csr-active-config Eintrag + Big Sur Installation Frage

Beitrag von „ron“ vom 17. November 2020, 22:24

Ich möchte von Catalina nach Big Sur updaten.

Opencore neueste Version + Kexte intalliert auf Catalina. Soweit läuft alles bestens.

Momentan unter Catalina mit opencore habe ich in meiner config-plist für csr-active-config folgendes stehen FF070000

csrutil status

System Integrity Protection status: disabled.

Jetzt möchte ich big sur update machen:

Muß ich diesen Wert von csr-active-config ändern bevor ich Big Sur zu installieren beginne ? Habe nämlich gelesen, daß für "sip disabled" in Big Sur der Wert `FF0F0000` aufweisen sollte.

Mir ist nicht klar, ob ich das bereits unter Catalina eintrage in config.plist, dann erstmal damit Catalina neu boote und dann anschliessend big sur update anstoße

oder

ob ich mit bestendem FF070000 Eintrag den update big sur veranlasse und das dann später wenn big Sur läuft auf `FF0F0000 ändern muß`

Merci !

Beitrag von „griven“ vom 17. November 2020, 23:29

Wenn BigSur erstmal läuft ist es relativ egal was Du für die CSRActive Config einstellst solange Du darauf achtest das CSR_ALLOW_DEVICE_CONFIGURATION ausgeklammert bleibt denn sobald man dieses Setting deaktiviert schlagen sämtliche Updates die mit BigSur zu tun haben fehl (werden entweder gar nicht angezeigt oder aber der Download schlägt fehl). Der von Dir

zitierte Wert FF0F0000 steht für folgende Konfiguration der SIP:

Code

1. CSR_ALLOW_EXECUTABLE_POLICY_OVERRIDE
2. CSR_ALLOW_UNAPPROVED_KEXTS
3. CSR_ALLOW_ANY_RECOVERY_OS
4. CSR_ALLOW_DEVICE_CONFIGURATION
5. CSR_ALLOW_UNRESTRICTED_NVRAM
6. CSR_ALLOW_UNRESTRICTED_DTRACE
7. CSR_ALLOW_APPLE_INTERNAL
8. CSR_ALLOW_KERNEL_DEBUGGER
9. CSR_ALLOW_TASK_FOR_PID
10. CSR_ALLOW_UNRESTRICTED_FS
11. CSR_ALLOW_UNTRUSTED_KEXTS

Alles anzeigen

und ist eigentlich nicht wirklich ideal eben weil CSR_ALLOW_DEVICE_CONFIGURATION auch gesetzt ist. Man muss sich halt auch überlegen ob es wirklich sinnvoll ist alles was möglich ist bei der SIP zu deaktivieren oder ob man nicht lieber die Strategie verfolgt soviel wie möglich von der SIP aktiv zu halten und somit den Schutz den sie bietet mitzunehmen. Ich persönlich nutze den Wert 67F was für folgende Einstellungen steht:

Code

1. CSR_ALLOW_EXECUTABLE_POLICY_OVERRIDE
2. CSR_ALLOW_UNAPPROVED_KEXTS
3. CSR_ALLOW_UNRESTRICTED_NVRAM
4. CSR_ALLOW_UNRESTRICTED_DTRACE
5. CSR_ALLOW_APPLE_INTERNAL
6. CSR_ALLOW_KERNEL_DEBUGGER
7. CSR_ALLOW_TASK_FOR_PID
8. CSR_ALLOW_UNRESTRICTED_FS
9. CSR_ALLOW_UNTRUSTED_KEXTS

Mit der Einstellung fahre ich mit BigSur und Catalina ohne Probleme und ohne spürbare Einschränkungen durch die SIP. Musst halt selbst gucken und überlegen was genau Du brauchst und ob Dein Usecase ein komplettes abschalten der SIP wirklich notwendig macht. Am langen Ende ist die SIP eigentlich etwas gutes von dem wir auch auf unseren Kisten profitieren können. Es gibt wenige Dinge die wir ggf. wirklich brauchen wie zum Beispiel CSR_ALLOW_KERNEL_DEBUGGER oder CSR_ALLOW_UNRESTRICTED_FS alles andere kann man

aber getrost aktiviert lassen und wird dadurch keine wirklichen Einschränkungen im Betrieb erfahren.

Beitrag von „ron“ vom 17. November 2020, 23:58

Danke für die schnelle INfo !

Jetzt fällt mir auf, daß FF070000 und `FF0F0000` dasselbe Ergebnis ausspucken wenn ich den CsrDecode Befehl bemühe um zu den Ergebnissen wie bei Dir unter "Code" (1-11 / 1-9) aufgeführt zu kommen. Nämlich: >>

Code:

Please type a CsrActiveConfig value (m for main menu): FF070000

Active values:

CSR_ALLOW_EXECUTABLE_POLICY_OVERRIDE

CSR_ALLOW_UNAPPROVED_KEXTS

CSR_ALLOW_ANY_RECOVERY_OS

CSR_ALLOW_DEVICE_CONFIGURATION

CSR_ALLOW_UNRESTRICTED_NVRAM

CSR_ALLOW_UNRESTRICTED_DTRACE

CSR_ALLOW_APPLE_INTERNAL

CSR_ALLOW_KERNEL_DEBUGGER

CSR_ALLOW_TASK_FOR_PID

CSR_ALLOW_UNRESTRICTED_FS

CSR_ALLOW_UNTRUSTED_KEXTS

Please type a CsrActiveConfig value (m for main menu): FF0F0000

Active values:

CSR_ALLOW_EXECUTABLE_POLICY_OVERRIDE

CSR_ALLOW_UNAPPROVED_KEXTS

CSR_ALLOW_ANY_RECOVERY_OS

CSR_ALLOW_DEVICE_CONFIGURATION

CSR_ALLOW_UNRESTRICTED_NVRAM

CSR_ALLOW_UNRESTRICTED_DTRACE

CSR_ALLOW_APPLE_INTERNAL

CSR_ALLOW_KERNEL_DEBUGGER

CSR_ALLOW_TASK_FOR_PID

CSR_ALLOW_UNRESTRICTED_FS

CSR_ALLOW_UNTRUSTED_KEXTS

Somit könnte ich auf FF0F0000 umstellen ohne Änderung. Catalina bootet damit genauso und das Ergebnis von

csrutil status

System Integrity Protection status: disabled.

bleibt gleich.

Beitrag von „griven“ vom 18. November 2020, 00:15

Catalina bootet auf alle Fälle damit wieso sollte es auch nicht?

Generell ist es aber auch eigentlich egal ob die SIP aktiv ist oder nicht zumindest solange man einen modernen Bootloader verwendet und dem Bootloader das Injecten des Extensions überlässt. Wie ich schon schrieb die SIP kümmert uns eigentlich in unserem Tun nicht wirklich denn durch die Kext Injection durch den Bootloader umgehen wir Restrictions wie CSR_ALLOW_UNAPPROVED_KEXTS und CSR_ALLOW_UNTRUSTED_KEXTS indem wir die Extensions schon vor dem Start des Kernels in den Prelinked Kernel (bis Catalina) bzw. in die Kernel Collections (ab BigSur) einbringen. Alles was durch die SIP eingeschränkt wird passiert erst nachdem der Kernel bereits gestartet ist. Anders gesprochen allem was den Weg in den Prelinked Kernel bzw. in die Kernel Colletions gefunden hat wird per se vertraut die SIP sorgt lediglich zur Laufzeit dafür das dort nichts hinein gelangt was durch die Einschränkungen durch die SIP dort nichts zu suchen hat.

Beitrag von „kexterhack“ vom 2. Januar 2021, 20:37

griven

Ich habe das Problem das mein SIP wohl meinen Proper Tree blockiert nach dem neuesten kleinen BigSur update.

Wie kann ich übers Terminal nun deinen Wert 67F einstellen?

Will mir ungern kommende Updates madig machen.

Danke vorab!

Edit: obwohl disabled - läuft proper tree nicht

Beitrag von „griven“ vom 2. Januar 2021, 23:16

Hö? In wie fern läuft ProperTree nicht welche Fehlermeldung gibt es denn?

Beitrag von „kexterhack“ vom 2. Januar 2021, 23:50

griven Danke!

Phyton crasht, aber mir wurde gerade schon geholfen, im Proper Tree Thread.

Ich musste einfach phyton von der offiziellen page installieren, obwohl korrekt auf dem system.

Und habe eine andere version von PT verwendet und dann lief es wieder.

Nach Stunden der suche und installieren von homebrew und co. war es dann doch so einfach.

Ich war so dumm und habe einen NVRAM Reset gerade eben kurz vor der Lösung gemacht,

und dachte es hilft. Nun ist das eine Problem gelöst und jetzt beschäftige ich mich schon mit dem nächsten.

Der Hacki bootet nicht mehr ohne Rescue Stick.

Ne schnelle Idee wo ich da ansetzen kann um das nun schnell zu fixen?

Nicht mein Tag heute.

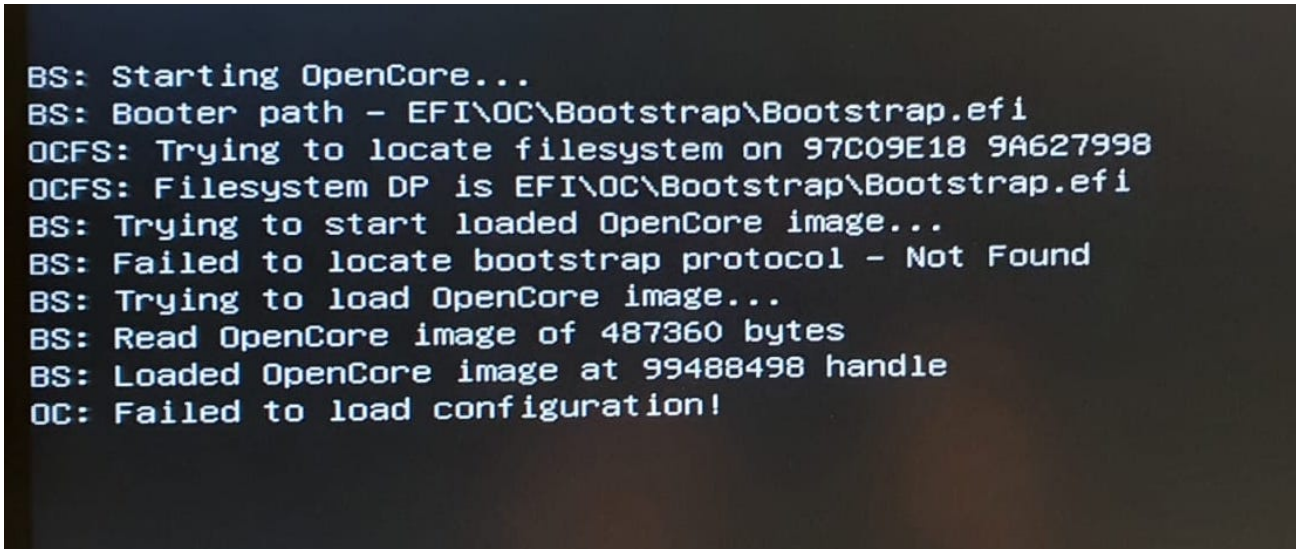
Beitrag von „griven“ vom 2. Januar 2021, 23:55

Hum dann muss in Deiner eigentlichen EFI/Config was anders sein als auf dem Rescue Stick (-> NVRAM Bereich vermutlich) musst mal die beiden configs vergleichen denke ich. Gibt es denn eine Kernelpanik/Fehlermeldung oder irgendwas sonst oder wie definiert sich bootet nicht mehr genau?

Beitrag von „kexterhack“ vom 3. Januar 2021, 00:04

griven

Er findet das bootstrap protokoll nun nicht mehr



Beitrag von „griven“ vom 3. Januar 2021, 00:07

Hum okay da stimmt was mit der config nicht...

Magst Du die config mal hochladen das man da mal einen Blick drauf werfen kann? Irgendwas hängt da jedenfalls schief...

Beitrag von „kexterhack“ vom 3. Januar 2021, 00:27

Klar danke

Hab hier beim Sample plist compare eine abweichung gefunden

Nur komisch, dass ich vor wenigen stunden erst geupdatet habe und gerade die alte gesicherte efi vor dem NVRAM Reset kopiert habe und dennoch diese abweichung bleibt.

Werde das mal ändern und sehen ob es wieder läuft ohne stick.

```
 ##########################################################
 #                  OC Config Compare                     #
##########################################################

Checking for values missing from User plist:

config.plist -> NVRAM -> Add -> 7C436110-AB2A-4BBB-A880-FE41995C9F82 -> prev-lang:kbd - Type Difference: Strin
g --> Data
config.plist -> UEFI -> Audio -> PlayChime - Type Difference: Boolean --> String

Checking for values missing from Sample:

Sample.plist -> DeviceProperties -> Add - Missing Key: PciRoot(0x0)/Pci(0x1,0x0)/Pci(0x0,0x0)
Sample.plist -> NVRAM -> Add -> 7C436110-AB2A-4BBB-A880-FE41995C9F82 -> prev-lang:kbd - Type Difference: Data
--> String
Sample.plist -> UEFI -> Audio -> PlayChime - Type Difference: String --> Boolean

Press [enter] to return...
```

Beitrag von „griven“ vom 3. Januar 2021, 00:34

Wenn Du schon dabei bist setzte unter Misc -> Security dann den Punkt BootProtect von Bootstrap auf None um das Bootstrap Thema ebenfalls zu erschlagen. Der Wert für Bootstrap ist in den neueren OC Versionen standardmäßig auf none gestellt unter anderem deshalb weil das bei diversen Boards zu Problemen geführt hat (Bricked UEFI)...

Beitrag von „kexterhack“ vom 3. Januar 2021, 00:45

Danke mache ich.

Dann teste ich mal direkt.

Bei dem NVRAM Add stand bei mir vorher de:3 ich erinnere mich vage, dass ich da mal was geändert hatte. Den Wert konnte ich nicht wieder übernehmen und hab es so wie oben eingetragen aus der sample plist.

Was mich wundert, dass die sample plist aus dem OC Ordner immer leicht anders ist als die

sample plist die OC Config Compare zu Verfügung stellt?!

EDIT:

Leider ohne Erfolg

hier die geänderte config.plist

Edit2:

Hab nochmal ein wenig nachgedacht, da es mich sehr stutzig machte das es obwohl ich die gesicherte EFI vor dem NVRAM Reset nahm es dennoch nicht lief.

Bin dann mal ins Bios und hab da nochmal was geändert und zack läuft es wieder.

Der USB Stick stand nämlich plötzlich an 1 Boot Stelle.

Was mich nochmal sehr interessieren würde, wofür ich aber wohl mal einen neuen Thread brauche ist, wieso die Sample Plist so viele Änderungen hat und Neuerungen die mir beim Compare Vergleich mit dem TOOL gar nicht angezeigt werden?

Ich meine es läuft alles und ich ändere immer das was der Vergleich mir sagt, aber das mit dem Bootstrap was du mir empfahlst, hat er nicht angezeigt, wäre es daher mal besser einfach die sample plist zu nehmen und daraus eine neue EFI zu machen? -oder ist das so ok wenn alles läuft?

Beitrag von „griven“ vom 3. Januar 2021, 08:54

Ich halte es generell immer so das ich die config immer wieder aus der jeweils mitgelieferten Sample.plist neu aufbaue wenn ich OC Update. Im Grunde dauert das auch nicht länger als über compare die Änderungen zu ermitteln und umzusetzen. Der Vorteil in meiner Vorgehensweise liegt in meinen Augen darin das man garantiert eine config hat die zur eingesetzten OC Version passt auf die Weise lassen sich einige Fehlerquellen ausschließen. 😉

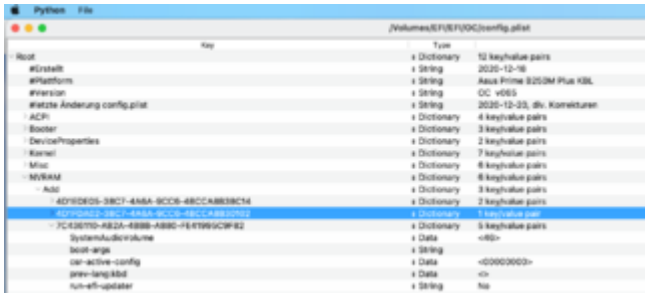
Beitrag von „Arkturus“ vom 3. Januar 2021, 10:40

Bootstrap wird nur benötigt, um bei Installationen von Windows oder Linux Konflikte mit der EFI zu vermeiden. Wer das nicht vorhat, kann Boostrap ohne Probleme in Rente schicken.

wie kommst Du darauf, dass ProperTree ein disabled SIP verlangt? kexterhack

Ich habe dir das gestern geschrieben, dass es mit enabled SIP bei mir unter BS 11.2 beta bestens funktioniert. csr-avtive-config = 00000000

wenn Du hier mal schauen willst, Bitteschön:



Beitrag von „kexterhack“ vom 3. Januar 2021, 17:39

griven

Danke, werd mir die config dann nxt mal durchgehen und schauen was wichtig ist im Detail. Was ich ändern muss und was nicht- also dann anpassen auf der sample plist.

Ist nicht immer ganz klar, und die Change List ist ja ziemlich riesig sodass es wenn man die wichtigen Parameter nicht ad hoc weiß schon sehr lange dauern kann.

Never change a running system, aber manchmal vll. besser. 😉

Arkturus

Weil sascha nach deinem post schrieb es ist wohl ein SIP Problem. Und du hattest eine Beta drauf die ich nicht habe. Deshalb- sry dafür.

Habe bootstrap auf none. Sollte beim dual boot mit windows aber auch auf lange sicht keine probleme geben?

Also zB wenn ich ein update bei windows mache?

Die nvme vom hacki jedes Mal rauszufummeln wäre doof. Liegt auf getrennten nvmes win und macOS.

Beitrag von „Arkturus“ vom 4. Januar 2021, 18:51

Ja, Windows-Update fummelt auch am Bios rum. Habe das gerade erst gemerkt, beim letzten Update vorige Woche. Kann mich nicht erinnern das es mir früher schon mal aufgefallen wäre.

Beitrag von „kexterhack“ vom 4. Januar 2021, 19:06

@Arkturus

Macht es Sinn dann Bootstrap doch zu verwenden?

bzw. kann ich wenn was an der EFI sein sollte, einfach das Backup Efi reinholen!?

Beitrag von „Arkturus“ vom 4. Januar 2021, 20:00

Da muss ich passen. Bootstrap übernimmt das BIOS. Nicht mein Ding.

EDIT: würde ich Windows produktiv nutzen, also für mich wäre das zwei drei mal die Woche oder mehr, würde ich mich mit Bootstrap befassen.