Zarządzanie urządzeniami Apple

Zunifikowana teoria zarządzania urządzeniami Mac, iPad, iPhone oraz AppleTV

—

Charles Edge
Rich Trouton

Apress®

Apress®

Charles Edge
Rich Trouton

Zarządzanie urządzeniami Apple

Zunifikowana teoria zarządzania urządzeniami Mac, iPad, iPhone oraz AppleTV

APN Promise, Warszawa 2021

Zarządzanie urządzeniami Apple. Zunifikowana teoria zarządzania urządzeniami Mac, iPad, iPhone oraz AppleTV

First published in English under the title
Apple Device Management: A Unified Theory of Managing Macs, iPads, iPhones, and AppleTVs by Charles Edge and Rich Trouton

Polish language edition published by APN PROMISE S.A., Copyright © 2021

Autoryzowany przekład z wydania w języku angielskim, zatytułowanego: Apple Device Management: A Unified Theory of Managing Macs, iPads, iPhones, and AppleTVs by Charles Edge and Rich Trouton, opublikowanego przez APress Media, LLC, oddział Springer Nature.

APN PROMISE SA, ul. Domaniewska 44a, 02-672 Warszawa
tel. +48 22 35 51 600, fax +48 22 35 51 699
e-mail: wydawnictwo@promise.pl

ISBN: 978-83-7541-440-0 (druk), 978-83-7541-444-8 (ebook)

Przekład: WITKOM - Mariusz Rogulski i Witold Sikorski
Redakcja: Marek Włodarz
Korekta: Ewa Swędrowska
Skład i łamanie: MAWart Marek Włodarz

Spis treści

Wstęp

Firma Apple w ciągu 35 lat rozprowadziła 25 wydań systemu operacyjnego dla komputerów Mac. Potem pojawił się iPhone, iPad i Apple TV. Sukces urządzeń iPhone i unikatowe wyzwania związane z zarządzaniem urządzeniami mobilnymi oznaczają, że musiały zostać ustanowione nowe paradygmaty dla tych zadań. Wynikało stąd, że zarządzanie urządzeniami firmy Apple musiało się zmienić. Ta ewolucja była nieunikniona od chwili, gdy sprzedaż iPhone'ów dwukrotnie przekroczyła sprzedaż komputerów Mac i stawało się to coraz bardziej jasne.

Ta ewolucja w zarządzaniu urządzeniami jest teraz niezaprzeczalna i nieodwracalna. Końcowy wynik tej ewolucji nie jest jeszcze przesądzony, ale zmiana jest już na progu. Ta książka ma na celu skodyfikowanie tych zmian i identyfikację najlepszych praktyk.

Dla kogo jest ta książka?

Mówiąc najprościej, jest to książka dla administratorów pracujących w organizacjach, które chcą integrować się z nowymi produktami Apple. Wiele organizacji zaczęło przygotowywać się do tego, co nadchodzi. Nieuchronnie pojawiło się wiele narzekań dotyczących aspektów budowania infrastruktury i usług. Jednak najdroższa firma na świecie nie wykazała chęci zezwalania na wyjątki od głoszonych przez siebie zasad.

Książka ta opisuje, czego potrzebują organizacje, aby osiągnąć efektywną pracę na platformie Apple, co obejmuje nie tylko infrastrukturę, ale również sposób myślenia, który trzeba przyjąć dla osiągnięcia sukcesu, sposób myślenia, który zmusza do porzucenia dogmatów obowiązujących od 30 lat. I można do woli narzekać, ale im szybciej uda się to opanować, tym szybciej da się osiągnąć sukces na tej platformie.

Ta książka ma pomóc w opanowaniu nowego stylu zarządzania. Ponieważ on nigdzie nie odejdzie i pozostanie z nami na jakiś, zapewne nie taki krótki czas.

Rzut oka na rozdziały

Książka ta zawiera wskazówki. Są one podzielone na rozdziały, które dają wgląd w każde obszerniejsze zagadnienie związane z zarządzaniem urządzeniami firmy Apple. Większość obejmuje filozofię i projekt historii zarządzania urządzeniami firmy Apple. Jeśli nie jest to podane w tytule, dążymy do ujednolicenia historii zarządzania w różnych systemach operacyjnych, czyli w iOS, macOS i tvOS. W każdym rozdziale odnotowujemy różnice między nimi.

Rozdział 1. Ewolucja zarządzania urządzeniami firmy Apple

Jak tu się znaleźliśmy? Pomocne będzie zrozumienie historii ewolucji zarządzania urządzeniami firmy Apple w ciągu ostatnich 30 lat (z górą). Wiedza, skąd przyszliśmy, powinna ułatwić akceptację wyborów Apple i lepiej zrozumieć, dokąd nas zabiera firma Apple, zewnętrzni sprzedawcy oprogramowania i społeczność IT. Rozdział 1 zapewnia podstawy do rozpoczęcia działań.

Rozdział 2. Zarządzanie oparte na agentach

Nie ma czegoś takiego, jak rozwiązania dla zarządzania bez agentów. W tym rozdziale przyglądamy się agentom zarządzania, które nie obejmują MDM, a także to, kiedy musimy używać agentów, a kiedy innych opcji.

Rozdział 3. Profile

Profil to plik, który można wykorzystać do skonfigurowania ustawień na urządzeniu Mac lub iOS. Gdy zainstalujemy rozwiązania związane z zarządzaniem, możemy umieścić te profile na urządzeniu lub wdrożyć je na komputerach Mac za pomocą skryptów. Opisujemy tu, jak tworzyć profile i instalować tak, aby uzyskać najbardziej potrzebne ustawienia urządzeń.

Rozdział 4. Wnętrze MDM

Czym jest MDM (Mobile Device Management, Zarządzanie urządzeniami mobilnymi) i jak działa wewnętrznie? Dzięki poznaniu sposobu funkcjonowania MDM zrozumiemy, co musi się stać w naszych sieciach, aby pozwolić na działanie MDM, a także jaki jest najlepszy sposób zapewnienia minimalnego niezbędnego dostępu do serwerów lub usług.

Rozdział 5. Wyposażanie systemu iOS

Rozdział opisuje, jak przygotować urządzenia z systemami iOS, tvOS i iPadOS do wdrożenia, w tym posługiwanie się profilami, MDM, Apple Configurator, App Store i innymi narzędziami przygotowującymi te urządzenia do pracy.

Rozdział 6. Wyposażanie komputerów Mac

Konfigurowanie Maców stanowiło coś w rodzaju ruchomego, trudnego do osiągnięcia celu, co zaczęło się od rezygnacji z tradycyjnego tworzenia obrazu systemu i przejścia na wdrożenia bez udziału użytkownika z wykorzystaniem DEP. Ten rozdział omawia, jak przygotować komputery Mac do wdrożenia z wykorzystaniem wielu różnych metod, w tym narzędzi firmy Apple i dostawców zewnętrznych.

Rozdział 7. Szyfrowanie na urządzeniu końcowym

Gdy już mamy skonfigurowanego Maca lub urządzenie iOS, ludzie zaczną dodawać do nich dane, które muszą być chronione. Ochronę tę zapewnia szyfrowanie, a ten rozdział opisuje, jak to działa, jak je włączyć i jak zarządzać nią na wszystkich swoich urządzeniach firmy Apple.

Rozdział 8. Zabezpieczenie swojej floty

Administrator chcący w pełni zabezpieczyć urządzenia może je po prostu zamknąć w szafie pancernej. Jeszcze lepiej byłoby je wyłączyć i rozwalić młotkiem. Bezpieczeństwo to stawianie na to, że populacja naszych urządzeń będzie rosnąć. Każda organizacja

ma swoje podejście do bezpieczeństwa i gdy już wprowadzimy na swoich urządzeniach ustawienia i apki, zajmiemy się aplikowaniem własnego podejścia do bezpieczeństwa poprzez dostosowanie ustawień do swoich potrzeb.

Rozdział 9. Kultura automatyzacji i ciągłego testowania

Wdrażanie ustawień na urządzeniach bez wcześniejszego testowania może sprawić, że współpracownicy nie będą mieli pojęcia, gdzie co jest na ich urządzeniach, będą mogli zostać wywaleni ze swoich sieci, a to i wiele innych rzeczy może sprawić, że Mikołaj przyniesie nam rózgę zamiast prezentu. Podczas wdrażania kolejnych iteracji systemów, konfiguracji ustawień i pobieranego oprogramowania nie da się wszystkiego przetestować ręcznie. W tym rozdziale zajmiemy się uzyskaniem standardowego środowiska QA (pytań i odpowiedzi), aby można było przeprowadzać testy bez wykonywania wszystkiego ręcznie.

Rozdział 10. Usługi katalogowe

Active Directory było kiedyś przekleństwem dla wielu administratorów komputerów Mac. Jednak w ostatnich latach zagadnienie powiązania i istnienia w środowisku Active Directory zwykle było bezproblemowe. W istocie dzisiaj największym wyzwaniem nie jest *jak*, ale *dlaczego*, biorąc pod uwagę bogactwo możliwości posługiwania się usługami katalogowymi (Directory Services). W tym rozdziale omawiamy sposoby sprawienia, aby Mac działał z Active Directory i funkcjonował jako obywatel pierwszej kategorii w sieciach, w których przeważa system Windows.

Rozdział 11. Dostosowywanie wrażeń użytkowników

Nie można omawiać zarządzania urządzeniami bez przedstawienia jednego z podstawowych powodów, dla których ludzie chcą tego zarządzania: aby życie ich współpracowników było lepsze. Do tego miejsca zajmowaliśmy się wdrażaniem i drobniejszymi szczegółami technicznymi. Popatrzymy teraz na techniki i narzędzia pozwalające wykorzystać niektóre rzeczy, które poznaliśmy, aby zapewnić światowej klasy poziom wsparcia i ułatwiający cykl pracy.

Rozdział 12. Tożsamość i zaufane urządzenia

Sfederowane tożsamości są ważne, gdyż nie musimy przesyłać naszych haseł przez sieć. Pozwala to na łatwy dostęp do zasobów w sieciach i jednocześnie większe bezpieczeństwo. Co można ulepszyć? W tym rozdziale omawiamy typowe rozwiązania sfederowanej tożsamości i nowe sposoby jej wykorzystania.

Rozdział 13. Zarządzanie urządzeniami firmy Apple w przyszłości

Do tego miejsca każdy ma już zapewne dość i chce, aby autorzy zrobili podsumowanie. Rozumiemy to. Ale jeśli ktoś jeszcze czyta tę książkę, to tu znajdzie prognozy, które należy rozważyć, aby nasze wdrożenia były zabezpieczone przed przyszłymi zmianami.

Inne myślenie

W jakim stopniu możemy być szablonowi? Oczywiście w dużym. Istnieje jednak ważne pojęcie, o którym trzeba wspomnieć, a jest nim postawa. Apple wykuwa swoją własną ścieżkę w świecie IT. Wspólnie z takimi firmami, jak Amazon, Google i Microsoft, zajmuje miejsce w gronie najbogatszych firm, jakie kiedykolwiek istniały. I nie zamierza przez kolejnych 30 i więcej lat ulegać dogmatom panującym w branży IT. A przynajmniej tak zwykle przedstawia swoje perspektywy w branży.

Jak zobaczymy w rozdziale 1, firma Apple postępuje teraz z masowym zarządzaniem urządzeniami podobnie, jak to robiła od lat osiemdziesiątych XX wieku. Ekrany wyglądają podobnie, opcje wyglądają podobnie, czasami operując tymi samymi słowami. Ale ze względu na poufne dane zawarte w systemach i łatwość kradzieży tożsamości, znacznie większą wagę przykłada się do prywatności użytkownika. Urządzenia firmy Apple to nadal nie urządzenia Windows. Jednak współdzielą coraz większą bazę kodu, co prowadzi do bardziej zbliżonych technik zarządzania, niż kiedykolwiek wcześniej.

Najważniejszym, co trzeba wziąć pod uwagę, jest unikanie prób wtłoczenia urządzeń firmy Apple w przestarzałe tryby zarządzania informacjami, czyli to, czy potrafimy przyjąć stanowisko Apple w sprawie zarządzania. Jeśli ktoś nie jest gotowy, aby przyjąć postawę zarządzania na sposób proponowany przez Apple, może nie być gotowy na zarządzanie urządzeniami tej firmy.

O autorach

Charles Edge jest dyrektorem działu Marketplace w firmie Jamf. Ma 30 lat doświadczenia jako programista, administrator, architekt sieci, menedżer produktu i CTO. Jest autorem 20 książek i ponad 6000 postów na blogu na temat technologii. Pełnił również funkcję redaktora i współautora wielu publikacji. Często występuje w konferencjach branżowych na całym świecie, takich jak DefCon, BlackHat, LinuxWorld, the Apple Worldwide Developers Conference oraz w licznych wydarzeniach skoncentrowanych na rozwiązaniach firmy Apple. Jest również twórcą strony krypted.com i współgospodarzem podkastu MacAdmins.

Rich Trouton pracował jako administrator systemów i serwerów Macintosh przez ponad 20 lat i zajmował się obsługą Maców w wielu różnych środowiskach, w tym uniwersyteckich, rządowych, badań medycznych, reklamowych oraz przy projektowaniu oprogramowania dla przedsiębiorstw. Obecnie pracuje w firmie SAP, gdzie wraz z resztą zespołu Apple CoE zapewnia wsparcie dla społeczności użytkowników rozwiązań Apple i SAP.

O recenzencie technicznym

Ahmed Bakir jest autorem, wykładowcą i wynalazcą, koncentrującym się na technologiach iOS. Pracował przy ponad 30 projektach mobilnych, poczynając od doradzania start-upom po projektowanie apek dla firm z listy Fortune 500. W roku 2014 opublikował swoją pierwszą książkę, *Beginning iOS Media App Development*, po czym pojawiło się pierwsze wydanie *Program the Internet of Things with Swift for iOS* w roku 2016, oraz drugie wydanie w roku 2018. W roku 2015 został poproszony o opracowanie wykładów i nauczanie programowania dla iOS na UCSD. Obecnie buduje zadziwiające rzeczy w Tokio! Można go znaleźć online na stronie `devatelier.com`.

Rozdział 1

Ewolucja zarządzania urządzeniami firmy Apple

Dawno, dawno temu, w odległej krainie, istniał sobie w próżni Mac. Pozostawiony samemu sobie, gdzieś z boku głównego nurtu korporacji, w najlepszym przypadku przeoczony przez działy IT zorientowane na system operacyjny Windows, a w najgorszym zakwalifikowany do wycofania i usunięcia. W tamtych czasach powszechne było postrzeganie sieci Maców działającej jako silos, często z dedykowanym modemem kablowym do dostępu do Internetu, a czasem nawet z dedykowanym serwerem pocztowym w celu wspierania kreatywnych. I faktycznie, było to rozwiązanie prawie wyłącznie dla osób kreatywnych.

Wydawało się, że platforma umiera, gdyż sprzedaż Apple spadała, a oferta Microsoftu zdominowała rynki konsumenckie i korporacyjne. Z czasem zastosowanie sprzętu firmy Apple ograniczyło się do małych grup roboczych, z jednym wyjątkiem, który stanowiła edukacja.

Szkoły na całym świecie nadal korzystały z platformy firmy Apple w trudnych dla niej czasach. W tamtym okresie każdy, kto miał doświadczenie w zarządzaniu systemami Apple na większą skalę, prawie na pewno pracował w szkole lub na jakiejś uczelni. Wszystko to zaczęło się zmieniać wraz z pojawieniem się iPhone'a. Nagle przedsiębiorstwa zaczęły szukać porad dotyczących wdrażania dużej liczby urządzeń Apple, dyrektorzy IT pytali swoje działy, dlaczego nie wspierają nowego MacBooka Air prezesa, pracownicy niektórych szkół zaczęli przenosić się do dużych firm, a wymagania, z którymi musiano się mierzyć, zaczęły ulegać zmianom.

Im bardziej rzeczy się zmieniają, tym bardziej pozostają takie same, aczkolwiek nie do końca. Gdy firma Apple poprosiła mnie o zajęcie się aktualizacją wykładu i książki o usługach katalogowych, korzystaliśmy z systemu Mac OS X Server, aby przechowywać ustawienia związane z zarządzaniem, tożsamościami i autoryzacją w jednym miejscu: w Open Directory. Jednak większość chciała wykorzystywać tożsamości i autoryzacje przechowywane w innym katalogu (LDAP lub Active Directory). Wtedy wydawało się, że nikt już nie chciał zajmować się usługami katalogowymi i skupiano się na przejściu od zarządzania opartego na katalogach (Workgroup Manager) do MDM. Obecnie uczymy się głównie integracji rozwiązań MDM z różnymi zewnętrznymi dostawcami tożsamości (IdP). Najzabawniejszą częścią tej pracy jest próba zrozumienia – co będzie dalej?

—Arek Dreyer, Dreyer Network Consultants, autor kilku książek na temat systemów macOS i macOS Server

Powodów tej zmiany jest mniej więcej tyle samo, ilu jest fanów firmy Apple. Tej zmiany jednak nie można zakwestionować. Rozwój obecności firmy Apple w obszarze korporacyjnym i wzrost doprowadziły do szeregu pochodzących od niej innowacji. Historia zarządzania całkowicie się zmieniła wraz z pojawieniem się systemu Mac OS X, obecnie nazywanego macOS. Ale zaczęło się to znacznie wcześniej.

W tym rozdziale przyjrzymy się historii zarządzania – począwszy od średniowiecza, poprzez renesans, w którym wyłonił się system Mac OS X, odradzający się niczym feniks z popiołów systemu NeXT, aż do współczesnej ery zarządzania za pomocą systemów macOS i iOS. Rozpoczniemy od Apple II.

Klasyczny system operacyjny Maców

Apple II został wprowadzony w czerwcu 1977 roku i zmienił świat. To był tak naprawdę pierwszy komputer produkowany masowo, a zatem faktycznie dostępny. W tamtych czasach, jeśli na środowisko składał się więcej niż jeden komputer, zarządzanie urządzeniami obejmowało chodzenie od jednego do drugiego z dyskietkami używanymi do uruchamiania komputerów. Masowe zarządzanie urządzeniami stało się rzeczywistością znacznie, znacznie później.

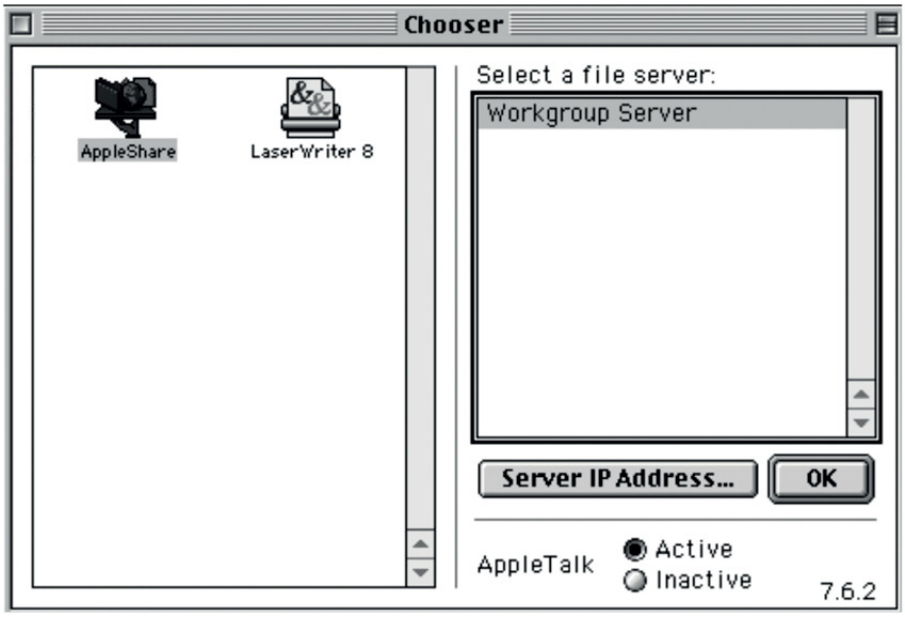
W 1984 roku został wprowadzony Macintosh, wyznaczając pierwszy szczebel wspinaczki do miejsca, w którym jesteśmy dzisiaj. Nie zamierzamy opisywać zarządzania urządzeniami firmy Apple na każdym etapie, począwszy od Apple II aż do dziś. Przede wszystkim dlatego, że niemożliwe byłoby znalezienie zbyt wielu osób, które potrafiłyby przypomnieć sobie fakty z tamtych czasów, zaś do połowy pierwszej dekady XXI wieku nie było zbytnio o czym mówić. Pomiędzy systemami operacyjnymi System 6 i Mac OS 9 zarządzanie komputerami Mac przez sieć zwykle opierało się na protokole sieciowym AppleTalk (który został wprowadzony w 1985 r. i zakończył swe istnienie na wersji 10.6 w 2009 r.), a nie na TCP/IP. Oprócz tego, że nie był on wspierany przez żadną inną platformę, metody komunikacji sieciowej wykorzystywane w protokole AppleTalk przez wielu były postrzegane jako niepotrzebnie „przegadane". Ta kolejna charakterystyczna dla Apple cecha oraz trudność w zarządzaniu urządzeniami Apple za pomocą narzędzi do zarządzania firmy Microsoft doprowadziły do opinii, którą wielu kierowników ze starych czasów IT podtrzymuje do dziś: „Urządzenia firmy Apple nie działają zbyt dobrze w sieciach korporacyjnych".

Protokoły sieciowe

Wciąż pojawiają się pytania, czy urządzenia firmy Apple mogą powodować problemy w nowoczesnych sieciach. Najkrótsza odpowiedź brzmi: jeśli urządzenie firmy Apple może uszkodzić sieć, to ta sieć jest do niczego. Możemy zatem zdementować tę plotkę. Ale prawdą jest, że kiedyś urządzenia firmy Apple mogły tak rozprowadzać ruch protokołu AppleTalk w sieci, że powodowało to burze pakietów lub inne problemy. Jednak to samo mogło się dziać przy korzystaniu z protokołów IPX lub NetBIOS, wydanych po raz pierwszy w 1983 roku.

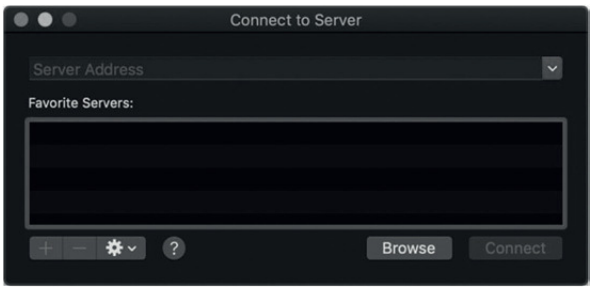
Mechanizmy sieciowe, w postaci protokołu AppleNet, zostały pierwotnie wprowadzone w komputerze Lisa w 1983 roku. Protokół AppleNet został zastąpiony przez protokół AppleTalk w 1985 r., zaś firma Apple ostatecznie porzuciła obsługę AppleTalk w 2009 r., chociaż od czasu wprowadzenia systemu Mac OS X nie był on już używany zbyt często. Urządzenia Apple były w stanie podłączyć się do sieci TCP/IP w 1988 r. po wprowadzeniu MacTCP, umożliwiając dostęp do większości typów urządzeń, z którymi może połączyć się komputer Mac.

Przed systemem Mac OS X narzędziem używanym do łączenia się z sieciowymi serwerami plików i drukarkami był Chooser. Jak pokazano na rysunku 1.1, Chooser był w stanie przeskanować sieć w poszukiwaniu urządzeń AppleTalk i wyświetlić je, umożliwiając wybór urządzenia do zamontowania. Ponieważ sieci się rozrastały, a protokoły wykrywania nie zawsze znajdowały urządzenia w sieci, można było również zdefiniować adres IP, z którym chcieliśmy się połączyć, jeśli host nie pojawił się na liście – było to przydatne również podczas łączenia się z innymi sieciami LAN lub przez WAN.



Rysunek 1.1 *Chooser z lat 90*

Wraz z pojawieniem się w roku 2001 systemu Mac OS X, Chooser został zastąpiony opcją Connect to Server (Łączenie z serwerem) (rysunek 1.2), która zawierała wszystko, co było potrzebne do połączenia się z serwerami plików, WebDAV i FTP, dostępnymi w większości standardowych środowisk TCP/IP. W 2002 roku firma Apple dodała do systemu Mac OS X protokół Rendezvous, umożliwiając komputerom Mac znajdowanie urządzeń i usług przy użyciu TCP/IP. Ta niewymagająca konfiguracji technologia, której nazwa została zmieniona w 2005 r. na Bonjour, wykorzystuje mDNS (multicast Domain Name System) do lokalizowania i łączenia się z urządzeniami lub usługami w sieciach na tym samym poziomie wygody, jaki oferował protokół AppleTalk.



Rysunek 1.2 *Okno dialogowe Connect to Server*

Czasami obawy o urządzenia firmy Apple w sieciach korporacyjnych były słuszne. Podczas masowych wdrożeń systemu Windows 95, a następnie Windows 98, wiele środowisk nadal korzystało z sieci Novell lub „na wszelki wypadek" pozostawiano na komputerach włączoną obsługę protokołu IPX/SPX. Często były również włączone protokoły NetBIOS, a później NetBEUI, powodując, że przez starsze węzły przechodził duży ruch. Dodanie AppleTalk do tej mieszanki mogło generować zbyt duży ruch, jak na możliwości sprzętu sieciowego z tamtej epoki. Na szczęście AppleTalk mamy już za sobą. Ponadto począwszy od początku tego wieku wiele urządzeń sieciowych zaczęło być wyposażanych w Spanning Tree Protocol (STP). Komputery Mac mogły mieć problemy z protokołem STP, zwłaszcza jeśli nie został wyłączony protokół AppleTalk. Jednak malejąca potrzeba używania protokołu AppleTalk w systemach Mac OS X oznaczała, że wyłączanie AppleTalk w sieciach było dobrą praktyką już w połowie pierwszej dekady obecnego wieku, chyba że konieczne było zachowanie wstecznej kompatybilności ze starym sprzętem.

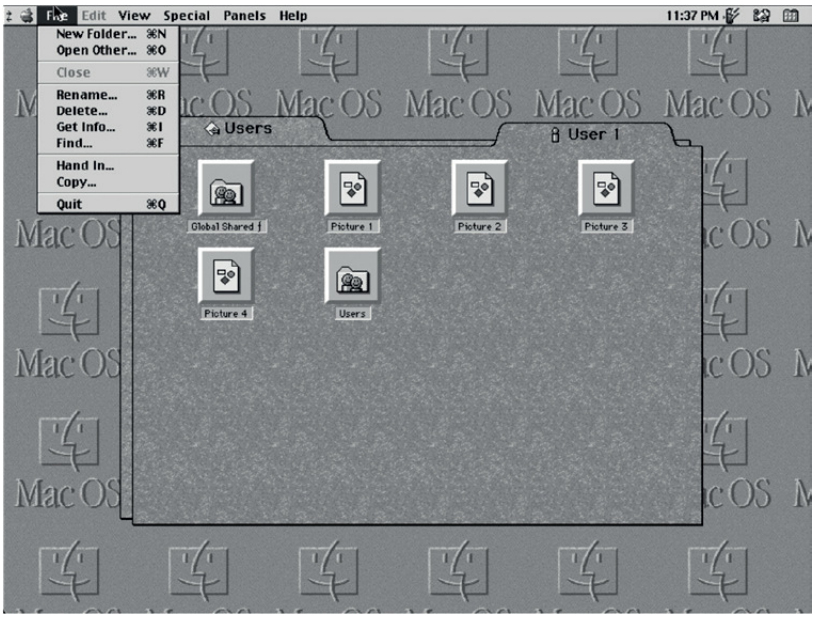
Biorąc pod uwagę, że na platformie istniała łączność sieciowa, większe środowiska naturalnie szukały możliwości zarządzania urządzeniami poprzez tę sieć.

Wczesne zarządzanie urządzeniami

Jednak wtedy urządzenia nie były zarządzane tak misternie. Nie tylko protokoły sieciowe były inne, ale także znacząco odmienne były stosy technologiczne. Nie było tak wielu urządzeń zarządzanych z centralnej lokalizacji i nie mieliśmy trzydziesto- czy czterdziestoletniej wiedzy na temat tego, jak ułatwiać życie naszym współpracownikom, studentom, a nawet sobie samym. Być może zarządzaliśmy rozszerzeniami (jako Desk

Accesories) za pomocą narzędzia Font/DA Mover lub launcherów. Pozwalało to na instalowanie czcionek i takich rzeczy, jak wygaszacze ekranu – jednak narzędzia firmy Apple do scentralizowanego zarządzania ustawieniami komputerów Macintosh w zasadzie nie były dostępne aż do lat 90.

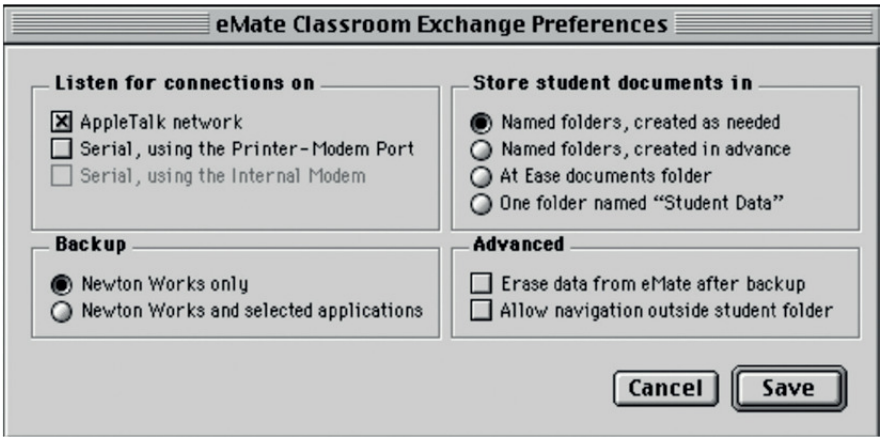
Następnie firma Apple wprowadziła At Ease. Było to alternatywne środowisko graficzne wydane w 1991 r. dla System 7, które oferowało uproszczone środowisko graficzne dla wielu użytkowników w celu korzystania i udostępniania plików – czyli funkcjonalność, która nie była w tym czasie w żaden inny sposób obsługiwana na komputerach Mac. W miarę ewolucji środowiska At Ease firma Apple wydała również At Ease for Workgroups. To nowe narzędzie oferowało możliwości konfiguracji klienta i ograniczony tryb programu Finder, a także folder domowy, który można było przechowywać na serwerze AppleShare IP, zaś komputer eMate z narzędziem Hand In umożliwiał przekazywanie studentom prac domowych na zajęciach (rysunek 1.3). Ten ograniczony tryb programu Finder rozwinął się później do postaci środowiska wieloużytkownikowego systemu operacyjnego w Mac OS 9 i narzędzia Simple Finder, które jest nadal obecne we współczesnych systemach macOS.



Rysunek 1.3 *Użycie Hand In... do przekazywania pracy domowej w zarządzanym środowisku*

Oto kilka ważnych rzeczy, o których należy pamiętać w miarę upływu lat:

- W pewnym momencie At Ease było ujednoliconym narzędziem do zarządzania współużytkowanymi plikami, drukarkami, ustawieniami i urządzeniami mobilnymi (Newton).
- At Ease sprawiało pewne pozory trybu wielu użytkowników, ale ówczesny system operacyjny komputerów Mac nie interpretował tego tak, jak dzieje się to obecnie.
- Wiele z filozofii, które można znaleźć w At Ease, jest wciąż takich samych, mimo że ich implementowanie na urządzeniach jest teraz zupełnie inne. Jest tak z powodu przejścia z AppleTalk na Ethernet, a następnie na sieć bezprzewodową oraz przyjęcia założenia, że urządzenia nie są już włączone do sieci lokalnej (LAN).
- eMate (rysunek 1.4) był używany do wymiany danych z innymi urządzeniami, w tym Newton (w przypadku korzystania z Apple Newton Works), co czyni go przodkiem Apple Classroom (aczkolwiek przodkiem mniej bogatym w funkcje).



Rysunek 1.4 *Ustawienia zarządzania eMate są podobne do ustawień Classroom*

At Ease nie rozwiązywało każdego problemu w każdym przypadku użycia. Kolejnym ważnym wydarzeniem w tej epoce była pierwsza fala rozwiązań pochodzących od zewnętrznych firm do zarządzania urządzeniami. W sierpniu 1991 roku (w tym samym roku, w którym narodził się Internet), na targach Macworld w Bostonie został przedstawiony netOctopus. To zapoczątkowało erę narzędzi zewnętrznych firm, które umożliwiały organizacjom zarządzanie urządzeniami firmy Apple. Do 1993 roku, gdy wydano

Filewave, firma Apple pozwalała, a nawet aktywnie wspierała myślenie, jak umieszczać takie mechanizmy w urządzeniach Mac, co było początkiem scentralizowanego zarządzania i kontroli. To samo działo się w systemie Windows, gdzie można było z centralnej lokalizacji edytować pliki .ini. Można było dostrzec również ewolucję plików .zap i podobnych formatów (obecnie pliki .mst), które będą mogły być dystrybuowane z centralnej lokalizacji w nadchodzącej erze systemu Windows 95.

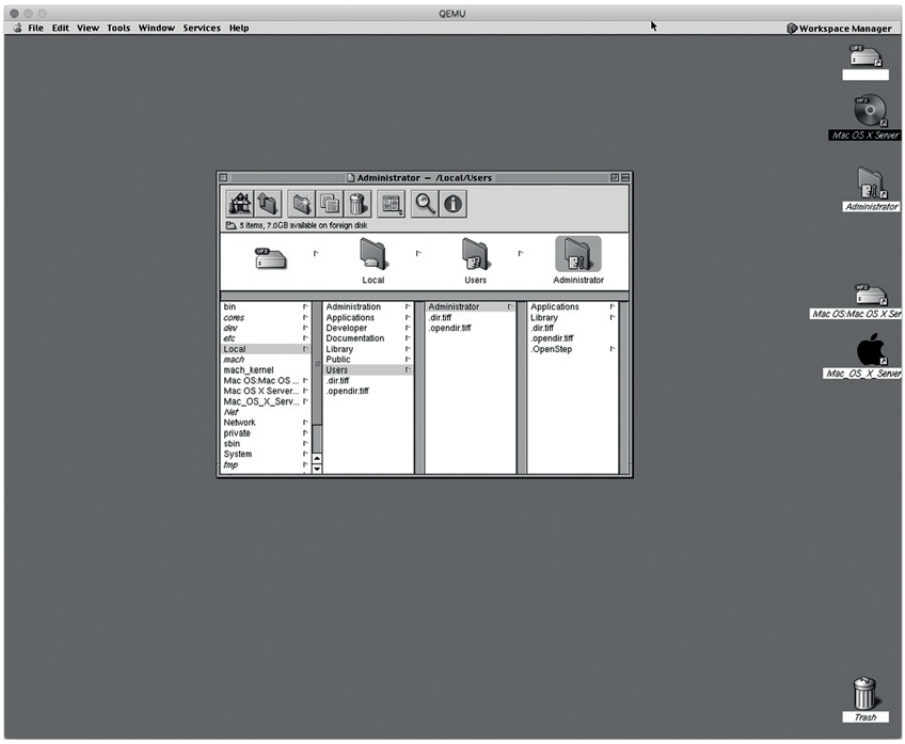
Następnym dużym produktem zewnętrznego podmiotu, który pojawił się na rynku, było DAVE firmy Thursby Software – narzędzie do udostępniania plików i drukarek dla Maców, wypełniające lukę w stosunku do udziałów SMB/CIFS znanych z serwerów Windows. Microsoft oferował serwer AFP o nazwie File Sharing Services for Mac, ale nigdy nie dorównał on temu, czego oczekiwała większość organizacji. Wprowadzenie oprogramowania DAVE w 1996 roku umożliwiło Macom w środowiskach skoncentrowanych wokół produktów firmy Microsoft na łączenie się z serwerami plików SMB i uzyskiwanie dostępu do nich, co z kolei oznaczało, że komputery Mac nie potrzebowały własnych serwerów plików specyficznych dla danej platformy do wykonywania użytecznych zadań. Thursby za pomocą ADmitMac pomógł również wypełnić lukę w obszarze łączenia użytkowników z Active Directory, co umożliwiło komputerom Mac łączenie się z domeną Active Directory i działanie jak stacje robocze Windows.

Komputery tej epoki pozostawiały wiele do życzenia. Macintosh II, Macintosh LC, Macintosh Portable, PowerBook, Quadra, Performa i Centris były przeważnie w mniejszości w organizacjach, które w tym czasie potrzebowały scentralizowanego zarządzania w wyniku inwazji, która była jedną z najważniejszych rewolucji technologicznych w historii, czyli ery komputerów PC. Ale wszystko to przygotowywało się do zmiany. Coś się szykowało.

NeXT

Steve Jobs opuścił firmę Apple w 1985 roku i założył swoją następną firmę, trafnie nazwaną NeXT. Pierwsze komputery NeXT pojawiły się w sprzedaży w 1988 roku. Posiadały system operacyjny NeXTStep, który stał się rdzeniem tego, co później przekształciło się w system Mac OS X, gdy Steve Jobs powrócił do Apple. Z tego powodu ekosystem zarządzania systemu NeXT nadał ton zarządzaniu urządzeniami Mac na następne 18 lat.

Najważniejszą rzeczą, jaka wydarzyła się na komputerze NeXT, było to, że została na nim udostępniona przez Tima Berners-Lee pierwsza strona internetowa. Miało to miejsce 6 sierpnia 1991 r. w Europejskiej Organizacji Badań Jądrowych CERN. Aha, to na NeXT powstał także Doom – co wprowadziło nas w zupełnie nową erę gier. Gdy Steve Jobs powrócił do Apple w 1997 r., technologie stacji roboczych NeXT dojrzały na tyle, że firma Apple mogła zacząć zastępować Mac OS 9 systemem Mac OS X (który później wyewoluował w macOS). NeXT miał wiele oczywistych podobieństw do Maców, co widać na rysunku 1.5.



Rysunek 1.5 *NeXT (znany także jako Inbetween)*

W kwestii koncepcji zarządzania urządzeniami, od firmy NeXT pochodzi kilka ważnych rzeczy, które później miały wpływ na komputery Mac, a następnie system iOS. Najważniejsza z nich to obiektowa natura systemu NeXTStep, a druga to środowisko programistyczne. Jak na ironię, wywodząca się z systemu Unix natura OpenStep jest tym, co zaprowadziło komputery Mac tak daleko w tak krótkim czasie. „Otwarte"

komponenty systemu operacyjnego są jednak aktywnie usuwane, ponieważ eliminowane są duże porcje otwartego kodu źródłowego dla urządzeń Mac. Mimo tego, Darwin, Xcode i części systemu iOS są nadal hostowane i regularnie aktualizowane na `opensource.apple.com`, zaś Webkit i Swift to udane projekty open source pochodzące od firmy Apple. Właścicielem licencji na nie jest jednak firma Apple i wydaje się, że usuwa ona komponenty, z którymi mogą wiązać się w przyszłości konsekwencje prawne.

Z komputerów NeXT pochodzą również pewne technologie, takie jak typ pliku „lista właściwości", które stanowią podstawę wszystkich nowoczesnych metod zarządzania ustawieniami na urządzeniach Mac. Po części z NeXT pochodzi również Objective-C, jądro Mach oraz Dock. Dzięki niemu powstał także Electronic AppWrapper (poprzednik App Store), Mail, Chess.app, TextEdit i, co najważniejsze, Workspace Manager, który wyglądał trochę jak Finder z systemu Mac OS 9, a później stał się programem Finder dla systemu Mac OS X.

Inna ważna i krytyczna część ewolucji komputerów Mac również rozpoczęła się w erze maszyn NeXT. W 1991 roku NeXT zaczął przechodzić na procesory 80486. Do tego momentu nie istniała współpraca między firmami Apple i Intel. Ale przejście NeXT na architekturę x86 (Marklar) zapoczątkowało erę partnerstwa z firmą Intel, tym bardziej, gdy firma Apple nabyła NeXT i zaczęła planować wprowadzenie nowego systemu operacyjnego, który istnieje do dziś (chociaż w erze Rhapsody był w nim kiepski port chipsetu PowerPC). Jednak przejście na architekturę opartą na x86 nie tylko ułatwiło firmie Apple kupowanie gotowych chipów od firmy Intel; dało to lepszą wirtualizację systemu Windows na urządzeniach Mac i skłoniło dyrektorów IT do zastanowienia się i dostrzeżenia prawdziwego potencjału firmy Apple oraz tego, iż – być może – można zaufać jej urządzeniom i użyć ich w swoich sieciach.

Mac + Unix = Mac OS X

Firma Apple rozpoczęła integrację technologii NeXT z nowym systemem operacyjnym, używając nazwy kodowej Rhapsody. Z tej integracji pochodzi wiele narzędzi, których nadal używamy. Pojawienie się systemu Mac OS X wniosło ze sobą model zarządzania podobny do systemu Unix, zastępując tym samym model jednego użytkownika wykorzystywany w systemach Mac OS 9 i wcześniejszych. Mac OS X przyniósł prawdziwy tryb wielu użytkowników i początek tego, co przekształciło się w zasady zarządzania.

Nowe zarządzanie oparte na zasadach pojawiło się w postaci Managed Preferences lub MCX (Managed Computing for X). Są one dostępne w /System/Library/CoreServices/ManagedClient.app. MCX umożliwiał administratorom wstępne ustawianie grup preferencji lub kontrolowanie ustawień stosowanych w tych kluczach, podobnie jak wielu administratorów w świecie Windows było przyzwyczajonych do korzystania z rejestru w systemie Windows oraz analogicznie do blokowania dostępu do paneli sterowania w środowisku At Ease. Przez wiele lat Managed Preferences było głównym sposobem kontrolowania ustawień na urządzeniach Mac, co stworzyło mechanizm, który późniejsze narzędzia mogły wykorzystać, aby zaoferować scentralizowane zarządzanie ustawieniami na komputerach Mac.

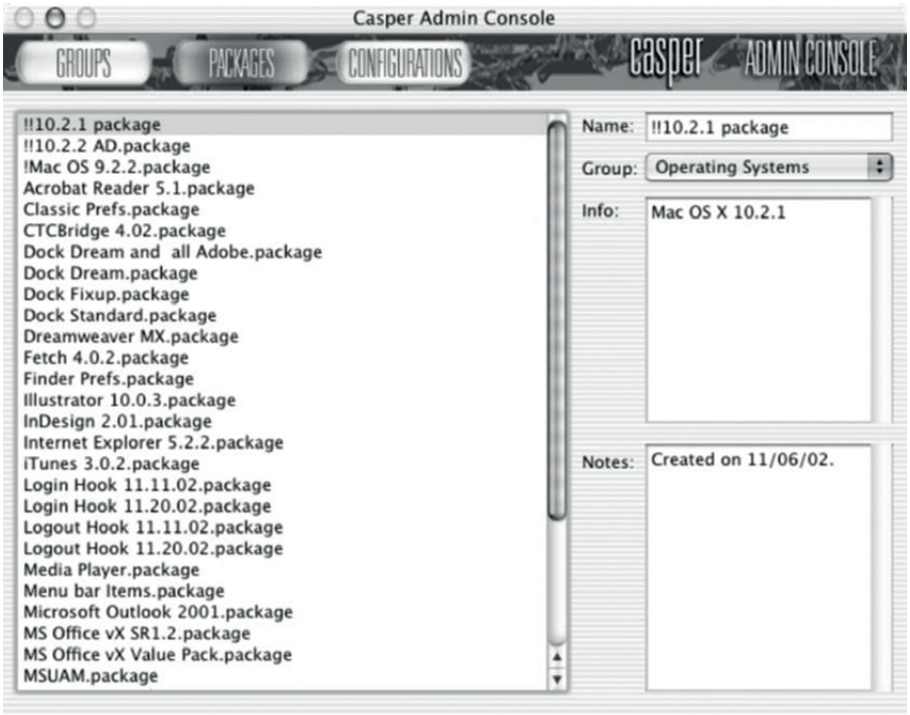
Z kontrolą zasad dostępną na komputerze z wieloma użytkownikami, Mac kontynuował pochód w kierunku pełnoprawnego obywatela w korporacjach, dodając po drodze flagi do polecenia `dsconfigad` używanego do łączenia się z Active Directory oraz integrację z DFS. Dodatkowo, standardowa implementacja LDAP oraz możliwość natywnego łączenia się z udziałami plikowymi zostały wzmocnione dzięki możliwości zarządzania nimi ze scentralizowanej lokalizacji.

> *Kierunek mojego życia zawodowego zmienił się, gdy zdaliśmy sobie sprawę, że chociaż firma Apple zaoferowała świetne narzędzie At Ease, możemy jednak pójść dalej. Apple zawsze oferowała klientom produkt, który może wykonywać zadania w szczególnych okolicznościach, ale często oczekuje, aby wkraczali zewnętrzni programiści i zajmowali się przypadkami użycia, które nie były dokładnie tym, co mieli na myśli. Zaoszczędziliśmy klientom czas i zapewniliśmy lepsze wrażenia z korzystania z netOctopus. Było to całkiem podobne do tego, jak współczesne wdrożenia wykorzystują obecnie jeden z wielu produktów zewnętrznych firm, zamiast Profile Manager firmy Apple.*
>
> *— Martin Bestman, założyciel netOctopus*

Wkrótce po powrocie Steve'a Jobsa do firmy Apple, w 1998 roku został wprowadzony iMac Bondi Blue. Doprowadziło to do eksplozji liczby zarządzanych urządzeń w większych środowiskach. Administratorzy komputerów Mac wkrótce zaczęli wykorzystywać drugą dużą falę zewnętrznych rozwiązań do zarządzania urządzeniami Apple. Były one zbudowane na frameworkach przeniesionych na komputery Mac z maszyn NeXT,

które wciąż narzucały sposoby, jakimi pewne rzeczy pojawiały się na urządzeniach Mac, ale także poszły dalej i pozwalały na wprowadzanie pakietów oprogramowania (.pkgs) oraz centralnie zarządzanych plików preferencji. Po kilku latach stosowania tych technik, w 2002 roku pojawił się pierwszy duży projekt open source do zarządzania komputerami Mac – Radmind pochodzący z University of Michigan. Wprowadzono również Casper Suite 1.0, który wyewoluował w to, co jest teraz znane jako Jamf Pro.

W tym momencie zarządzanie urządzeniami polegało głównie na przypisywaniu pakietów lub podobnych konstrukcji danych do urządzeń, jak widać na rysunku 1.6, który przedstawia ekran pakietów programu Casper 1.0.



Rysunek 1.6 *Konsola administracyjna programu Casper pochodząca z podręcznika użytkownika Casper 1.0*

Działało to na zasadzie przypisywania agenta (lub często demona) do urządzenia. Agent ten następnie komunikował się z centralnym serwerem, aby pobierać polecenia lub konfiguracje dla urządzeń. W celu wprowadzania zmian w systemie Filewave

i Radmind przyjęły podejście oparte na plikach, polegające na ich umieszczaniu w określonym miejscu w systemie plików. Zamiast tego do wprowadzania zmian w urządzeniach NetOctopus i Jamf wykorzystały natywne technologie firmy Apple, w tym pakiety oprogramowania (pkgs).

Później firma Apple zaczęła się przyglądać technologii bez agentów, z którą zapoznamy się w dalszej części tego rozdziału, gdy zaczniemy mówić o MDM. Jednak pakiety mogły (i nadal mogą) być używane do konfigurowania ustawień, instalowania oprogramowania i wykonywania innych zadań. Sam PackageMaker został usunięty z systemu operacyjnego w 2015 roku, chociaż w razie potrzeby nadal można go zainstalować za pomocą Xcode.

> *Gdy wydaliśmy pierwszą wersję FileWave w 1992 roku, zarządzanie punktami końcowymi było w powijakach i bardzo fragmentaryczne. Większość narzędzi dostępnych na rynku była specjalistycznymi, częściowymi rozwiązaniami (jak stare narzędzie Timbuktu do zdalnego sterowania). FileWave być może jest jedynym nadal używanym narzędziem, które pochodzi z tamtych czasów i myślę, że powodem tego jest jego ciągły rozwój. Rozrastaliśmy się wraz z Apple, aby obsługiwać nowoczesne aplikacje, MDM i każdą nową wersję systemu operacyjnego, ale dodaliśmy również zarządzanie systemami operacyjnymi Windows i Google, uznając, że bardzo niewiele organizacji może pozwolić sobie na luksus ograniczenia punktów końcowych do jednego systemu operacyjnego.*
>
> *—Nurdan Eris, prezes zarządu Filewave*

Do 2008 r. rozumienie w społeczności dojrzało do tego stopnia, że zarządzanie oparte na agentach dorównywało już temu, które było dostępne dla systemów Windows przy użyciu narzędzi, takich jak Altiris. W rzeczywistości Altiris i inne rozwiązania do zarządzania systemami Windows zawierały agenty dla Maców. Narzędzia kładące większy nacisk na markę Apple, takie jak FileWave, Jamf i LANrev, mogą zarządzać Macami jako pełnoprawnymi obywatelami w sieciach korporacyjnych.

W 2008 roku Greg Neagle rozpoczął pracę nad open source'owym agentem do zarządzania urządzeniami Mac o nazwie Munki. Pierwsze publiczne zatwierdzenia kodu miały miejsce na początku 2009 roku, otwierając drogę dla open source'owych alternatyw do zarządzania Macami. Wykorzystanie Munki rosło na przestrzeni lat, powodując,

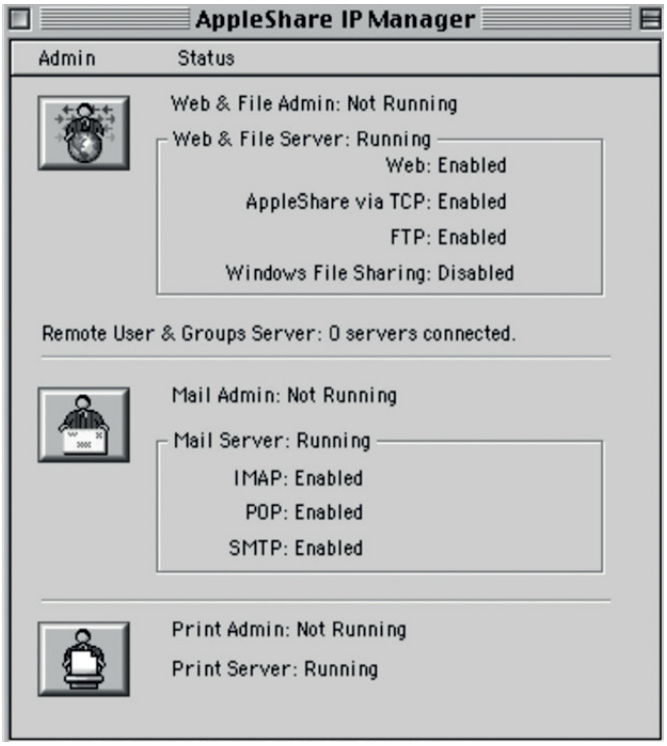
że zarządzanie stało się dostępne dla wielu środowisk, które wcześniej nie mogły sobie na to pozwolić lub które potrzebowały bardziej konfigurowalnych sposobów postępowania niż te, które były dostępne w rozwiązaniach innych firm. Wraz z pojawieniem się MDM, które omówimy w dalszej części tego rozdziału, Munki odegrał również kluczową rolę w dostarczaniu opartych na agentach funkcjonalności dla środowisk, które również używały MDM. Ale co najważniejsze, Munki wprowadził do administrowania urządzeniami Apple styl bardzo zbliżony do DevOps, umożliwiając wielu administratorom zarządzanie Macami w taki sam sposób, w jaki zarządzają kodem.

W dzisiejszych czasach mamy skłonność do myślania o zarządzaniu jako działaniu opartym na zasadach w celu osiągnięcia pewnego poziomu idempotencji na urządzeniach firmy Apple. Inaczej mówiąc, chodzi o znany stan, w którym naszym zdaniem znajduje się urządzenie. Jednak pierwsze zadania zarządzania polegały na kontrolowaniu wyglądu systemu i wrażeniach, jakie użytkownik mógł uzyskiwać podczas dostępu do aplikacji i potrzebnych danych. W pewnym sensie zagubiliśmy się, szukając sposobów na ułatwienie naszej pracy, ale od czasu pojawienia się iOS zaczęliśmy na nowo odkrywać ten cel, jakim jest poprawa komfortu użytkownika, a nie kontrolowanie go. Im mniej można wprowadzić zmian w systemie operacyjnym, tym lepiej wiemy, w jakim stanie znajduje się urządzenie. Dlatego, chociaż nadal istnieje luka w znajomości dokładnego stanu urządzenia, mamy obecnie dobry ekosystem, który pozwala nam egzekwować zasady, nie niszcząc wrażeń, jakie firma Apple wypracowała dla urządzeń.

Serwery

Firma Apple, począwszy od 1987 roku aż do dziś, ma w swojej ofercie produkty serwerowe. Kilka opcji związanych z udostępnianiem plików i drukarek posiadał już At Ease. Ale stary serwer AppleShare (później nazywany AppleShare IP, pokazany na rysunku 1.7) był używany głównie do dostarczania zasobów sieciowych dla Maców w latach 1986-2000, przy czym główną oferowaną usługą było udostępnianie plików. Firma Apple miała również swój udział w początkowym etapie rozwoju sprzętu serwerowego w postaci Apple Network Server, który był serwerem opartym na PowerPC, sprzedawanym w latach 1996–1997 z systemem operacyjnym AIX. AppleShare IP funkcjonował aż do wersji 9.2.2 systemu Mac OS. W erze poprzedzającej, gdy na przykład wymagaliśmy uwierzytelniania SMTP, AppleShare IP mógł być z łatwością używany

do wszystkiego, począwszy od usług udostępniania plików po usługi pocztowe. Starsza Quadra zapewniła świetny serwer pocztowy, dzięki czemu nasze firmy mogły przestać płacić dostawcom usług internetowych za dziwaczne adresy e-mail i zdobyć własną domenę już w 1999 roku!



Rysunek 1.7 *Wczesne serwery firmy Apple były dość łatwe w zarządzaniu*

Tymczasem usługi sieciowe były głównym wymaganiem w systemach NeXTStep i OpenStep. Założenia systemu UNIX umożliwiały kompilowanie wielu pakietów oprogramowania o otwartym kodzie źródłowym. Dzięki temu, jak wspomniano wcześniej w tym rozdziale, pierwszy serwer WWW był hostowany na komputerze NeXTcube. Po przejściu do firmy Apple, AppleShare IP i usługi NeXT zbliżyły się do siebie pod względem wyglądu i działania, a później zostały przekształcone w Mac OS X Server.

Kilka pierwszych wydań systemu Mac OS X Server oznaczało konieczność przyśpieszonej nauki dla wielu typowych administratorów urządzeń firmy Apple i w rzeczywistości spowodowało zmianę pokoleniową w zarządzaniu systemami. W 2000 i 2002 roku

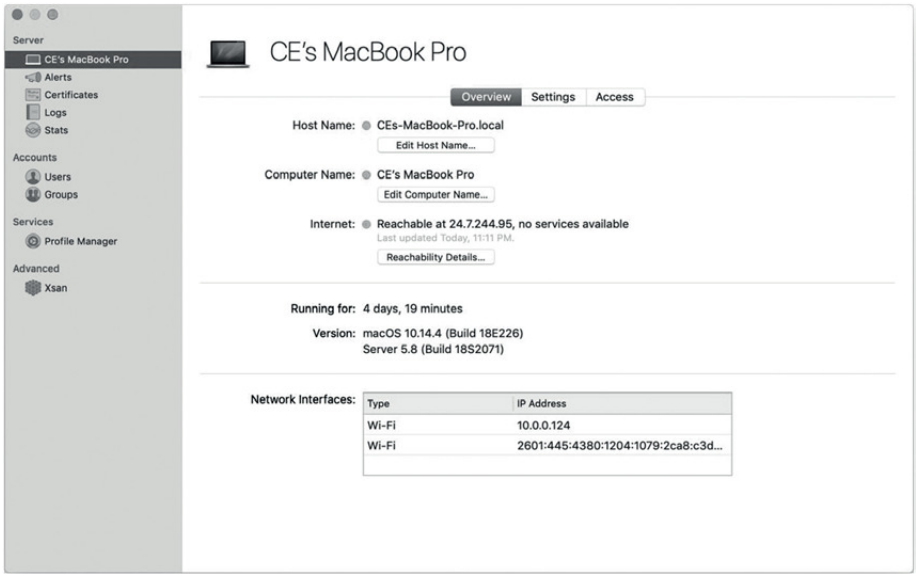
John Welch napisał książki, które pomogły administratorom nabrać tempa. W 2002 roku został wprowadzony Xserve, a w 2003 roku – Xserve RAID. Zajęło trochę czasu, by wokół tych produktów zaczęła formować się społeczność. Nieżyjący już Michael Bartosh opracował przełomowe dzieło *Essential Mac OS XPanther Server Administration*, wydane przez O'Reilly Media w 2005 roku. Charles Edge (współautor tej książki) w 2006 roku wydał *The Mac Tiger Server Little Black Book*.

Aż do tego momentu firma Apple nigdy publicznie nie potwierdziła, że firmy lub przedsiębiorstwa używają jej urządzeń, zatem pojawienie się reklamy Xserve było pierwszym ogłoszeniem tego faktu. Firma Apple kontynuowała ulepszanie produktu o nowe usługi do roku 2009, gdy wydano system Mac OS X Server 10.6. W tym momencie firma Apple miała włączone do swojego produktu większość usług niezbędnych do prowadzenia standardowego działu IT, w tym serwer Web (w postaci Apache), pocztę, oprogramowanie do pracy grupowej, DHCP, DNS, usługi katalogowe, udostępnianie plików, a nawet usługi webowe i wiki. Istniały również usługi dotyczące nietypowych zastosowań, takie jak Podcast Producer do automatyzacji przepływów związanych z wideo i treściami, Xsan, czyli klastrowy system plików, zaś w 2009 roku została nawet zakupiona firma Artbox, której produkt został przemianowany na Final Cut Server.

Był to jednak punkt zwrotny. Jak widać w tabeli 1.1 (na stronach 18-19), mniej więcej w tym samym czasie firma Apple pracowała nad iPadem, wydanym w 2010 roku (chociaż zapewne pierwszą iteracją był Knowledge Navigator, którego koncepcja powstała w 1987 roku). Wybuchowy wzrost sprzedaży iPhone'a doprowadził do podjęcia trudnych decyzji. Firma Apple nie potrzebowała już kontrolować całego ekosystemu za pomocą swojego produktu serwerowego i zamiast tego zaczęła przenosić jak najwięcej zespołów do pracy nad obszarami o wyższych marżach, zmniejszając koncentrację na obszarach odciągających uwagę wartościowych programistów próbujących rozwiązywać wiele problemów, które już dawno zostały lepiej rozwiązane przez innych dostawców.

W 2009 roku została zakończona produkcja Xserve RAID, a w następnym roku zniknął Xserve. Przez kolejnych kilka lat od serwera powoli były odłączane kolejne usługi. Obecnie produkt Mac OS X Server został zmigrowany do zwykłej aplikacji dostępnej w sklepie App Store, jak widać na rysunku 1.8. Aktualnie, macOS Server ma uruchamiać narzędzie Profile Manager i działać jako kontroler metadanych dla Xsan, klastrowego systemu plików firmy Apple. Produkty, które kiedyś konkurowały z platformą,

są obecnie akceptowane przez większość społeczności. Zazwyczaj dzieje się tak dlatego, że firma Apple pozostawiła firmie Microsoft lub systemom opartym na systemie Linux pewne obszary rynku dotyczące dostarczania funkcjonalności, które są często unikalne dla poszczególnych firm i nie mają na celu poprawiania wrażeń użytkowników końcowych.



Rysunek 1.8 *Uproszczona aplikacja macOS Server*

Obecnie tworzenie produktów serwerowych, które starają się robić wszystko dla wszystkich, dla wielu osób w firmie Apple wydaje się być odległym wspomnieniem. Natomiast nadal zwracana jest uwaga na możliwość poprawy warunków działania urządzeń marki Apple. Widać to po wbudowanej w macOS usłudze Caching (przeniesionej tam z macOS Server) i po tym, że niektóre produkty, takie jak Apple Remote Desktop, są wciąż całe i zdrowe.

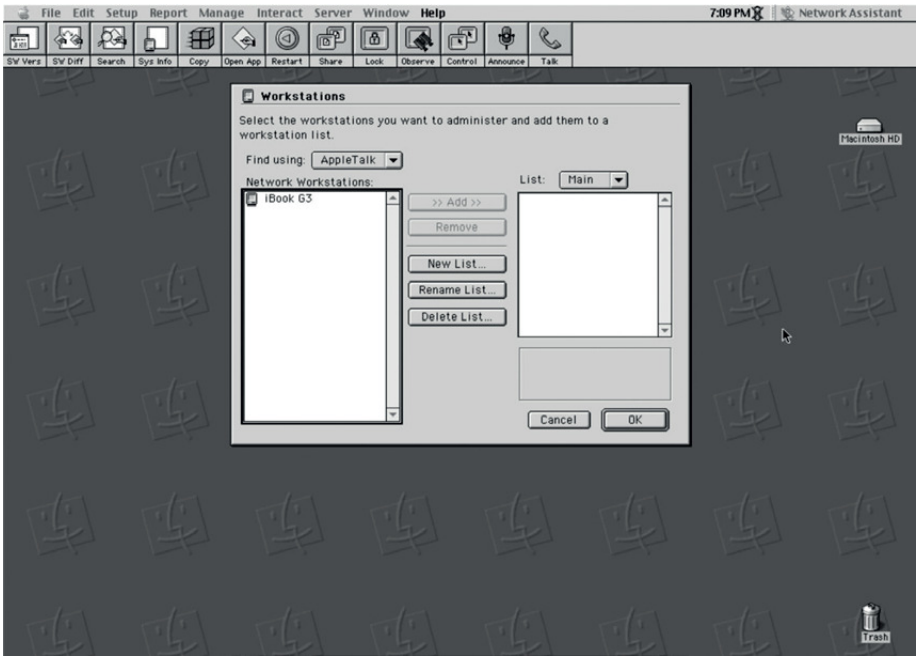
Tabela 1.1 *macOS Server wspiera teraz znacznie mniej usług niż kiedyś*

10.3	10.4	10.5	10.6	10.7	10.8	10.9	10.1	10.11	10.12	10.13
2003	**2005**	**2007**	**2009**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**
15	19	24	24	22	18	21	21	21	21	14
AFP	AFP	AFP	AFP	AFP	AFP	AFP	AFP	AFP	AFP	
NFS	NFS	NFS	NFS	NFS	NFS	NFS	NFS	NFS	NFS	
Web	Web	Web	Web	Web	Websites	Websites	Websites	Websites	Websites	Websites
Open Directory	Open Directory	Open Directory	Open Directory	Open Directory	Open Directory	Open Directory	Open Directory	Open Directory	Open Directory	Open Directory
NetBoot	NetBoot	NetBoot	NetBoot	NetBoot	NetInstall	NetInstall	NetInstall	NetInstall	NetInstall	NetInstall
FTP	FTP	FTP	FTP	FTP	FTP	FTP	FTP	FTP	FTP	
Windows	Windows	SMB	SMB	SMB	SMB	SMB	SMB	SMB	SMB	
Mail	Mail	Mail	Mail	Mail	Mail	Mail	Mail	Mail	Mail	Mail
DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
DHCP	DHCP	DHCP	DHCP	DHCP		DHCP	DHCP	DHCP	DHCP	DHCP
VPN	VPN	VPN	VPN	VPN	VPN	VPN	VPN	VPN	VPN	VPN
	Software Updates	Software Updates	Software Updates	Software Updates	Software Updates	Software Updates	Software Updates	Software Updates	Software Updates	Software Update
	iChat	iChat	iChat	iChat	Messages	Messages	Messages	Messages	Messages	Messages
		iCal	iCal	iCal	Calendar	Calendar	Calendar	Calendar	Calendar	Calendar
		Wiki	Wiki	Wiki	Wiki	Wiki	Wiki	Wiki	Wiki	Wiki
			Address Book	Address Book	Contacts	Contacts	Contacts	Contacts	Contacts	Contacts

10.3	10.4	10.5	10.6	10.7	10.8	10.9	10.1	10.11	10.12	10.13
2003	**2005**	**2007**	**2009**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**
				Time Machine	Time Machine	Time Machine	Time Machine	Time Machine	Time Machine	
				Profile Manager	Profile Manager	Profile Manager	Profile Manager	Profile Manager	Profile Manager	Profile Manager
					Xsan	Xsan	Xsan	Xsan	Xsan	Xsan
						Caching	Caching	Caching	Caching	
						Xcode	Xcode	Xcode	Xcode	
	Web Objects	Web Objects								
Application Server	Application Server	Tomcat	Tomcat							
Print	Print	Print	Print							
QTSS	QTSS	QTSS	QTSS							
NAT	NAT	NAT	NAT	NAT						
	Xgrid	Xgrid	Xgrid	Xgrid						
		RADIUS	RADIUS	RADIUS						
		Podcast	Podcast	Podcast						
			Mobile Access							
		MySQL								

Apple Remote Desktop

Do 1997 r. Apple Network Administrator Toolkit, który był używany do instalacji At Ease, był również dostarczany z narzędziem Apple Network Assistant. Przedstawiony na rysunku 1.9 program Apple Network Assistant wyglądał bardzo podobnie do współczesnych programów do administracji komputerami Mac. Można było zdalnie kontrolować ekran Maca, blokować ekrany, udostępniać ekran, kopiować pliki, zdalnie otwierać aplikacje, wysyłać wiadomości na pulpit i wykonywać inne podstawowe, sieciowe zadania administracyjne poprzez sieć AppleTalk.



Rysunek 1.9 *Network Assistant, przodek Apple Remote Desktop*

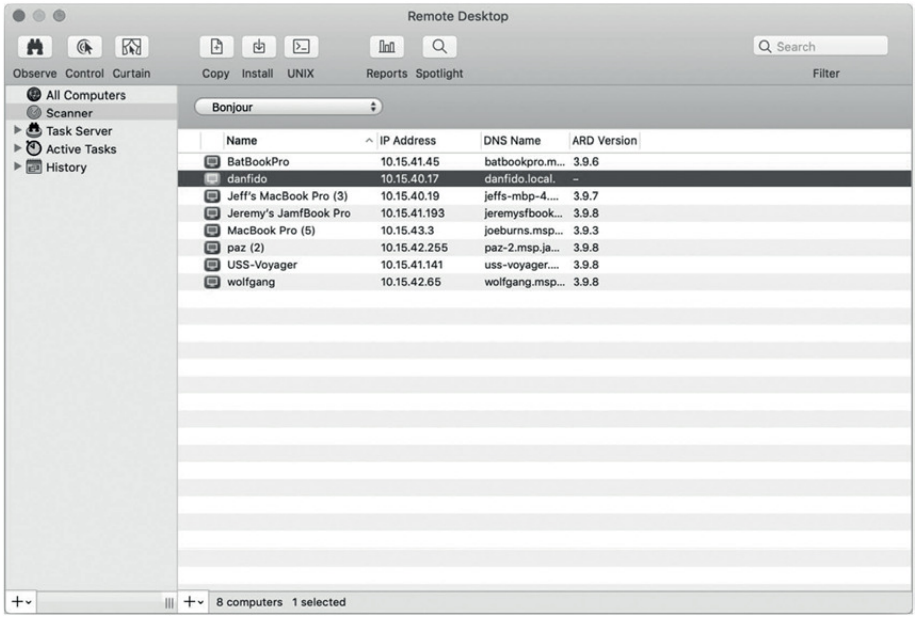
Po pojawieniu się systemu Mac OS X firma Apple wypuściła w 2002 roku nowe narzędzie o nazwie Remote Desktop. Jest ono nadal dostępne w Mac App Store i pozwala administratorom na przejmowanie pulpitów systemów swoich klientów, wysyłanie skryptów powłoki do klientów oraz wykonywanie szeregu innych zadań przydatnych w tego typu tymczasowym zarządzaniu. Remote Desktop działa również dobrze w połączeniu

z innymi narzędziami, ponieważ są one głównie używane do tworzenia obrazów, zarządzania konfiguracją oprogramowania i wdrażania. Większość funkcjonalności z Apple Network Assistant została przeniesiona do Apple Remote Desktop, stworzony też został nowy protokół ARD w celu ułatwienia wyszukiwania i kontrolowania klientów przez UDP.

> *Remote Desktop firmy Apple pozwolił administratorom kontrolować komputery Mac i wysyłać skrypty do urządzeń. Było to świetne w przypadku wielu środowisk i niedrogie! Wraz z rozwojem organizacji i dojrzewaniem ich potrzeb, ARD ułatwiło przejście na bardziej tradycyjne rozwiązania do zarządzania, ponieważ pakiety i skrypty były świetnymi fundamentami, na których można je było zbudować.*
>
> *—Chip Pearson, współzałożyciel Jamf Software*

W 2004 roku stało się jasne, że istnieją lepsze możliwości kontroli ekranu niż protokół oparty na UDP. Na bazie VNC został zbudowany Apple Remote Desktop 2, oferujący znacznie więcej. Był on również wyposażony w serwer zadań, dzięki czemu można było umieszczać polecenia w kolejce do wysłania. Oprócz tego, że Remote Desktop był doskonały do wprowadzania konkretnych, natychmiastowych zmian lub przeprowadzania działań na komputerze, zapewniał również dobry punkt startowy do korzystania z narzędzi do zarządzania i testowania instalacji nienadzorowanych.

Obecnie w wersji 3.9 (rysunek 1.10), Apple Remote Desktop ma za sobą drogę przez wiele różnych miejsc w ekosystemie firmy Apple. Polecenia zarządzania zostały przeniesione do workflowów opartych na APN w innych produktach, zaś Apple Remote Desktop umożliwia łączność tylko przez sieć LAN, chyba że w celu sterowania urządzeniami zostały otwarte porty dla połączeń przychodzących z WAN. Podobny efekt może dać użycie innych narzędzi, takich jak Bomgar, TeamViewer, GoToMy PC, Splashtop, ISL i wielu innych rozwiązań. Nic dziwnego, że firma Apple nie inwestuje tak wiele w refaktoryzację produktu, który obecnie w Mac App Store kosztuje 79,99 USD i ma tylko 1,7 gwiazdki na 5 możliwych. Co więcej, Apple Remote Desktop odbiega od nieco nowocześniejszego sposobu myślenia w firmie Apple: użytkownicy muszą jawnie zatwierdzać wszelkie naruszenia ich prywatności.



Rysunek 1.10 *Apple Remote Desktop nadal posiada wiele funkcjonalności narzędzia Network Assistant*

Współistnienie ekosystemów

Wraz z wydaniem bardziej nowoczesnego i elastycznego systemu operacyjnego firma Apple wprowadziła tryb wielu użytkowników. To zaś umożliwiło użycie jednego z nich do obsługi kont usług katalogowych. Konta te zaś dawały użytkownikom możliwość logowania się do ich lokalnego komputera przy użyciu tego samego hasła, które było używane na serwerze w celu uzyskania dostępu do ich poczty i innych usług świadczonych przez organizację.

Można było również uzyskać dane zasad za pośrednictwem usług katalogowych w postaci rozszerzonego schematu Active Directory zawierającego dane MCX, który był znacznie łatwiejszy do masowego zarządzania, niż wspomniany wcześniej lokalny MCX. Nie każda organizacja była w stanie rozszerzyć swoje schematy (czy kiedykolwiek udało Wam się spotkać administratora Active Directory, który chciał rozszerzyć swój schemat???), dlatego też opracowano techniki łączenia komputerów klientów zarówno

z Active Directory, jak i Open Directory firmy Apple i pozwalające na zagnieżdżanie użytkowników i grup w Open Directory w celu możliwości wdrażania Managed Preferences na klientach bez konieczności rozszerzania schematu Active Directory. Było to znane jako Magiczny Trójkąt.

Wcześniej wspomnieliśmy o ADmitMac, natomiast w 2005 roku został wprowadzony inny produkt, Centrify, rozwiązanie, które w bardziej scentralizowany sposób pomagało w dostarczaniu zasad do Maców. Od tego czasu Centrify skupiło się na byciu dostawcą tożsamości (Identity Provider – IdP). W celu ułatwienia wdrażania zasad wprowadzono także Quest Authentication Services. Jednak im bardziej przyjazną technologię tworzyła firma Apple, tym mniej każde z tych rozwiązań było potrzebne, a około 2011 roku niemal wszystkie już spaliły na panewce. Zasady są czymś, do czego zawsze było ciężko przekonać działy IT (mimo że wiele z nich rozszerzało swój schemat dziesiątki razy). W środowiskach, w których trudno było o rozszerzanie schematów, zazwyczaj również nie chciano dodawać serwerów firmy Apple jako dodatkowej usługi katalogowej. W kilku ostatnich wydaniach macOS, MCX powoli było wycofywane na rzecz zarządzania opartego na profilach, które wyewoluowało w wyniku ponownego przemyślenia zarządzania opartego na zasadach dla iOS.

> *MCX od Apple było dla administratorów potężnym i elastycznym sposobem na zarządzanie ustawieniami oprogramowania firmy Apple oraz innych firm. Preferowany przez Apple zamiennik, profil konfiguracji, nie posiada części elastyczności dostępnej w MCX. Wielu z nas miało nadzieję, że z czasem Apple z powrotem doda brakujące funkcje do profili konfiguracji, ale teraz wydaje się to mało prawdopodobne. To oznacza powrót do źle pisanych skryptów powłoki!*
>
> *— GregNeagle, twórca Munki i współautor Enterprise Mac Managed Preferences wydawnictwa Apress*

Podczas gdy wtedy wielu administratorów zajmowało się zarządzaniem serwerami, dziś przeszli oni do zarządzania stanami urządzeń, najpierw za pomocą usług katalogowych i MCX, a następnie w kierunku bardziej nowoczesnych technik zarządzania, takich jak te pomagające administratorom w zarządzaniu iPhone'ami i iPadami. W tym miejscu pojawiają się profile, które pokrywają wiele potrzeb administratorów, ale nie wszystkie.

Zarządzanie urządzeniami w iOS

Komputery Mac rozszerzały swoją obecność w wielkich firmach, ale już nadchodziła kolejna duża zmiana. Tym razem, zamiast próbować działać w ramach korporacyjnego dogmatu dotyczącego sposobu prowadzenia biznesu IT, Apple zacznie podążać własną drogą. Było to możliwe dzięki rosnącej dominacji urządzeń iPhone łączących się z serwerami Exchange oraz faktowi, że nagle pracownicy zaczęli pojawiać się z iPhone'ami i używali ich w pracy. Firmy musiały zacząć zarządzać systemem operacyjnym dostarczanym na iPhone'a, systemem iOS.

Pierwszy iPhone został wydany w 2007 roku, zaś zarządzanie systemem iOS początkowo odbywało się ręcznie przez iTunes. Można było przenieść aplikację na urządzenie, zostawała ona wtedy wysłana do telefonu poprzez kabel USB, a niektóre ustawienia były wystawiane w iTunes. W tych czasach, aby korzystać z urządzenia z iOS, trzeba było je zarejestrować w Apple, podłączając je do iTunes. Za pomocą iTunes można było także wykonać kopię zapasową i przywrócić urządzenie, co wiązało się z określonymi wyzwaniami, jak na przykład to, iż konto użyte do zakupu aplikacji podążało za „obrazem" nowego urządzenia. Ponadto, jeśli kopia zapasowa była zaszyfrowana lub nie została określona, mogło być konieczne ponowne wprowadzenie tego, co było przechowywane w kopii zapasowej i niektórych dodatkowych informacji.

Doprowadziło to do powstania profili. Profile były tworzone za pomocą wydanego w 2008 r. narzędzia o nazwie iPhone Configuration Utility. Profil to mały plik xml, który umożliwia wprowadzenie podanej konfiguracji na urządzeniu z systemem iOS. Było to konieczne, ponieważ programiści chcieli kontrolować to, co można zrobić na urządzeniach z systemem iOS. Jedną z tych opcji konfiguracyjnych była możliwość zainstalowania bezprzewodowo aplikacji hostowanej na własnym serwerze organizacji, pod warunkiem podania na takim serwerze typu MIME dla .ipa. W zasadzie odzwierciedlało to, co robił App Store i utorowało drogę wewnętrznym sklepom z aplikacjami oraz profilom hostowanym na serwerach. Dzięki temu obydwie te rzeczy można było instalować za pośrednictwem własnych sklepów z aplikacjami.

Profile były ogromną zmianą paradygmatu. Zamiast powiększać bibliotekę skryptów, których klienci musieli się uczyć, modyfikować i wdrażać, profile pozwoliły nam poruszać się w tym samym, ujednoliconym kierunku, chcąc konfigurować ustawienia

w systemie operacyjnym i aplikacjach, zarówno w systemie iOS, jak i macOS. Myślę, że reprezentatywne dla powodu, dla którego firma Apple tak silnie akceptowała to podejście, było to, iż umożliwiało to na stosunkowo szybkie przebudowanie głównych aspektów platformy, co pozwalało usunąć bariery związane z jej przyjęciem.

—Zach Halmstad, współzałożyciel Jamf

Wydany w 2009 roku iPhone OS 3.1 był dostarczany z klientem poczty, który pobierał i stosował zasady Exchange ActiveSync (EAS). Były to zasady konfigurowane na serwerze Exchange, które potem były pobierane przez klientów. Dały one w rezultacie możliwość kontroli nad różnymi funkcjami urządzenia, takimi jak ograniczenie korzystania z aparatu lub wymuszanie użycia hasła podczas wybudzania urządzenia. Zasady EAS zostały wprowadzone przez firmę Microsoft w 2005 r. jako część wydania Exchange 2003 SP2, aczkolwiek głównie były używane do zarządzania urządzeniami z systemem Windows Mobile.

W tym momencie firma Apple przeprowadzała większe wdrożenia i szybko stało się jasne, że podłączanie urządzeń do iTunes i długie czekanie na przywracanie urządzeń w trybie monolitycznych obrazów po prostu nie działa. Pierwsza iteracja technik zarządzania urządzeniami iOS, która przetrwała do dziś, wprowadziła profile. Jednak sukces iPhone'a 4 w 2010 roku i iPhone'a 4s w 2011 roku oznaczał, że potrzebowaliśmy lepszych narzędzi, niż iTunes do przywracania urządzeń oraz iPhone Configuration Utility do stosowania profili. W 2012 roku możliwość ich tworzenia i stosowania na urządzeniach została przeniesiona do nowego narzędzia o nazwie Apple Configurator, które jest nadal używane do tworzenia niestandardowych profili.

Apple Configurator może jednak zrobić znacznie więcej, niż tylko instalować profile. Apple Configurator dał również możliwość tworzenia kopii zapasowych, przywracania i instalowania aplikacji z App Store przy użyciu kodów zakupów grupowych. Można też budować złożone działania wykonujące powyższe czynności, podłączając urządzenie z systemem iOS tylko raz. Obecnie najważniejszą rzeczą, jaką Apple Configurator może zrobić, jest automatyczne przeniesienie urządzenia iOS do rozwiązania zajmującego się zarządzaniem urządzeniami mobilnymi.

Zarządzanie urządzeniami mobilnymi

W 2009 roku zostały wprowadzone powiadomienia Apple Push Notifications, a rok później na bazie tego rozwiązania zostało zbudowane MDM. MDM, skrót od Mobile Device Management, zostało wprowadzone w 2010 roku wraz z iOS 4. Początkowo było to używane do zarządzania profilami w iOS, dlatego firma Apple nazwała swoją usługę MDM w systemach macOS jako Server Profile Manager. Oprócz zarządzania profilami w pierwotnej wersji były obsługiwane trzy działania: zlokalizuj, zablokuj i wyczyść.

Począwszy od pierwotnej wersji, na przestrzeni lat możliwości MDM rozwijały się. Pokazano to w tabeli 1.2. Każda aktualizacja wnosiła coś nowego do MDM i oznaczała, że administratorzy urządzeń, aby zarządzać różnymi właściwościami, mogli pisać i wykonywać wymagane przez siebie działania.

Tabela 1.2 *Możliwości MDM z podziałem na wersję systemu operacyjnego i rok*

Wersja iOS	Wersja macOS	Rok	Nowe możliwości
4	nd.	2010	Volume Purchase Program (VPP), Mobile Device Management (MDM), MDM dla komputerów Mac
5	10,7	2011	Bezprzewodowe aktualizacje systemu operacyjnego, zarządzanie Siri, wyłączenie kopii zapasowej iCloud
6	10.8	2012	API dla programistów zewnętrznych, Managed Open In, nadzorowanie urządzeń
7	10.9	2013	Zarządzanie TouchID, obejście Activation Lock, zarządzanie konfiguracją aplikacji
8	10.10	2014	Program Device Enrollment, rejestrowanie konfiguracji Apple
9	10.11	2015	VPP opartych na urządzeniach, B2B App Store, przypomnienia o nadzorze, włączanie i wyłączanie aplikacji, sterowanie ekranem głównym, tryb kiosku/blokada aplikacji
10	10.12	2016	Restart urządzenia, wyłączenie urządzenia, Lost Mode, APFS
11	10.13	2017	Zarządzanie Classroom 2.0, zarządzanie Face ID, AirPrint. Dodawanie urządzeń do DEP, wykorzystująca kody QR rejestracja w niektórych MDM, User Approved Kernel Extension Loading dla komputerów Mac, zatwierdzanie przez użytkownika rejestracji MDM dla komputerów Mac
12	10.14	2018	Apple Business Manager, OAuth dla zarządzanych kont Exchange, zarządzana instalacja aplikacji tvOS, ograniczenia w automatycznym uzupełnianiu haseł