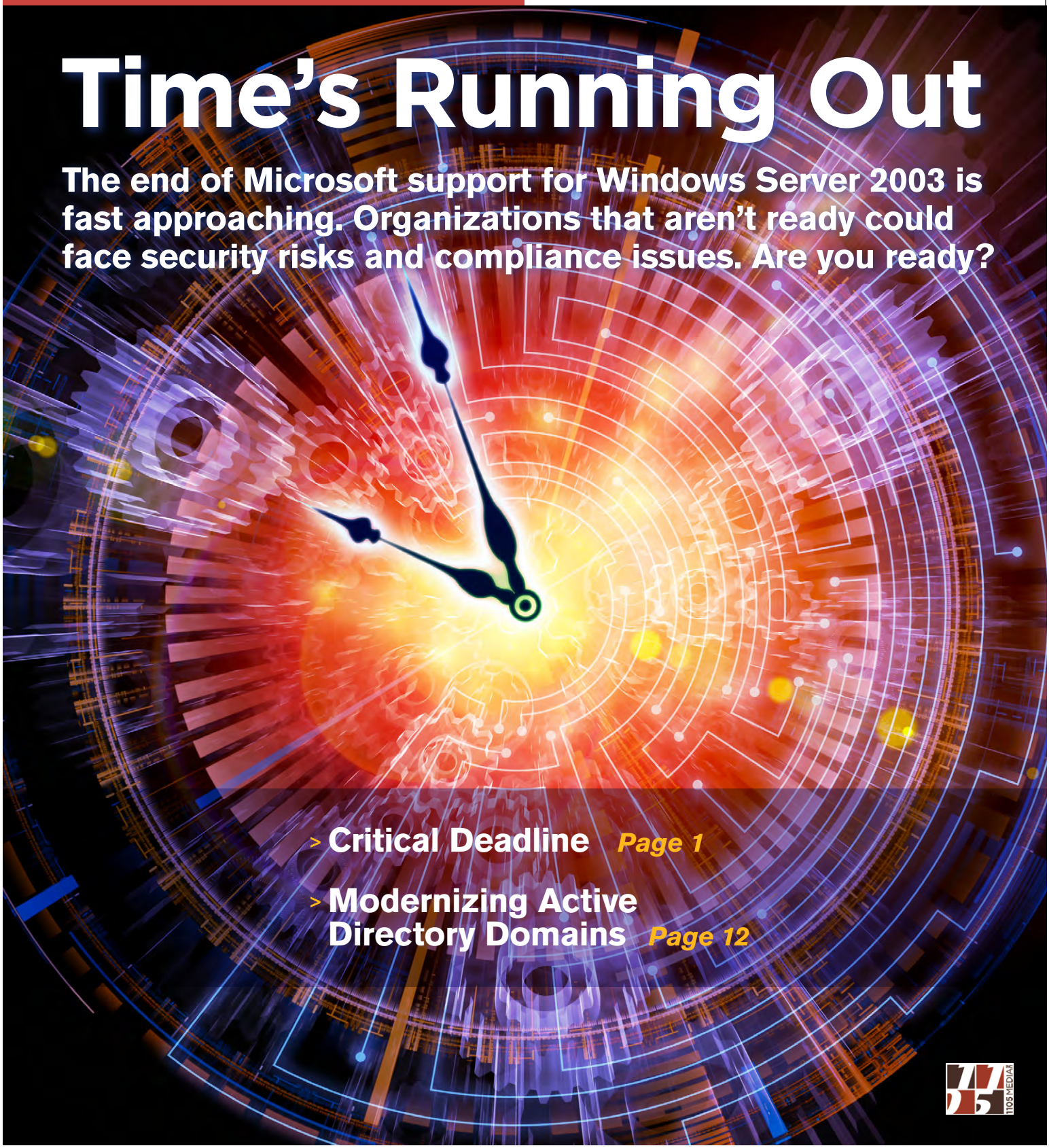
CONTENT PROVIDED BY

Redmond
THE INDEPENDENT VOICE OF THE MICROSOFT IT COMMUNITY

Time's Running Out

The end of Microsoft support for Windows Server 2003 is fast approaching. Organizations that aren't ready could face security risks and compliance issues. Are you ready?



1105 MEDIA

Critical Deadline

In less than five months, Microsoft will discontinue support for Windows Server 2003, meaning millions of systems could pose security risks and fail to meet compliance requirements. Are you ready?

BY JEFFREY SCHWARTZ

In the midst of planning the rollout of an electronic medical records (EMR) system throughout its network of hospitals and outpatient facilities, the IT organization at MaineHealth discovered numerous old servers scattered throughout the network that were running Windows Server 2003. Those servers must be decommissioned by July 14 of this year. That's not a deadline set by the powers that be at MaineHealth—it's the last day Microsoft will support the server OS.

Microsoft announced the end-of-service date many years ago, consistent with the lifecycle of its OSes. In keeping with the sunset dates for its OSes, after July 14, 2015, Microsoft won't issue security patches for Windows Server 2003. For many organizations governed by industry

"We have a few customers that have 3,000-plus systems on 2003 and there's no way they're going to get 100 percent of those by the deadline."

Rory McCaw, Managing Principal Consultant, Infront Consulting Group

or legal regulations such as the Sarbanes-Oxley Act (SOX) for publicly traded companies, the Payment Card Industry Data Security Standard (PCI for short) for those processing payments or the Health Insurance Portability and Accountability Act (HIPAA) for health-care providers like MaineHealth, that means those systems will no longer be in compliance.

It's unknown how many systems running Windows Server 2003 are still in production throughout the world, but the most recent estimates as of last month ranged from 8 million to 20 million—and that could mean instances or physical systems. Even with the largest guestimates, that may sound like a paltry number compared to the staggering amount of PCs running Windows XP that IT organizations had to remediate last year, which were likely in the hundreds of millions last April.

The expiration of Windows Server 2003 won't be as high-profile to the general public as the demise of Windows XP (see "This Is the End," April 2014, **Redmondmag.com/WinXP14**), but experts say it's as important if not more so that IT upgrade them. Unpatched servers have the potential to do more harm given the number of devices, network nodes and client devices the servers touch experts say. Moreover, like Windows XP, many IT managers don't see a need to upgrade those systems, many of which either perform perfunctory functions, while others run mission-critical systems or hardware that can't easily be upgraded to newer server OSes.

"Windows Server 2003 was a very popular product for us and our partners," said Mark Linton, senior director of portfolio and product management within the Microsoft Worldwide OEM division, speaking at a media gathering in New York organized by Dell Software. "The challenge with that is having folks migrate off a popular operating system. We've had that Windows XP discussion and it's a similar story here."

Clock Is Ticking

Just like many organizations let last year's Windows XP end-of-service deadline come and go, many will do the same with Windows Server 2003, though many have it on their agenda for this year. Nearly one-third or about 32 percent of *Redmond* readers indicated

that upgrading old Windows Server 2003 systems is top priority this year, as noted in last month's cover story ("Marching Orders," **Redmondmag.com/Orders2015**). It ranked fourth and was closely behind related activities that include virtualizing servers, replacing aging server hardware and upgrading network infrastructure.

Nevertheless, many organizations may not beat the clock. A survey of 500 IT professionals conducted throughout last year by application remediation tool vendor AppZero Inc. found that 65 percent will not complete their Windows Server 2003 migrations by July 14. Some, 29 percent, will complete those upgrades by the end of the year, while 10 percent said sometime in 2016 and 27 percent claim they don't know. Nearly one-third (31 percent) have no upgrade plan while 16 percent said they didn't even know that Windows Server 2013 comes out of service on July 14. Many are still researching their options.

Rory McCaw, managing principal consultant with Infront Consulting Group, says his clients started to get more serious about the pending deadline at the beginning of the year.

Rory McCaw, managing principal consultant with Toronto-based Infront Consulting Group, says his clients started to get more serious about the pending deadline at the beginning of the year. But he warns some with larger Windows Server 2003-based systems may not get them all mitigated in time. Those facing that situation will have to prioritize, McCaw says. "We have a few customers that have 3,000-plus systems on 2003 and there's no way they're going to get 100 percent of those by the deadline," he says. "They're really looking at the mission-critical apps, what they can decommission, and maybe even the very easy workloads, like Web workloads that can migrate pretty easily, and getting those converted."

Migration Planning

Microsoft offers its own tool, called the Microsoft Assessment and Planning (MAP) toolkit. "That's where we recommend customers go to first," Linton explained at the New York media event. "It allows you to do a basic profile of your network and look at your Windows Server 2003 boxes or instances and understand what workloads you're running. That's the first step. Are you doing identity, branch office solutions, is it a SQL Server box running a departmental line-of-business app, or is it more complex? Being able to categorize what the servers are doing is really the first step in saying 'where am I at, are these basic workloads?' because that's a faster migration. If I have a bunch of custom code, 32 bit apps that I wrote 15 years ago, that's more complex."

KEEP YOUR WINDOWS SERVER 2003 SYSTEMS SECURE AFTER END OF LIFE.

ENDPOINT THREAT PREVENTION

+

DETECTION AND RESPONSE IN SECONDS

www.bit9.com/Windows2003EndofLife

Bit9 + CARBON BLACK

ARM YOUR ENDPOINTS.

In addition to Dell, there are a variety of partners that offer a variety of Windows Server 2003, application and Active Directory migration tools including AppZero, Binary Tree, BlueStripe Software, Hewlett-Packard Co., Flexera Software and Lakeside Software Inc.

Linton said depending on the complexity of an infrastructure, number of applications and hardware that require migration or mitigation, it can take anywhere from eight to 12 months to complete and that presumes they already have the budget and needed go-ahead to do so. Like anything, though, McCaw says it depends on the infrastructure. "We try to break it down per application or per server, so we're looking at an average of between five and 30 hours per server or per app," McCaw explains. "That's a pretty big range, I understand, but it depends how complicated and complex the application is."

The biggest issue facing those who need to move applications or data running on Windows Server 2003 systems is Active Directory remediation because the domain controller structure on newer versions of Windows Server aren't compatible.

Often the Windows Server 2003 systems deployed are on old towers, predating the introduction of server blades, as well as converged systems now available. It's not uncommon for them to be scattered and it's typical that they're not virtualized. "In most cases what we're finding is that customers are taking this opportunity to virtualize those systems," says Michael Tweddle, executive director of product management at Dell Software.

Taking those old systems out of service in many cases requires a number of key decisions, including what version of Windows Server to move to and whether to move the applications and data to a cloud service rather than deploying new servers. Among the key issues, many applications and hardware interfaces developed for Windows Server 2003 and its predecessors are 32-bit and in a good number of cases won't simply run on a newer version (Windows Server 2008 and higher is 64-bit-only). The biggest issue facing those who need to move applications or data running on Windows Server 2003 systems is Active Directory remediation because the domain controller structure on newer versions of Windows Server aren't compatible. Overall the effort can be costly.

"It's very expensive to move," warns AppZero CEO Gary O'Connor. "If you're assuming the application doesn't have source code, and you're going to migrate, some of the system integrator partners that we have will charge you somewhere between $2,000 and $5,000

per machine. If you have 10,000 machines, it can cost $20 to $50 million and probably two or three times that if you have to buy new software and a landing pad. You can quickly get into a $100 million budget. Even though these are large banks with lots of money, that's expensive."

Many organizations will have no choice but to bring in outside help, given their already burdened IT staffs. In the case of MaineHealth, Paul Caron, supervisor of information services, said at the Dell Software event his IT team, while engaged in a Windows Server 2003 and Active Directory DC consolidation effort to enable access

Keep Your Systems Secure

If a third-party security providers tells you can keep your Windows Server 2003-based system secure, Microsoft is reminding customers to not believe it, because only Redmond has the ability to issue patches for any of its OSes.

"Only Microsoft is able to do the patches because it's in the core operating system itself," said Mark Linton, senior director of portfolio and product management within the Microsoft Worldwide OEM division, at a recent media event in New York, which was sponsored by Dell Software. "So complacency is really a risky thing."

Likewise, Microsoft is warning against trying to mitigate the security risk by virtualizing Windows Server 2013. "If you put it in a virtual sandbox and say, 'If I whitelist the app running on top of it, it may make it more safe,' but the answer is it isn't safe," Linton added. "There are different vectors at which security exploits can come in. They can come from the network layer through the app layer. We really don't recommend that approach."

Additionally, anti-malware software like Microsoft System Center Endpoint Protection and Forefront Endpoint Protection will no longer receive updated malware protection data. Windows Server 2003 has been a consistent recipient of monthly security fixes. In 2014 alone, Windows Server 2003 received seven security updates rated "critical" and 18 rated "important" by Microsoft.

The potential threats that may arrive once July's deadline has passed was enough for the United States Computer Emergency Readiness Team (US-CERT) to issue an alert in November 2014, saying those running Windows Server 2003 will leave them open to attacks that could compromise "… confidentiality, integrity, and/or availability of data, system resources and business assets."

— J.S. with Chris Paoli Contributing

to the EMR system from any location, had only so much bandwidth for the project. "I supervise a team of 10 that deals with a lot of things including VMware, Citrix, SQL Server, physical servers, virtual servers, and I don't want my staff to become migration experts," he said. "We have so much in the hopper."

Caron said his team initially tried doing it themselves using the various free migration tools from Microsoft including the MAP tool for Windows Server 2003 for an e-mail migration. "We had a poor experience with the data tools before we engaged with Dell," he said. "We were able to piece together what we needed and we made it work, but there were too many planets lined up for that migration. Things worked well, but we really doubted we would ever get that again. We had great partners on the opposite side," referring to Dell Services and Microsoft.

MaineHealth found it had many more Windows Server 2003-based machines than it realized.

Like many embarking on the migration will find during the discovery phase, MaineHealth found it had many more Windows Server 2003-based machines than it realized. That was the result of shadow IT, where people with limited skills were putting boxes under their desks. "In the one organization that had one domain controller, we asked how many servers do you have, they responded, 'Two. Well … three, really. Well … really four.' Of those servers, two were server-class hardware, two were running on PCs. They didn't know."

Legacy Systems

Once the discovery is made, Active Directory must be reconfigured when running on a newer version of Windows Server (see "Modernizing Your Active Directory Domains," p. 12). Because MaineHealth wanted to consolidate its Active Directory domains irrespective of the Windows Server 2003 deadline, that became an opportunity for Caron. MaineHealth decided to collapse the 21 Active Directory domains covering all of the hospitals in the network to just one to provide common authentication and security of the patient records stored in the new EMR system. "Our biggest business driver was one patient, one record," Caron says. "If anybody has had to stop into the emergency room and has to fill out the 27 pages worth of medical history, it's a pain in the behind. With our vision of one page, one record, if you're at another hospital that's part of the MaineHealth family, they would have access to your records in a secure fashion."

"I will let you know from personal experience, I have yet to find an issue where a schema has been unable to be upgraded or is damaged after the fact, unless you're running a very old version of Exchange still and that was the biggest gap that we had, or unless you had some developers who were cowboys and decided to go off and randomly change object IDs inside Active Directory, and just screw something up."

Rick Claus, Senior Technical Evangelist, Microsoft

Like many IT organizations in Caron's shoes, MaineHealth didn't have the internal resources to take on that project so it brought in Dell Services, the consulting and systems integration division of the Round Rock, Texas, computer and systems provider. Not surprisingly, Dell Services used a variety of tools from Dell Software, primarily those it gained in its 2012 acquisition of Quest Software, such as ChangeBASE for compatibility testing and Migration Manager for upgrading the Active Directory domains.

Besides consolidation of the domains, there are numerous other disparities between the iteration of Active Directory in Windows Server 2003 and the current release, says Alan West, founder of XMS Solutions Inc., a Henderson, Nev.-based provider of migration services.

"There are also authentication security differences between the two operating systems from an Active Directory standpoint and Kerberos authentication differences with NTLM," West says. Among other authentication-level differences are Server Message Block (SMB) signing, he adds. "It was supported in 2003 but it wasn't the default. Things like just moving a file from the file server to someplace else, now in a modern OS requires that you authenticate I am who I say I am, this file actually coming to me and not that you're spoofed with SMB signing."

Overall, updating Active Directory schema to migrate to newer versions of Windows Server isn't a risky or difficult undertaking, says Rick Claus, a senior technical evangelist at Microsoft, who spoke about Windows Server 2003 migration at the most recent TechMentor conference in Orlando, Fla., which is produced by *Redmond* parent company 1105 Media Inc.

"I will let you know from personal experience, I have yet to find an issue where a schema has been unable to be upgraded or is damaged after the fact, unless you're running a very old version of Exchange still and that was the biggest gap that we had, or unless you had some developers who were cowboys and decided to go off and randomly change object IDs inside Active Directory, and just screw something up," Claus explains.

Key Choices

Microsoft and others recommend organizations needing to rid themselves of any number of Windows Server 2003 systems (and in some cases Windows 2000 and even Windows NT, which Microsoft stopped supporting long ago) to upgrade to modern server architectures or consider a hybrid or even public cloud alternative. In instances where the IT decision makers have opted to replace it with on-premises-based systems, Microsoft and most experts advise choosing the most current version of the OS—Windows Server 2012 R2. Don't bother waiting for a new version of Windows Server this year—Microsoft last month announced the new version, dubbed vNext, won't arrive until 2016.

Microsoft will selectively offer large enterprises that have migration strategies in place some refuge.

Microsoft will selectively offer large enterprises that have migration strategies in place some refuge. Through custom support agreements, the company will continue to offer specialized updates, though the price is high: anywhere from $1 million to $2 million per year and the fee will double every year (Microsoft wouldn't officially confirm those figures). But after three years, even that option goes away. "The big challenge is after three years there is no more support agreements and some of these enterprises have 20,000 machines and you can only move 3,000 a year, so I think that's going to be a big problem for a lot of people," says AppZero's O'Connor.

File and Print Servers

In many organizations, especially branch offices, file and print servers are still running on Windows Server 2003-based systems. Many organizations can use that as an opportunity to modernize their network infrastructures with bandwidth acceleration hardware or services from the likes of Akamai Technologies, Cisco Systems Inc., F5 Networks Inc. or Riverbed Technology. By doing so they can centralize their file services now while getting the same performance available when they were stored locally.

Alternatively, others are using the Windows Server 2003 end-of-service deadline as an opportunity to eliminate local servers by moving to cloud services such as Office 365. By moving all these features off-premises, often the only time a server is even needed in a small or branch office is if it's running a legacy phone system or, perhaps, routing jobs to network printers.

One way to eliminate print servers is to use third-party tools such as PrinterLogic, which creates printer objects and uses the DNS settings on the local network to route the print job to the user's printer of choice. The system can be managed by an administrator off-site, if the location doesn't have one, says Jarrrett Taylor, founder and CTO of PrinterLogic. "It's a real fertile time to say, 'Do we need these print servers?'" he says. "With our platform, you just get rid of them, and you put an agent on the desktop and you use our administrative console to manage the printer objects. And then our agent takes care of it on the desktop and then they don't need to have those servers at the branch locations."

Regardless of size, undergoing a Windows Server 2003 migration effort will inevitably result in some unexpected findings along the way.

Expect Surprises

Regardless of size, undergoing a Windows Server 2003 migration effort will inevitably result in some unexpected findings along the way. Caron at MaineHealth said the best approach is to push back with management when unrealistic expectations are set.

"Expect the unexpected," he said "We faced a variety of challenges, whether it was senior management tapping us at the door saying we need this done by June, or servers crashing while we were in the process of just looking at them," he said. "We never found high-quality systems that were well designed that we could take over rather than keep them in place. We've had to demolish and push out as quickly as we could so we could get rid of some of these older clunkers." R

Jeffrey Schwartz is editor in chief of Redmond.

AN EMPLOYEE JUST LEFT WITH INTELLECTUAL PROPERTY

IT'S GONNA HIT

BE THE ONE WHO SAW IT COMING.
BE THE ONE WHO PURCHASED SPECTOR 360 RECON.
BE THE ONE WHO STOPS THE THREAT & GETS THE RAISE.

- Complete, accurate, contextual log of all user activity
- Timely alerts on known threat indicators
- Ability to retrieve detailed evidence if needed

SpectorSoft

Get It At: www.spectorsoft.com/hitthefan

MODERNIZING

Active Directory Domains

Migrating from Windows Server 2003 requires organizations to decommission existing Global Catalogs and domain controllers to conform with Active Directory schema in newer versions of the server OS. BY JOHN O'NEILL SR.

Migrating your Windows Server 2003 Active Directory DCs to Windows Server 2012 R2 doesn't have to be a showstopper.

Of the many remediation efforts IT organizations must undergo when migrating off Windows Server 2003, the decommissioning of antiquated Active Directory domain controllers to implement the more robust Active Directory functionality in Windows Server 2012 R2 is a top priority. It's not optional and, in addition to application- and hardware-compatibility issues, is a key reason many organizations have put off sunsetting their Windows Server 2003-based systems, even though Microsoft has made clear for years that it'll no longer support it after July 14, 2015.

But migrating your Windows Server 2003 Active Directory DCs to Windows Server 2012 R2—the most recent and, hence, recommended target platform to replace the decommissioned servers—doesn't have to be a showstopper. This step-by-step, click-by-click process through a test environment's AD schema will demonstrate how to upgrade your AD schema, raise the forest functional level to get a Windows Server 2012 R2 Global Catalog (GC) DC up and running. It will also explain how to take the necessary step of decommissioning existing Windows Server 2003 GCs and DCs.

For this article, the test environment consists of a single forest, a single domain AD with a single Windows Server 2003-based DC. Therefore, this DC is also the AD GC and holds all five Flexible Single Master Operations (FSMO) roles. In addition, the server acts as

the internal DNS server for the AD domain. The AD forest functional level is Windows Server 2003. Although this functionality list might seem daunting, with a bit of planning and a methodical approach, migrating all of these functions is a straightforward process.

Raise and Verify AD Forest Functional Levels

Pro Tip No. 1: If your organization's AD forest and/or domain functional level is still Windows 2000, it must be raised before going any further. Installing a Windows Server 2012 R2 DC into an existing domain requires the forest and domain functional level to be Windows Server 2003 or higher.

If your organization's AD forest and/or domain functional level is still Windows 2000, it must be raised before going any further.

Verify the functional level of the domain by logging into the Windows Server 2003 DC with a domain admin-level account. Click Start, expand Administrative Tools and then click Active Directory Domains and Trusts. In AD Domains and Trusts, right-click the domain name and then select Raise Domain Functional Level. If it shows anything less than Windows Server 2003 as the current domain functional level, drop down the list box for available functional levels. Select Windows Server 2003, then click the Raise button. Click OK when prompted and then you've raised the functional level. No reboot of the server should be required, but if multiple DCs exist, allow ample time for the changes to replicate throughout the domain. Replication time required could vary from 15 minutes to four hours or more, depending on your particular network design.

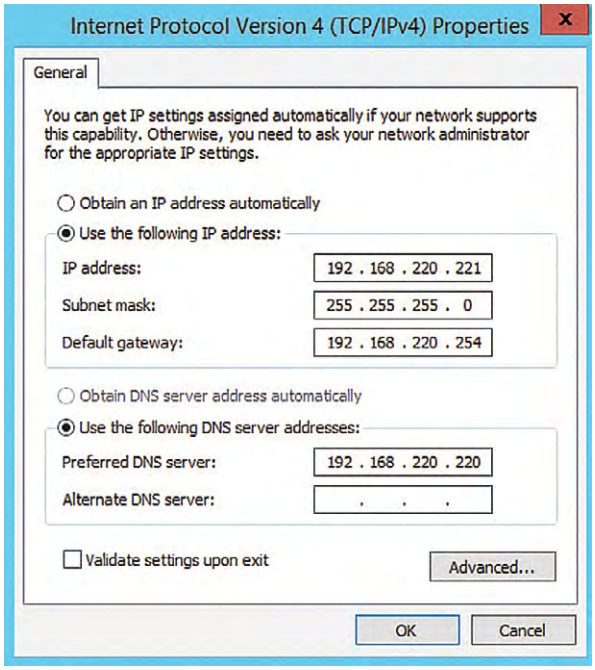


Figure 1. *Make sure your DNS settings are consistent with your network.*

Verifying the functional level of the forest is done in much the same manner. Log into the Windows Server 2003 DC with a domain admin-level account. Click Start, expand Administrative Tools and then click Active Directory Domains and Trusts. In AD Domains and Trusts, on the left side of the screen, right-click Active Directory Domains and Trusts. Note that this isn't the domain name as used in the previous step. After right-clicking Active Directory Domains and Trusts, a context-sensitive menu appears. Select Raise Forest Functional Level. Again, if the current forest functional level list box displays anything earlier than Windows Server 2003, select Windows Server 2003, then click the Raise button. Click OK to

confirm understanding that the change is permanent and affects the entire AD forest. Click OK when prompted that raising the forest functional level completed successfully. Just as when raising the domain functional level, no reboot of the server should be required. As always when making domain architecture changes, if multiple DCs exist, allow ample time for the changes to replicate throughout the domain. Remember, replication time required could vary from 15 minutes to four hours or more, depending on your particular network design.

Step 1: Prepare a Windows Server 2012 R2 Server

Set up Windows Server 2012 R2 on a new host, either physical or virtual.

Begin with the basics. Set up Windows Server 2012 R2 on a new host, either physical or virtual. After installation, set a static IP and configure the subnet mask, gateway and DNS server settings consistent with the network (see **Figure 1**, page 13). Install any available critical and recommended Windows Updates. As a final step, join the new server to the existing AD domain. A basic Windows Server 2012 R2 member server is now up and running!

Step 2: Add the AD DS Role on the New Server

To set up your target, log on to the Windows Server 2012 R2 server using an account with domain admin permissions. Open Server Manager. By default, the Dashboard view will display. Under Configure this local server click Add roles and features. The Add Roles and Features Wizard will open. Click Next. Click the radio button for Role-based or feature-based installation. Click Next.

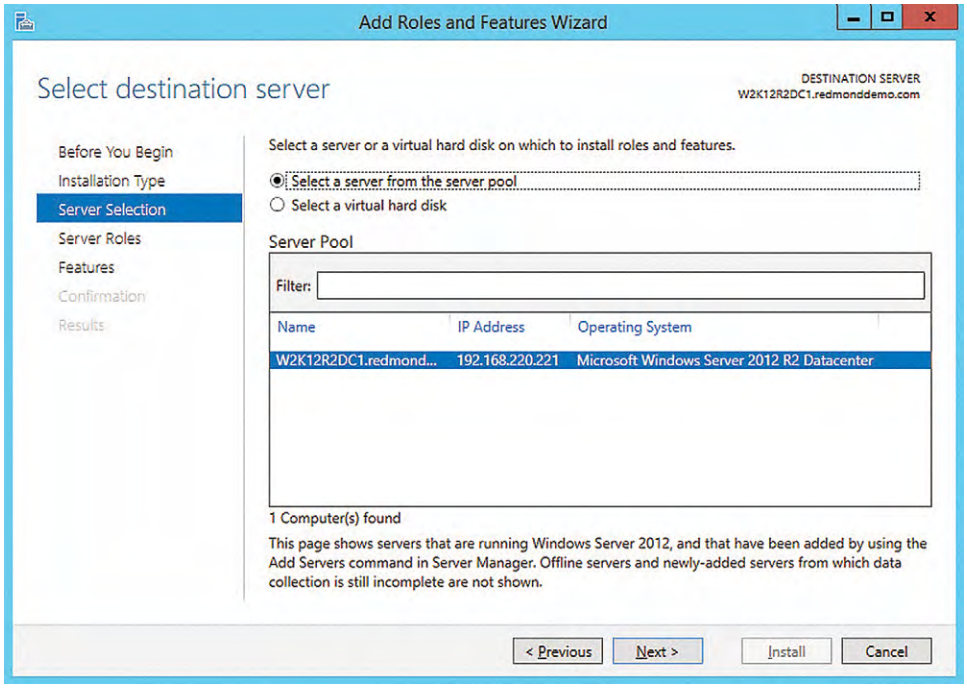


Figure 2. *Selecting the destination sever and verifying the appropriate target.*

Click the radio button for Select a server from the server pool. In the list of displayed servers, verify the current server is highlighted (see **Figure 2**). Click Next.

From the list of displayed roles, find and click the

checkbox for Active Directory Domain Services. This will pop up a dialog asking to Add features required by Active Directory Domain Services. Click the checkbox to Include management tools (if applicable). Click the Add Features button to continue.

From the list of displayed roles, verify the Active Directory Domain Services checkbox is still selected. Find and click the checkbox for DNS Server. Click Next.

Notice in the Features list some options are already selected. Some of these represent previously installed features while others were selected when the Add features required by Active Directory Domain Services option was chosen earlier. Click Next.

The final page of the Add Roles and Features Wizard displays a summary of the options selected for configuration.

The next step of the wizard displays a bit of background information regarding Active Directory Domain Services. Nothing mind-blowing or mind-boggling is presented here. Click Next. Another informational page explains DNS and its integration with AD. Click Next.

The final page of the Add Roles and Features Wizard displays a summary of the options selected for configuration. Click Install and watch the wizard work its magic! The wizard will confirm installation was successful while reminding you that additional steps are necessary to promote this server to DC functionality. Click the link to Promote this server to a domain controller (see **Figure 3**). The Active Directory Domain Services Configuration Wizard opens.

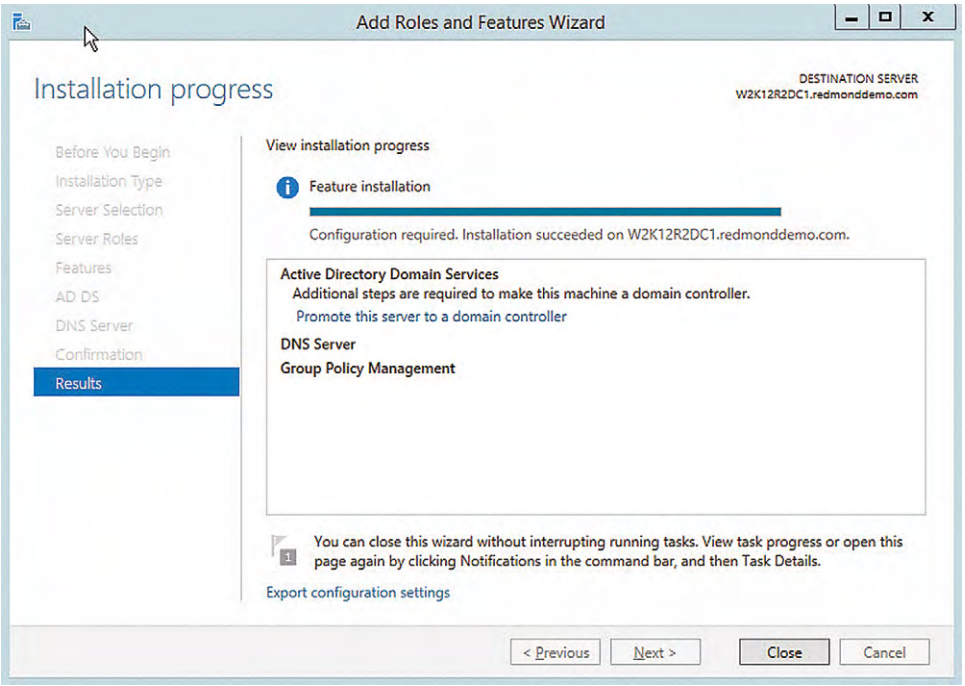


Figure 3. *After successful installation of the DNS Server is confirmed, choose Promote this server to a domain controller.*

Step 3: Promote the Windows Server 2012 R2 Server to a DC

On the initial page of the Active Directory Domain Services Configuration

Wizard, select the radio button for Add a domain controller to an existing domain. Because this server is already a member of the domain, and is logged in using an account with domain admin-level privileges, the wizard will automatically populate the Domain and Credential information. Confirm everything, then click Next to continue.

Pro Tip No. 2: A warning appears that "A domain controller running Windows 2008 or later could not be located in this domain…" This warning applies to read-only DC (RODC) installation. Because you're not installing an RODC the warning can, and should, be ignored.

The next screen appears with the site name selected and both DNS Server and GC options already checked. If for some reason this isn't the case, select the appropriate site from the dropdown list and click the checkboxes beside the DNS Server and GC options.

Think up a secure Directory Services Restore Mode password.

Think up a secure Directory Services Restore Mode password. Mix capital and lowercase letters, numbers, and special characters. Type it in both the Password and Confirm password boxes. Try and cheat the system with a simple password and an error will appear. Click Next.

On the next screen, ignore the warning "A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found…" Click Next.

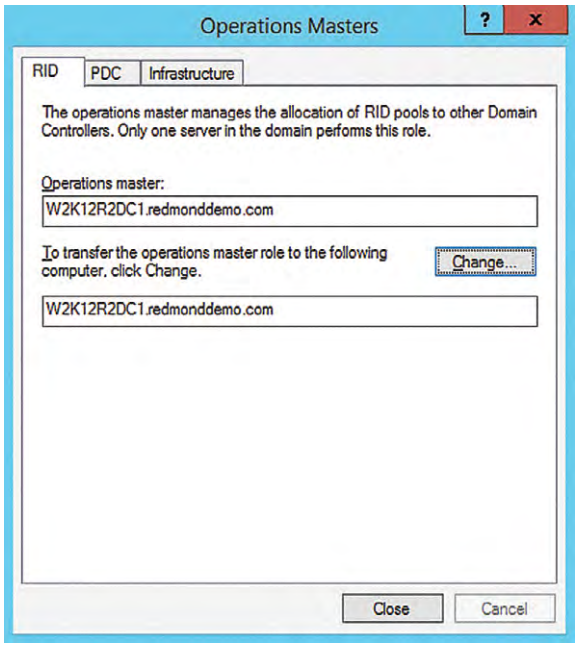


Figure 4. *Transfer the operations master role to the new server.*

Click Next on the Additional Options, Paths and Preparation Options screens. No changes are required.

On the Review Options screen, verify all the earlier selections. Interested in the Windows PowerShell commands that will run behind the scenes completing the DC promotion? Click the View Script button. Notepad opens displaying the necessary cmdlets, complete with customized parameters. The entire process is completed using just two cmdlets.

Click Next. A Prerequisite check runs, ultimately displaying warnings about the DNS delegation error encountered earlier and a note about security setting defaults in Windows Server 2012 R2. These issues

won't prevent completing promoting the server to a DC. Scroll down the results window and a green checkmark is displayed next to: All prerequisite checks passed successfully. Click "Install" to begin installation. This information is also displayed at the top of the window and is the all clear to proceed. Note, the server will automatically reboot after promotion to a DC. Click the Install button to kick things off.

The actual promotion process takes a few minutes. There's a lot to be done! The entire AD schema is being upgraded. The saying "patience is a virtue" comes to mind. Once the server reboots on its own, log on with a domain admin-level account. Congratulations! A new Windows Server 2012 R2 DC and DNS server is now up and running!

The entire AD schema is being upgraded.

Step 4: Transfer the FSMO Roles

Transferring the five Flexible Single Master Operation (FSMO) roles isn't as difficult as it might seem. In fact, simply decommissioning the existing Windows Server 2003 DC will automatically transfer the FSMO roles. While automatic is attractive, manually transferring the roles isn't difficult and has the added benefit of granular control.

To transfer the Relative ID (RID) Master, PDC Emulator and Infrastructure Master Roles, log on to the newly minted Windows Server 2012 R2 DC using an account with domain admin-level privileges. On the Start screen begin typing Active Directory Users and Computers. The Search Charm opens. Click Active Directory Users and Computers from the results list. The AD Users and Computers app opens on the desktop. Right-click the domain name in the left pane, then select Operations Masters from the context-sensitive menu. The Operations Masters window appears, displaying three tabs; RID, PDC and Infrastructure. Each tab displays the current operations master for that role. The current server is also displayed along with a change button enabling the transfer of each role.

On the RID tab, click the Change button. When prompted, click Yes to transfer the role to the current server. A message box quickly confirms the role transferred successfully. Click OK to dismiss the message. The current server is now the RID operations master (see **Figure 4**, page 16). Complete the same process for the PDC and Infrastructure tabs. Click the Close button, exiting the Operations Masters dialog. Close the Active Directory Users and Computers app. Three roles down, two to go!

On the Windows Server 2012 R2 Start Screen, type Active Directory Domains and Trusts. The Search Charm will open displaying Active Directory Domains and Trusts in the results (see **Figure 5**). Click Active Directory Domains and Trusts, or simply hit Enter, to open the application.

In the left pane, right-click Active Directory Domains and Trusts right above the domain name. Click Operations Masters in the context-sensitive menu that appears. As before, an Operations Masters dialog will open. Click the Change button. Click Yes to confirm the role transfer and then click OK to dismiss the transfer successful message box. Click Close and exit the Active Directory Domains and Trusts app.

Transferring the Schema Master role is a bit involved.

Transferring the Schema Master role is a bit more involved. Log on to the Windows Server 2003 DC using an account with domain admin-level privileges. Click Start, then Run. In the Run dialog box, type regsvr32 schmmgmt.dll, then click OK. A message box displays, confirming the schmmgmt.dll registration succeeded. Click OK to dismiss the message box.

Click Start, then Run. Type MMC and hit Enter. An empty Microsoft Management Console will open on the desktop. Press Ctrl and M simultaneously to open the Add or Remove Snap-ins dialog. If you prefer, clicking File, then Add/Remove Snap-in accomplishes the same thing. Click the Add button. From the list of available snap-ins, select Active Directory Schema. Click the Add then Close button. Click the OK button to close the Add/Remove Snap-in dialog.

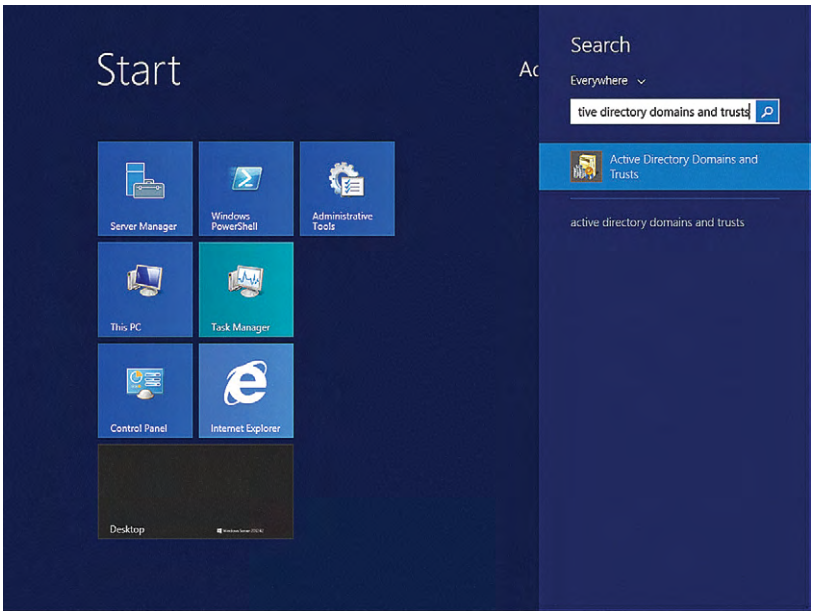


Figure 5. *Using the Search Charm to open Active Directory Domains and Trusts.*

In the left pane of the MMC window, right-click Active Directory Schema. Click Change Domain Controller. Click Specify Name, type the name of the Windows Server 2012 R2 DC, and then click OK. Almost done. Right-click Active Directory Schema in the left-pane again, then click Operations Masters. Click

Change, confirm by clicking Yes, then click OK when the transfer successful message box pops up. All five FSMO roles are transferred!

Step 5: Decommission the Windows Server 2003 DC

The final step is to decommission the Windows Server 2003 DC. Logged onto the Windows Server 2003 DC with a domain admin-level account, click Start, and then Run. Type DCPromo and click OK. The Active Directory Installation Wizard opens. Because the system is already a DC, the wizard will remove Active Directory Services demoting the DC to a member server.

Click Next. A warning cautions that another Global Catalog server must be on the network before this DC is decommissioned. There's nothing to worry about because the Windows Server 2012 R2 DC commissioned earlier was configured as a GC. Click OK to continue the wizard.

Make absolutely sure the checkbox next to "This server is the last domain controller in the domain" is not selected.

Make absolutely sure the checkbox next to "This server is the last domain controller in the domain" is not selected. I repeat, *do not* check this checkbox!

Click Next. Type a password to be used for the local administrator account. Type the password again to confirm, then click Next.

Click Next one last time on the summary screen. The demotion takes a few minutes. Once the process completes, click Finish, and then Restart Now. That's it! The Windows Server 2003 DC is decommissioned.

Even those organizations still running Windows Server 2003 DCs needn't panic over the looming Windows Server 2003 end of support. Following this guide, you can quickly, and fairly painlessly I might add, migrate a Windows Server 2003 AD to the much more stable and robust Windows Server 2012 R2 AD. Of course, completing the process before the July 14 deadline certainly lowers the overall stress level! R

John O'Neill senior is a Microsoft MVP and has 20 years of experience as an IT pro working in various roles as a consultant, architect executive, speaker and author. Follow him on Twitter at: @JohnONeillSr.