NETWORKWORLD Reprint

THE CONNECTED ENTERPRISE = NOVEMBER 07, 2016

Review: Four ways to manage Macs in a Microsoft world

Parallels, Centrify and Thursby go beyond what's offered by Microsoft/Apple.

BY TOM HENDERSON, NETWORK WORLD

Credit: Thinkstock, Microsoft, Apple

Traditionally, Macs have been second-class citizens in the Windows-centric enterprise world, but it doesn't have to be so. In this review, we looked at four ways to manage Macs in a Microsoft Active Directory (AD) network.

We tested the Microsoft/Apple in-the-box management combination, as well as third-party products Centrify Suite 2016 for Mac, Thursby Software's ADMitMac 10, and Parallels Mac Management for SCCM.

We found if your organization uses Microsoft's System Center Configuration Manager (SCCM), then Microsoft and Apple deliver the bare minimum in terms of management and control.

Parallels Mac Management adds significant Mac administration features to SCCM. Parallels has an edge in terms of management features that would likely suit your current Windows infrastructure, and leverage what you already know in terms of SCCM activities and control.

Centrify can manage Macs very well on Active Directory, and although they want you to use their other identity management type products, that's not necessary to achieve good and flexible control over Macs.

If you simply need compliance and reasonable Mac management in a smaller Windows environment, Thursby's ADMitMac products cover Macs nicely -- even older Macs going back to OSX 10.4.

The MacOS-Active Directory problem

Microsoft certainly knows how to lockdown Active Directory networks, but a long-standing line of demarcation exists when Windows-like controls need to be imposed on non-Windows clients.

Even when System Center Configuration Manager is used in conjunction with the Active Directory connectivity that Apple supplies, the controls are a bare minimum. The BYOD era increased Microsoft's ActiveSync API for mobile devices, but control of Macs hasn't been a strong agenda item for either vendor.

There are many scenarios that could require integrating Macs into Active Directory networks: a new Mac on a local net, machines used by more than one person in a shift or day, external users/contractors needing Active Directory-constrained resources, internal pockets of Macs that have been used in relative/total isolation to Active Directory, and those that have been already linked through Apple Directory Utility basics.

Microsoft's Active Directory is standard in enterprise networks, but Windows on the desktop has been eroded by Macs, and to a far smaller extent, Linux. Organizational policy and regulatory compliance in terms of encryption, file/information sharing/accessibility have led to the development of many products that are focused on Active Directory and Windows, to the detriment of Mac users.

What's offered In MacOS

If Apple's Server Edition isn't being used, any Mac can make use of Apple's Directory Utility to connect to Microsoft Active Directory. Apple has moved towards a CIFS-based plug-in interoperability model using proxy authentication where MacOS Server has been adopted for workgroup control.

MacOS Server editions, via Workgroup Manager or Profile Manager, can talk to Active Directory, and are more common in workgroup-sized installations. Although we have not reviewed MacOS Server since the demise of Apple's Xserve product line, there are a number of workgroups, even

some large organizations, that use the Open Directory/LDAP fundamentals included in the Server Edition.

However, for most Mac users in large organizations, logon to Active Directory comes via a Directory Utility app. Using a URL, users gain rudimentary access to Active Directory resources, although users logging in through a VPN may need to use DNS pointers just to find an Active Directory-authorizing server entry point. Apple's VPN client does not add a specified DNS search mechanism (even though there's a blank for it) when logging in via a VPN.

Once Directory Utility CIFS Shared Resources are exposed, simple file shares are used for shared work product storage. Administrative controls made in the Active Directory can control file and resource access—if minimally. Macs become a part of Active Directory more as an inventory item than a manageable/controllable end-device.

Macs logged in this way aren't subject to useful Windows Group Policies, although group membership access controls are in place. Common Windows apps become more manageable for Mac devices: Outlook/Exchange and Microsoft's SQL Server. Lack of Mac-specific Active Directory controls is where the gap begins for Windows Active Directory admins.

The Directory Utility is minimalist, but it works. As a Mac user or administrator, you need to know the resources you need, as you're limited in Active Directory resource discovery. Much of initial setup can be scripted within the Apple realm to reveal static resources, and many networks are setup using static resources for Macs because of this.

The upshot is that your current session won't be subject to advanced Group Policy Objects, and you may have encryption boundaries, depending on the application used and obtained from the Active Directory, and how your organization uses Kerberos.

Your anti-virus/anti-malware is already much different (usually) than what's found in the Windows world. And unaided, imaging Mac payloads isn't really possible without extras.

Offsite users need a lot of deliberate configuration work, including the aforementioned DNS manipulation, as without working DNS, the Active Directory will laugh at you. This and other connectivity issues can make administration of individual Macs in a geographically dispersed network difficult.

Net results

COMPANY	Centrify	Parallels	Thursby Software
PRODUCT	Centrify Suite 2016 for Mac	Parallels Mac Management for SCCM	Thursby ADmitMac
PRICE	$4 per user per month	$30 annually per Mac	Single license, $179; 25-license pack, $3,600.
PROS	Great enterprise-grade control of Macs for AD admins; flexible architecture	Total, equal control of Macs in AD	Much better than Apple's Directory Utility; simple migration
CONS	Documentation can be daunting	You must have Microsoft SCCM	Add-ins are only basic

Thursby ADMitMac 10

Thursby has a number of Mac to Active Directory connectivity products. We tested ADMitMac 10 and found it solves a significant part of the connectivity problems between Mac clients and an Active Directory Network.

It has add-ons for Group Policy Controls, Active Directory management specifically for Macs, and ties to a Mac administrator's use of WorkGroup Manager or Profile Manager where installed and in use.

Think of ADMitMac as a network driver stack plug-in that replaces the CIFS stack that Apple provides, coupled with discovery and useful AD-Mac admin utilities. ADMitMac is administered through the Directory Utility or AD Commander via the ADMitMac MacOS plug-in. It also works with Apple's discontinued Workgroup Manager, and with the current MacOS Server app Profile Manager.

ADMitMac 10 arrived as a disk image/.dmg file that contains two central components, including an all-important replacement for the CIFS connectivity that Apple offers to Mac users. Installing the package on our Macs was incredibly simple.

Active Directory volumes to be mounted are simple, and can be administratively stored for all users, or just the user logged in. A script-savvy Mac admin can also whip together an automated installer for each user by either user name or machine name. There is a Deployment Utility available for "Volume Installations," but this wasn't examined or tested.

Kerberos authentication works correctly. It's also possible to prevent unauthorized users of the Mac machine from logging into the Active Directory.

Included is a Home Mover utility that moves the MacOS user's home directory reference point to something that the Active Directory admin controls. And it can be located in a special area where the root folder is unexposed, which makes it handy for public or uncontrolled environments.

We could also create login scripts, and hybrid scripts that were active depending on user and Active Directory status. In other words, we could control where the user `home/~' was located for datafile, tempfile, and other purposes.

We set up an Active Directory print test bed and printed successfully both locally, as well as through Active Directory auspices. Ensuring that there are correct drivers doesn't matter, as most Macs will adjust, but it's smarter to have printers already setup in a Mac to make this work.

For administrators, there is an AD Commander utility that allows manipulation of an AD in terms of controls. New users, their groups and characteristics, and Organizational Units relating to the Active Directory were easily manipulated using a conjoined Apple/Windows metaphor.

A final app, unused in our testing, was an ADMitMac Tracing Utility that automates and gathers situational information that can be saved, then emailed to Thursby tech support for resolution of support calls. It's a nice detail.

Overall, Thursby's plan is very Apple admin-friendly, and for workgroups to moderate-sized installations, appealed to us. It's a well-done advance over the default connectivity Apple includes, and an easy answer to the question: How do we get some control over those pesky Macs on our network?

Centrify For Mac

Centrify for Mac has client, server, and optional cloud controls. The client-server components are $4 per client per month, and the cloud options adds single sign-on for a total of $6 per client per month. Our review is focused on Centrify for Mac.

The product comes with a 307-page PDF "adminguide" that we found to be excellent, if daunting. The guide recommends creating a separate organizational unit for its use, in a configuration called Auto Zone.

A zone within Active Directory is used to aggregate Mac-specific resources into an Active Directory object that becomes easier for admins to manage. The guide itself is basic enough to educate Mac admins or Windows admins to each other's situational management needs. Daunting, but quite thorough.

But we looked at Centrify for Mac after we tried to just install it ourselves from binaries, and judged that if you're sufficiently savvy at both Mac and Windows Active Directory, you can do it all at once.

The client-side is installed and connects quickly, and has better diagnostics and tests to get an initial Mac connected to the Active Directory than Thursby's equivalent.

On the Windows side, Centrify will query the subnets it lives on, or other subnets we specified, to find Mac citizens and make them part of our Active Directory empire.

The discovery process also found a number of hosts which it had no business trying to tie into the Active Directory, like routers. This said, the discovery process took a while, and did find the Macs correctly—save the ones it's no longer compatible with.

And therein lies only a small rub, which is that Centrify's docs say that MacOS 10.9 support will be deprecated in their next release. MacOS Sierra has been added. Earlier versions of the Mac OS that have been dropped from the current release do not undergo continued testing after they have been dropped. Although older Macs continue to be supported, they don't get features supported by the latest release.

Thursby's other products go back to the Dark Ages of Apple, by comparison, but many organizations simply can't have unsupported operating systems in use for compliance and regulatory adherence. And unsupported OS releases in general are an enormous security risk.

Once both sides, client and server were installed, we found we could establish a network home directory for users, and that this directory is available on other shares than just the Active Directory.

This home directory can then be synchronized, allowing portable/mobile operation easily. Apple File Share (AFS) and Network Filing System (NFS) homing and synching are also possible, but this is about use with the Active Directory and so we didn't go there.

Support for Radius authentication and Centrify's certificate management is perhaps the best of the three products we tested. We could also impose FileVault encryption key management on Macs with MacOS 10.9+, but we didn't test this.

Centrify has explicit printer definition and permissions setup possibilities. Our simple test of finding and using an Active Directory-based print queue was without drama. It's possible to setup comparatively sophisticated zones for purposes of managing localization and feature sets to shared print resources, but we didn't test this heavily. The bits appear to be there.

Group Policy Active Directory objects that Centrify allowed us to install permitted direct control of virtually everything in the Systems Preferences app of our Macs. Herein lies the greatest value, we feel, of Centrify's Mac controls: Once logged into the Active Directory, a Mac is bolted down, administratively, in much of the same way as a Windows machine in terms of settings.

Active Directory admins need learn only a few small facts to make it work. Common denominator settings between MacOS and Windows, like time, interactive logons, password controls, etc. can be set empirically in the Active Directory controls for both. The specific zones/organizational units built for Centrify (read Mac) users then allow Mac-specific constraints and permission.

A long list of Group Policy controls then manage everything from where apps can be downloaded from to firewall settings, sharing, remote management, and security/sharing capabilities on the Mac. If you have run GPO controls before, it's very simple and intuitive—but it's all explained if you need detail.

You get even more if you choose the optional SSO, but that's crux of a different review. The base $4 per month package buys all of the guts necessary to resolve the differences between Macs and Windows clients as far as the Active Directory is concerned. It's incredibly well explained in Centrify docs, and it has the slick feel of a Citrix-like installation and is likely to be enterprise ready. But we pounded none of these with 5,000+ Macs on a bad Monday morning.

A long list of Group Policy controls then manage everything from where apps can be downloaded from to firewall settings, sharing, remote management, and security/sharing capabilities on the Mac. If you have run GPO controls before, it's very simple and intuitive—but it's all explained if you need detail.

You get even more if you choose the optional SSO, but that's crux of a different review. The base $4 per month package buys all of the guts necessary to resolve the differences between Macs and Windows clients as far as the Active Directory is concerned. It's incredibly well explained in Centrify docs, and it has the slick feel of a Citrix-like installation and is likely to be enterprise ready. But we pounded none of these with 5,000+ Macs on a bad Monday morning.

Scorecard

	Thursby	Centrify	Parallels
Installation, Architectural Flexibility	3.5	4.5	4
Features and Security	4	4.5	4.25
AD Controls for Macs	3.5	4.25	4.5
Administration, Docs	4	4.25	4.5
Total	3.75	4.375	4.3

Parallels Mac Management for SCCM

Parallels Mac Management takes a different approach. If you want a Mac to be essentially a Windows machine for purposes of Systems Center Configuration Manager, it will do this.

But there's a catch: If you use or are about to commence implementing Microsoft's System Center Configuration Manager, the installation process can sometimes be gruesome.

An SCCM installation needs to be rock-solid. We found an error in ours, and it took a while to discern what was wrong. Our mistake. Parallels has a snap-in that enables a number of features, and there is an easily-installed client-side component.

The strongest feature, not found anywhere else, is the ability to fully provision a new Mac system's operating system and software, stem to stern, from scratch or bare metal.

At initial installation, this is made possible through installing a NetBoot server option during Parallels Mac Management installation as an option. Image generation is not quite as tough as it is on Windows clients, but we could see that varying Mac license versions and configurations could cause as much image sprawl for Mac images as it does Windows variations. This said, no one else does it.

As MacOS is now free to use on Mac hardware, licensing issues aren't quite as gruesome as on Windows client devices. You may not, however, provision for VDI use. Or at least Apple hasn't launched stormy litigation that we've heard of.

The same provisioning could be used for a wipe, although a restoration from Time Machine network backup resources still requires different work and methods. Classrooms or office buildings full of Macs could be provisioned/re-provisioned in just a few commands, providing homogeneity of image sources suitable for differing models. It took a very long time, the better part of a long day, for us to build all of the steps necessary to make images, then do an over-the-network (VPN) provisioning of a machine, a Macbook Pro, in our case. Subsequent re-imaging is faster as it's possible to generate "gold images" for subsequent versioning control, amounting to almost the same forklift process needed to do Windows "gold images".

Likewise, SCCM includes the Mac add-ins to inventory components, hardware it can find, software assets, and licensing both through discovery and manual addition. While discovery and enrollment can take a while, we could build a fairly fat database of our test Macs; a higher population probably should be done in groups, perhaps by logical network/geography assays, as it generates a bit of traffic while building info.

Parallels for Mac lives inside SCCM, and creates a separate area for Mac control not unlike Thursby and Centrify for Mac, and items like inventory and reporting are treated as equals to Windows client assets. Parallels adds information that's Mac specific, such as when AppleCare coverage expires.

The client side installs come either through a process of auto-discovery, or by manually downloading the app and installing it—and this could be scripted if we took the time to invent the script. In either case, once the client app is installed, it becomes part of the SCCM managed domain.

We found the installation partially problematic, as it requires ssh to be enabled, and thus Systems Preferences > Sharing, and then allows remote control, but this will be seen as a feature by an administrator and necessary to push policies and control desktops.

Security professionals know that sharing remote logon in this way also opens a security hole on the client which needs to be carefully managed. In our experience, the ssh port becomes enabled, then forgotten, until it's probed by something malicious.

Bringing machines into compliance becomes the crux of scripts pushed to clients, including configuration management components, and profiles to aid in both management and the reported policy compliance desired.

The scripts can be delivered and executed on queue, and the results easily audited in near lock-step with how SCCM treats Windows clients. What's missing is a long list of pre-fab scripts. This means the scripts need to be cobbled together by an administrator with scripting skills using the Admin Guide for Parallels for Mac Management. Reports from SCCM can be differentiated Windows to Mac, if needed, or in one large desirable lump entitled: Here's The Query.

Parallels for Mac does patch management fully, instead of the control in updates found in Centrify. It's more sophisticated, and has a higher degree of control, but it's also a Pandora's Box to manage in terms of an additional level of complexity.

It does, however, pay off for organizations seeking very granular control over how updates are managed. As we predict that Apple updates may need to be disambiguated in the same way as organizations have manufactured tight control over Windows updates, we laud the control, not the reasons for it.

We found FileVault 2 encryption can also be managed through Parallels for Mac, including key escrow, although we didn't try this. Configuration management is done via SCCM.

The Parallels Mac Management scheme adds sophistication to an Active Directory shop's use of SCCM, leveraging an already sophisticated platform that takes lots of CapEx and OpEx investment. It can do tricks that makes SCCM treat Mac clients as a near equal to Windows clients. It's not as egalitarian as Centrify in terms of client-side choices or innate GPO controls—doing much control from a different direction in both administration and configuration.

It's a different way of getting Macs and Active Directory embracing each other, if from the Windows Systems Center cultural side.

Summary

We wouldn't go out and deploy SCCM 2012 just to control Macs, as SCCM is an armada of components tied onto a hefty platform, but if an organization is using SCCM already and has some fluency, Parallels Mac Management extensions to SCCM are invaluable.

By contrast, Centrify contains a very strong and professional approach to tying Macs to a controlled platform under the control and aegis of the Active Directory tools that every Active Directory admin already knows, but it lacks a few of the secret sauce ingredients that Parallels for Mac SCCM has.

And life is not only simpler with Thursby's ADMitMac, but it will appeal to Mac admins who may be (begrudgingly) only now connecting to an Active Directory Network. AdMitMac connects the dots that Apple and Microsoft left out of the box in a satisfying, thoughtful, and uncomplicated experience.

If we had all of the budget and personnel power, we'd go Parallels, but the other two are close and for different reasons.

Tom Henderson runs ExtremeLabs, in Bloomington, Ind. He can be reached at kitchen-sink@extremelabs.com.