, space sharing
• Encryption

Block copies not possible with APFS volumes
APFS Volume Replication with ASR

Volume 1

Volume 2

Stream

Container
APFS Volume Replication with ASR

Decryption / encryption part of generation / restore

Diagram showing the relationship between Volume 1, Volume 2, Container, Stream, and Container.
**APFS Volume Replication with ASR**

Decryption / encryption part of generation / restore

Volume is defragmented as stream is generated
Restore Options

Restoring to an existing target volume (erasing prior content)
Restore Options

Restoring to an existing target volume (erasing prior content)

# Restore, erasing a target volume
% sudo asr restore --source file.dmg --target /Volumes/Volume2 --erase
Restore Options
Restoring to an existing target volume (erasing prior content)

# Restore, erasing a target volume
% sudo asr restore --source file.dmg --target /Volumes/Volume2 --erase
Restore Options
Restoring to a newly created target volume

Container
Source Volume

Target before restore

Container
Volume 1
Volume 2
# Creates a new volume during restore

```bash
% sudo asr restore --source file.dmg --target /dev/disk1
```
Restore Options

Restoring to a newly created target volume

# Creates a new volume during restore
% sudo asr restore --source file.dmg --target /dev/disk1
Snapshots
Point-in-time capture of volume state
Snapshots
Point-in-time capture of volume state
Snapshots
Point-in-time capture of volume state
Snapshots
Point-in-time capture of volume state
Snapshots
Point-in-time capture of volume state

- Added to live volume
- Deleted from live volume
Restoring with Snapshots

Snap 1

Snap 2
Restoring with Snapshots

# Restore a snapshot

```bash
% sudo asr restore --source file.dmg --target /Volumes/Target --toSnapshot Snap1
```
# Restore a snapshot

% sudo asr restore --source file.dmg --target /Volumes/Target --toSnapshot Snap1
Restoring with Snapshots
Restoring with Snapshots

Snap 1

Snap 2
# Restore a snapshot delta

% sudo asr restore --source file.dmg --target /Volumes/Target --fromSnapshot Snap1 \
--toSnapshot Snap2
Restoring with Snapshots

# Restore a snapshot delta
% sudo asr restore --source file.dmg --target /Volumes/Target --fromSnapshot Snap1 \ --toSnapshot Snap2
Replication Summary
Replication Summary

New features in APFS require new models of replication
Replication Summary

New features in APFS require new models of replication

APFS Volume replication best done with ASR
Replication Summary

New features in APFS require new models of replication

APFS Volume replication best done with ASR

• Gives highest fidelity
Replication Summary

New features in APFS require new models of replication

APFS Volume replication best done with ASR

• Gives highest fidelity
• Handles encryption
Replication Summary

New features in APFS require new models of replication

APFS Volume replication best done with ASR
- Gives highest fidelity
- Handles encryption

ASR can restore snapshots, snapshot deltas
External File Access for iOS

Bill Stouder-Studenmund, CoreOS
USB Storage
USB Storage

Unencrypted APFS
USB Storage

Unencrypted APFS

Unencrypted HFS Plus
USB Storage

Unencrypted APFS
Unencrypted HFS Plus
FAT, ExFAT
Network Shares

Supports SMB 3.0
Network Shares

Supports SMB 3.0

Connect over WiFi, Cellular, and Ethernet
Network Shares

Supports SMB 3.0

Connect over WiFi, Cellular, and Ethernet

Search using Windows Search Protocol
Network Shares

Supports SMB 3.0

Connect over WiFi, Cellular, and Ethernet

Search using Windows Search Protocol

And we've added Windows Search to macOS Catalina’s SMB server
What This Means for You
What This Means for You

Enabled by default for apps linked on or after iOS 13
What This Means for You

Enabled by default for apps linked on or after iOS 13

Pay attention to volume capability attributes
What This Means for You

Enabled by default for apps linked on or after iOS 13

Pay attention to volume capability attributes

NSURL.resourceValues(forKeys:)
What This Means for You

Enabled by default for apps linked on or after iOS 13

Pay attention to volume capability attributes

`NSURL.resourceValues(forKeys:)`

File movement now may take time
What This Means for You

Enabled by default for apps linked on or after iOS 13

Pay attention to volume capability attributes

`NSURL.resourceValues(forKeys:)`

File movement now may take time

Put your temp files near the working files
What This Means for You

Enabled by default for apps linked on or after iOS 13

Pay attention to volume capability attributes

`NSURL.resourceValues(forKeys:)`

File movement now may take time

Put your temp files near the working files

`fileManager.url(for: .itemReplacementDirectory,
               in: .userDomainMask,
               appropriateFor: yourFile,
               create: true)`
What This Means for You
What This Means for You

External devices can suddenly go away
What This Means for You

External devices can suddenly go away
• mmap can be dangerous
What This Means for You

External devices can suddenly go away
• mmap can be dangerous
• Use NSData.ReadingOptions.mappedIfSafe
What This Means for You

External devices can suddenly go away
• mmap can be dangerous
• Use `NSData.ReadingOptions.mappedIfSafe`

External devices have higher latencies than the internal Flash Storage
What This Means for You

External devices can suddenly go away
• mmap can be dangerous
• Use `NSData.ReadingOptions.mappedIfSafe`

External devices have higher latencies than the internal Flash Storage
• For best results, keep multiple large operations in-flight at once
Summary

We are making the root volume read-only for enhanced security
We are making the root volume read-only for enhanced security.

You can use ASR to perform volume replication, including snapshot deltas.
Summary

We are making the root volume read-only for enhanced security.

You can use ASR to perform volume replication, including snapshot deltas.

We now support accessing external files on USB Storage and Network Shares.
More Information

developer.apple.com/wwdc19/710

<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filesystem Lab</td>
<td>Wednesday, 5:00</td>
</tr>
<tr>
<td>Introducing Combine and Advances in Foundation</td>
<td>Thursday, 10:00</td>
</tr>
<tr>
<td>What’s New in File Management and Quick Look</td>
<td>WWDC App</td>
</tr>
</tbody>
</table>