



Client Management

Best Practices for Managing Mac Systems

White Paper

October 2007

Contents

Page 3	Executive Overview
Page 4	Prepare Image creation Hardware scanning and tagging
Page 6	Deploy Apple Software Restore Network Install
Page 9	Maintain Apple Remote Desktop 3 Task Server Software Update Server
Page 11	Control and Monitor Managed Client for Mac OS X Apple Remote Desktop 3
Page 13	Retire
Page 14	Conclusion
Page 15	Appendix A: Third-Party Client Management Solutions
Page 16	Appendix B: Disk Image Creation
Page 17	Appendix C: Levels of Client Management

Executive Overview

One of the greatest challenges facing any institution is the maintenance of a large number of computer systems. By instituting well-considered policies and taking advantage of the easy-to-use tools available today, managing client systems can be simple and effective. When properly performed, lifecycle management—from the loading dock to the recycler—maximizes your return on investment, keeps your users more productive, and protects the security of your computer systems and your enterprise data. What's more, all of these goals can be achieved while reducing the load on IT staff.

In general, client management involves the following steps:

Prepare. Each enterprise needs to determine the ideal workstation configuration (or different configurations for different purposes) and create the appropriate master disk image(s), ready to use when new systems are delivered. Also, to ensure that workstations are tracked through their entire lifecycles, a system needs to be in place to log them into inventory as soon as they arrive.

Deploy. When a new computer arrives, it is not yet ready to be deployed into a large enterprise. The operating system is in a default state, no local user accounts have been created, and no organization-specific applications have been loaded. The deployment phase of the client lifecycle should fully configure the workstation with the proper settings and applications for its specific work environment—with minimal IT effort.

Maintain. Once the computer has been deployed, it is critical to keep its operating system and applications up to date. Without proper patch management, you cannot keep your systems consistent or secure.

Control and monitor. A major aspect of client management is controlling what users are allowed to do and monitoring the state and use of computers.

Retire. Every computer reaches an age where replacing it is less expensive than maintaining it. Before that point, however, many institutions “cascade” older hardware to less demanding users and roles. Using client management tools, you can maintain a hardware inventory that will help you get the most out of each workstation before it finally needs to be retired.

This paper discusses each of these steps in more detail, with an emphasis on best practices for managing Mac computers. Apple and other vendors offer tools that can address every stage of the Mac lifecycle. These tools allow organizations to smoothly integrate Mac systems into their networks and client management efforts.

Prepare

The lifecycle of new computers begins even before they arrive at your shipping dock. Effective client management entails preparation of a master installation image for incoming client systems and readiness to log the computers into your asset inventory as soon as they arrive.

Image creation

Creating a master image enables you to deploy new workstations quickly and consistently. A time-honored way of configuring a master image has been to set up one workstation, load all of the necessary software on it, configure the proper settings, and then capture an image of the system's hard drive. This method, however, is prone to mistakes and undesirable side effects. It's nearly impossible, for example, to remember to document every tweak you make, and you have to remove caches and other clutter after every testing session. Also, if you deploy the image to a machine with different hardware, some settings may not work properly.

For these reasons, Apple strongly recommends that you use Mac OS X Installer packages to install your system image onto a volume that is never booted before it is deployed to a Mac. This method effectively eliminates issues that arise when using an active system to install software and test settings. Not only should all software be installed with packages, but local users should also be created with a startup item that is installed by a package. Furthermore, most application and operating system settings should derive from management policies.

A fully package-based installation offers the following advantages:

- Packages use a standard format.
- Packages can be installed by a variety of client management products.
- Packages can run scripts.
- Packages are auditable.

Modularizing the imaging process by using packages improves consistency by eliminating the need to manually tweak files or run scripts. Also, packages are easy to audit, enabling you to quickly determine every file that you have installed or modified on the deployment image.

You can create packages with several tools, such as PackageMaker from Apple and Composer from JAMF Software. When it's time to install your software, you can select from a wide range of tools that support the PKG file format, including Apple's Installer, the Casper Suite from JAMF Software, and FileWave.

Whenever you order a new batch of computers or redeploy older systems, check your master image to see whether it needs updating. If you are redeploying hardware that is the same age or older than the computer on which the master image was created, the existing deployment image will probably suffice. Otherwise, you should create a new image based on your latest hardware. In isolated cases, different images may be needed for different hardware models. Careful testing and evaluation are needed to make these determinations.

Hardware scanning and tagging

As soon as a new system arrives, it should be entered into your organization's resource inventory. Prompt inventorying of new systems permits comprehensive management and reduces the incidence of "lost" hardware. In the case of a Mac computer, the MAC addresses and serial number can be scanned into your client management system from the sticker on the outside of Apple's shipping box.

Apple also recommends as a best practice that you attach a physical asset tag to each computer, because subsequent hardware repairs could result in a change of MAC address or serial number. Asset tagging links a computer's physical and electronic identities, providing identification that can be maintained for its entire life. The tag number can be entered into a field in your client management software.

Deploy

Third-party client management products

Many third-party solutions are available for deploying and maintaining Mac clients. They range from commercial products such as Casper and FileWave to open source tools such as puppet and radmin.

Third-party solutions can offer more flexibility and power than their Apple equivalents, but they often cost more or require greater knowledge and effort by the administrator.

A comprehensive list of third-party utilities for Mac client management is included in Appendix A.

Once you have a master deployment image, you'll want to get it onto your Mac systems with the least amount of effort possible. Depending on your needs, you can select Apple Software Restore, Network Install, or a third-party product.

Apple Software Restore

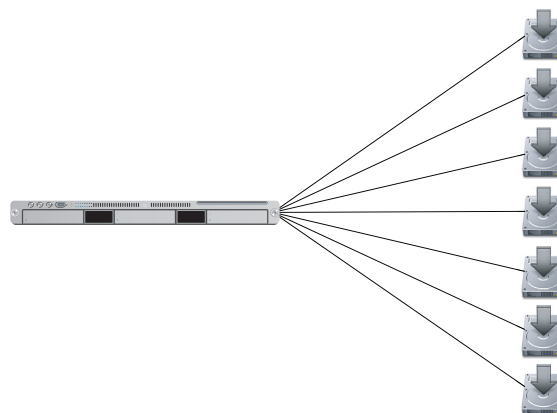
Apple Software Restore (ASR) is Apple's tool for imaging drives. System administrators can access ASR directly from the Mac OS X command line, or through GUI-based front ends. ASR can be used in several different ways.

Local-to-local imaging uses ASR to deploy an image directly from one drive to another. In many cases, the source is a bootable external disk containing the deployment image. This method does not scale very well, but it can be useful for reimaging in the field.

Alternatively, you can run Apple Software Restore in conjunction with Apple's NetBoot software. NetBoot is used to start up multiple Mac systems from a single server-based disk image. When you want to deploy a fresh system image, NetBoot eliminates the need to make individual DVDs or configure multiple external disks for booting the target systems.

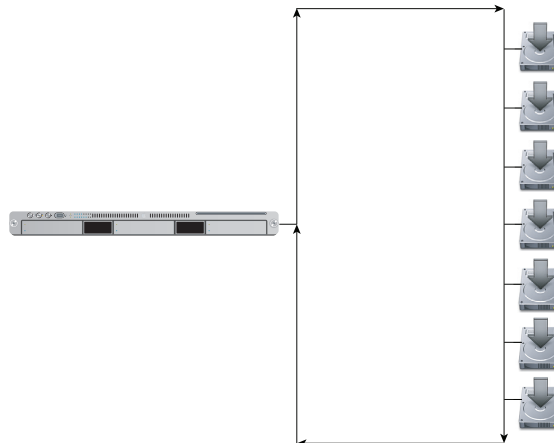
ASR and NetBoot offer both unicast and multicast options.

- Unicast ASR imaging with NetBoot is analogous to local imaging. NetBoot on the server boots all of the clients into ASR. Each client then retrieves and installs the master disk image from the server. Due to the I/O limitations of multiple Mac systems accessing a single image, unicast imaging has a practical performance limit of 10 to 15 simultaneous deployments.



In unicast mode, each client queries the Apple Software Restore server for the master disk image.

- Multicast ASR (mASR) broadcasts the image over the network from a Mac that has ASR and the master disk image. Clients running ASR receive the broadcast. Similar to a multicast QuickTime broadcast, clients can join the stream at any time. Clients that join in the middle of the broadcast will catch up on the earlier data when the mASR server loops the stream. Because only one process (the ASR server) is reading the image at a time, multicast ASR avoids the scaling issues of unicast distribution. It effectively scales to the capacity of your network.



In multicast mode, the Apple Software Restore server sends the master disk image out as a continuous stream. Clients join the broadcast to receive the image.

Note that any multicast operation can have a significant effect on your overall network performance. Before starting a multicast, be sure to consult with a network administrator to determine what settings to use to minimize bandwidth and give higher priority to more urgent tasks. A best practice with any deployment method, particularly multicasting, is to isolate the deployment network entirely. That way, you can tune your mASR settings to deliver maximum performance without having to worry about the impact on your production network.

Many organizations already deploy Windows computers with Symantec Ghost Multicast Server. Your network administrator can help you leverage existing multicast settings—such as address ranges and router configurations—for multicast ASR sessions.

Two products are available that enable administrators to perform ASR tasks through a graphical user interface (GUI):

- Apple's Disk Utility software (which comes on every Mac) offers a very basic GUI for ASR. Disk Utility can create, scan, and restore disk images.
- NetRestore from Bombich Software offers access to every function of ASR. It has many automation features and also benefits from a robust support community. It can be used in conjunction with NetBoot to fully automate the deployment of multiple Mac clients. Apple highly recommends NetRestore when you want to deploy with Apple Software Restore. The program is available through the Macintosh Products Guide at guide.apple.com.

Note: For highest performance, ASR can perform a block copy clone of a drive. When deploying an image, select the Erase Destination Drive option to enable the block copy operation.

Network Install

Apple's Network Install software (commonly called NetInstall) is a form of NetBoot that boots to a customized installer rather than a Finder session. In contrast to Apple Software Restore, NetInstall looks and feels as if you have booted the client system from an installer DVD, when in fact it has booted from the network. (Note that NetInstall images can be burned to a DVD, space permitting, to create a bootable installer. Compared with installing from a NetBoot server, this method is slow, but it offers an inexpensive way to distribute custom installers to remote locations.)

NetInstall images are created with the System Image Utility. Installers can be customized to include other software via the aforementioned Apple package format.

Maintain

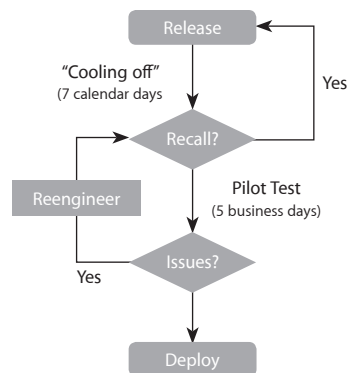
Once you have deployed your Mac clients, it's important to develop an effective policy for updating them. Your policy should prevent bad updates from being deployed, while also eliminating the need to redeploy known good systems.

Apple recommends the following three-phase update policy:

- When an operating system or application update is released, there should be a “cooling-off” period of seven calendar days. This delay allows time for the vendor to issue patch recalls or revisions, and for IT to perform basic functionality testing.
- After the cooling-off phase, the update should be deployed to a pilot group for five business days. Deploying to a limited group of users helps ensure that production will not be affected in case of problems with the update. The pilot group should cover a range of operational tasks and be composed of “power users” who are able to give effective feedback.
- Upon completion of the pilot phase, the update can be delivered to all workstations and integrated into the master deployment image.

If issues arise during any phase, your policy should call for a restart of that phase. For example, if Apple releases a security update that is revised five days later, then a new seven-day cooling-off period should begin.

Update Methodology



The three-phase policy cycle minimizes the risks of widely deploying buggy updates.

Apple Remote Desktop 3 Task Server

The Task Server in Apple Remote Desktop (ARD) 3 can be used to deploy update packages to workstations and servers. The updates are queued on the Task Server, and then sent to each client Mac the next time it checks in with the server. ARD lets you distribute updates to systems that may not always be on the corporate network, such as laptop computers. The Task Server can distribute Mac software packages from Apple and other vendors, as well as custom packages that you have created.

Software Update Server

If you do not have ARD, you can distribute updates efficiently by using the Software Update Server utility in Mac OS X Server. Software Update Server creates a local mirror of Apple's own update servers. Implementing your own server greatly reduces bandwidth needs when updates are released. Even more important, it gives you control over when updates are made visible to your workstations. Software Update Server distributes Apple updates only.

As with Apple's standard Software Update utility, users of Software Update Server need to have administrator privileges on their Mac systems to apply updates. Also, a major disadvantage of user-applied updates is that there is no way to ensure that they have been made. These issues can be mitigated to some extent by using the Send UNIX Command function in Apple Remote Desktop software to install updates from your update server without user intervention. Note, however, that environments with Apple Remote Desktop will find little need for Software Update Server, because the Task Server in Apple Remote Desktop is a better method of deploying updates in a managed environment.

Control and Monitor

After preparing, deploying, and devising policies for maintaining your Mac computers, you're ready to enter the phase most commonly associated with the term "client management." Controlling and monitoring will continue for the lifetime of your systems.

Managed Client for Mac OS X

Managed Client for Mac OS X (MCX) is the policy framework in Mac OS X. MCX is Apple's equivalent of Group Policy Objects (GPOs) in a Microsoft Active Directory environment. MCX policies can manage almost anything, from operating system settings to end-user applications.

The management policies in Mac OS X can work with any directory service. They are native to Apple's Open Directory architecture and can be added to NIS, LDAP, eDirectory, or Active Directory by using third-party products or simple Apple-provided schema extensions. Schema extensions are the most robust solution and are recommended by Apple when you are deploying the Mac OS X management policy system to a non-Apple directory service such as Active Directory. Please see the *Best Practices: Implementing Mac OS X with Active Directory* white paper at http://images.apple.com/itpro/pdf/AD_Best_Practices_2.0.pdf for more information on integrating Mac systems into Active Directory for client management.

You can access many management policy settings through Apple's Workgroup Manager tool. Workgroup Manager, available as a free download from Apple's website, can be used to create management policies for any directory service. It contains presets for the most common system settings and can also manage any setting that is configured using the standard Mac OS X preferences. For example, you could allow the use of iTunes, but not access to the iTunes Store or sharing of music files. Any application that uses standard Mac OS X programming practices—including third-party programs—can be managed with similar granularity.

Apple Remote Desktop 3

Apple Remote Desktop is Apple's client management software suite. ARD licenses are assigned to administration workstations, not to clients; the per-console fee allows you to manage an unlimited number of Mac systems.

The Application Usage report in ARD 3 details how applications are being used on your systems, including how much time users spend in each application and which programs are used the most. Such accuracy helps you pay for only licenses that you really need and simultaneously helps ensure that you pass licensing audits.

ARD includes a robust set of help desk tools, including remote control capabilities that can be used solely by an administrator or shared with a user. Curtain Mode gives administrators additional security when configuring sensitive information by allowing them to block the remote user's view of the desktop with a virtual "curtain." Users who require assistance can request it directly from the menu bar of their Mac systems. ARD has a built-in chat capability for communicating with users.

Apple Remote Desktop also offers many administrative and maintenance tasks that can be applied to groups of workstations at once. For example, it has easy-to-use templates for the Send UNIX Command feature. You can use the templates to execute remote scripts and actions on multiple workstations simultaneously, without having to learn command-line tools or establish an SSH session with each machine individually.

Retire

Determining when hardware needs to be retired can be difficult, but companies in many industries have adopted three-year lifecycles. Although the actual lifespan of any individual computer will vary, estimating a three-year hardware cycle will allow you to better plan for future purchases.

When a certain Mac is no longer meeting the needs of its current user, it can usually be moved to a less demanding role. For example, a Mac that is no longer meeting a creative agency's needs for high-performance video production will still be more than sufficient for someone doing business tasks. When cascading eliminates the need for the oldest or least powerful Mac systems, those computers can be sold, donated, or recycled.

Conclusion

By tracking and managing every computer from the day it is first received until the day it leaves, you can maximize the efficiency of a cascading hardware refresh cycle and achieve the highest possible return on your investment.

With the versatile and easy-to-use tools available from Apple and other companies, your organization can find the solutions it needs to manage Mac clients efficiently and cost-effectively.

Appendix A: Third-Party Client Management Solutions

This appendix lists many of the products that can be used to manage Mac OS X clients. Information about products not manufactured by Apple is provided for information purposes only, and does not constitute Apple's recommendation or endorsement. Please contact the manufacturer for additional information.

- Altiris Client Management Suite (www.altiris.com)
- BigFix Software Distribution (www.bigfix.com)
- BMC Configuration Management (www.bmc.com)
- Casper Client Management Suite from JAMF Software (www.jamfsoftware.com)
- Centrify DirectControl (www.centrify.com/directcontrol/mac_os_x.asp)
- Deep Freeze Mac from Faronics (www.faronics.com/html/DFMac.asp)
- FileWave (www.filewave.com)
- HP OpenView (www.openview.hp.com/)
- Hyperic HQ (www.hyperic.com)
- Kace KBOX (www.kace.com/)
- LANDesk Management Suite (www.landesk.com/Products/LDMS/MAC/Index.aspx)
- LANrev (<http://www.lanrev.com/>)
- MacShield Enhanced Edition from Centurion Technologies (www.centuriontech.com/products/macshieldenhanced/)
- ManageSoft (www.managesoft.com)
- Puppet from Reductive Labs (reductivelabs.com/projects/puppet/)
- QMX extensions for SMS 2003 (<http://www.quest.com/quest-management-xtensions-for-sms/>)
- Radmind from the University of Michigan (rsug.itd.umich.edu/software/radmind/)
- Timbaktu Pro for Mac OS X from Netopia (www.netopia.com/software/products/tb2/mac/)
- Thursby ADmitMac (www.thursby.com/products/admitmac-eval.html)

Appendix B: Disk Image Creation

Apple's Disk Utility simplifies the creation of master disk images.

Apple Software Restore (ASR) requires a properly created disk image for most efficient operation. By using the Image from Folder function in Disk Utility, you can easily create a defragmented image.

To image a volume:

1. Set up the source volume the way you want it.
2. In Disk Utility, choose Images > New > Image from Folder... Select the root of the volume. Save the image as read-only or compressed.
3. Scan the image with Images > Scan Image for Restore.

Appendix C: Levels of Client Management

This scale will help you assess how you're currently managing your Mac client computers. Armed with that information, you can decide whether you should increase your level of management. This scale is based on common deployment styles.

The charts in this appendix describe various management levels for these categories:

- Imaging: Are new systems deployed from master images? If so, how are those images created?
- Deployment: How are images and applications deployed? How scalable is the method used?
- Directory services: What information is included in the directory service, if it is used at all?
- Support: How easily can IT staff support Mac systems and assist users?
- Policies: Have management policies been implemented?
- Maintenance: How easy is it to update the operating system and applications?
- Security: How secure is the computer?
- Bottom line: What is the overall approach to management at this level?

Level 1: Wild Mac computers

Imaging	None. Mac computers are handed out in boxes.
Deployment	None. Mac computers are handed out in boxes. Applications are installed by users.
Directory Services	None. All users are local, created by users themselves, and are likely created as administrative accounts.
Support	Hard. No remote control and no inventorying.
Policies	None. Users can do (or fail to do) whatever they want.
Maintenance	Hard. No way to vet, deploy, or control updates.
Security	Minimal. You are trusting users to do the right thing.
Bottom Line	Scary. Works for some, but not for most. Huge security risks.

At this level, there is essentially no management of Mac clients at all. There is no standard deployment and no user management. This laxity allows users to do whatever they want. It can therefore lead to loss of intellectual property or other confidential data if a laptop is lost.

For most organizations, this may look like a low-cost approach at first glance. However, it's actually the least cost-effective because it results in high support costs. With no computer in a known good state, help desk staff must start from scratch every time they get a call.

Without directory services in place, there is no easy way to kill an account. This level, therefore, may fall short of the organization's defined SOX policies.

Level 2: Consistent Deployments

Imaging	Basic. Apple Software Restore (ASR) images are created from configured Mac systems.
Deployment	Basic. ASR disk images are deployed disk to disk with local booting. Applications can either be included in the base image or installed later by IT.
Directory Services	None. All users are local, created by users themselves, and are likely created as administrative accounts.
Support	Hard. No remote control and no inventorying.
Policies	None. Users can do (or fail to do) whatever they want.
Maintenance	Hard. No way to vet, deploy, or control updates.
Security	Minimal+. You are trusting users to do the right thing. Non-admin users may be created during configuration of the image.
Bottom Line	Better. ASR normalizes and speeds deployments. Security risks remain. Hard to maintain Mac computers once they're deployed.

Level 2 adds imaging. With the move to Apple Software Restore, a basic level of consistency is brought to deployments. New installs are all the same, and Mac clients can be reimaged to a known good state for troubleshooting.

The technician imaging the Mac for deployment should take the time to create a local admin account and a non-admin user account.

Without a maintenance system in place, software will either become stale, fall off the approved list, or be updated too quickly. To allow users to update software, they need to have administrative privileges on the Mac, which can potentially lead to security and reliability problems if that ability is misused.

Level 3: Light Management

Imaging	Basic. ASR images are created from configured Mac systems.
Deployment	Basic. ASR disk images are deployed disk to disk by booting each system locally. Applications can either be included in the base image or installed later by IT.
Directory Services	Centralized user database (Open Directory, Active Directory, LDAP, and so on).
Support	Easy. ARD allows for remote control and assistance. Directory services make user accounts a known entity.
Policies	None. Users can do (or fail to do) whatever they want.
Maintenance	Hard. No way to vet, deploy, or control updates.
Security	Better. Directory services allow for central account management, password policies, and single-point user kill. Most users are not at the admin level.
Bottom Line	Getting there. Centralizing users can tighten security. Remote assistance capability reduces the need to visit systems in person, minimizing support costs.

At Level 3, the addition of directory services significantly increases supportability, deployment ease, and security.

Mac OS X can use your choice of popular directory service architectures to centralize user accounts. The directory provides a single place to edit accounts and passwords. Because user accounts are now a known entity, support is simplified.

Security is much better now because users don't need administrative privileges, password policies are easily enforced, and accounts can be killed with a single mouse click.

The use of Apple Remote Desktop (ARD) for remote control and assistance greatly simplifies support. Users can request help, text chat, and receive support without leaving their desk or even picking up the phone.

Level 4: Medium-Bodied Management

Imaging	Basic. ASR images are created from configured Mac systems.
Deployment	Network. Disk images are deployed with NetBoot and NetRestore. Policies are implemented via MCX. Applications can either be included in the base image or installed later by IT.
Directory Services	Centralized user database (Open Directory, Active Directory, LDAP, and so on).
Support	Easy. Apple Remote Desktop allows for remote control and assistance. Directory services make user accounts a known entity.
Policies	MCX. The user experience is regulated. Application access and preferences are controlled. Operating system settings are managed. Unauthorized applications can be blocked.
Maintenance	Hard. No way to vet, deploy, or control updates.
Security	Good. Directory services allow for central account management, password policies, and single-point user kills. Policies keep users contained.
Bottom Line	Good. Centralized user database and deployment are enhanced by management policies. Greater control of Mac clients further reduces support costs.

Level 4 adds MCX policies and NetBoot for Apple Software Restore deployment.

NetBoot-based deployments scale much better than disk-to-disk imaging and allow multiple Mac clients to be imaged at the same time. Deployment is simplified by the use of policies to manage operating system and application settings.

At this level, users can't run applications to which they don't have rights. They can't install unauthorized applications from the Internet. Operating system settings are managed, eliminating the need for administrative staff to configure them.

Once a computer is deployed onto the network, it picks up the settings and preferences it needs. These settings are dynamic; if you need to change a setting on all systems, simply change it in Workgroup Manager, and the workstations will pick it up automatically.

With management policies in place, deployment and support efforts—and therefore IT costs—are reduced considerably.

Level 5: Robust Management

Imaging	Advanced. Local ASR images are created through an automated workflow.
Deployment	Advanced. Uses ASR or Apple's Custom Software Solutions (CSS) group. Disk images are deployed via NetBoot, multicast ASR, and NetRestore. Asset tagging ties physical to electronic records. Applications can be included in the base image or installed by CSS.
Directory Services	Centralized user database (Open Directory, Active Directory, LDAP, and so on).
Support	Very easy. ARD allows remote control and assistance. Directory services make user accounts a known entity. Inventorying enables hardware troubleshooting.
Policies	MCX. The user experience is regulated. Application access and preferences are controlled. Operating system settings are managed. Unauthorized applications can be blocked.
Maintenance	Managed. Tools such as ARD and Casper keep track of hardware and software. Updates are vetted, applied, and tracked. A management solution is used to deploy applications.
Security	Very good. Software and hardware control prevents unauthorized modifications.
Bottom Line	Great. There's a full software and hardware inventory. This accurate inventory allows for "cascading" redeployment strategies. Asset tags and electronic records track each Mac from cradle to grave. User and security policies lead to less IP leakage. Full management of software deployment leads to lower TCO.

Level 5 adds maintenance, advanced imaging, and advanced deployment.

Deployment image creation at level 5 is automated and modular, using installer packages. This approach reduces the support effort and increases the consistency of deployments. The process can be streamlined even further by automating first-round QA testing with Eggplant.

Apple Software Restore running in multicast mode makes the deployment of images massively scalable. The speed at which Mac clients can be imaged is restricted only by the number of network ports.

Support is even easier at this stage because there are full hardware and software inventories. All hardware and software are now in a known state.

Maintenance is now managed. Operating system and application updates are deployed programmatically to the installed base as a whole. Software updates are run through the recommended update policy (see the "Maintain" section of this paper), so each application is known to work properly and not affect production before it is deployed widely. Application of updates is tracked and known. Patch levels can be audited at any given time, even if a specific Mac is not currently on the network.

Comprehensive inventorying clears the way for large projects such as an operating system upgrade. Before you devote engineering hours to a project, you know exactly which computers can receive the update. A "cradle-to-grave" inventory allows for effective use of a "cascading" redeployment strategy. Every user has an appropriate Mac for his or her tasks, and no one has outdated equipment.

Application usage tracking in Apple Remote Desktop enables you to monitor license consumption and tweak it as needed. This helps you save money by reducing unneeded license purchases.

Summary

Level	1	2	3	4	5
Imaging	None	Basic	Basic	Basic	Advanced
Deployment	None	Basic	Basic	Network	Advanced
Directory Services	None	None	Centralized users	Centralized users	Centralized users
Support	Hard	Hard	Easy	Easy	Very easy
Policies	None	None	None	MCX	MCX
Maintenance	Hard	Hard	Hard	Hard	Managed
Security	Minimal	Minimal+	Better	Good	Very good
Bottom Line	Scary	Better	Getting there	Good	Great

Note that many deployments do not fit neatly into one specific level. For those cases, you can “mix and match” levels to some degree. Even in such instances, however, you can still use this scale to effectively grade your deployment.

For More Information

www.apple.com/remotedesktop

www.apple.com/server/macosx/netbootnetworkinstall.html

www.apple.com/server/macosx/workgroupmanagement.html

www.apple.com/server/macosx/softwareupdateserver.html

For more information, please contact your local Apple Authorized Reseller.