Securing Privileged Access for the AD Admin: Part 2

techcommunity.microsoft.com/blog/coreinfrastructureandsecurityblog/securing-privileged-access-for-the-ad-admin-part-2/259167

Blog Post

First published on TechNet on Sep 18, 2017

Hello everyone, my name is still David Loder, and I'm still PFE out of Detroit, Michigan. Hopefully you've read Securing Privileged Access for the AD Admin – Part 1. If not, go ahead. We'll wait for you. Now that you've started implementing the roadmap, and you're reading this with your normal user account (which no longer has Domain Admin rights), we'll continue the journey to a more secure environment. Recall the overarching goal is to create an environment that minimizes tier-0 and in doing so establishes a clear tier-0 boundary. This requires understanding the tier-0 equivalencies that currently exist in the environment and either planning to keep them in tier-0 or move them out to a different tier.

Privileged Access Workstations (PAWs) for AD Admins

You've (hopefully) gone through the small effort to have a credential whose only purpose is to manage AD. Let's assume you now need to go do some actual administering. The only implementation that prevents expansion of your tier-0 equivalencies would be to physically enter your data center and directly log on to the console of a Domain Controller. But that's not very practical for any number of obvious reasons and I think everyone would agree that an AD Admin being able to perform their admin tasks remotely from a DC console is a huge productivity gain. Therefore, you now need a workstation.

I'm going to guess that most of you use the one workstation that was handed out by your IT department. That workstation which uses the same base image for every employee in the organization. That workstation which is designed to be managed by your IT department for ease of support. Yes, that workstation.

Recall last time we spent almost all our time talking about tier-0 equivalencies. Guess what? I'm going to sound like a broken record. Item #3 from our elevator speech in part one stated "Anywhere that tier-0 credentials are used is a tier-0 system." What is the new system we just added to tier-0? That workstation. Now, any process that has administrative control over that workstation is a tier-0 equivalency. Consider patching, anti-virus, inventory and event log consolidation. Is each of those running as local system on your workstation and managed by a service external to the laptop? Check, check, check and check. Does it have Helpdesk personnel as local admins? Check. I'll ask again how big is your tier-0?

I hear some of you starting to argue 'I don't actually log on to my workstation with my AD admin credential, I use [X].' What if you use RunAs? That workstation is still a tier-0 system. What if you use it to RDP into a jump-box? That workstation is still a tier-0 system. What if you have smartcard logons? Still a tier-0 system. Some of the supplemental material goes into the details of the various logon types, but the simple concept is 'secure the keyboard.' Whatever keyboard you're using to perform tier-0 administration is a tier-0 system.

Now that we've established that your workstation really is a tier-0 system, let's treat it as such. Start acting like your workstation is a portable Domain Controller. Think of all those plans, procedures and systems you have in place to manage the DCs. You need to start using them to manage your workstation. My fellow PFE Jerry Devore has an in-depth look at creating a PAW to be your admin workstation.

Should your PAW be a separate piece of hardware? Preferably, yes. That way it is only online when it needs to be used, helping to reduce the expansion of tier-0 to the minimum necessary. If your organization can't afford separate hardware you can virtualize on one piece of hardware. But the virtualization needs to occur in the opposite direction than you might ordinarily expect. The PAW image will still need to run as the host image, and your corporate desktop would be virtualized inside. This keeps any compromise of your unprivileged desktop from elevating access into your PAW.

This is another big step/small step decision. PAWs will be a change for your organization. If you can start small by implementing it for a few AD Admins, you can show your enterprise that using PAWs can be a sustainable model. At later phases in the roadmap you can expand PAWs to more users.

With a PAW in place you now have a tier-0 workstation for your tier-0 credential to manage your tier-0 asset. Congratulations, by implementing the first two steps down the SPA roadmap, you now have the beginnings of a true tier-0 boundary.

Unique Local Admin Passwords for Workstations

So far, we've been talking about protecting your personal AD Admin accounts. But everyone knows AD has its own built-in Administrator account that is shared across all DCs. Ensure you have some process in place to manage that specific "break in case of fire" account. Maybe two Domain Admins each manage half of the password, and those halves are securely stored. The point is: have a procedure for managing this one account. Be careful if you decide to implement an external system to manage that password. Do you want that external system to become tier-0 just to manage one AD Admin account? I can't answer that question for you, but I can point out that it is a tier-0 boundary decision. Your new PAWs, on the other hand, will have one built-in Administrator account per PAW. How do we practically secure those multiple Administrator accounts without increasing the size of tier-0?

The answer is to implement Microsoft's Local Administrator Password Solution (LAPS). Simply put, LAPS is a new Group Policy Client Side Extension (CSE), available for you to deploy at no additional cost. It will automatically randomize the local Administrator account on your tier-0 PAWs on an ongoing basis, store that password in AD and allow you to securely manage its release to authorized personnel (which should only be the tier-0 admins). Since the PAW and AD are both already tier-0 systems, using one to manage the other does not increase the size of tier-0. That fits our goal of minimizing the size of tier-0.

These new PAWs that you just introduced into the environment also become the perfect place to begin a pilot deployment of LAPS. Install the CSE on the PAWs, create a separate OU to hold the PAW computer objects, create the LAPS GPO and link it to the PAW OU. You'll never have to worry about the local admin password on your PAW again. As another big step/small step decision, using LAPS to manage the new PAWs should be an easier step than starting out using LAPS for all your workstations.

If you're interested in how LAPS allows us to help combat Pass the Hash attacks, here are a few additional resources you can review.

Unique Local Admin Password for Servers

Building on your previous work of where you want your tier-0 boundary to be, start running LAPS on those member servers that are going to remain part of tier-0. Again, a smaller step than LAPS everywhere, and not much else to say on the subject. By this point you should be familiar with LAPS and are just expanding its usage.

End of the Stage 1 and the Roads Ahead

If you expand LAPS to cover all workstations and all servers, congratulations, you have now followed the roadmap to the end of Stage 1.

Stage 2 and Stage 3 of the roadmap involves expanding the use of the PAWs to all administrators, implementing advanced credential management that begins to move you away from password-only credentials, minimizing the amount of standing, always-on, admin access, implementing the tier-0 boundary you already decided upon, and increasing your ability to detect attacks against AD. You can also start looking at implementing Windows Server 2016 and taking advantage of some of our newest security features.

In these stages, we're looking at implementing new capabilities that defend against more persistent attackers. As such, these will take longer to implement than Stage 1. But if you've already gotten people familiar with the tiering model and talking about your tier-0 boundary you'll have an easier time implementing this guidance, with less resistance, as all the implementations are aligned to the singular goal of minimizing your tier-0 surface area.

2.1. PAW Phases 2 and 3: all admins and additional hardening

Get a PAW into the hands of everyone with admin rights to separate their Internet-using personal productivity end user account from their admin credentials. Even if they're still crossing tiers at this point in time, there is now some separation from the most common compromise channel.

2.2. Time-bound privileges (no permanent administrators)

If an account has no admin rights, is it still an admin credential? The least vulnerable administrators are those with admin access to nothing. We provide tooling in current versions of both AD and Microsoft Identity Manager to deliver this functionality.

2.3. Multi-factor for time-bound elevation

Passwords are no longer a sufficient authentication mechanism for administrative access. Having to breach a secondary channel significantly increases the attackers' costs.

Also have a look at some of our current password guidance.

2.4. Just Enough Admin (JEA) for DC Maintenance

Allowing junior or delegated Admins to perform approved tasks, instead of having to make them full admins, further reduces the tier-0 surface area. You can even consider delegating access to yourself for common actions you perform all the time, fully eliminating work tasks that require the use of a tier-0 credential.

2.5. Lower attack surface of Domain and DCs

This is where all the up-front work of understanding and defining your tier boundaries pays off in spades. When you reach this step, no one should be surprised about what you intend to do. If you've decided to keep tier-0 small and are isolating the security infrastructure management from the general Enterprise management, everyone has already agreed to that. If you've decided that you must keep some of those systems as tier-0, you've hardened them like they are DCs and have elevated the maturity of those admins to treat their credentials like the tier-0 assets they are.

2.6. Attack Detection

Seeing Advanced Threat Analytics (ATA) in action, and providing visibility into exactly what your DCs are doing, will likely be an eye-opening revelation for most environments. Consider this your purpose-built Identity SIEM instead of simply being a dumping ground for events in general.

And, while not officially on the roadmap at this time, if you have SCOM, take a look at the great work some of our engineers have put into the Security Monitoring Management Pack.

3.1. Modernize Roles and Delegation Model

This goes together with lowering the attack surface of the Domain and DCs. You can't accomplish that reduction without providing alternate roles and delegations that don't require tier-0 credentials. You should be trying to scope tier-0 AD admin activity to actions like patching the OS and promoting new DCs. If someone isn't performing a task along those lines, they likely are not tier-0 admins and should instead be delegated rights to perform the activity and not be Domain Admin.

3.2. Smartcard or Passport Authentication for all admins

More of the same advice that you need to start eliminating passwords from your admins.

3.3. Admin Forest for Active Directory administrators

I'm sure your AD environment is perfectly managed. All the legacy protocols have been disabled, you have control over every account (human or service) that has admin rights on any DC. In essence, you've already been doing everything is the roadmap.

No?

Your environment doesn't look like that?

Sometimes it's easier to admit that it's going to be too difficult to regain administrative control over the current Enterprise forest. Instead, you can implement a new, pristine environment right out of the box and shift your administrative control to this forest. Your current Enterprise forest is left mostly alone due to all the app-compat concerns that go along with everything that's been tied to AD. We have lots of guidance and implementation services to help make sure you build this new forest right and ensure it's only used for administration purposes. That way you can turn on all the new security features to protect your admins without fear of breaking the old app running in some forgotten closet.

3.4. Code Integrity Policy for DCs (Server 2016)

Your DCs should be your most controlled, purpose-built servers in your environment. Creating a policy that locks them down to exactly what you intended helps keep tier-0 from expanding as your DCs can't just start running new code that isn't already part of their manifest.

3.5. Shielded VMs for virtual DCs (Server 2016 Hyper-V Fabric)

I remember the first time I saw a VM POST and realized what a game-changer virtualization was going to be. Unfortunately, it also made walking out the door with a fully running DC as easy as copy/paste. With Shielded VMs you can now enforce boundaries between your Virtualization Admins and your AD Admins. You can allow your virtualization services to operate at tier-1 while being able to security host tier-0 assets without violating the integrity of the tier boundary. Can you say "Game changer"?

Don't Neglect the Other Tiers

While this series focused on tier-0, the methodology of tackling the problem extends to the other tiers as well. This exercise was fundamentally about segmentation of administrative control. What we've seen, is that over the years, unintentional administrative control gets granted and then becomes an avenue for attack. Be especially on the lookout for service accounts that are local admin on lots of systems and understand how those credentials are used and if they are present on those endpoints in a manner that allows them to be reused for lateral movement. If you've gone through the effort to secure tier-0 but you have vulnerable credentials with standing admin access to all of tier-1, where your business-critical data is stored, you probably haven't moved the needle as much as you need to. Ideally you get to the point where the compromise of a single workstation or a single server is contained to that system and doesn't escalate into a compromise of most of the environment.

I know this has been a lot of guidance over these two posts. Even if you can't do everything, I know you can do something to improve your environment. Hopefully I provided some new insight into how you can make your environment more secure than it is currently and exposed you to the volumes of guidance in the SPA roadmap. Now get out there and start figuring out where your tier-0 boundary is and where you want it to be!

Thanks for spending a little bit of your time with me.

-Dave

#proudmicrosoftemployee

Updated Apr 04, 2020

Version 5.0
DavidLoder