macOS Support Essentials 10.14

Support und Fehlerbehebung für macOS Mojave
Handbuch zur Prüfungsvorbereitung

Inhaltsverzeichnis

Zertifizierung als Apple Certified Support Professional

Die Zertifizierung als Apple Certified Support Professional (ACSP) richtet sich an Helpdesk-Mitarbeiter, technische Koordinatoren und Power-User, die macOS Benutzer unterstützen, Netzwerke verwalten oder technischen Support für Mac Benutzer leisten. Die Zertifizierung als ACSP bestätigt deine Kenntnisse der Kernfunktionen von macOS sowie deine Fähigkeit für Folgendes:

- Konfiguration wichtiger Dienste.
- Durchführung grundlegender Fehlerbehebungsmaßnahmen.
- Unterstützung mehrerer Mac Benutzer.

Für die Zertifizierung als ACSP musst du die Prüfung „macOS Support Essentials 10.14“ bestehen. Weitere Informationen findest du auf der Website zu Training und Zertifizierung.

Vorteile der Zertifizierung als ACSP

Eine Zertifizierung als ACSP ist wertvoll, da sie dich als versierten Benutzer und Supportspezialisten für macOS Mojave 10.14 auszeichnet. Du bist dann berechtigt, das „Apple Certified Professional“-Logo auf deinem Lebenslauf sowie deinen Visitenkarten und Websites zu verwenden. Diese Zertifizierung verschafft dir einen Wettbewerbsvorteil auf dem immer anspruchsvoller werdenden Arbeitsmarkt. Mit ihr kannst du auch die Attraktivität der Marke Apple nutzen.

Bevor du die Zertifizierungsprüfung absolvierst, musst du über einen Account im Apple Zertifizierungssystem verfügen (bzw. einen anlegen). Wenn du die Prüfung bestehst, bekommst du eine E-Mail mit Details darüber, wie du dein Apple Zertifikat erhältst und eine gerahmte Ausführung des Zertifikats bestellst. Diese E-Mail enthält Symbole für LinkedIn, Facebook und Twitter, über die du auf diesen Websites ankündigen kannst, dass du deine Zertifizierung bekommen hast. Du kannst dich dann beim Apple Zertifizierungssystem anmelden und folgende Aktionen ausführen:

- dein Profil aktualisieren und auf Wunsch deine Apple Zertifizierung im Apple Certified Professionals Registry anzeigen lassen;
- deinen Zertifizierungsfortschritt verfolgen;
- dein Zertifizierungslogo laden, um es auf Visitenkarten, Lebensläufen, Websites usw. zu verwenden;
- potenziellen Arbeitgebern die Überprüfung deiner Zertifizierungen ermöglichen.

Vorbereitung auf die Prüfung

Die folgende Prüfungsvorbereitung wird empfohlen:

- Absolviere den Kurs „macOS Support Essentials 10.14".

  Autorisierte Apple Trainingsanbieter (AATPs) bieten Kurse an, in denen du macOS in der Praxis kennenlernen und vom Know-how der Apple Certified Trainer und deiner Kollegen profitieren kannst. LearnQuest ist einer dieser AATPs. Schau doch mal auf der Website nach Kursen in deiner Nähe.

- Lies das Buch *macOS Support Essentials 10.14* von Arek Dreyer und Adam Karneboge aus der Apple Pro Training Series.

  Das Buch *macOS Support Essentials 10.14* aus der Apple Pro Training Series ist die Grundlage der ASCP Prüfung. Du kannst es bei verschiedenen Anbietern kaufen:

  - Apple Books: Auf einem iOS Gerät oder Mac kannst du es im Apple Books Store kaufen.
  - Peachpit: Über die Peachpit Website bekommst du 30 % Rabatt.

  Womöglich ist das Buch auch in Übersetzung erhältlich. Näheres dazu findest du auf der Peachpit Website.

- Sammle Erfahrungen mit macOS.

  Am besten lernst du die macOS Technologie, indem du sie einfach benutzt. Nachdem du das Buch gelesen bzw. am Kurs teilgenommen hast oder beides, solltest du dir die Zeit nehmen, dich mit macOS noch vertrauter zu machen, um die Zertifizierungsprüfung erfolgreich ablegen zu können.

- Lies dieses Handbuch, mache die Beispielaufgaben und beantworte die Kontrollfragen.

  Wenn du dir die nötigen Kenntnisse selbst angeeignet oder Kurse belegt hast, die nicht auf dem Lehrplan der Apple Pro Training Series basieren, kannst du dich dennoch auf die Zertifizierungsprüfung vorbereiten, indem du die Aufgaben in diesem Handbuch löst und die Kontrollfragen beantwortest. Die Aufgaben und Fragen decken alle Wissensgebiete ab, die bei der ASCP Prüfung bewertet werden. Während die Aufgaben und Kontrollfragen im vorliegenden Handbuch allerdings in Lektionen oder Wissensgebiete unterteilt sind, werden die Fragen in der Prüfung willkürlich ausgewählt.

- Konsultiere einige der vielen Referenzen, Fehlerbehebungsinformationen und Online-Tutorials von anderen Anbietern für Benutzer verschiedener Ebenen, vom Neuling bis zum Power-User.

- Stelle etwaige Fragen im macOS Diskussionsforum, das Apple bereitstellt.

Prüfungsdetails

Bei der Prüfung „macOS Support Essentials 10.14“ (Nr. 9L0-852) handelt es sich um einen computergestützten Test, der bei autorisierten Apple Trainingsanbietern (AATPs) angeboten wird. Den nächstgelegenen AATP findest du auf der LearnQuest Website. (Unser globaler Trainingspartner heißt LearnQuest.) Wenn bei deinem nächstgelegenen AATP kein Prüfungstermin geplant ist, erfrage direkt bei LearnQuest, ob ein Prüfungstermin eingeplant werden kann. Alle AATPs bieten die macOS Prüfung an, auch wenn sie den entsprechenden Kurs nicht veranstalten.

Hier die näheren Details zur Prüfung „macOS Support Essentials 10.14“:

- Die Prüfung umfasst auch fünf demografische Fragen, die nicht gewertet werden und für die du 5 Minuten Zeit hast.
- Die Prüfung selbst besteht aus 100 bewerteten technischen Fragen, für die du 150 Minuten Zeit hast.
- Der Prüfung liegen ein Pool aus Multiple-Choice-Fragen und Fragen mit interaktiven Medien zugrunde, aus denen nach dem Zufallsprinzip gewählt wird.
- Die erforderliche Punktzahl beträgt 75 Prozent. Punktzahlen werden nicht gerundet.
- Details zur Prüfungsbewertung findest du auf der Seite Fragen und Antworten zur Prüfung und Zertifizierung.
- Du darfst während der Prüfung nicht auf Ressourcen oder Referenzmaterialien zugreifen.
- Einige Prüfungen sind in mehreren Sprachen verfügbar. Besuche für Details die Kursseite macOS Support Essentials 10.14 auf der Apple Training-Website.

Besuche bei Fragen zu Apple Zertifizierungsprüfungen die Seite Fragen und Antworten zur Prüfung und Zertifizierung.

Teil 1: Installation und Konfiguration

Lektion 1 – Einführung in macOS

Ziele

- macOS beschreiben
- Neue Funktionen in macOS Mojave 10.14 beschreiben

Kontrollfragen

1. Welche beiden Industriestandards wurden mit der Entwickler-Community geteilt und trugen zum Erfolg von macOS bei?
2. Was ist das standardmäßige Dateisystem für Mac Computer mit macOS Mojave?
3. Was geschieht beim Upgrade auf macOS Mojave mit dem Startvolume?
4. Was sind einige der neuen Funktionen von macOS Mojave?
5. Welche vier iOS Apps werden mit macOS Mojave eingeführt?
6. Welche Datenschutz- und Sicherheitsverbesserungen stehen mit macOS Mojave zur Verfügung?
7. Was ist eine verbesserte Funktion von Siri in macOS Mojave 10.14?
8. Wo findest du eine Einführung zu den neuen Funktionen von macOS Mojave 10.14 und der Navigation auf deinem Mac?

Antworten

1. Multicast DNS für Netzwerke und die Programmiersprache Swift sind zwei Industriestandards, die mit der Entwickler-Community geteilt wurden und zum Erfolg von macOS beitrugen.
2. Das standardmäßige Dateisystem für alle Mac Computer ist Apple File System (APFS).
3. Das Startvolume wird beim Upgrade auf macOS Mojave automatisch in APFS konvertiert.
4. Neue Funktionen in macOS Mojave:
   - Dunkelmodus: ein Oberflächendesign, mit dem du dich besser auf deine Arbeit konzentrieren kannst.
   - Finder: eine verbesserte Suchfunktion, die automatisch geöffnet wird. Sie wird am oberen und unteren Bildschirmrand angezeigt und bleibt geöffnet, während du andere Apps verwendest.
   - Stapel: eine Funktion, die per Klick bei gedrückter ctrl-Taste deinen Schreibtisch organisiert und übersichtlich hält.
   - Schnellaktionen: Mit dieser Funktion kannst du Aktionen an einer Datei ausführen, z. B. ein Bild drehen oder Audio- oder Videoclips trimmen, ohne die Datei zu öffnen.
   - Übersicht: Diese Funktion ermöglicht, den Inhalt vieler gängiger Dateitypen anzusehen, auch wenn die entsprechenden Apps nicht installiert sind.
   - Dienstprogramm für Bildschirmfotos: Mit dieser Funktion kannst du mithilfe der Tastenkombination Umschalt-Befehl-5 ein Bildschirmfoto oder den Bildschirminhalt aufnehmen.
   - Integrationskamera: Mit dieser Funktion kannst du deine Fotos von deinem iOS Gerät auf deinen Mac importieren und scannen und dann in ein Dokument einfügen.

5. Die vier Apps, die mit macOS Mojave eingeführt wurden:
   - News
   - Aktien
   - Home
   - Sprachmemos
6. macOS Mojave Datenschutz und Sicherheit umfasst folgende Verbesserungen:
   - App-Berechtigungsanforderungen: Eine App muss die entsprechende Erlaubnis erhalten, bevor sie auf Kamera, Mikrofon oder vertrauliche Informationen wie Standortdaten, deine Nachrichten oder deine Maildatenbank zugreifen kann.
   - Intelligenter Tracking-Schutz: Er verringert die Datenmenge, die Websites über deinen Browser und dein Gerät erfassen können, und beschränkt die Tracking-Möglichkeit für Werbetreibende.
7. Siri kann HomeKit kompatible Geräte steuern, deine gespeicherten Passwörter finden und mehr Informationen über Essen, Stars und Motorsport entdecken. Siri kann auch Geräte finden, die mit deinem iCloud Account verknüpft sind, wenn „Mein iPhone suchen", „Mein iPad suchen" bzw. „Meinen Mac suchen" aktiviert ist.
8. Du kannst auch eine Einführung im Finder sehen, wenn du das Menü „Hilfe" wählst. Du hast die folgenden Optionen:
   a. Neue Funktionen in macOS?
   b. Neu beim Mac? Die Grundlagen im Überblick.
   c. Lerne dein MacBook Pro kennen

Lektion 2 – macOS aktualisieren, upgraden und erneut installieren

Ziele

- Unterschiede zwischen Update, Upgrade und Neuinstallation von macOS beschreiben
- Das macOS Installationsprogramm beschreiben
- macOS aktualisieren
- macOS upgraden
- macOS neu installieren
- Systeminformationen verifizieren
- Probleme bei Upgrade oder Neuinstallation von macOS beheben

Kontrollfragen

1. Worin unterscheiden sich Updates, Upgrades und Neuinstallationen von macOS?
2. Was solltest du vor dem Upgrade auf macOS Mojave tun?
3. Welche Systemvoraussetzungen sind für das Upgrade auf macOS Mojave erforderlich?
4. Wie überprüfst du deinen Mac auf Updates?
5. Woher weiß das macOS Installationsprogramm, welche Firmwareupdates es für den Mac laden muss?
6. Wie bekommst du das macOS Installationsprogramm?
7. Wie installierst du macOS neu?
8. Was kannst du zur Behebung von macOS Installationsproblemen tun?

Antworten

1. Unterschiede zwischen Update, Upgrade und Neuinstallation von macOS:
   - macOS Update: Installation einer neuen Unterversion des bestehenden Mac Betriebssystems, aber kein Upgrade auf die nächste eigenständige Version.
   - macOS Upgrade: Installation der nächsten eigenständigen Version.
   - Neuinstallation: Installation derselben eigenständigen macOS Version, die auf dem Volume bereits installiert war. Damit werden die vorhandenen Systemdateien überschrieben, jedoch bleiben Apps, Benutzerordner und andere Dateien unverändert.
2. Vor einem Upgrade auf macOS Mojave solltest du die folgenden Schritte ausführen:
   a. Installationsvoraussetzungen verifizieren.
   b. Notebooks an eine Stromversorgung anschließen.
   c. App-Kompatibilität überprüfen.
   d. Backup von wichtigen Inhalten erstellen.
   e. Netzwerkeinstellungen dokumentieren.
   f. Softwareupdate oder den App Store öffnen.
3. Systemvoraussetzungen für das Upgrade auf Mojave:
   - OS X Mountain Lion 10.8 oder neuer
   - 2 GB Arbeitsspeicher
   - 12,5 GB freier Speicherplatz für eine Neuinstallation (bzw. bis zu 18,5 GB freier Speicherplatz für ein Upgrade von OS X Yosemite 10.10 oder früher)

- Kompatibler Internetanbieter
- Apple ID für einige Funktionen

4. Um zu prüfen, ob Updates für deinen Mac vorliegen, öffne den App Store, klicke auf „Updates“ und dann für die gewünschten App-Updates jeweils auf „Aktualisieren“. Du kannst auch auf „Alle aktualisieren“ klicken, um alle Updates zu installieren.
5. Das Installationsprogramm erkennt anhand der Mac Modellnummer, welche spezifischen Firmwareupdates es für deinen Mac suchen und laden muss.
6. Das macOS Installationsprogramm kann kostenlos aus dem App Store geladen werden.
7. Gehe für die Neuinstallation von macOS zu „Dienstprogramme“, wähle „macOS installieren“, und fahre mit der Lizenzvereinbarung fort. Wenn du mit ihr einverstanden bist, klicke auf „Zustimmen“, wähle dein Volume oder „Alle Volumes anzeigen“ aus. Klicke dann auf dein Volume und auf „Installieren“.
8. Um Probleme bei der macOS Installation über die Menüleiste des macOS Installationsprogramms zu beheben, kannst du das Menü „Window“ öffnen und das Installationsprotokoll ansehen.

Lektion 3 – macOS einrichten und konfigurieren

Ziele

- macOS Erstkonfiguration vornehmen
- Gängige Systemeinstellungen anpassen
- Ein Konfigurationsprofil finden und installieren

Kontrollfragen

1. Welches Tool leitet den Benutzer durch die Erstkonfiguration von macOS Mojave?
2. Mit welchem Feature lässt sich die Sicherheit der Apple ID auf Mac Computern bei aktiviertem iCloud deutlich erhöhen?
3. Welche wichtigen Features erhältst du durch die Einrichtung von iCloud?
4. Wo kannst du iCloud Einstellungen verwalten, nachdem du macOS Mojave konfiguriert hast?
5. Was ist ein Konfigurationsprofil? Wie verwaltest du ein Konfigurationsprofil?
6. Wo findest du Informationen zum System sowie zur Reparatur- und Garantieabdeckung des Mac?

Antworten

1. Der Systemassistent leitet den Benutzer durch die Konfiguration von macOS Mojave.
2. Wenn iCloud aktiviert ist, lässt sich die Sicherheit der Apple ID mit der Zwei-Faktor-Authentifizierung erhöhen.
3. Wesentliche Funktionen von iCloud sind cloudbasierte Speicher- und Kommunikationsdienste für Apps wie iCloud Drive, Fotos, Kontakte, Kalender, Erinnerungen, Safari, Siri, Notizen und „Meinen Mac suchen". Der iCloud Schlüsselbund wird ebenfalls aktiviert, wenn die eingegebene Apple ID Zwei-Faktor-Authentifizierung verwendet. Gehört die eingegebene Apple ID zur Domäne @mac.com, @me.com oder @icloud.com domain, wird auch Mail konfiguriert.
4. Du kannst iCloud Einstellungen verwalten, nachdem du macOS Mojave eingerichtet hast.
5. Ein Konfigurationsprofil ist ein Dokument mit dem Dateinamensuffix „.mobileconfig", das Systemeinstellungen enthält, welche von einem Administrator definiert wurden. Beim Öffnen eines Profildokuments installiert macOS Mojave das Profil und konfiguriert die Einstellungen. Installierte Profile kannst du über die Systemeinstellung „Profile" verwalten.
6. Informationen zum System sowie zur Reparatur- und Garantieabdeckung des Mac findest du im Fenster „Über diesen Mac".

Lektion 4 – Die Befehlszeilenoberfläche nutzen

Ziele

- Beschreiben, wann die Befehlszeilenoberfläche nützlich ist
- man-Seiten verwenden, um weitere Informationen über Befehle zu finden
- Dateien über die Befehlszeilenoberfläche manipulieren

Kontrollfragen

1. Welche Vorteile hat die Befehlszeilenoberfläche?
2. Aus welchen vier Teilen besteht ein Befehl?
3. Mit welchem Terminalbefehl kannst du folgende Aufgaben erledigen?
   a. Arbeitsverzeichnis drucken
   b. Auflisten
   c. Verzeichnis ändern
   d. Übergeordnetes Verzeichnis anzeigen
   e. Benutzerordner des aktuellen Benutzers anzeigen
   f. Ordner erstellen
   g. Befehl mit Root-Accountzugriff ausführen
   h. Terminalbildschirm leeren
4. Mit welcher Taste kannst du Datei-, Pfad- und Befehlsnamen automatisch vervollständigen?

Antworten

1. Die Befehlszeilenoberfläche hat folgende Vorteile:
   - Zusätzliche Administrator- und Problembehebungsoptionen.
   - Umfassenderer Zugriff auf das Dateisystem.
   - Entfernte Anmeldung per SSH-Protokoll.
   - Jeder Administrator kann Befehle als Systemadministrator- oder root-Benutzer mit „sudo“ ausführen.
   - Fähigkeit, wiederholte Aufgaben per Scripting zu automatisieren.
   - Fähigkeit, mit Apple Remote Desktop mehrere, sogar Tausende Mac Computer gleichzeitig entfernt zu verwalten.
2. Ein Befehl besteht aus diesen vier Teilen:
   - Befehlsname
   - Befehlsoptionen
   - Argumente
   - Erweiterungen

3. Die genannten Aufgaben lassen sich mit diesen Befehlen ausführen:
   a. Arbeitsverzeichnis drucken: `pwd`
   b. Auflisten: `ls`
   c. Verzeichnis ändern: `cd`
   d. Übergeordnetes Verzeichnis anzeigen: `..`
   e. Benutzerordner des aktuellen Benutzers anzeigen: `~`
   f. Ordner erstellen: `mkdir`
   g. Befehl mit Root-Accountzugriff ausführen: `sudo`
   h. Terminalbildschirm leeren: `clear` oder Befehlstaste-L drücken
4. Datei-, Pfad- und Befehlsnamen kannst du mit der Tabulatortaste automatisch vervollständigen.

Lektion 5 – Die macOS Wiederherstellung nutzen

Ziele

- Über die macOS Wiederherstellung auf Dienstprogramme zugreifen
- macOS über die macOS Wiederherstellung neu installieren
- Ein externes macOS Wiederherstellungsvolume erstellen

Kontrollfragen

1. Wann wirst du aufgefordert, ein Firmware-Passwort einzugeben?
2. Welche Dienstprogramme sind verfügbar, wenn du über die macOS Wiederherstellung startest?
3. Welche Optionen mit zugehörigen Start-Tastenkombinationen gibt es bei der macOS Wiederherstellung?
4. Wie kannst du einen externen macOS Installationsdatenträger erstellen?

Antworten

1. Du siehst eine Eingabeaufforderung für ein Firmware-Passwort, nachdem du deinen Mac über macOS Wiederherstellung startest.

   Die Eingabeaufforderung für das Firmware-Passwort wird angezeigt, wenn du deinen Mac neu startest oder einschaltest und dann sofort Befehl-R gedrückt hältst. Du lässt die Tasten los, wenn du das Apple Logo, einen sich drehenden Globus, oder die Eingabeaufforderung für ein Firmware-Passwort siehst.

2. Die macOS Wiederherstellung bietet Zugriff auf die Wiederherstellung aus einem Time Machine Backup, die Installation/Neuinstallation von macOS Sierra, die Online-Hilfe über Safari, das Festplattendienstprogramm, das Startvolume, das Startsicherheitsdienstprogramm, das Netzwerkdienstprogramm, Terminal und die Option „Passwort zurücksetzen".
3. Je nach Start-Tastenkombination installiert die macOS Wiederherstellung unterschiedliche Versionen von macOS:
   a. Befehlstaste-R: Installiert die zuletzt auf deinem Mac installierte macOS Version, ohne ein Upgrade auf die neueste Version durchzuführen.
   b. Wahltaste-Befehlstaste-R: Installiert ein Upgrade auf das neueste mit dem Mac kompatible macOS.
   c. Umschalttaste-Wahltaste-Befehlstaste-R: Installiert das macOS, mit dem dein Mac geliefert wurde, bzw. die Version, die dem entsprechenden macOS am nächsten liegt und noch verfügbar ist.
4. Mit dem Befehlszeilenprogramm `createinstallmedia` im macOS Installationsprogramm kannst du ein macOS Wiederherstellungsvolume erstellen, das die Tools und Installationsressourcen für macOS Mojave enthält.

Lektion 6 – macOS aktualisieren

Ziele

- Einstellungen für automatisches macOS Software-Update in der Systemeinstellung „Softwareaktualisierung“ konfigurieren
- Einstellungen für automatische App Store Software-Updates in den App Store Einstellungen konfigurieren
- Apple Software automatisch aktualisieren
- Apple Software manuell aktualisieren
- Eine MDM Lösung zur Aktualisierung von macOS verwenden.

Kontrollfragen

1. Welche Apps werden bei einem Softwareupdate zu aktualisieren versucht?
2. Was brauchst du, um die Systemeinstellung „Softwareaktualisierung“ und die Einstellungen in der App Store App zu ändern?
3. Wie teilt dir macOS mit, dass im App Store ein Softwareupdate verfügbar ist?
4. Wie teilt dir macOS mit, dass eine Systemaktualisierung verfügbar ist?
5. Welche App solltest du öffnen, um Apple Softwareupdates zu initiieren?
6. Was wird bei automatischen Softwareupdates standardmäßig immer installiert?
7. Wie kannst du steuern, welche Softwareprogramme auf dem Mac automatisch aktualisiert werden?
8. Wer kann Systemupdates über den App Store installieren?
9. Wo bekommst du Apple Softwareupdates her, wenn du sie manuell installieren musst?
10. Wie lässt sich am einfachsten herausfinden, welche Software auf einem Mac installiert ist?

Antworten

1. macOS Softwareupdate versucht, folgende Software zu installieren:
   - Derzeit installierte Apple Software
   - macOS Software-Bundles
   - Im App Store gekaufte Software
2. Du brauchst einen Administrator-Account, um die Systemeinstellung „Softwareaktualisierung“ und die Einstellungen in der App Store App zu ändern.
3. Wenn Softwareupdates zur Installation verfügbar sind, zeigt macOS den Hinweis „Updates verfügbar“ mit einem App Store Symbol an. Zusätzlich wird ein rotes Badge neben dem App Store Symbol angezeigt.
4. Wenn Systemupdates verfügbar sind, zeigt macOS den Hinweis „Updates verfügbar“ mit einem Systemupdate-Symbol an. Zusätzlich wird ein rotes Badge neben dem Systemeinstellungssymbol angezeigt.
5. Softwareupdates solltest du über den App Store initiieren.
6. Systemdateien und Sicherheitsupdates werden standardmäßig automatisch installiert, sobald sie verfügbar sind.
7. Automatische Softwareupdates steuerst du über die App Store Einstellungen. Du kannst darüber hinaus die Möglichkeit eines Benutzers zur Nutzung des App Store einschränken, indem du für den betreffenden Benutzeraccount die Kindersicherung konfigurierst.

8. Benutzer mit Administrator-Accounts können Systemupdates über den App Store installieren.
9. Du kannst alle Apple Softwareupdates unter https://support.apple.com/de_DE/downloads suchen und laden.
10. In den Systeminformationen wird alle über den App Store und das Installationsprogramm installierte Software angezeigt, ob von Apple oder anderen Anbietern.

Teil 2: Benutzeraccounts

Lektion 7 – Benutzeraccounts verwalten

Ziele

- Verschiedene Arten von Benutzeraccounts und Benutzerattribute kennenlernen
- Benutzeraccounts erstellen und verwalten
- Einstellungen für Anmeldung und schnellen Benutzerwechsel anpassen

Kontrollfragen

1. Welche Arten von lokalen Benutzeraccounts gibt es in macOS Mojave? Inwiefern unterscheiden sie sich voneinander?
2. Welche anderen Arten von Benutzeraccounts kann macOS zusätzlich zu lokalen Benutzeraccounts verwenden?
3. Was sind Account-Attribute?
4. Wie kannst du den vollen Zugriff eines Benutzeraccounts auf alle Apps beschränken?
5. Was ermöglicht dir der schnelle Benutzerwechsel?

Antworten

1. In macOS gib es folgende lokale Benutzeraccounts:
   a. Administrator: Administrator-Benutzeraccounts gehören zur Admin-Gruppe.Sie haben vollen Zugriff auf alle Apps, Einstellungen und freigegebenen Ressourcenorte.
   b. Standard: Standardbenutzer können fast alle Ressourcen und Funktionen des Mac nutzen, in der Regel jedoch nichts ändern, was sich auf andere Benutzer auswirken könnte.
   c. Verwaltet mit Kindersicherung: Ein verwalteter Account ist ein Standardaccount mit aktivierter Kindersicherung.
   d. Gast: Der standardmäßige Gastbenutzer ähnelt dem Standard-Benutzer, erfordert aber kein Passwort. Wenn sich ein Gastbenutzer abmeldet, wird der Benutzerordner gelöscht – auch Objekte, die normalerweise gesichert würden, etwa Einstellungsdateien oder der Webbrowserverlauf.
   e. Nur Freigabe: Accounts dieses Typs können Dateien mit jemandem auf einem anderen Computer teilen, sich aber nicht auf deinem Mac anmelden.
   f. Systemadministrator (Root-Account): Der Systemadministrator-Account hat unbegrenzten Zugriff auf nahezu alles auf dem Mac. In macOS ist er standardmäßig deaktiviert.
   g. Gruppe: Ein Gruppenaccount ist eine Liste mit Benutzeraccounts, wodurch sich der Datei- und Ordnerzugriff besser kontrollieren lässt.
2. Neben den lokalen verwendet macOS zwei weitere Benutzeraccounts:
   a. Netzwerk-Benutzeraccounts: Verfügbar für mehrere Mac Computer und auf einem gemeinsam genutzten Verzeichnisserver gespeichert, z. B. Active Directory, damit Identifizierungs-, Authentifizierungs- und Autorisierungsdaten an einer zentralen Stelle zugreifbar sind. Der Benutzerordner eines Netzwerkaccounts wird gewöhnlich auf einem Netzwerkdateiserver gespeichert.
   b. Mobiler Benutzeraccount: Ein Netzwerkbenutzeraccount, der mit der lokalen Benutzerdatenbank synchronisiert wurde, damit du einen mobilen Benutzeraccount verwenden kannst, selbst wenn dein Mac nicht auf den gemeinsam genutzten Verzeichnisserver zugreifen kann. Der Benutzerordner eines mobilen Benutzeraccounts wird gewöhnlich auf dem Startvolume gespeichert.

3. Account-Attribute sind die einzelnen Informationseinheiten, mit denen Benutzeraccounts definiert werden. Beispiele dafür sind: Benutzer-ID, Gruppe, Accountname, vollständiger Name, Anmelde-Shell, Benutzerordner, Universally Unique ID (UUID), Apple ID und Aliasdateien.
4. Mit der Kindersicherung kannst du die Möglichkeiten der Benutzer einschränken.
5. Durch den schnellen Benutzerwechsel kann der Mac zwischen Benutzeraccounts wechseln, ohne dass der Benutzer sich abmelden oder Apps schließen muss.

Lektion 8 – Benutzerordner verwalten

Ziele

- Benutzerordner beschreiben
- Benutzeraccount löschen und Inhalte des Benutzerordners archivieren
- Benutzerordner migrieren und wiederherstellen

Kontrollfragen

1. Welche Ordner sind im Benutzerordner standardmäßig enthalten?
2. Wie aktivierst du das Feature „Stapel“, um deinen Schreibtisch zu organisieren?
3. Was ist die Standardeinstellung für den Ordner „Library“ im Finder?
4. Über welchen Ordner lässt sich eine Datei mit einem anderen öffentlichen Benutzer teilen?
5. Welche Optionen hast du beim Löschen eines lokalen Benutzeraccounts?
6. Was kannst du mit dem Migrationsassistenten tun?
7. Wie verknüpfst du in macOS einen neuen lokalen Benutzeraccount mit einem manuell migrierten oder wiederhergestellten Benutzerordner?

Antworten

1. Die Standardordner im Benutzerordner eines Benutzers sind „Schreibtisch“, „Dokumente“, „Downloads“, „Filme“, „Musik“, „Bilder“ und „Öffentlich“.
2. Zum Aktivieren von „Stapel“ klickst du in den Schreibtisch, damit der Finder die aktive App ist. Dann wählst du „Stapel verwenden“ aus dem Menü „Darstellung“. Du kannst auch bei gedrückter ctrl-Taste auf den Schreibtisch klicken und die Option „Stapel verwenden“ wählen.
3. Der Ordner „Library“ ist in der Standardansicht des Finders ausgeblendet. Der Ordner „Library“ enthält benutzerspezifische Einstellungsdateien, Schriften, Kontakte, Schlüsselbunde, Mailboxen, Favoriten, Bildschirmschoner und andere App-Ressourcen.
4. Jeder Benutzer verfügt über einen Dropbox Ordner in seinem Ordner „Öffentlich“, über den sich Dateien an andere Benutzer übertragen lassen. Andere Benutzer können in deinem Ordner „Öffentlich“ keine Dateien hinzufügen oder ändern.
5. Beim Löschen eines lokalen Benutzeraccounts hast du drei Optionen:
   a. Den Benutzerordner in einem Image sicher
   b. Den Benutzerordner unverändert lassen
   c. Den Benutzerordner löschen
6. Mit dem Migrationsassistenten kannst du Einstellungen, Benutzeraccounts und Inhalte von einem Mac oder Windows Computer bzw. aus einem Time Machine Backup auf deinen Mac übertragen.
7. Geh wie folgt vor, um einen neuen lokalen Benutzeraccount mit einem manuell migrierten oder wiederhergestellten Benutzerordner zu verknüpfen:
   a. Kopiere den wiederhergestellten Benutzerordner in den Ordner /Benutzer.
   b. Öffne die Systemeinstellungen und wähle „Benutzer und Gruppen“.
   c. Erstelle einen neuen lokalen Benutzeraccount mit demselben Accountnamen, der auch für den Benutzerordner verwendet wurde. Jetzt fordert macOS dich auf, den neuen lokalen Benutzeraccount mit dem wiederhergestellten Benutzerordner zu verknüpfen.

Lektion 9 – Sicherheit und Datenschutz verwalten

Ziele

- Arten von Passwörtern und ihre Verwendung beschreiben
- Geheime Informationen im Schlüsselbund verwalten
- Dienstprogramm für sicheres Setup verwalten
- iCloud Schlüsselbund aktivieren und verwalten
- Vom Benutzer genehmigte MDM-Registrierung erhalten
- Systemweite Sicherheit und Benutzerdatenschutz verwalten
- Laden von Kernel-Erweiterungen genehmigen

Kontrollfragen

1. Mit welchen Arten von Passwörtern kannst du einen Mac absichern?
2. Welche Objektarten kannst du in einem Schlüsselbund sichern?
3. Wie trägt die Schlüsselbundverwaltung zum Schutz deiner Daten bei?
4. Wo sind die Schlüsselbunddateien gesichert?
5. Mit welcher App kannst du die Schlüsselbundeinstellungen verwalten?
6. Inwiefern bietet die Zwei-Faktor-Authentifizierung zusätzlichen Schutz für die Apple ID?
7. Wann und warum würdest du einen iCloud Sicherheitscode verwenden?
8. Welche drei macOS Funktionen erfordern die Verwaltung von sicherheitsrelevanten Einstellungen und vom Benutzer genehmigte MDM Registrierung?
9. Auf welche drei Arten kannst du eine vom Benutzer genehmigte MDM Registrierung erhalten?
10. Welche macOS systemweiten und persönlichen Einstellungen kannst du unter „Sicherheit“ verwalten?
11. Welches Feature kannst du aktivieren, um einen verlorenen Mac Computer zu suchen?
12. Wie kannst du die Nutzung von Ortungsdiensten einschränken?
13. Wie kannst du sicherstellen, dass die mit der Diktierfunktion erstellten Tonaufnahmen vertraulich bleiben?
14. Welchen drei Kategorien gehören Kernel-Erweiterungen (KEXTs) in der Regel an?

Antworten

1. Die verschiedenen Arten von Passwörter, mit denen du einen Mac absichern kannst:
   a. Passwort des lokalen Benutzeraccounts – zur Anmeldung an deinem Mac.
   b. Apple ID und Passwort – für iCloud, iTunes und den App Store
   c. Schlüsselbundpasswörter – zum Schutz von Authentifizierungsressourcen in verschlüsselten Schlüsselbunddateien
   d. Ressourcenpasswörter – etwa für E-Mails, Websites, Dateiserver, Apps und verschlüsselte Images
   e. Firmwarepasswort – hindert den Mac daran, von anderen Volumes als deinem festgelegten Startvolume zu starten
2. In einem Schlüsselbund kannst du Ressourcenpasswörter, Zertifikate, Schlüssel, Websiteformulare, Informationen zum automatischen Ausfüllen in Safari und sichere Notizen speichern.

3. Die Schlüsselbundverwaltung verwaltet verschlüsselte Dateien, die zum sicheren Speichern deiner Daten genutzt werden. Ohne das Schlüsselbundpasswort sind sie absolut unzugänglich. Wenn du dein Schlüsselbundpasswort vergisst, sind die Dateiinhalte auf immer verloren.
4. Schlüsselbunddateien werden für verschiedene Benutzer und Ressourcen überall auf macOS gespeichert.
   a. Lokale Anmeldeschlüsselbunde werden in /Benutzer/*Benutzername*/Library/Keychain/login.keychain gespeichert.
   b. Andere lokale Schlüsselbunde werden in /Benutzer/*Benutzername*/Library/Keychains/*others*.keychain gespeichert.
   c. iCloud Schlüsselbunde werden in /Benutzer/*Benutzername*/Library/Keychains/*UUID*/.
   d. Systemschlüsselbunde werden in /Library/Keychains/System.keychain gespeichert.
   e. System-Root-Schlüsselbunde für vertrauenswürdige Netzwerke werden standardmäßig nicht angezeigt, können jedoch hier eingesehen werden: /System/Library/Keychains/
   f. Andere Schlüsselbunde sind anderswo in macOS gespeichert. Du solltest diese Dateien niemals bearbeiten, es sei denn, eine vertrauenswürdige Quelle fordert dich dazu auf, um ein Problem zu beheben.
5. Mit der Schlüsselbundverwaltung kannst du die meisten Schlüsselbundobjekte einsehen und modifizieren.
6. Mit der Zwei-Faktor-Authentifizierung können nur vertrauenswürdige Geräte wie dein iPhone, iPad oder Mac auf deinen Apple ID Account zugreifen.
7. Beim iCloud Sicherheitscode handelt es sich um eine separate Technologie, mit deren Hilfe deine Geheimnisse im iCloud Schlüsselbund noch besser geschützt sind. Er wird genutzt, wenn du iCloud Schlüsselbund mit einer Apple ID ohne Zwei-Faktor-Authentifizierung aktivierst. Wenn die Zwei-Faktor-Authentifizierung nicht aktiviert ist, fordert dich macOS auf, deinen iCloud Sicherheitscode einzugeben oder zu erstellen, damit du dem Gerät vertrauen kannst. Du kannst den iCloud Sicherheitscode auch verwenden, um anderen Geräten Zugriff auf deine Apple ID zu gewähren.
8. Die folgenden macOS Funktionen erfordern die Verwaltung von sicherheitsrelevanten Einstellungen und Anmeldung mit einer vom Benutzer genehmigten MDM Registrierung:
   - Richtlinie zum Laden von Kernel-Erweiterungen
   - Autonomer Einzel-App-Modus
   - Benutzerzustimmung für Datenzugriff
9. Drei Möglichkeiten, eine vom Benutzer genehmigte MDM-Registrierung zu erhalten:
   a. Registriere deinen Mac über Apple Business Manager oder Apple School Manager automatisch bei einer MDM Lösung. Seine Registrierung ist gleichbedeutend mit „Vom Benutzer genehmigt".
   b. Installiere macOS 10.13.4 oder neuer. Wenn ein Mac vor seiner Aktualisierung auf macOS 10.13.4 oder neuer bei einem nicht vom Benutzer genehmigten MDM registriert war, wird er auf eine vom Benutzer genehmigte Registrierung umgestellt.
   c. Befolge für die Registrierung bei MDM die Aufforderungen in den Systemeinstellungen. Lade ein Registrierungsprofil oder sende es per E-Mail an dich selbst, und doppelklicke auf das Registrierungsprofil.
10. macOS systemweite und persönliche Einstellungen, die unter „Sicherheit" verwaltet werden können:

a. Allgemeine Einstellungen: Bieten die Option, ein Passwort zum Aktivieren eines Mac nach dem Ruhemodus oder Bildschirmschoner und eine Verzögerung zu definieren, bevor diese Voraussetzung aktiv ist. Hier kannst du auch eine individuelle Meldung festlegen, die im Anmeldefenster oder bei gesperrtem Bildschirm angezeigt wird.

b. Erweiterte Einstellungen: Damit lässt sich einstellen, dass Benutzer automatisch nach einer bestimmten Dauer der Inaktivität von Accounts abgemeldet werden, und dass für systemweite Einstellungen ein Administratorpasswort erforderlich ist.

c. FileVault Einstellungen: Bietet die Option, FileVault zu aktivieren und zu konfigurieren.

d. Firewall-Einstellungen: Erlaubt, persönliche Netzwerk-Firewall-Einstellungen zu aktivieren und zu konfigurieren.

11. „Meinen Mac suchen" in iCloud ermöglicht dir entfernten Zugriff auf die Ortungsdienste eines verlorenen Mac, um ihn wiederzufinden.

12. In der Systemeinstellung „Sicherheit" kannst du im Bereich „Datenschutz" Apps den Zugriff auf Ortungsdienste, Kontakte, Kalender, Erinnerungen und soziale Netzwerkdienste gewähren oder verweigern. Wenn eine neue App Informationen anfordert, die als privat gelten, bittet macOS dich um Erlaubnis.

13. Um sicherzustellen, dass deine Tonaufnahmen vertraulich bleiben, kannst du deine Einstellungen für die erweiterte Diktierfunktion manuell festlegen. Die erweiterte Diktierfunktion ist standardmäßig aktiviert. Mit der erweiterten Diktierfunktion erstellte Tonaufnahmen werden direkt in Text umgewandelt, jedoch nicht an Apple gesendet. Wenn du die erweiterte Diktierfunktion deaktivierst oder Siri verwendest, werden Tonaufnahmen an Apple gesendet und dann in Text umgewandelt. Dazu verfolgt Apple andere Informationen wie deinen Namen, Spitznamen, Standort und viele deiner Benutzerdaten, die von deinem Gerät gesendet werden.

14. Die drei Kategorien, denen Kernel-Erweiterungen (KEXTs) in der Regel angehören:

a. Systemnahe Gerätetreiber

b. Netzwerkfilter

c. Dateisystem

Lektion 10 – Passwortänderungen verwalten

Ziele

- Bekannte Passwörter ändern
- Verlorene Benutzerpasswörter zurücksetzen
- Ein Firmwarepasswort einrichten, um den macOS Startvorgang abzusichern
- Sichere Boot- und externe Boot-Optionen für Mac Computer mit dem Apple T2 Chip verwalten

Kontrollfragen

1. Wie kannst du das Passwort deines lokalen Computeraccounts ändern?
2. Wie kannst du in macOS Mojave das Passwort eines anderen Benutzeraccounts ändern?
3. Wie wirkt es sich auf den Anmeldeschlüsselbund des Benutzers aus, wenn das Passwort für seinen Account zurückgesetzt wird?
4. Wann kannst du ein Anmeldepasswort mit einer Apple ID zurücksetzen?
5. Wie kannst du das verlorene Accountpasswort eines Benutzers zurücksetzen, der sich auf seinem Mac nicht mehr anmelden kann?
6. Wie kann das Firmware-Passwortdienstprogramm verhindern, dass Benutzer nicht autorisierte Passwortänderungen vornehmen?
7. Welche beiden zusätzlichen Features bietet das Dienstprogramm zur Startsicherheit, um unautorisierten Zugriff auf einen Mac mit Apple T2 Chip zu verhindern?

Antworten

1. Du kannst deine eigenen lokalen Accountpasswörter in der Systemeinstellung „Sicherheit“ im Bereich „Allgemein“ oder in der Systemeinstellung „Benutzer & Gruppen“ ändern. In beiden Fällen wählst du „Passwort ändern“ und gibst dann im Eingabefeld einmal dein altes Passwort und zweimal dein neues Passwort ein. Zum Abschluss wählst du „Passwort ändern“.
2. Passwörter anderer Benutzeraccounts kannst du zurücksetzen, wenn du Zugriff auf einen Administrator-Account an einem Mac hast. Zum Zurücksetzen über die Systemeinstellung „Benutzer & Gruppen“ authentifizierst du dich als Administrator, wählst den zu ändernden Benutzeraccount und klickst auf „Passwort zurücksetzen“. Anschließend gibst du das neue Passwort ein und bestätigst es.
3. Wenn dein Anmeldepasswort nicht mit dem Passwort deines Anmeldeschlüsselbunds übereinstimmt, erstellt macOS neue leere Schlüsselbundobjekte, die mit deinem Anmeldeschlüsselbund übereinstimmen. Wenn der Benutzer sein altes Passwort kennt, kannst du den archivierten Schlüsselbund abrufen.
4. Wenn du bei Erstellung deines ersten Benutzeraccounts mit dem Systemassistenten deine Apple ID angegeben hast, kannst du mit dieser dein Anmeldepasswort zurücksetzen.

   Das ist auf zwei Arten möglich:

   a. Aktiviere FileVault und verknüpfe es mit deiner Apple ID. Führe die korrekten Schritte aus und wähle „Mit Apple ID zurücksetzen“.

   b. Starte deinen Mac in der macOS Wiederherstellung neu. Führe die korrekten Schritte aus, und wähle „Passwort vergessen“.

5. Du kannst das vergessene Passwort eines Benutzers mithilfe des Assistenten „Passwort zurücksetzen“ in der macOS Wiederherstellung zusammen mit der Option zur Wahl eines lokalen Benutzers zurücksetzen.

6. Mit dem Dienstprogramm für Firmwarepasswörter kann ein Benutzer das Firmwarepasswort aktivieren und so verhindern, dass Benutzer, die es nicht kennen, von anderen Volumes als dem festgelegten Startvolume starten.
7. Das Dienstprogramm zur Startsicherheit bietet zwei zusätzliche Features, um unautorisierten Zugriff auf einen Mac mit Apple T2 Chip zu verhindern. Sie werden nachfolgend beschrieben:
   a. Sicheres Booten: Stellt sicher, dass ein Mac nur mit einer legitimen und vertrauenswürdigen Version eines Betriebssystems startet, inklusive macOS oder Microsoft Windows.
   b. Externes Booten: Ermöglicht festzulegen, ob dein Mac mit einem Apple T2 Chip von einer externen Festplatte, einem USB-Stick oder anderen externen Medien gestartet werden kann.

      Die standardmäßige und sicherste Einstellung ist „Starten von externen Medien nicht zulassen".

Teil 3: Dateisysteme

Lektion 11 – Dateisysteme und Speicher verwalten

Ziele

- Von macOS unterstützte Systeme erkennen
- Datenträger, Partitionen und Volumes verwalten
- Probleme mit Partitionen und Volumes beheben und reparieren

Kontrollfragen

1. Wie nennt man die logische Aufteilung von Speicher in Partitionen, Container und Volumes?
2. Wann solltest du Partitionen anstelle von Volumes verwenden?
3. Welches Partitionsschema verwenden Mac Computer standardmäßig?
4. Welche gängigen Volumeformate unterstützt macOS Mojave?
5. Welche Vorteile bietet APFS?
6. Mit welchen sieben Methoden kannst du ein Volume bzw. Laufwerk im Finder deaktivieren und auswerfen?
7. Mit welchen beiden in macOS Mojave integrierten Apps lassen sich Informationen zu Speichergeräten ermitteln?
8. Was macht das Feature „Erste Hilfe" des Festplattendienstprogramms?

Antworten

1. Formatieren ist der Vorgang der logischen Aufteilung von Speicher in Partitionen, Container und Volumes.
2. In den folgenden Fällen solltest du Partitionen anstelle von Volumes verwenden:
   a. Du musst mehrere Arten von Betriebssystemen installieren.
   b. Du möchtest Windows mit dem Boot Camp Assistenten installieren.
3. GUID Partitionstabelle (GPT): Dies ist das standardmäßige Partitionsschema auf Mac Computern.
4. macOS Mojave unterstützt diese gängigen Volumeformate:
   - APFS: Der Standard mit macOS Mojave
   - Mac OS Extended: Wurde mit und vor macOS High Sierra verwendet; auch bekannt als HFS Plus
   - FAT: Ein altes Volumeformat von Windows PCs
   - ExFAT: Wurde speziell für Flash Laufwerke über 32 GB entwickelt
   - NTFS: Neuere Versionen von Windows verwenden dies als Standardformat für native Volumes. macOS kann NTFS Volumes lesen, aber nicht darauf schreiben oder darüber starten.
5. APFS bietet die Vorteile, dass es die unverzügliche Ausführung gängiger Aufgaben (etwa Dateien und Verzeichnisse kopieren) ermöglicht, Daten bei Stromausfällen und Systemabstürzen schützt und Dateien durch native Verschlüsselung absichert.

6. Die sieben Methoden, mit denen du ein Volume oder einen Datenträger im Finder deaktivieren und auswerfen kannst:
   a. Das Laufwerkssymbol auf das Papierkorbsymbol ziehen
   b. In der Seitenleiste des Finders auf die kleine Auswurftaste neben dem Volume klicken, das du deaktivieren und auswerfen möchtest
   c. Den Datenträger auswählen, den du deaktivieren und auswerfen möchtest, und „Ablage" > „Auswerfen" wählen
   d. Das Volume auswählen, das du deaktivieren und auswerfen möchtest, und „Ablage" > „*Datenträgername* auswerfen" wählen
   e. Das Volume auswählen, das du deaktivieren und auswerfen möchtest, und den Tastaturkurzbefehl Befehlstaste-E drücken
   f. Das Volume auswählen, das du deaktivieren und auswerfen möchtest, und per Sekundärklick (oder Klick bei gedrückter ctrl-Taste) ein Einblendmenü aufrufen und „*Datenträgername* auswerfen" wählen
   g. Den Datenträger auswählen, den du deaktivieren und auswerfen möchtest, auf die Schaltfläche „Aktion" in der Finder Symbolleiste (sieht aus wie ein Zahnrad) klicken und dann „*Datenträgername* auswerfen" wählen
7. Informationen zu Speichergeräten können sowohl mit dem Festplattendienstprogramm als auch den Systeminformationen ermittelt werden.
8. Mit dem Feature „Erste Hilfe" des Festplattendienstprogramms kannst du das Partitionsschema und die Verzeichnisstrukturen eines Volumes überprüfen oder reparieren.

Lektion 12 – FileVault verwalten

Ziele

- Beschreiben, wie FileVault beim Datenschutz hilft
- FileVault Schutz aktivieren
- Beschreiben, wie man nach Verlust der Passwörter aller lokalen Benutzeraccounts auf einen durch FileVault geschützten Mac zugreifen kann

Kontrollfragen

1. Wie schützt FileVault Benutzerdaten?
2. Was sind die Unterschiede zwischen Systemverschlüsselung und Volumeverschlüsselung, und wie geht FileVault jeweils damit um?
3. Wie kannst du FileVault aktivieren, wenn du es bei Aufforderung im Systemassistenten nicht getan hast?
4. Auf welche zwei Arten lässt sich der VileFault Wiederherstellungsschlüssel sichern, wenn man in der Systemeinstellung „Sicherheit" FileVault aktiviert?

Antworten

1. FileVault verschlüsselt das Startvolume, um Benutzerdaten zu schützen.
2. Unterschiede zwischen Systemverschlüsselung und Volumeverschlüsselung und die jeweiligen FileVault Anforderungen:
   - Systemverschlüsselung: Verwendet in Mac Computern mit einem T2 Chip.

     Die Systemverschlüsselung erfolgt automatisch und integriert die Funktion von mehreren Controllern, die andere Mac Computer verwenden. In diesem Fall sollte FileVault zur zusätzlichen Sicherheit aktiviert werden, da andernfalls deine verschlüsselten SSDs automatisch aktiviert werden, wenn sie an deinen Mac angeschlossen werden.
   - Volumeverschlüsselung: Verwendet in Mac Computern ohne T2 Chip.

     FileVault verhindert per Volumeverschlüsselung den unbefugten Zugriff auf dein Startvolume. FileVault führt die Verschlüsselung auf Systemtreiberebene von macOS durch.
3. Du kannst FileVault jederzeit in der Systemeinstellung „Sicherheit" aktivieren.
4. Mit der FileVault Wiederherstellung kannst du verlorene FileVault Passwörter auf zwei Arten wiederherstellen:
   a. Verwende deine Apple ID, um das FileVault Volume zu entsperren und dein Passwort zurückzusetzen. Damit wird ein zufälliger FileVault Wiederherstellungsschlüssel generiert und in deinem iCloud Account auf Servern von Apple gesichert.
   b. Du kannst dir den von FileVault zufallsgenerierten Schlüssel aufschreiben. Du musst die Buchstaben und Ziffern des Schlüssels an einem sicheren Ort und nicht auf deinem verschlüsselten Startvolume aufbewahren.

Lektion 13 – Berechtigungen und Freigabe verwalten

Ziele

- Eigentums- und Zugriffsrechte einer Datei beschreiben
- In macOS standardmäßig freigegebene Ordner erkunden
- Datei- und Ordnerzugriff sicher verwalten

Kontrollfragen

1. Wie ermittelst du die Eigentums- und Zugriffsrechte einer Datei oder eines Ordners im Finder?
2. Welche Ebenen von Eigentumsrechten werden mit POSIX-Berechtigungen verwendet, um spezifische Berechtigungsregeln für jede Datei und jeden Ordner separat zu definieren?
3. Wie unterscheiden sich Zugriffssteuerungslisten (ACLs) von Standard-Dateisystemberechtigungen von UNIX?
4. Wie ermöglicht die standardmäßige Organisation des Dateisystems es mehreren Benutzern, auf sichere Weise lokale Dateien und Ordner zu teilen?
5. Was ist das Besondere an den Zugriffsrechten des Ordners „/Benutzer/Für alle Benutzer“?

Antworten

1. Die Eigentümer- und Zugriffsrechte für ein Objekt können im Informationsfenster des Finder angezeigt werden. Im Finder kannst du das Fenster „Informationen“ für jede Datei und jeden Ordner öffnen und deren Zugriffsrechte einsehen. Jede Datei und jeder Ordner verfügt über Zugriffsrechte für Eigentümer, Gruppen und alle Benutzer.
2. Die Ebenen von Eigentumsrechten, die mit POSIX-Berechtigungen verwendet werden, um spezifische Berechtigungsregeln für jede Datei und jeden Ordner separat zu definieren:
   a. Eigentümer: Standardmäßig ist der Eigentümer der Benutzer, der das Objekt erstellt oder auf den Mac kopiert hat.
   b. Gruppe: Standardmäßig werden die Gruppenrechte für ein Objekt von dem Ordner übernommen, in dem das Objekt erstellt wurde.
   c. Alle: Damit definierst du den Zugriff für alle Benutzer, die nicht Eigentümer sind und nicht der Gruppe des Objekts angehören.
3. Zugriffssteuerungslisten (ACLs) erweitern die Standard-Berechtigungsarchitektur von UNIX um größere Datei- und Ordnerzugriffskontrolle. macOS hat einen ähnlichen Stil von Zugriffsteuerungslisten (ACLs) wie in Windows-basierten NTFS und UNIX Dateisystemen übernommen.
4. Jeder Benutzerordner enthält einen Ordner „Öffentlich“, den andere Benutzer lesen können, sowie einen Dropbox Ordner, in den andere Benutzer schreiben können. Alle anderen Unterordner eines Benutzerordners (mit Ausnahme des optionalen Ordner „Websites“) weisen Standardberechtigungen auf, die anderen Benutzern keinen Zugriff gewähren. Der Ordner „Für alle Benutzer“ ist ebenfalls so konfiguriert, dass alle Benutzer Objekte teilen können.
5. Der Ordner „Für alle Benutzer“ ermöglicht, dass lokale Benutzer Dateien lesen und schreiben können. Doch nur der Benutzer, der Eigentümer eines Objekts ist, kann dieses Objekt aus dem Ordner „Für alle Benutzer“ löschen. Die Berechtigungseinstellung „Sticky-Bit“ des Ordners hindert andere Benutzer daran, Objekte zu löschen, deren Eigentümer sie nicht sind.

Teil 4: Datenverwaltung

Lektion 14 – Ausgeblendete Objekte, Kurzbefehle und Dateiarchive verwenden

Ziele

- Zu ausgeblendeten Dateien und Ordnern navigieren
- Pakete und Bundles untersuchen
- Aliasdateien und Links verwalten
- ZIP-Archive und Images erstellen und öffnen

Kontrollfragen

1. Warum sind im Finder bestimmte Ordner auf der Root-Ebene des Systemvolumes unsichtbar?
2. Mit welchen beiden Methoden lassen sich Objekte in macOS ausblenden?
3. Was ist der Unterschied zwischen einem Paket und einem Bundle?
4. Welche drei primären Linktypen verwendet macOS im Dateisystem?
5. Wie unterscheidet sich eine Aliasdatei von einem symbolischen Link?
6. Wann sollte man eine Archivdatei statt eines Image verwenden? Wann sollte man ein Image statt einer Archivdatei verwenden?
7. Welche Art von Datei erstellt der Finder, wenn du die Option „Archivieren" wählst?
8. Welche Aktion führt macOS Mojave standardmäßig aus, um ZIP-Archivdateien zu entpacken?

Antworten

1. Der Finder verbirgt bestimmte Ordner (die Ressourcenobjekte für macOS Prozesse enthalten) vor den normalen Benutzern im Root-Verzeichnis des Systemvolumes, da die meisten Benutzer keinen Zugriff auf diese Objekte benötigen. Solltest du Zugriff auf diese ausgeblendeten Dateien und Ordner benötigen, kannst du das Terminal verwenden.
2. Mit diesen beiden Methoden lassen sich Objekte in macOS ausblenden:
   a. Mithilfe von Terminal einen Punkt an den Beginn des Dateinamens setzen
   b. Das Dateiattribut „Ausgeblendet" aktivieren (Das Dateiattribut „Ausgeblendet" verbirgt die Objekte nur im Finder.)
3. Der Unterschied zwischen einem Paket und einem Bundle:
   - Paket: Jeder Ordner, den der Finder dem Benutzer so anzeigt, als würde es sich um eine einzelne Datei handeln.
   - Bundle: Ein Ordner mit einer standardisierten hierarchischen Architektur, der ausführbaren Code und die von diesem verwendeten Ressourcen enthält.
4. macOS verwendet drei primären Linktypen im Dateisystem:
   a. Aliasse
   b. Symbolische Links
   c. Hard-Links

5. Sowohl Aliasdateien als auch symbolische Links fungieren als Verknüpfung zu einem ursprünglichen Objekt. Eine Aliasdatei enthält allerdings noch weitere Informationen, anhand derer das System das ursprüngliche Objekt verfolgen kann, wenn dieses umbenannt oder innerhalb desselben Volumes verschoben wird. Du kannst eine Aliasdatei im Finder erstellen, aber Terminal erkennt diese nicht. Dagegen machen jegliche Änderungen am ursprünglichen Objekt den zugehörigen symbolischen Link unbrauchbar. Du kannst symbolische Links nur in Terminal erstellen, aber der Finder folgt symbolischen Links zu einem Originalobjekt.
6. Wann du ein ZIP-Archiv anstelle eines Disk-Image bzw. ein Disk-Image anstelle eines ZIP-Archivs verwenden solltest:
   - Für geringe Datenmengen solltest du Dateien und Ordner in ZIP-Archive komprimieren.
   - Für größere Datenmengen oder das vollständige Dateisystem solltest du ein Disk-Image anlegen.

   Zudem können Archivdateien viel einfacher im Finder erstellt werden und sind mit Betriebssystemen anderer Anbieter kompatibel. Images sind schwieriger zu erstellen und zu verwalten, bieten jedoch mehr Flexibilität, vor allem weil sie sich mühelos modifizieren und konvertieren lassen. Bedenke, dass nur Mac Computer auf macOS Mojave Disk-Images zugreifen können. Andere Systeme benötigen Software von Drittanbietern, um auf Mac Disk-Images zuzugreifen.
7. Der Finder erstellt eine komprimierte ZIP-Archivdatei, wenn du die Option „Archivieren“ wählst.
8. Standardmäßig wird in macOS Mojave durch Doppelklicken auf eine ZIP-Archivdatei das System angewiesen, den Inhalt des ZIP-Archivs zu entpacken.

Lektion 15 – Systemressourcen verwalten

Ziele

- Das macOS Dateilayout kennenlernen und verstehen
- Übliche Systemdateien, ihren Speicherort und ihren Zweck erkennen
- Systemintegritätsschutz beschreiben
- Schriftressourcen verwalten

Kontrollfragen

1. Was sind die vier obersten Standardordner, die im Finder angezeigt werden?
2. Nenne sechs häufig genutzte Systemressourcen. Welchen Zweck haben die verschiedenen Ressourcen?
3. Wie heißen die vier Systemressourcen-Domains? Welchen Zweck haben die verschiedenen Domains?
4. Welchen Zweck hat der Ordner ~/Library/Containers? Welche Objekte befinden sich in diesem Ordner?
5. Wie hilft der Systemintegritätsschutz bei der Absicherung der macOS Mojave Systemressourcen?
6. Mit welcher App solltest du eine Schrift aktivieren, deaktivieren, validieren oder der lokalen Schriftbibliothek hinzufügen?
7. Wie lassen sich doppelte Schriften identifizieren?

Antworten

1. Die vier obersten Standardordner, die im Finder angezeigt werden, sind:
   a. „Programme“: Enthält Apps, auf die lokale Benutzer Zugriff haben
   b. „Library“: Enthält Systemressourcen, auf die lokale Benutzer Zugriff haben
   c. „System“: Enthält Systemressourcen
   d. „Benutzer“: Enthält lokale Benutzerordner
2. Die sechs häufig genutzten Systemressourcen und ihr jeweiliger Zweck:
   a. Erweiterungen: Binden sich an den Betriebssystem-Kernel an und bieten Unterstützung für Hardware- und Peripheriegerätetreiber
   b. Frameworks: Gemeinsame Code-Bibliotheken, die zusätzliche Softwareressourcen für Apps und Systemprozesse bereitstellen
   c. Schriften: Dateien, die Schriftarten für die Anzeige am Bildschirm und die Druckausgabe beschreiben. Das Schriftmanagement wird später in dieser Lektion behandelt.
   d. Einstellungsdateien: Enthalten App- und Systemkonfigurationsinformationen
   e. LaunchAgents und LaunchDaemons: Werden von `launchd` genutzt, um Dienste bereitzustellen, die bei Bedarf automatisch beim Systemstart oder bei der Benutzeranmeldung gestartet werden
   f. Protokolle: Textdateien, die Fehler- und Fortschrittseinträge aus fast jeder App bzw. jedem Systemdienst enthalten
3. Die vier Systemressourcen-Domains und ihr jeweiliger Zweck:
   a. Benutzer: Enthält Apps und Systemressourcen, die für den jeweiligen Benutzeraccount spezifisch sind
   b. Lokal: Enthält Apps und Systemressourcen, die allen Benutzern auf einem lokalen Mac zur Verfügung stehen
   c. Netzwerk (optional): Enthält Apps und Systemressourcen, die allen Mac Computern mit automatisierter Netzwerkfreigabe zur Verfügung stehen

d. System: Enthält Apps und Systemressourcen für die grundlegende Systemfunktionalität

4. Der Ordner ~/Library/Containers enthält Ressourcen für Apps, die in einer Sandbox laufen. macOS Mojave erstellt und pflegt einen separaten Container-Ordner für jede in einer Sandbox laufende App, die der Benutzer öffnen kann. Eine in einer Sandbox laufende App ist sicherer, da sie nur auf Objekte zugreifen kann, die sich im zugehörigen Container befinden. Nur Objekte, die zur Freigabe bestimmt sind, befinden sich in einem Gruppencontainer-Ordner.
5. Der Systemintegritätsschutz hindert Benutzer und Prozesse mit Administrator- oder Root-Zugriff daran, zentrale macOS Mojave Objekte zu modifizieren. Zu diesen geschützten Objekten zählen die Ordner /System, /bin, /sbin und /usr sowie zentrale macOS Mojave Apps.
6. Du kannst mithilfe von „Schriftsammlung" eine Schrift aktivieren, deaktivieren, validieren oder der lokalen Schriftbibliothek hinzufügen.
7. Die App „Schriftsammlung" zeigt einen kleinen Punkt neben dem Namen von Schriften, die doppelte Ressourcen aufweisen.

Lektion 16 – Metadaten, Spotlight und Siri verwenden

Ziele

- Beschreiben, wie macOS Metadaten speichert und verwendet
- Dateien mit Metadaten organisieren, etwa Tags und Kommentare
- Mit Spotlight und Siri nach lokalen und Internetressourcen suchen

Kontrollfragen

1. Was sind Dateisystem-Metadaten? Nenne einige Beispiele.
2. Was sind einige Dateiattribute, die macOS Mojave häufig verwendet?
3. Was sind Dateisystemattribute? Wo findet man Attribute in der Benutzeroberfläche?
4. Wie nutzt die Spotlight Suche Metadaten?
5. Wo sichert Spotlight seine Metadaten-Indexdatenbanken und Plug-Ins?
6. Nenne einige Datenschutz- und Sicherheitsbedenken zu Spotlight.
7. Wie solltest du vorgehen, wenn eine Spotlight Suche nicht die richtigen Objekte findet?
8. Wie kannst du sichergehen, dass Siri Audioaufnahmen nicht an Apple sendet?

Antworten

1. Metadaten sind Informationen, die außerhalb einer Datei bzw. eines Ordners gesichert werden. Sie liefern zusätzliche Informationen über Dateien und Ordner. Beispiele sind Dateiattribute, erweiterte Dateiattribute und Zugriffsrechte.
2. Gängige Dateiattribute sind das Attribut „Geschützt" (es schützt die Datei vor Änderungen) sowie das Attribut „Unsichtbar" (es versteckt das Objekt im Finder).
3. Dateisystemattribute sind Metadaten, mit denen du Objekten schnell Schlagwörter bzw. „Tags" zuweisen kannst. Ein Benutzer kann die Tag-Bezeichnungen und -Farben anpassen sowie mehrere Tags für eine einzelne Datei anlegen.
4. Die Spotlight Suche erstellt Indexdatenbanken von Dateisystem-Metadaten, sodass für gewöhnlich zeitintensive Suchvorgänge enorm schnell durchgeführt werden können. Dateisystemattribute befinden sich in der Seitenleiste des Finder, in der Spotlight Suche und in allen Dialogen zum Öffnen oder Sichern von Dokumenten.
5. Metadaten-Indexdatenbanken von Spotlight werden in der Root-Ebene jedes Volumes im Ordner /.Spotlight-V100 gesichert. Allerdings wird die Datenbank eines mit dem bisherigen FileVault gesicherten Benutzers in dessen verschlüsseltem Benutzerordner gesichert. Die Mail App wiederum nutzt eine eigene Datenbank im Benutzerordner jedes Benutzers unter ~/Library/Mail/V2/MailData/Envelope Index. Spotlight Plug-Ins können sich in jedem der Library Ordner in einem Ordner namens „Spotlight" befinden.
6. Obwohl Spotlight Datei- und Ordnerzugriffsrechte indiziert, können andere Benutzer den Inhalt lokal angeschlossener Volumes durchsuchen, wenn der Eigentümer dieser Volumes ignoriert wird. Dies gilt allerdings nur für Volumes, bei denen es sich nicht um Systemvolumes handelt.
7. Bei Problemen mit der lokalen Dateisuche kannst du Spotlight dazu zwingen, die Indexdatenbanken neu zu erstellen, indem du sie löschst und den Mac neu startest oder die Spotlight Einstellungen nutzt.
8. Um Siri daran zu hindern, Audioaufnahmen an Apple zu senden, deaktivierst du Siri einfach in den Siri-Einstellungen.

Lektion 17 – Time Machine verwalten

Ziele

- Time Machine beschreiben
- Time Machine für Datenbackups konfigurieren
- Daten oder macOS aus einem Time Machine Backup wiederherstellen

Kontrollfragen

1. Was kannst du mit Time Machine alles sichern?
2. Wie pflegt Time Machine den Backup-Verlauf des Dateisystems?
3. Welche Dateitypen werden bei Time Machine Backups immer ausgelassen?
4. Warum ist Time Machine kein effizientes Mittel für die Sicherung großer Datenbanken?
5. Was geschieht, wenn du versuchst, ein APFS Volume als Time Machine Backup zu wählen?
6. Welches Feature hilft Time Machine, Daten wiederherzustellen, wenn dein Time Machine Backup-Volume nicht verfügbar ist?
7. Mit welchen vier Methoden können Daten aus einem Time Machine Backup wiederhergestellt werden?

Antworten

1. Mit Time Machine kannst du den gesamten Mac sichern, darunter Systemdateien, Apps, Musik, Fotos, E-Mails und Dokumente.
2. Um Platz zu sparen, ignoriert Time Machine alle Dateien, die nicht gesichert werden müssen, weil sie nach einer Wiederherstellung neu erstellt werden können. Im Allgemeinen ignoriert Time Machine temporäre Dateien, Spotlight Indizes, Objekte im Papierkorb und alle Daten, die als Cache interpretiert werden können. Softwareentwickler können Time Machine auch anweisen, spezifische App-Daten zu ignorieren, die nicht gesichert werden müssen.
3. Time Machine ist kein effizientes Mittel für die Sicherung großer Datenbanken, da es bei jeder noch so geringen Änderung an der Datenbank eine Sicherungskopie der gesamten Datenbank anlegt.
4. Wenn du ein Backup-Volume wählst, das als APFS, FAT32 oder ein anderes Dateisystem außer HFS Plus formatiert ist, bietet Time Machine an, das Volume im unterstützten Format von HFS Plus zu formatieren.
5. Ein zuvor gesichertes Objekt ist dann nicht verfügbar, wenn das Backup-Volume voll wurde und Time Machine bereits ältere Objekte löschen musste, um Platz für neuere Objekte zu schaffen.
6. Time Machine erstellt lokale Schnappschüsse auf deinem integrierten Startvolume, auf die es zurückgreifen kann, wenn dein Backup-Volume nicht verfügbar ist.
7. Es gibt folgende Methoden zum Wiederherstellen aus einem Time Machine Backup:
   - Bestimmte Objekte aus einem Time Machine Backup wiederherstellen
   - Wiederherstellung mit Migrationsassistent
   - Wiederherstellung des gesamten Systems mit der macOS Wiederherstellung
   - Manuelle Wiederherstellung mit dem Finder

Teil 5: Apps und Prozesse

Lektion 18 – Apps installieren

Ziele

- Apps aus dem App Store installieren
- App-Support beschreiben und Sicherheitsprobleme erkennen
- Apps mithilfe von Softwarepaketen und Drag&Drop installieren

Kontrollfragen

1. Wie kannst du auf einem Mac gekaufte Apps auf einem anderen Mac installieren?
2. Welche Programme ermöglichen Unternehmen und Bildungseinrichtungen den Erwerb mehrerer Lizenzen für App Store Objekte?
3. Wie viele Apple IDs dürfen in einer Familienfreigabegruppe sein?
4. Wo kannst du den Zugriff auf den App Store kontrollieren und erlaubte Apps für Kinder verwalten?
5. Aus welchen beiden Quellen erlaubt macOS das Öffnen von Apps?
6. Mit welchen Sicherheitstechnologien schützt der Mac den Benutzer, wenn er Apps anderer Anbieter installiert?
7. Wie installierst du Apps, die es im App Store nicht gibt?
8. Nenne drei Möglichkeiten, um Apps zu deinstallieren.

Antworten

1. Wenn du mehr als einen Mac hast, kannst du automatische Downloads gekaufter Apps auf deinem anderen Mac aktivieren.
2. Über die Programme Apple Business Manager und Apple School Manager können Unternehmen und Bildungseinrichtungen mehrere Lizenzen für App Store Objekte erwerben.
3. Eine Familienfreigabegruppe darf bis zu sechs Mitglieder umfassen.
4. Mithilfe der Kindersicherung kannst du den Zugriff deiner Kinder auf Apps steuern. Im Tab „Apps“ kannst du verwalten, auf welche Apps deine Kinder zugreifen können, und verhindern, dass sie auf den App Store zugreifen. Im Tab „Stores“ kannst du die App Store Einkäufe und verfügbare Objekte abhängig vom Alter beschränken.
5. macOS ermöglicht dir, Apps aus dem App Store und von vertrauenswürdigen Entwicklern zu öffnen. Allerdings kannst du diesen Schutz umgehen.
6. Mit diesen Sicherheitstechnologien schützt der Mac den Benutzer, wenn er Apps anderer Anbieter installiert:
   - Prozesssicherheit: Darunter fallen Sicherheitsmechanismen wie SIP, die Zugriff auf Ressourcen nur bei ausdrücklicher Erlaubnis gewähren. Systemweite Zugriffsrechte werden nur bei Bedarf gewährt.
   - App-Sandboxing: Apps dürfen nur auf Objekte zugreifen, die sie unbedingt brauchen.
   - Codesignierung: Dadurch erkennt das System die Authentizität und Integrität von Software.
   - Dateiquarantäne: Beim Versuch, ein aus externen Quellen als dem Internet geladenes Objekt zu öffnen, wird eine Warnung angezeigt.
   - Malware-Erkennung: macOS führt eine Liste mit bekannter Schadsoftware, die bei jedem macOS Softwareupdate automatisch aktualisiert wird.

- Beurkundung: Gibt an, dass Apple eine Sicherheitsprüfung der Software durchgeführt hat und keine Schadsoftware gefunden wurde.

7. Abseits vom App Store kannst du Software per Drag&Drop Installation oder Installationspaket installieren.
8. Apps lassen sich auf drei Arten deinstallieren:
   a. Die App per Launchpad deinstallieren
   b. Die App in den Papierkorb ziehen
   c. Ein angepasstes Deinstallationspaket verwenden

Lektion 19 – Dokumente verwalten

Ziele

- Dokumente mit Launch Services und Übersicht öffnen
- Mit Apps arbeiten, die „Automatisch sichern" und „Versionen" unterstützen
- Dokumente in iCloud sichern und öffnen
- Lokalen Speicher optimieren, um auf dem Systemvolume Platz zu schaffen

Kontrollfragen

1. Woran erkennt macOS, welche App beim Doppelklicken auf ein Dokument geöffnet werden soll?
2. Wie aktiviert man die Übersicht? Welche Apps unterstützen die Übersicht?
3. Welche Technologie befähigt die Übersicht, eine Vorschau so vieler Dateitypen anzuzeigen?
4. Welche integrierten Schnellaktionen sind im Finder verfügbar?
5. Was ist „Automatisch sichern"? Wie erkennt man eine App, die „Automatisch sichern" unterstützt?
6. Wie weit reicht der Versionsverlauf einer Datei zurück, wenn diese per E-Mail versendet wird?
7. Welche Apps können das Sperren von Dokumenten verwalten?
8. Wo kannst du Optionen für „Automatisch sichern" und „Fortsetzen" einstellen? Wie kannst du „Automatisch sichern" deaktivieren?
9. Was geschieht beim Upgrade auf iCloud Drive mit deinem Benutzerordner?
10. Wenn du „iCloud Schreibtisch und Dokumente" auf einem Mac aktiviert hast und dann auf einem anderen Mac aktivierst, was passiert mit den Ordnern „Schreibtisch" und „Dokumente" des Benutzers?
11. Was passiert mit den Ordnern „Schreibtisch" und „Dokumente" des Benutzers, wenn du „iCloud Schreibtisch und Dokumente" deaktivierst?
12. Welche vier Empfehlungen gibt die Speicherverwaltung für die Optimierung des Speichers?

Antworten

1. macOS Mojave bestimmt den Dokumenttyp anhand der Dateinamensuffixe von Dokumenten. Der Prozess „Launch Services" führt eine Datenbank der installierten Apps und der Dokumenttypen, die diese Apps öffnen können.
2. Die Übersicht aktivierst du durch Drücken der Leertaste, wenn ein Dokument ausgewählt ist. Die Apps „Finder", „Time Machine", „Mail" sowie die meisten Browser-Dialogfenster zum Öffnen und Sichern unterstützen die Übersicht.
3. Die Übersicht nutzt Plug-Ins, um Vorschauen von Dokumenten anzuzeigen. Diese Plug-Ins befinden sich in „QuickLook" Ordnern in den verschiedenen Library Ordnern in macOS Mojave.
4. Die Liste der verfügbaren Schnellaktionen hängt von der Art der Datei bzw. Dateien ab, die du ausgewählt hast. „Schnellaktionen" umfasst die folgenden integrierten Aktionen:
   a. Ein Bild oder einen Film drehen: „Nach links drehen" ist der Standardbefehl, aber du kannst die Wahltaste gedrückt halten, um ihn in „Nach rechts drehen" zu ändern.
   b. Ein Dokument oder Bild markieren: Nachdem du „Markierung" gewählt hast, wird die Datei in einem Markierungsfenster geöffnet. Mehr über das Markierungsfenster erfährst du im nächsten Abschnitt.
   c. Einen Film oder eine Audiodatei kürzen: Wähle „Kürzen", und verwende dann die gelben Aktivpunkte in der Trimmleiste. Klicke auf „Wiedergabe", um deine Änderungen zu testen. Klicke dann auf „Letzte Version" oder auf „Fertig", um deine Änderungen zu sichern und das Fenster zu schließen. Nach dem

Klick auf „Fertig“ fordert macOS dich auf, deine Originaldatei zu ersetzen, abzubrechen oder deine Änderungen in einem neuen Clip zu sichern.

d. Anpassen: Wähle „Anpassen“, um die Erweiterungseinstellungen in den Systemeinstellungen zu öffnen.

5. Mit „Automatisch sichern“ können kompatible macOS Mojave Apps Änderungen an Dokumenten von Benutzern automatisch sichern. Ein Benutzer speichert ein Dokument nur einmal. Danach braucht er sich nie mehr Gedanken über das Sichern von Änderungen zu machen. Das Menü „Ablage“ von Apps, die das Feature „Automatisch sichern“ unterstützen, enthält die Befehle „Duplizieren“, „Umbenennen“ oder „Bewegen in“.
6. Bei per E-Mail versendeten oder auf andere Weise an einen gemeinsamen Speicherort kopierten Dokumenten wird kein Versionsverlauf gesichert.
7. Jede App, die „Automatisch sichern“ unterstützt, sowie der Finder können das Sperren von Dokumenten steuern.
8. Du kannst „Beim nächsten Anmelden alle Fenster wieder öffnen“ im Dialogfenster zur Bestätigung der Abmeldung deaktivieren. In der Systemeinstellung „Allgemein“ kannst du Folgendes machen:
   - „Fenster beim Beenden eines Programms schließen“ deaktivieren
   - „Fragen, ob Änderungen beim Schließen von Dokumenten beibehalten werden sollen“ auswählen und so das Feature „Automatisch sichern“ deaktivieren
9. Nach dem Upgrade des iCloud Accounts auf iCloud Drive kannst du auf Dokumente aus OS X Yosemite 10.10 oder älter bzw. iOS 8 oder älter nicht mehr zugreifen. Wenn du OS X Yosemite 10.10 oder älter verwendest, kannst du weiterhin über die iCloud Website auf Cloud Drive Objekte zugreifen: www.icloud.com.
10. Wenn du „iCloud Schreibtisch und Dokumente“ auf weiteren Mac Computern aktivierst, werden die „Schreibtisch“- und „Dokumente“-Inhalte dieser Mac Computer in Unterordner der iCloud Schreibtisch- und Dokumentenordner verschoben. Wenn du z. B. den Mac „MeinMac“ hinzufügst, werden in den Ordnern „Schreibtisch“ und „Dokumente“ die Unterordner „MeinMac – Schreibtisch“ und „MeinMac – Dokumente“ erstellt.
11. Wenn du „iCloud Schreibtisch und Dokumente“ deaktivierst, werden die darin enthaltenen Objekte in einen Unterordner in iCloud Drive verschoben. Außerdem werden die lokalen Ordner „Schreibtisch“ und „Dokumente“ als neue leere Ordner für den lokalen Benutzer erstellt. Anschließend muss der Benutzer seine Dateien manuell aus iCloud Drive in die neuen (leeren) Ordner „Schreibtisch“ und „Dokumente“ kopieren.
12. Empfehlungen zur Speicheroptimierung:
    - In iCloud speichern: Alle Dateien, Fotos und Nachrichten werden in iCloud gespeichert, und nur neuere Dateien und optimierte Fotos verbleiben im lokalen Speicher.
    - Speicher optimieren: Das Entfernen von bereits gesehenen Filmen und Fernsehsendungen in iTunes wird aktiviert.
    - Papierkorb automatisch löschen: Objekte, die länger als 30 Tage im Papierkorb sind, werden automatisch entfernt.
    - Chaos reduzieren: Sieh Dokumente und andere Inhalte durch, die auf deinem Mac gespeichert sind, und lösche die nicht mehr benötigten.

Lektion 20 – Apps verwalten und Probleme behebeben

Ziele

- App-Typen beschreiben und unterstützen
- App-Erweiterungen und Widgets in der Mitteilungszentrale verwalten
- Prozesse und Apps überwachen und steuern
- Problembehebungstechniken für Apps kennenlernen

Kontrollfragen

1. Weshalb sollte man eine App im 32-Bit Modus öffnen?
2. Welche Funktionen fügen App-Erweiterungen in macOS Mojave hinzu?
3. Wie installiert man neue App-Erweiterungen? Wie kann man die Sichtbarkeit der App-Erweiterungen verwalten, nachdem diese installiert wurden?
4. Wie kannst du feststellen, welche Apps auf dem Mac installiert sind?
5. Mit welcher App kannst du in macOS Mojave geöffnete Apps überwachen?
6. Welche Schritte sollten zur Fehlersuche bei App-Problemen durchgeführt werden?
7. Mit welchen drei Möglichkeiten kannst du eine App sofort über die Benutzeroberfläche beenden?
8. Welche Aufgabe hat das Feature zum Erstellen von Diagnoseberichten?
9. Welches Dateiformat wird häufig für Einstellungsdateien verwendet? Wie kann man den Inhalt von Dateien dieser Art anzeigen?
10. Wo sind die Einstellungen von Apps gesichert?

Antworten

1. Mit dem Informationsfenster des Finders kann man erzwingen, dass ein Programm im 32-Bit Modus geöffnet wird. Dieser Schritt ist notwendig, damit 64-Bit Apps ältere 32-Bit Plug-Ins bzw. App-Ressourcen unterstützen.
2. Mit App-Erweiterungen können Apps verschiedener Entwickler miteinander interagieren, als wären sie in die App integriert.
3. App-Erweiterungen werden automatisch installiert, da sie in der App integriert sind, die die Erweiterung bereitstellt. Du kannst installierte App-Erweiterungen in den Erweiterungseinstellungen aktivieren oder deaktivieren.
4. Mit den Systeminformationen kannst du problemlos alle App-Speicherorte scannen und eine Liste der installierten Apps ausgeben.
5. Mit der Aktivitätsanzeige kannst du geöffnete Prozesse und Apps überwachen.
6. Gängige Problembehebungstechniken für Apps:
   a. Die App neu starten
   b. Ein anderes Dokument öffnen, das bekanntermaßen korrekt funktioniert
   c. Eine andere App ausprobieren
   d. Einen anderen Benutzeraccount ausprobieren
   e. Diagnoseberichte und Protokolldateien überprüfen
   f. Cache-Dateien löschen
   g. Einstellungsdateien ersetzen
   h. App-Ressourcen ersetzen

7. Die drei Möglichkeiten zum sofortigen Beenden einer App über die Benutzeroberfläche:
   a. Über das Dialogfeld „Sofort beenden“
   b. Aus dem Dock
   c. Über die Aktivitätsanzeige
8. Das Feature zum Erstellen von Diagnoseberichten erstellt immer dann automatisch ein Diagnoseberichtsprotokoll, wenn eine App abstürzt oder hängt. Du kannst den Diagnosebericht auch später mit der App „Konsole“ (in /Programme/Dienstprogramme/) ansehen. Er wird über das Internet an Apple gesendet.
9. Die meisten App-Einstellungen sind Eigenschaftslisten, also Dateien im XML-Format, welche das Dateinamensuffix „.plist“ aufweisen. Du kannst den Inhalt dieser Dateien in der Übersicht anzeigen und sie mit von Xcode bearbeiten, das du im App Store bekommst.
10. App-Einstellungen werden fast immer im Library Ordner eines Benutzers im Ordner ~/Library/Preferences gesichert. Neuere Apps, die in einer Sandbox laufen, müssen ihre Einstellungen im Ordner ~/Library/Containers/*Paket-ID*/Data/Library/Preferences sichern, wobei Paket-ID die eindeutige Paketkennung der App ist.

Teil 6: Netzwerkkonfiguration

Lektion 21 – Grundlegende Netzwerkeinstellungen verwalten

Ziele

- TCP/IP-Netzwerkkonzepte beschreiben
- Netzwerkeinstellungen konfigurieren und überwachen
- Mit einem WLAN Netzwerk verbinden

Kontrollfragen

1. Was ist eine MAC Adresse?
2. Wie sind IPv4-Adressen aufgebaut?
3. Was ist der Zweck von IPv4-Adressen (Internet Protocol v4) und Teilnetzmasken?
4. Welches Standardprotokoll verwendet macOS zum Abrufen einer IP-Adresse?
5. Wie überträgt IP Nachrichten zwischen verschiedenen Computern über ein WAN (Wide Area Network)?
6. Wie wird das Domain Name System (DNS) verwendet, um Netzwerknamen bereitzustellen?
7. Was wird verwendet, um ein WLAN Netzwerk zu identifizieren?
8. Welche WLAN Authentifizierungsprotokolle werden von macOS Mojave unterstützt?
9. Wie kann sich macOS Mojave automatisch mit einem WLAN Netzwerk verbinden?

Antworten

1. Über die MAC Adresse (Media Access Control) wird eine physische Netzwerkschnittstelle in einem lokalen Netzwerk identifiziert.
2. Die gängigsten IP-Adressen und Teilnetzmasken weisen dasselbe IPv4-Format auf. Eine IPv4-Adresse ist eine 32-Bit Zahl, die in vier Gruppen dreistelliger Zahlen von jeweils 8 Bit unterteilt ist. Diese sind durch Punkte voneinander getrennt. Jede 8-Bit Gruppe hat einen Wert zwischen 0 und 255.
3. Die IP-Adresse identifiziert den Standort eines bestimmten Netzwerkgeräts. IP-Adressen sind die primäre Identifizierung, die von der Internetprotokollfamilie TCP/IP sowohl für LANs als auch für WANs genutzt wird. Teilnetzmasken werden von Netzwerkgeräten dazu verwendet, den lokalen Netzwerkbereich zu identifizieren und zu bestimmen, ob ausgehende Daten für ein Netzwerkgerät im LAN bestimmt sind.
4. Mojave nutzt DHCP (Dynamic Host Configuration Protocol), um automatisch eine vorläufige TCP/IP-Konfiguration zu beziehen und IPv4-Adressierung zuzuweisen.
5. Ein Netzwerkclient verwendet die Teilnetzmaske, um festzustellen, ob sich die Ziel-IP-Adresse im LAN befindet. Wenn sich die Ziel-IP-Adresse nicht im LAN befindet, wird davon ausgegangen, dass sich die Zieladresse in einem anderen Netzwerk befindet. Der Client sendet die Daten dann an die IP-Adresse des lokalen Netzwerk-Routers. Der Netzwerk-Router sendet die Daten dann über eine WAN Verbindung zu einem anderen Router, den er näher am Ziel vermutet. Dies setzt sich über WAN Verbindungen von Router zu Router solange fort, bis die Daten ihr Ziel erreicht haben.
6. Über das DNS wird ein DNS-Name in die zugehörigen IP-Adressen aufgelöst.
7. Eine SSID (Service Set Identifier) wird dazu verwendet, einen WLAN Netzwerknamen und die zugehörige Konfiguration zu identifizieren.

8. macOS Mojave unterstützt verschlüsselte WLAN Netzwerke über die folgenden Authentifizierungsprotokolle: WEP, WPA/WPA2 Personal und WPA/WPA2 Enterprise (letzteres bietet Unterstützung für die 802.1X Authentifizierung).
9. Ein neuer Mac kann nur dann automatisch eine Verbindung zu WLAN Netzwerken herstellen, wenn diese über keinen standardmäßigen Authentifizierungsmechanismus verfügen, also mit sogenannten „offenen Netzwerken“. Allerdings kann ein konfigurierter Mac Verbindungen zu verschlüsselten WLAN Netzwerken automatisch wiederherstellen, wenn die entsprechenden Informationen im Schlüsselbundsystem gesichert wurden.

Lektion 22 – Erweiterte Netzwerkeinstellungen verwalten

Ziele

- macOS Netzwerkkonfigurationsarchitektur beschreiben
- Mehrere Netzwerkstandorte und Dienstschnittstellen verwalten
- Erweiterte Netzwerkeinstellungen konfigurieren

Kontrollfragen

1. Was ist eine Netzwerkumgebung? Wer kann auf Netzwerkumgebungen zugreifen?
2. Welche Schnittstellen und Protokolle werden standardmäßig von macOS Mojave unterstützt?
3. Wie wirkt sich die Priorität der Netzwerkdienste auf die Netzwerkkonnektivität aus?
4. Wie kannst du mithilfe der Systemeinstellung „Netzwerk" feststellen, welche Schnittstelle derzeit für Netzwerkaktivitäten genutzt wird?
5. Wie lassen sich VPN-Einstellungen in macOS Mojave am einfachsten konfigurieren?
6. Wie wird 802.1X auf Mac Computern konfiguriert?

Antworten

1. Eine Netzwerkumgebung ist ein gespeicherter Zustand der Systemeinstellung „Netzwerk", der alle Netzwerkschnittstelleneinstellungen enthält. Nur Administratoren können Netzwerkumgebungen definieren; wenn jedoch mehrere Umgebungen vorhanden sind, können alle Benutzer im Apple Menü zwischen den verschiedenen Netzwerkumgebungen wechseln.
2. macOS Mojave unterstützt die folgenden Netzwerkschnittstellen und -protokolle:
   - Ethernet IEEE 802.3 – Gruppe von Hardware-Netzwerkschnittstellenstandards
   - Wireless (Wi-Fi) IEEE 802.11 – Gruppe von Hardware-Netzwerkschnittstellenstandards
   - FireWire IEEE 1394 – Bridged Network Interface
   - Thunderbolt – Bridged Network Interface
   - Bluetooth – Drahtlose Hardware-Netzwerkschnittstelle
   - Mobilfunknetzwerke mit USB Adaptern oder iOS Geräte mit Mobilfunkdienst (Persönlicher Hotspot)
   - VPN (Virtual Private Network) – Virtuelle Netzwerkschnittstelle über das Protokoll L2TP (Layer 2 Tunneling Protocol) über IPSec (Internet Protocol Security); Cisco IPSec; und IKEv2 (Internet Key Exchange Version 2)
   - TCP/IP (Transmission Control Protocol/Internet Protocol), auch als Internetprotokollfamilie bezeichnet
   - DHCP (Dynamic Host Configuration Protocol)
   - DNS-Protokoll (Domain Name System)
   - NetBIOS (Network Basic Input/Output System) und WINS (Windows Internet Naming Service)
   - Authentifiziertes Ethernet über das Protokoll 802.1X
3. Anhand der Prioritätenliste der Netzwerkdienste wird die primäre Netzwerkdienstschnittstelle ermittelt, wenn mehrere Dienste aktiv sind. Der gesamte Netzwerkverkehr, der über eine lokale Verbindung mit einer aktiven Netzwerkdienstschnittstelle nicht besser abgewickelt wird, wird an die primäre Netzwerkdienstschnittstelle gesendet. In den meisten Fällen werden folglich der gesamte WAN-Datenverkehr, Internet-Datenverkehr und die DNS-Auflösung über die primäre Netzwerkdienstschnittstelle gesendet.

4. Netzwerkdienstschnittstellen, die in der Systemeinstellung „Netzwerk“ eine grüne Statusanzeige aufweisen, werden für Netzwerkaktivitäten genutzt. Der gesamte Netzwerkverkehr, der über eine lokale Verbindung nicht besser abgewickelt wird, wird an die primäre Netzwerkdienstschnittstelle gesendet. Die primäre Netzwerkdienstschnittstelle ist die oberste aktive Schnittstelle in der Liste. Du kannst deine Prioritätenliste der Netzwerkdienste manuell umstellen, indem du in der Systemeinstellung „Netzwerk“ die Option „Reihenfolge der Dienste festlegen“ wählst und die Einträge in die gewünschte Reihenfolge ziehst. Aktive Dienste haben weiterhin Vorrang vor inaktiven Diensten.
5. Die einfachste Methode zum Konfigurieren von VPN-Einstellungen ist die Nutzung eines Konfigurationsprofils mit allen relevanten VPN-Konfigurationsinformationen.
6. In macOS Mojave gibt es zwei Konfigurationsmethoden für 802.1X:
    a. Automatische Konfiguration durch Auswahl eines WLAN Netzwerks, das die Authentifizierung mittels WPA/WPA2 verlangt
    b. „Halbautomatische“ Konfiguration über ein 802.1X Konfigurationsprofil, das von einem Administrator bereitgestellt wird

Lektion 23 – Netzwerkprobleme beheben

Ziele

- Probleme mit der Netzwerkkonfiguration erkennen und beheben
- Netzwerkkonfiguration in der Systemeinstellung „Netzwerk“ prüfen
- Netzwerkdienstprogramm zur Problembehebung verwenden

Kontrollfragen

1. Nenne drei häufige Probleme, die Netzwerkdienste auf einem Mac Computer unterbrechen können.
2. Wie kannst du die MAC-Adressen aller Netzwerkschnittstellen des Mac Computers ermitteln?
3. Wie lautet die Bezeichnung für die aktuelle Datenrate einer WLAN Verbindung, und wo kannst du für eine bestimmte WLAN Verbindung auf diese Information zugreifen?
4. Wie kannst du die grundlegende Konnektivität zu einem anderen Netzwerk-Host überprüfen?
5. Wie kannst du überprüfen, ob die DNS-Hostnamenauflösung funktioniert?
6. Wie kannst du überprüfen, ob das System eine Verbindung zu einem entfernten Netzwerk-Host herstellen kann?

Antworten

1. Diese drei Probleme unterbrechen die Netzwerkdienste auf einem Mac häufig:
   a. Lokale Probleme, meist verursacht durch nicht ordnungsgemäß konfigurierte Netzwerkeinstellungen oder eine getrennte Netzwerkverbindung
   b. Netzwerkprobleme, deren Ursachen du mit der Netzwerkdiagnose ermitteln kannst
   c. Dienstprobleme, die mit dem Netzwerkgerät oder -dienst zusammenhängen, auf das bzw. den du zugreifen willst
2. Du kannst alle MAC-Adressen der Netzwerkschnittstellen des Mac Computers im Bereich „Informationen“ des Netzwerkdienstprogramms auslesen.
3. Du kannst die aktuelle Datenrate bzw. Tx-Rate einer ausgewählten WLAN Verbindung im WLAN Statusmenü einsehen. Das WLAN Statusmenü bietet dir Zugriff auf wichtige Informationen über deine Verbindungen und ermöglicht dir den Zugriff auf Tools zur Fehlerbehebung wie die Diagnose für drahtlose Umgebungen. Du kannst das WLAN Statusmenü öffnen, indem du bei gedrückter Wahltaste auf das WLAN-Symbol in deiner Menüleiste klickst.
4. Im Tab „Ping“ des Netzwerkdienstprogramms kannst du die grundlegende Konnektivität zu einem anderen Netzwerk-Host testen, indem du ein Ping-Paket versendest und dann auf dessen Rückkehr wartest.
5. Im Tab „Lookup“ des Netzwerkdienstprogramms kannst du die Namensauflösung des derzeit konfigurierten DNS-Servers testen.
6. Im Tab „Trace“ des Netzwerkdienstprogramms kannst du die Verbindungs-Hops zwischen deinem Mac und einem entfernten Host überprüfen.

Teil 7: Netzwerkdienste

Lektion 24 – Netzwerkdienste verwalten

Ziele

- Beschreiben, wie macOS auf geteilte Netzwerkdienste zugreift
- In macOS integrierte Netzwerk-Apps konfigurieren
- Netzwerkdateidienste mit dem Finder durchsuchen und darauf zugreifen
- Probleme mit geteilten Netzwerkdiensten beheben

Kontrollfragen

1. Welche Beziehung besteht zwischen Clients und Servern im Hinblick auf den Zugriff auf Netzwerkdienste?
2. Welche Beziehung besteht zwischen einem Netzwerkdienst und einen Netzwerkanschluss?
3. Welches ist die primäre Schnittstelle für die Konfiguration von Netzwerkdienstanwendungen?
4. Wie nutzt macOS Mojave dynamische Service Discovery Protokolle für den Zugriff auf Netzwerkdienste?
5. Welche beiden dynamischen Service Discovery Protokolle für den Zugriff auf Netzwerkdienste werden von macOS Mojave unterstützt?
6. Mit welchen fünf Netzwerkdateidiensten kann man im Finder im Dialogfenster „Mit Server verbinden“ eine Verbindung herstellen?
7. Welches standardmäßige Dateifreigabeprotokoll verwendet macOS, um einen Mac Computer, auf dem Mojave läuft, mit einem anderen Computer zu verbinden?
8. Wie werden die Objekte im Ordner „Netzwerk“ im Finder eingetragen?
9. Auf welche zwei Arten kann man eine Netzwerkfreigabe automatisch verbinden?
10. Nenne drei gängige Techniken zur Problembehebung, wenn du dich nicht mit Netzwerkdiensten verbinden kannst.
11. Wie kannst du überprüfen, ob ein bestimmter Netzwerkdienst eines Dienstanbieters verfügbar ist?

Antworten

1. Clientsoftware wird dazu verwendet, auf Netzwerkdienste zuzugreifen, die von Serversoftware bereitgestellt werden. Client- und Serversoftware kommunizieren über Netzwerkprotokolle und -standards miteinander.
2. Netzwerkdienste werden über ein gemeinsames Netzwerkprotokoll bereitgestellt. Das Protokoll gibt an, welche TCP- bzw. UDP-Portnummer für die Kommunikation verwendet wird.
3. Die Systemeinstellung „Internetaccounts“ ist die primäre Schnittstelle in macOS Mojave für die Konfiguration integrierter Netzwerk-Apps wie Mail, Kalender, Notizen, Erinnerungen, Kontakte und Nachrichten.
4. Einige Geräte, die einen Netzwerkdienst bereitstellen, geben ihre Verfügbarkeit über das dynamische Service Discovery Protokoll für den Zugriff auf Netzwerkdienste bekannt. Clients auf der Suche nach Diensten fragen diese Informationen ab und erhalten sie, um dem Benutzer eine Liste der verfügbaren Netzwerkdienste bereitzustellen.
5. macOS Mojave unterstützt Bonjour und SMB (Server Message Block) sowie die älteren dynamischen Service Discovery Protokolle für den Zugriff auf die Netzwerkdienste NetBIOS (Network Basic Input/Output System) und WINS (Windows Internet Naming Service). Bonjour stellt den primären Satz an dynamischen Service Discovery Protokollen dar, den native macOS Dienste und Apps nutzen.

6. Im Finder kann man über das Dialogfenster „Mit Server verbinden“ Verbindungen zu folgenden Diensten und Systemen herstellen:
   - Server Message Blocks/Common Internet File System (SMB/CIFS)
   - SMB2/SMB3
   - Apple File Protocol (AFP)
   - Network File System (NFS)
   - Web-based Distributed Authoring and Versioning (WebDAV)
   - Netzwerkdateidienste gemäß File Transfer Protocol (FTP)
7. SMB (Service Message Block) ist das standardmäßige und bevorzugte Dateifreigabeprotokoll, das MacOS Mojave verwendet.
8. Der Finder trägt im Ordner „Network“ Informationen ein, die von den dynamischen Service Discovery Protokollen für den Zugriff auf Netzwerkdienste bereitgestellt werden. Computer, die Dienste bereitstellen, werden im Ordner „Network“ als Ressourcen angezeigt; Service Discovery Zonen und Arbeitsgruppen werden als Ordner angezeigt. Alle derzeit verbundenen Server werden ebenfalls im Ordner „Network“ angezeigt.
9. Um bei der Anmeldung des Benutzers beim System automatisch eine Verbindung zu einer Dateifreigabe herzustellen, bewegst du in der Systemeinstellung „Benutzer & Gruppen“ die Freigabe aus dem Finder auf die Anmeldeobjekte des Benutzers. Du kannst die Freigabe auch auf die rechte Seite des Benutzerdocks bewegen. Dann wird automatisch eine Verbindung hergestellt, wenn der Benutzer auf das Freigabesymbol im Dock klickt.
10. Gehe die Systemeinstellung „Netzwerk“ sowie die Statistiken des Netzwerkdienstprogramms durch und versuche, Verbindungen zu verschiedenen Netzwerkdiensten herzustellen.
11. Um zu prüfen, ob ein bestimmter Dienst eines Dienstanbieters verfügbar ist, prüfe zunächst im Tab „Ping“ des Netzwerkdienstprogramms die grundlegende Konnektivität. Prüfe dann im Netzwerkdienstprogramm im Tab „Portscan“, ob die betreffenden Dienst-Ports geöffnet sind. Du solltest den Portscan immer auf die Ports begrenzen, die für den zu testenden Netzwerkdienst erforderlich sind.

Lektion 25 – Host-Sharing und persönliche Firewall verwalten

Ziele

- In macOS integrierte Host-Freigabedienste kennenlernen und aktivieren
- In macOS integrierte Inhaltscachingdienste kennenlernen und aktivieren
- Per Bildschirmfreigabe auf andere Netzwerk-Hosts zugreifen
- Dateien mit AirDrop schnell und einfach teilen
- Freigabedienste durch Konfiguration der persönlichen Firewall schützen
- Probleme mit Freigabediensten beheben

Kontrollfragen

1. Welche Freigabedienste kann macOS Mojave bereitstellen?
2. Was sind die Vorteile des Caching von Inhalten?
3. Welche App ermöglicht die Bildschirmfreigabe on-Demand, auch dann, wenn der Bildschirmfreigabedienst nicht aktiviert ist?
4. Welche(n) Netzwerkdienst(e) braucht die Bildschirmfreigabe in macOS Mojave?
5. Was ist AirDrop, und wie weißt du, ob ein bestimmter Mac AirDrop unterstützt?
6. Welche beiden Einstellungen auf dem Mac kannst du ändern, damit mehr Geräte angezeigt werden, wenn andere Geräte mit aktiviertem AirDrop nicht im AirDrop Browser angezeigt werden?
7. Worin unterscheidet sich die in macOS Sierra integrierte Firewall in erster Linie von herkömmlichen Netzwerk-Firewalls?
8. Welche Firewall-Einstellungen gibt es in macOS Mojave?
9. Wie beeinflusst die Aktivierung des Tarnmodus die Art, in der dein Mac mit anderen Hosts kommuniziert? Wie wird sie durch Blockieren aller eingehenden Verbindungen beeinflusst?

Antworten

1. In macOS Mojave gibt es folgende Freigabedienste:
   - Entfernte CD/DVD (zur CD/DVD-Freigabe)
   - Bildschirmfreigabe
   - Dateifreigabe
   - Druckerfreigabe (und Scannerfreigabe)
   - Entfernte Anmeldung
   - Entfernte Verwaltung (ARD)
   - Entfernte Apple Events
   - Internetfreigabe
   - Bluetooth Freigabe
   - Caching von Inhalten
2. Das Caching von Inhalten trägt zur verringerten Belastung der Internet-Bandbreite bei und beschleunigt Softwareinstallation und iCloud Inhaltsfreigabe auf Mac Computern, iOS Geräten und Apple TV Geräten.
3. Die App „Nachrichten" ermöglicht die On-Demand-Bildschirmfreigabe, die auch nutzbar ist, wenn der Bildschirmfreigabedienst nicht aktiviert ist.

4. In macOS Mojave erfolgt die Bildschirmfreigabe von Nachrichten über iMessage. Dafür müssen sich die Benutzer beider Mac Computer bei iCloud anmelden.
5. Mit AirDrop lassen sich Dateien in lokaler WLAN und Bluetooth Reichweite schnell und einfach teilen. AirDrop erstellt ein sicheres Peer-to-Peer-Netzwerk lokaler Geräte. Im Finder Menü "Gehe zu" kannst du feststellen, ob der Mac AirDrop unterstützt.
6. Auf neueren Mac Modellen gibt es zwei Einstellungen unten im AirDrop Browser, die die AirDrop Erkennung steuern. Die erste Einstellung erweitert die AirDrop Erkennung, sodass nicht nur Benutzer angezeigt werden, die in den eigenen Kontakten hinterlegt sind, sondern alle Benutzer innerhalb der Reichweite von AirDrop. Mit der zweiten Einstellung wird AirDrop auf die frühere Erkennungsmethode umgeschaltet, sodass der Mac auch ältere Mac Computer bzw. solche mit früheren Mac Betriebssystemversionen erkennt.
7. Mit der in macOS Mojave integrierten Firewall werden Verbindungen appspezifisch zugelassen bzw. gesperrt. Dies steht im Gegensatz zu herkömmlichen Netzwerk-Firewalls, bei denen die Zugriffsregeln auf den Portnummern der Netzwerkdienste basieren.
8. In macOS Mojave gibt es die folgenden Firewall-Einstellungen:
   - Alle eingehenden Verbindungen blockieren
   - Integrierter Software automatisch erlauben, eingehende Verbindungen zu empfangen
   - Geladener signierter Software automatisch erlauben, eingehende Verbindungen zu empfangen
   - Tarnmodus aktivieren
9. Bei aktiviertem Tarnmodus reagiert dein Mac nicht auf unbefugte Netzwerkverbindungen, z. B. Netzwerkdiagnoseprotokolle wie Ping, Traceroute und Portscan. Dein Mac reagiert immer noch auf andere zugelassene Dienste. Dazu zählt Bonjour, das die Präsenz deines Mac Computers ankündigt und verhindert, dass er im Netzwerk verborgen wird. Wenn du alle eingehenden Verbindungen blockierst, reagiert dein Mac nicht auf eingehende Verbindungen, es sei denn, diese sind für grundlegende Netzwerkdienste oder bereits bestehende Verbindungen erforderlich, etwa zum Surfen im Internet oder Prüfen der E-Mail. Damit wird verhindert, dass sich Freigabedienste oder Apps, die dein Mac bereitstellt, per Fernzugriff bedienen lassen.

Teil 8: Systemverwaltung

Lektion 26 – Probleme mit Peripheriegeräten beheben

Ziele

- Verbindung von Peripheriegeräten verwalten
- Bluetooth Geräte mit dem Mac verbinden
- Probleme mit Peripheriegeräten und Treibern beheben

Kontrollfragen

1. Welche vier primären Bustechnologien für Peripheriegeräte werden von Mac Computern mit macOS Mojave unterstützt?
2. Was muss geschehen, damit ein Mac mit einem Bluetooth Peripheriegerät kommunizieren kann? Wo kann man diese Kopplung konfigurieren?
3. Was ist ein Gerätetreiber? Nenne die drei primären Arten von Gerätetreibern.
4. Wie funktioniert in macOS Mojave die Unterstützung von Geräten anderer Anbieter, ohne dass Gerätetreiber anderer Anbieter erforderlich sind?
5. Welche Schlussfolgerungen kannst du über ein angeschlossenes Peripheriegerät ziehen, wenn es nicht in der App „Systeminformationen" angezeigt wird?

Antworten

1. Die vier primären Bustechnologien für Peripheriegeräte, die macOS Mojave unterstützt:
   a. Universal Serial Bus (USB)
   b. FireWire
   c. Bluetooth
   d. Thunderbolt
2. Bluetooth Geräte müssen gekoppelt werden, damit sie miteinander kommunizieren können. Die Systemeinstellung „Bluetooth" ist für das Koppeln eines Mac mit Bluetooth Peripheriegeräten zuständig. Über das Bluetooth Statusmenü kannst du schnell die Systemeinstellung „Bluetooth" öffnen.
3. Ein Gerätetreiber ist eine Software, die speziell dafür entwickelt wurde, die Kommunikation zwischen macOS Mojave und einem Peripheriegerät zu ermöglichen. Die drei Haupttypen von Gerätetreibern:
   a. Kernel-Erweiterungen
   b. Framework-Plug-Ins
   c. Eigenständige Apps
4. macOS Mojave nutzt für jede Geräteklasse integrierte, generische Treiber. Beispielsweise gibt es generische Treiber für Scanner und Drucker, die anstelle der offiziellen Treiber anderer Hersteller verwendet werden können.
5. Wenn ein angeschlossenes Peripheriegerät nicht in den Systeminformationen angezeigt wird, handelt es sich wahrscheinlich um ein Hardwareproblem. Führe entsprechende Fehlerbehebungsmaßnahmen durch.

Lektion 27 – Drucker und Scanner verwalten

Ziele

- Druckertechnologien in macOS beschreiben
- macOS für Drucker und Multifunktionsgeräte konfigurieren
- Druckaufträge verwalten und Probleme beheben

Kontrollfragen

1. Mithilfe welcher Apple Technologie findest du Drucker und kannst drucken, ohne Druckertreiber zu laden und zu installieren?
2. Welche Aufgabe hat CUPS?
3. Wie kannst du einen neuen Druckertreiber für einen bereits konfigurierten Drucker auswählen?
4. Welche beiden Aktionen musst du möglicherweise ausführen, um einen Windows-Computer zu ermitteln und mit deinem Druckdienst per CUPS-Freigabe zu verbinden?
5. Unter welchen Umständen kann ein Standardbenutzer (der kein Administrator ist) einen Drucker konfigurieren?
6. Wie gibt man Drucker für andere Benutzer frei?
7. Wie beeinflusst der Ruhemodus den Zugriff von Benutzern auf freigegebene Druckdienste?
8. Wie wird ein PDF-Dokument erstellt?
9. Welche drei Methoden können verwendet werden, um auf eine Druckerwartelisten-App zuzugreifen?
10. Was ist eine möglichst schnelle Lösung, wenn offenbar ein konfigurierter Drucker ein Problem ausweist?

Antworten

1. AirPrint.
2. CUPS verwaltet Druckaufgaben für macOS Mojave, einschließlich lokalen Druck und Druck auf freigegebenen Druckern.
3. Dies hängt vom Drucker ab. Manchmal kannst du in der Systemeinstellung „Drucker & Scanner" im Dialogfenster „Optionen & Füllstände" einfach einen neuen Druckertreiber wählen. In vielen Fällen musst du den Drucker jedoch löschen und dann erneut hinzufügen, um einen neuen Druckertreiber für einen bereits konfigurierten Drucker auswählen zu können.
4. Der Druckdienst per CUPS-Freigabe ermöglicht Netzwerkclients, mithilfe von Bonjour deine freigegebenen Druckerkonfigurationen zu lokalisieren. Jedoch können verschiedene Windows-Versionen verlangen, dass du weitere Treiber hinzufügst. Netzwerkclients können auch die IP-Adresse oder den Hostnamen deines Mac Computers eingeben, um auf deinen freigegebenen Mac Druckdienst zuzugreifen.
5. Bei den Standardeinstellungen von macOS Mojave kann ein Standardbenutzer im Druckfenster nur direkt angeschlossene bzw. lokale Netzwerkdrucker konfigurieren. Außerdem müssen die entsprechenden Treiber installiert sein, damit der Standardbenutzer den Drucker konfigurieren kann.
6. Benutzer können auf keinen freigegebenen Druckdienst an einem Mac im Ruhezustand zugreifen. Um sicherzustellen, dass der Ruhemodus die Druckfreigabe nicht stört, kannst du in der Systemeinstellung „Energie sparen" entweder das automatische Aktivieren des Ruhezustands deaktivieren oder die Option „Ruhezustand bei Netzwerkzugriff beenden" aktivieren.
7. Du kannst die Druckerfreigabe in der Systemeinstellung „Drucker & Scanner" bzw. „Freigaben" aktivieren.
8. Klicke im Dialogfeld „Drucken" auf „PDF". Du kannst dann eine der Optionen im PDF-Einblendmenü wählen, um die neue PDF-Datei zu sichern oder zu senden.

9. Wenn eine Drucker-Warteliste offen ist, kannst du auf ihr Symbol im Dock klicken. Wenn die Drucker-Warteliste aus dem Dock verschwindet, bevor du darauf klicken kannst, öffne die Systemeinstellung „Drucker & Scanner“, wähle links die Warteliste aus, und klicke auf „Drucker-Warteliste öffnen“. Du kannst eine Drucker-Warteliste auch manuell im Finder öffnen, indem du zu ~/Library/Printers/ navigierst und dann auf einen Drucker doppelklickst.
10. Wenn alle Drucker Probleme aufweisen, ist die schnellste Lösung das Zurücksetzen des gesamten Drucksystems. Klicke dafür mit gedrückter Befehlstaste in die Druckerliste und wähle dann die Option „Drucksystem zurücksetzen“.

Lektion 28 – Start- und Systemprobleme beheben

Ziele

- macOS Startvorgang beschreiben
- Essenzielle Dateien und Prozesse kennenlernen, die für einen erfolgreichen Systemstart nötig sind
- macOS Startmodi kennenlernen
- Probleme mit Start- und Anmeldeprozessen beheben

Kontrollfragen

1. Was ist die Rolle des T2 Chips bei einem macOS Mojave Start?
2. Was geschieht, wenn dein macOS mit einem T2 Chip Fehler erkennt und beim sicheren Startvorgang Probleme auftreten?
3. Welches sind die primären Systeminitialisierungsphasen von macOS Mojave? Welche optischen und akustischen Hinweise weisen auf die einzelnen Phasen hin?
4. Welche Aufgabe hat die Firmware? Was ist der Selbsttest beim Einschalten (Power-On Self Test, POST)?
5. Welche Rolle spielt der Prozess `launchd` beim Mac Systemstart?
6. Welche Objekte werden beim Mac Systemstart vom Prozess `launchd` automatisch gestartet?
7. Welches sind die primären Phasen von Benutzersitzungen in macOS Mojave? Welche optischen und akustischen Hinweise weisen auf die einzelnen Phasen hin?
8. Was ist der Unterschied zwischen LaunchDaemons, Startobjekten, LaunchAgents und Anmeldeobjekten?
9. Was versteht man unter „Sicherer Ruhezustand", „Standby" und „Power Nap"?
10. Was geschieht bei der Abmeldung des Benutzers?
11. Was geschieht beim Ausschalten des Mac?
12. Welcher Tastaturkurzbefehl wird für den sicheren Systemstart (gesicherter Modus) von OS X verwendet
13. Mit welcher Tastenkombination kann vorübergehend ein anderes Startvolume ausgewählt werden?
14. Welche Änderungen werden bei einem sicheren Systemstart von macOS Mojave vorgenommen?
15. Welche Objekte werden bei einem sicheren Systemstart von macOS Mojave nicht geladen?

Antworten

1. Der T2 Chip verifiziert jeden Schritt des Bootvorgangs, um sicherzustellen, dass Hardware und Software nicht manipuliert wurden.
2. Wenn dein macOS mit einem T2 Chip Fehler identifiziert und beim sicheren Start Probleme auftreten, wechselt dein Mac in macOS Wiederherstellung, den Apple T2 Security Chip Wiederherstellungsmodus oder den Apple T2 Chip DFU-Modus (Device Firmware Upgrade).
3. Die einzelnen Hauptphasen des Systemstarts werden durch Folgendes angezeigt:
   a. Firmware: Einschalten, Selbsttest beim Einschalten (POST), Startton (je nach Modell)
   b. Boot-Programm: Start des Boot-Vorgangs, das Apple Logo wird mittig auf dem primären Display angezeigt.
   c. Kernel: Kernel-Start, der Fortschrittsbalken wird angezeigt.
   d. Systembezogener `launchd`-Prozess: Start weiterer Objekte, das Apple Logo wird durch den Anmeldebildschirm ersetzt.

4. Die Firmware initialisiert die Hardware des Mac Computers und sucht die Startdatei auf einem Systemvolume. Der POST überprüft die grundlegende Hardwarefunktionalität beim Einschalten des Mac.
5. `launchd` startet macOS Mojave Prozesse. Er verwaltet außerdem die Initialisierung von macOS Mojave und startet den Prozess loginwindow.
6. Beim Systemstart von macOS Mojave startet `launchd` diese Daemons und Skripte:
   - /System/Library/LaunchDaemons
   - /Library/LaunchDaemons
7. Die einzelnen Hauptphasen einer Benutzersitzung werden durch Folgendes angezeigt:
   a. Der Anmeldebildschirm wird angezeigt.
   b. launchd lädt nach Authentifizierung des Benutzers Apps wie den Finder.
   c. Die Benutzerumgebung ist immer aktiv, wenn der Benutzer bei macOS Mojave angemeldet ist.
8. LaunchDaemons und Startobjekte werden beim Mac Systemstart vom `launchd`-Prozess des Administratoraccounts gestartet. LaunchAgents und Anmeldeobjekte werden bei Initialisierung der Benutzerumgebung durch die `launchd`-Prozesse des Benutzeraccounts geöffnet.
9. „Sicherer Ruhezustand" und „Standby" sind Modi für Mac Computer, die wenig oder keine Leistung zum Schutz von Daten nutzen. Wenn Mac Computer in den Ruhezustand wechseln, kopieren sie den vollständigen Inhalt des Systemspeichers in eine Image-Datei auf dem Systemvolume. Sollte also der Mac so lange im Ruhezustand bleiben, bis die Batterie komplett leer ist, gehen auch beim Abschalten des Mac keine Daten verloren.
   - Sicherer Ruhezustand: Dein Mac wechselt in diesen Modus, wenn die Batterie komplett leer ist oder du deinen Mac längere Zeit im Ruhemodus lässt. Um den Computer aus dem Ruhezustand zu aktivieren, startest du einen Mac genauso, als sei er ausgeschaltet gewesen. Alle mit macOS Mojave kompatiblen Mac Modelle unterstützen diesen Modus.
   - Standby: Dein Mac wechselt in diesem Modus als Energiespar-Standby, wenn er sich im Ruhemodus befindet und abhängig vom Herstellungsdatum länger als eine Stunde bzw. drei Stunden inaktiv ist. Um deinen Mac zu aktivieren, interagierst du mit der Tastatur, dem Trackpad oder der Maus. Du musst deinen Computer nicht neu starten. Diesen Modus nutzen neuere Mac Computer mit Flash-Speicher.

     „Power Nap" ist ein Status, der regelmäßig Updates ausführt, während sich dein Computer im Ruhezustand befindet.
   - Power Nap: Informationen werden regelmäßig auf deinem Mac aktualisiert, während er sich im Ruhezustand befindet. Die Art der aktualisierten Informationen variiert, abhängig davon, ob dein Mac mit Batterie läuft oder an das Stromnetz angeschlossen ist. Die Aktivierung von Power Nap variiert je nach Computertyp.
10. Bei der Abmeldung des Benutzers führt der benutzerbezogene Prozess loginwindow folgende Aufgaben durch:
    a. Er fordert auf, alle Benutzer-Apps zu beenden.
    b. Er beendet automatisch alle Hintergrundprozesse des Benutzers.
    c. Er führt Abmeldeskripte aus.
    d. Er zeichnet die Abmeldung in der primären Datei system.log auf.
    e. Er setzt Geräteberechtigungen und -einstellungen auf die Standardwerte zurück.
    f. Er beendet die benutzerbezogenen Prozesse „loginwindow" und `launchd`.

11. Beim Ausschalten des Mac meldet der Prozess loginwindow alle Benutzer ab und weist den Kernel dann an, alle übrigen macOS Mojave Prozesse zu beenden. Danach schaltet sich der Mac aus.
12. Halte beim Systemstart die Umschalttaste gedrückt, um den sicheren Systemstart zu veranlassen.
13. Wenn du beim Systemstart die Wahltaste gedrückt hältst, öffnet sich der Startup Manager, mit dem du vorübergehend ein anderes Startvolume auswählen kannst.
14. Beim sicheren Systemstart werden die folgenden permanenten Maßnahmen durchgeführt:
    a. Versuch, die Struktur des Systemvolumes zu reparieren
    b. Caches von System-Kernel-Erweiterungen (KEXT) anderer Anbieter werden gelöscht
    c. Schriftencaches werden gelöscht
15. Beim sicheren Systemstart lädt macOS Mojave keine Kernel-Erweiterungen (KEXTs), LaunchAgents, LaunchDaemons, Startobjekte und Schriften anderer Anbieter, keine Anmeldeobjekte von Benutzern und keine benutzerspezifischen LaunchAgents.