Securing Privileged Access for the AD Admin - Part 1

techcommunity.microsoft.com/blog/coreinfrastructureandsecurityblog/securing-privileged-access-for-the-ad-admin---part-1/259166

Blog Post

First published on TechNet on Sep 11, 2017

Hello again, my name is still David Loder, and I'm still a PFE out of Detroit, Michigan. I have a new confession to make. I like cat videos. Your end users like cat videos. You may like cat videos yourself. Microsoft will even help you find cat videos. Unfortunately, cat videos may have it out for you and your environment. How do you keep your environment secure when malicious cat videos are out there, waiting to pounce?

Microsoft has a significant amount of published guidance around Securing Privileged Access (SPA), Privileged Access Workstations and the Administrative Tier Model. My fellow PFEs have also contributed their own great thoughts around these topics. Go browse through our Security tagged posts to get easy access to them. As for myself, I was staff IT in the security department for a large, global corporation, prior to joining Microsoft, where we operated in a tiered administrative model and had implemented many, though not all, of the defenses highlighted in the SPA roadmap. So I'd like to share my perspective on the items in the roadmap and the practical implications from an Active Directory Administrator point of view.

But first a caveat for this series of articles. I love the SPA roadmap. I espouse its virtues to all my customers and anyone else who will listen. But there are times where the SPA roadmap takes a big step, and I know it can sometimes be difficult to get the people in charge to agree to a big step. In all the cases where I point this out it is possible to take a smaller step by limiting the scope by focusing solely on AD. I have a different purpose for this series of articles than the SPA roadmap itself. I want you to actually implement the guidance. That's a shocking statement, I know. Despite all the guidance, I still walk into environments that haven't implemented a single piece of this guidance. Maybe they don't know this guidance exists. Maybe they think they aren't a target. Maybe they think the guidance doesn't apply to them. My hope with this series is that a few more people know about the guidance, understand why they should care and have an easier time convincing others in their organization that the roadmap guidance should be implemented. Security is a journey. Through no fault of your own, the rules have changed. What you did to secure your environment yesterday is no longer sufficient for today's reality. So, let's get started.

Separate Admin Account for Admin Tasks

This is an easy one, right? Nothing about this guidance is new. It ranks right up there with not browsing the Internet from a server. But I am constantly seeing environments where normal user accounts, which have a mailbox and browse the Internet for cat videos, are

also in the Domain Admins group. Stop this. Stop this now. You need a separate credential for administrative tasks. Come up with a naming convention and a process to get an admin account for anyone who does admin work.

I know some of you are smiling and thinking to yourself 'of course we do this; the admins get their ADM_username accounts for performing admin work' (or their $username or their username.admin or whatever convention you use). But, have you made the correlation between tiering and admin accounts? To fully implement the guidance, a user with admin rights must have a **separate admin account per tier**!

Let that sink in for a minute. In a three-tier model, the AD Admins may require four separate credentials: user (non-privileged), tier-2 (workstation) admin, tier-1 (server) admin and tier-0 (security infrastructure) admin. This guidance is designed to avoid having a credential that has admin rights in multiple tiers. This helps prevent a pass-the-hash attack from elevating from a lower tier to a higher tier.

Now for the practical part. Yes, this gets hard to do. You may have processes in place that will get a second credential to admin users, but it wasn't designed to get them four. Maybe you have clear separation between server admins and workstation admins, so no one will need all four. We want the guidance to be actionable and most importantly to protect tier-0. Guidance that isn't followed because it is too burdensome isn't valuable. At a minimum, your AD Admins should have three accounts: user, admin, tier-0 admin. And your goal is to minimize the scope of tier-0. Tier-0 admin accounts should only be managed by other tier-0 admin accounts and not by a tier-1 system. Please don't have your normal Identity Management (IdM) system try to manage AD Admin accounts. Because you'll either fight with AdminSDHolder or you'll have to grant your IdM system Domain Admin rights and neither of those is a good choice.

Let's discuss the tiers for a moment. What does tier-0 really mean? The definition from the Administrative Tier Model is:

> **Tier 0** – Direct Control of enterprise identities in the environment. Tier 0 includes accounts, groups, and other assets that have direct or indirect administrative control of the Active Directory forest, domains, or domain controllers, and all the assets in it. The security sensitivity of all tier 0 assets is equivalent as they are all effectively in control of each other.

Control of a tier-0 system means control of the entire environment. The very nature of Active Directory means there should be at least two tiers in the environment: AD itself, and everything else. Splitting between tiers isn't a hard and fast line. The tiering is there to provide a security boundary that is supposed to be difficult to cross. You can certainly have user workstations that might need to be treated more like a tier-1 system because of the value they hold. The point is that your organization must decide which security boundaries should exist that define the tiers and the systems contained within those tiers. This is especially true of tier-0.

At a minimum tier-0 will contain Active Directory; specifically, the writeable Domain Controllers and the AD Admin credentials. Those credentials are any account that is a member of Domain Admins, Enterprise Admins, Builtin Administrators, etc. These groups are all equivalent. Don't think being Builtin Administrator is somehow more secure or different than being Domain Admin.

What else is tier-0? Look in your AD Admin groups. Every account in them is a tier-0 credential. Ideally, they are credentials only for people and they are unique to the management of AD infrastructure, following a naming convention that distinguishes them from your normal tier-1 admin accounts. In other words, the tier-0 credentials that are members of the AD Admin groups must be used for the sole purpose of managing AD infrastructure and for nothing else.

If you have service accounts in your AD Admin groups, those service accounts are tier-0 credentials. The servers where those service accounts are used are tier-0 systems. Anyone who is administrator on those servers has access to tier-0 credentials. Do you see how quickly this grows? While you may normally think of just AD as being tier-0, your tier-0 equivalency may be immense. In fact, you may not have a tier-1 or tier-2 layer at all. It is possible that you are operating an environment where everything is tier-0.

I will state again; the goal is to minimize tier-0. Your AD Admin groups should only have people in them, not service accounts. Use the delegation abilities within AD to grant those service accounts only the rights they need. Yes, it may be hard work to figure out what and where those rights are needed, but it's the job that needs to be done to keep things that should be tier-1 from being tier-0.

What else is tier-0? Are your DCs virtualized? If so your VM admins tier-0 admins. Your VM platform is a tier-0 system. Your VM storage is a tier-0 system. Your storage admins are tier-0 admins. Do you see how quickly this grows ? Hyper-V in Windows Server 2016 offers Shielded VMs to mitigate this risk.

What else is tier-0? What additional services run on your DCs? Which of those services are listening on the network and running as Local System? Which of them report into some kind of management console to receive instructions on what to do? Does that describe your SIEM agent, your anti-virus agent, your asset management agent, your configuration management agent? Your SIEM team has control over a tier-0 system. Your SIEM is a tier-0 system. Your AV platform is a tier-0 system. Your configuration platform is a tier-0 system. Do you have a standard corporate image that you use for all servers, including the servers that you will promote to become Domain Controllers? Everything added to that image has the possibility of being a tier-0 system. Do you see how quickly this grows?

What else is tier-0? Is your IdM system tier-0? Maybe. By our definition it should be since it has direct control of the enterprise identities. What if it is only delegated rights to a specific set of OUs and it doesn't use an AD Admin account to manage the users? If that system is compromised is tier-0 compromised? The integrity of the AD infrastructure is

still intact. It may no longer contain the user data you wanted it to contain but you still have administrative control over AD and can more easily recover. It that a bad day? Absolutely. But you can still point to a security boundary that wasn't crossed. A defense in-depth mindset would have more boundaries to cross when possible.

Control over your tier-0 equivalencies is likely the hardest part of the roadmap; which is why it practically shows up later in the roadmap. But I wanted to discuss it up front, as understanding the true nature of your own tier-0 definition is paramount to being able to have successfully implemented the roadmap at the end of the journey.

Now that we all understand the impact of tier-0 equivalencies, how many credentials in your enterprise (from both humans and service accounts) are tier-0 admins? Is it 5 or 100? How many do you want at that tier? 5 or 100? Personally, I'd vote for 5. Keep in mind that we're focusing on credentials. This shouldn't be a discussion that we trust, for example, the VM Admin team less than the AD one. It's that the more credentials and systems that exist at tier-0, the more surface area we have to consider in an assumed-compromised state.

Once you and your organization have made your decision about defining your intended tier-0 boundary, go make totally separate admin accounts for those that you want to end up operating at tier-0. Yes, managing three or four credentials is more difficult than one. But you're the AD admin for your enterprise and if you aren't taking the lead in enabling this change, **no one else will do so**. If you already have a separate admin account, but it's crossing tier boundaries (existing or planned), go get your third credential. Making use of the third is almost no additional effort beyond a second credential. Here's where you have one of those big step/small step decisions to make. If having separate admin accounts for everyone who does administration in your organization is too big of a change to make all at once, start small with only those admins who manage AD. Show everyone that the world doesn't end if you have to manage separate credentials for AD Admin purposes.

Ensure you have proper procedures for creating and managing the new tier-0 admin credentials. My first preference is to manage them manually, outside of the scope of any IdM platform you have in place, with proper, proactive scheduled reviews. Hopefully you've caught on to the hints that managing tier-0 will be easier when it's small. That allows manual management of tier-0 credentials to be successful. If you're in a more mature organization, then you can look to a dedicated tier-0 IdM system that can manage these credentials.

As a personal story from my previous life many years ago, the first time we had to integrate a non-AD workload into tier-0, we thought the sky was falling and it was the destruction of our security posture because a different team was suddenly involved. It took me a while to recognize that tier-0 doesn't exclusively mean AD. Every organization will have a unique combination of workloads and roles that will be their tier-0, and that's OK. What's important is define the boundary then make every workload and every person in tier-0 operate to the same standard.

To summarize this post into a 30 second elevator speech:

1. Active Directory Domain Controllers are tier-0 systems.
2. AD Admin credentials are a tier-0 credentials.
3. Anywhere that tier-0 credentials are used is a tier-0 system.
4. Anything or anyone that has administrative control over any part of 1, 2 or 3 is also a tier-0 credential/system.
5. Keeping 1, 2, 3 and 4 small makes tier-0 easier to manage and more secure.

That's it for now. The first step down the roadmap is both incredibly simple and incredibly hard at the same time. I want to give you a break to allow the full impact of the guidance to soak in. Check back in next week, where we'll continue our discussion of the roadmap. But please, go create your separate AD Admin account right now. I shudder to think you've been reading this with a browser running under AD Admin credentials, with your cat videos playing in another tab.

-Dave