Tracking Lateral Movement Part One - Special Groups and Specific Service Accounts

By kexugit

Archived: 2026-04-05 20:39:15 UTC

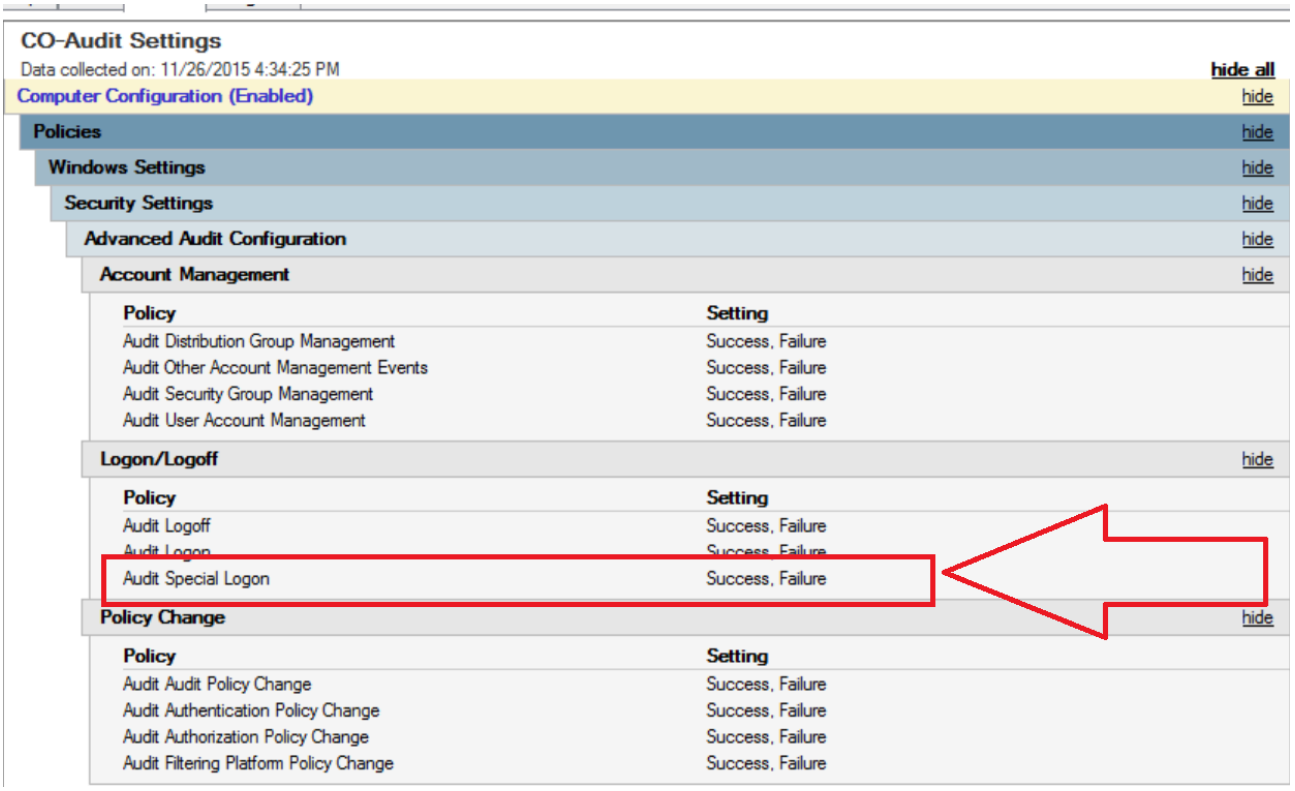
Lateral Movement - the moving of an attacker from one compromised host throughout your domain until they find what they are looking for - is something we see many just about all attackers doing during compromise. I've talked a lot about the attacker behavior and how to stop it - strong protective controls can serve as powerful detective controls.

The problem for most of our customers is that they lack the visibility/documentation to comfortably put Lateral Movement preventions in place without breaking everything. Even before we put the protective controls in place we can put some of the detective controls in place - which will give us greater insight into what is currently happening in the environment so we can get the protective controls in faster.

One very powerful detective control I mentioned in my Ignite Australia session on monitoring : Special Groups. Special Groups were introduced in Windows 2008/Vista as a way to track when particular accounts log onto a system. Which is pretty awesome from a security/Lateral Account Movement perspective. Especially since you get to define just what group is a special group! For Lateral Account Movement and credential hygiene, we want to know if administrative accounts or highly privileged (Tier 0 in MSFT speak) accounts logon to systems, especially systems in the workstation or member server tiers. When you enable Special Groups, you get a unique Event ID (4964) in the Security log that you can send to Windows Event Forwarding (which naturally you have in your environment now because of my blog post or the in depth Microsoft Virtual Academy session . :))

Getting Event ID 4964 to show up does require some configuration, which is best done via Group Policy Preferences.

First, we need to make sure the audit policies applied to our machines are in fact auditing for Special Logon. Configure your GPO so Computer Configuration\Windows Settings\Security Settings\Advanced Audit Configuration\Account Management\Audit Special Logon is set to log Success and Failure (we do want failure here, it's very useful once we get those protective controls in place.)



CO-Audit Settings

Data collected on: 11/26/2015 4:34:25 PM — hide all

Computer Configuration (Enabled) — hide

Policies — hide

Windows Settings — hide

Security Settings — hide

Advanced Audit Configuration — hide

Account Management — hide

Policy	Setting
Audit Distribution Group Management	Success, Failure
Audit Other Account Management Events	Success, Failure
Audit Security Group Management	Success, Failure
Audit User Account Management	Success, Failure

Logon/Logoff — hide

Policy	Setting
Audit Logoff	Success, Failure
Audit Logon	Success, Failure
Audit Special Logon	Success, Failure

Policy Change — hide

Policy	Setting
Audit Audit Policy Change	Success, Failure
Audit Authentication Policy Change	Success, Failure
Audit Authorization Policy Change	Success, Failure
Audit Filtering Platform Policy Change	Success, Failure

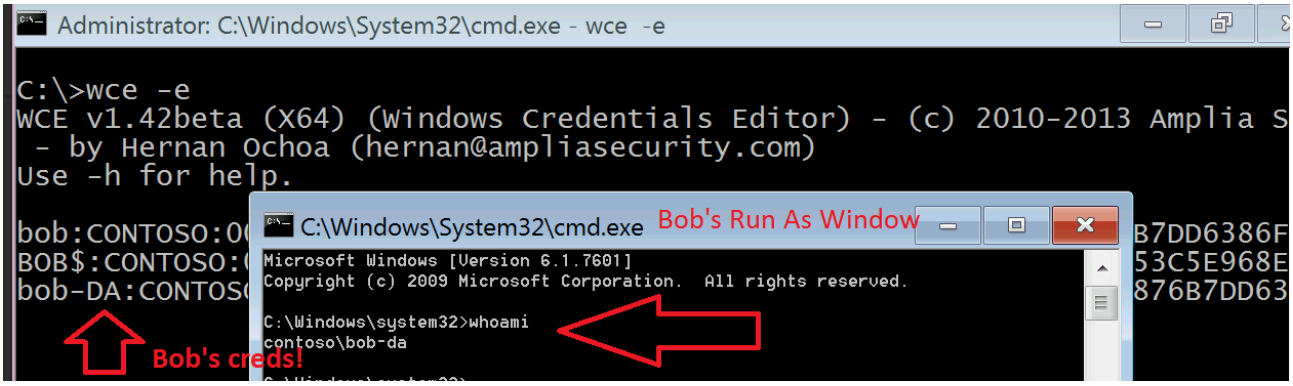
Next we need to determine who is a Special Group in the organization. For the purposes of tracking Bad Guy Behaviors as well as preparing for Lateral Account Movement lockdowns I'd really like at least the following things considered "Special Groups."

- Local Account : S-1-5-113 - this will help track the local accounts people may be using on your network so you can put the Lateral Movement blocks for Local Account in later without breaking things, as well as track Bad Guy Behavior.
- Domain Admins : S-1-5-21domain-512 - we need to know if there are any workflows that are currently in place in an organization that would lead to credential exposure before putting protective controls in place, and also alerts on Bad Guy Behavior.
- Enterprise Admins : S-1-5-21root domain-519 - same as Domain Admins, just Enterprise wide. Even if you only have one domain, monitor this.
- Special Group: I recommend creating a group specifically for things you want to track with Special Logon later, and adding it to the registry policy now. You could nest the other groups into it as well, but you might want those specifically defined. You can use this group to add Service Accounts to for instance, then if one is used across workstations, you know you have a problem.

I'd also like to see Built In Administrators : S-1-5-32-544 - we want to know when someone is logging on with admin privileges in general from a forensic stand point often. But this may be just far too noisy in some environments for the first pass. Give it a try if you can.

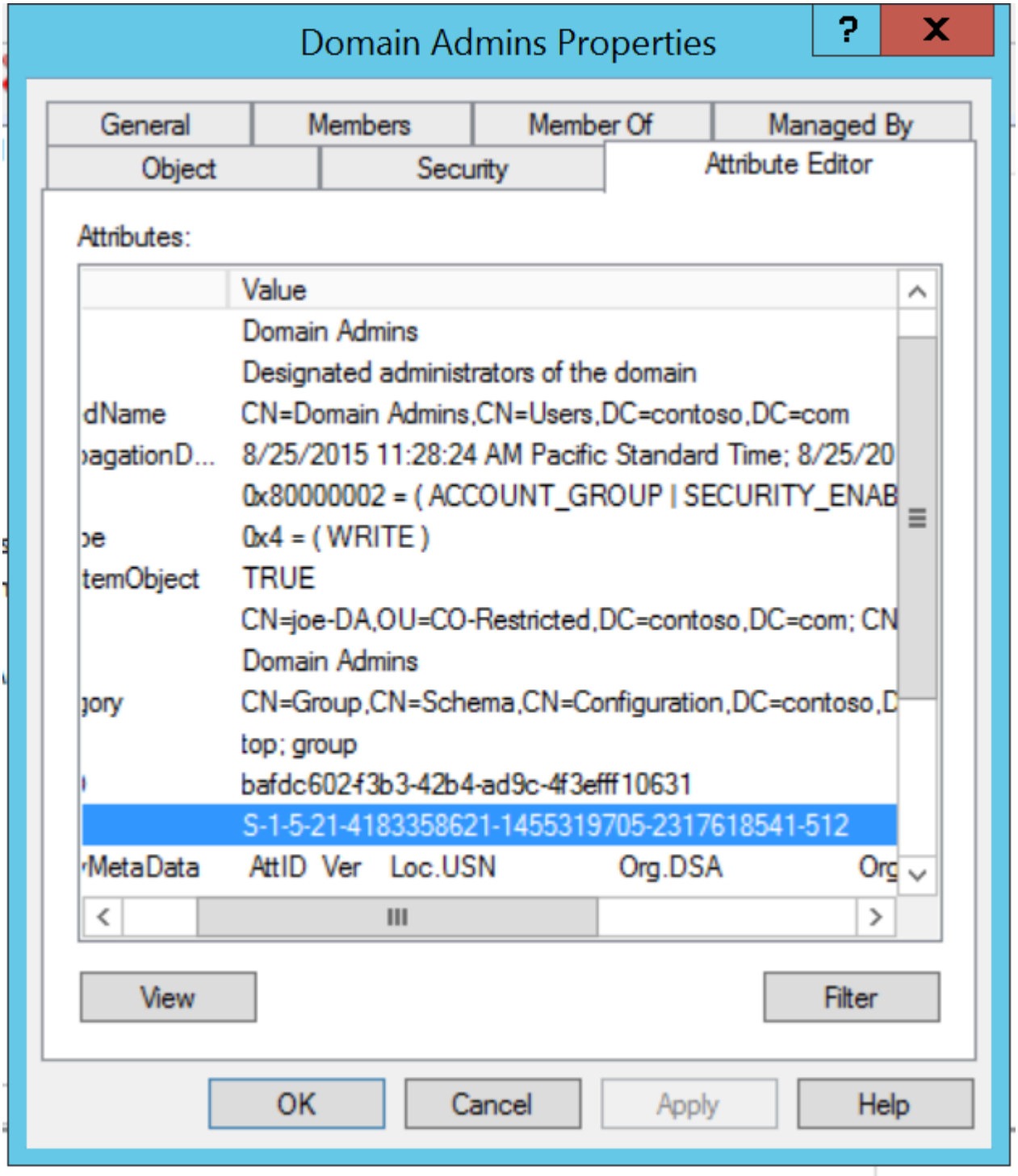
We're using Special Group not just to track Bad Guy Behavior, but potentially dangerous administrator behaviors that will be blocked by Lateral Movement mitigations. One of the workflows to worry about is Domain Admins using "Run as a Different User" on their normal workstations. Many people now have secondary admin accounts (which is great!) but use RunAs when they are doing admin activities - such as running Active Directory Users

and Computers from the same computer they are logged on and surfing the web/checking email. This behavior may seem safe, but a RunAs is a full interactive logon that leaves credentials behind in memory.

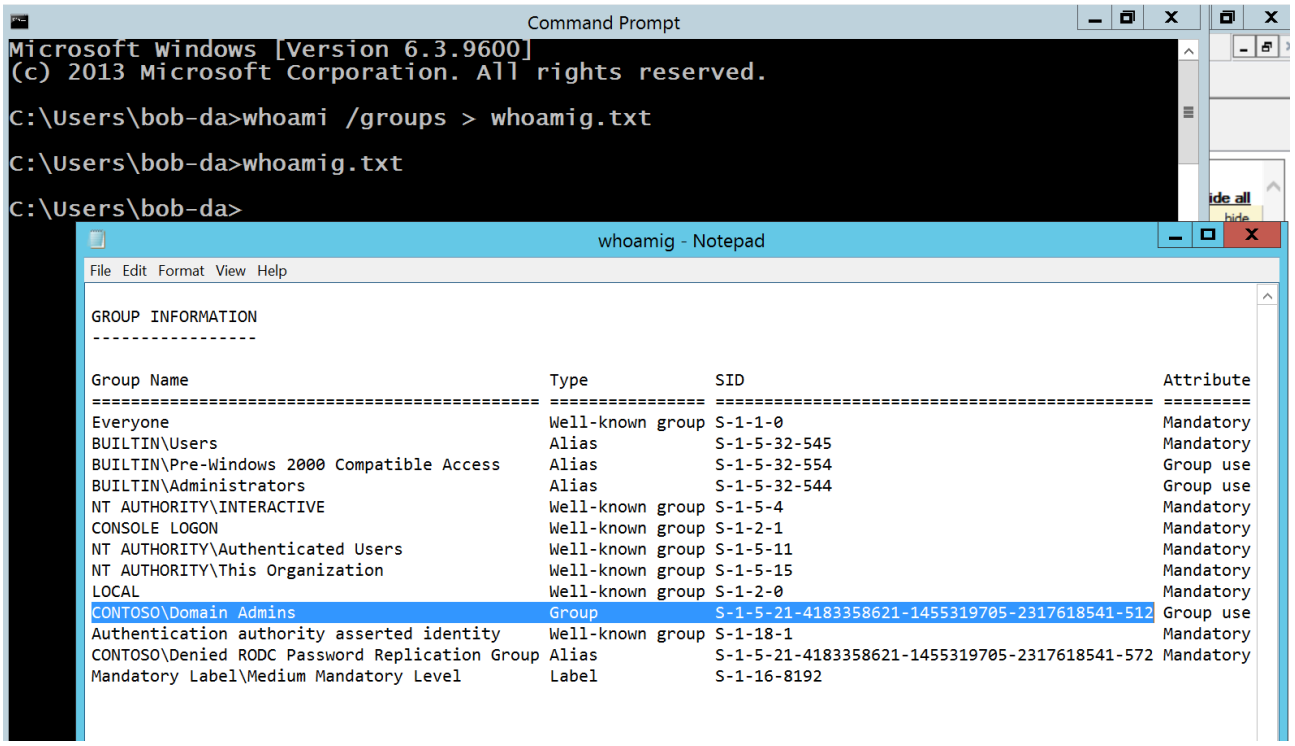


(This is why we stress the need for a hardware separation between regular and administrative credentials so much in the Pass the Hash Whitepapers.)

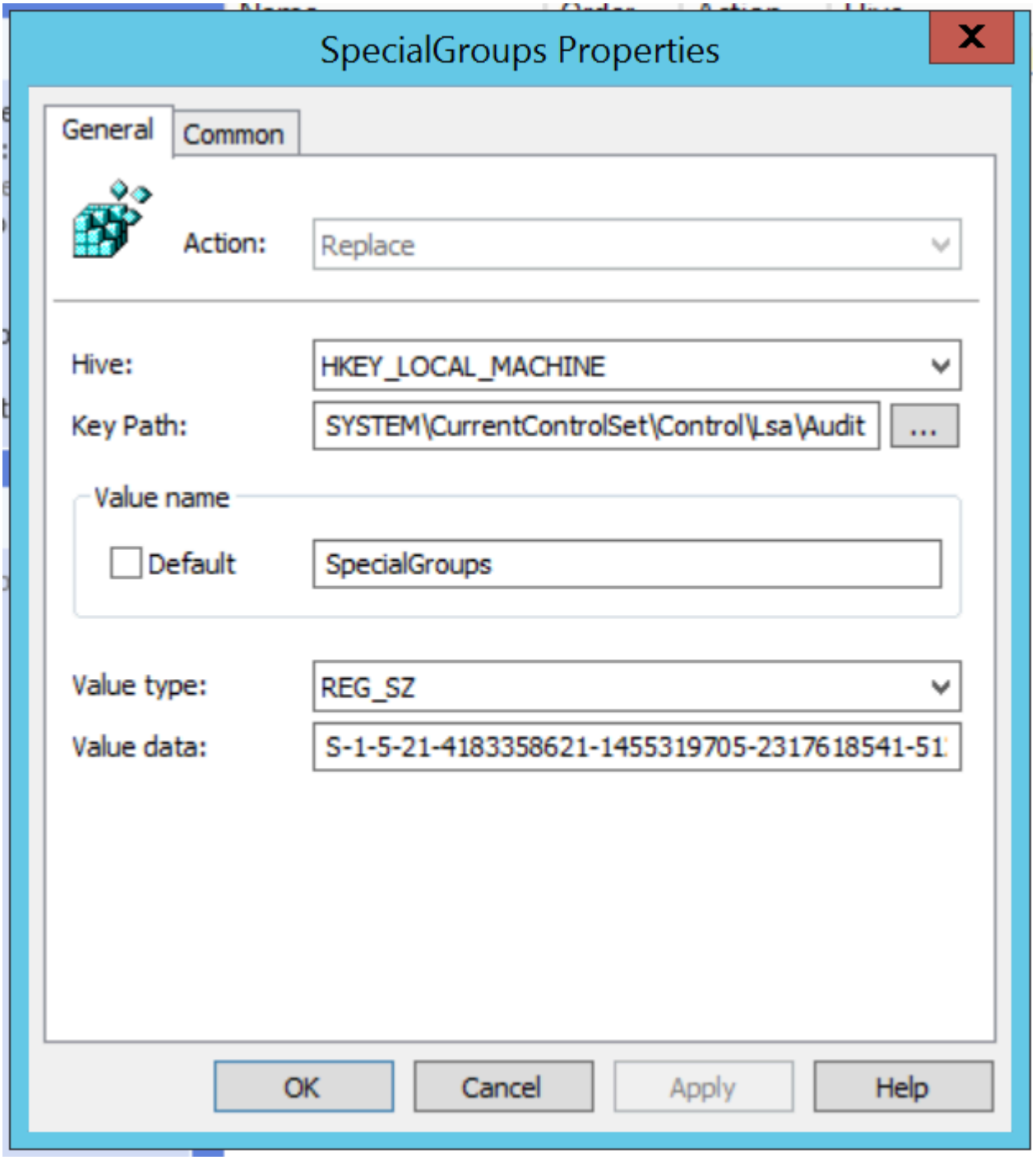
We need to now assemble our SIDs. Even for Domain/Enterprise Admins you can get the SID of from attribute editor, under the objectSID attribute.



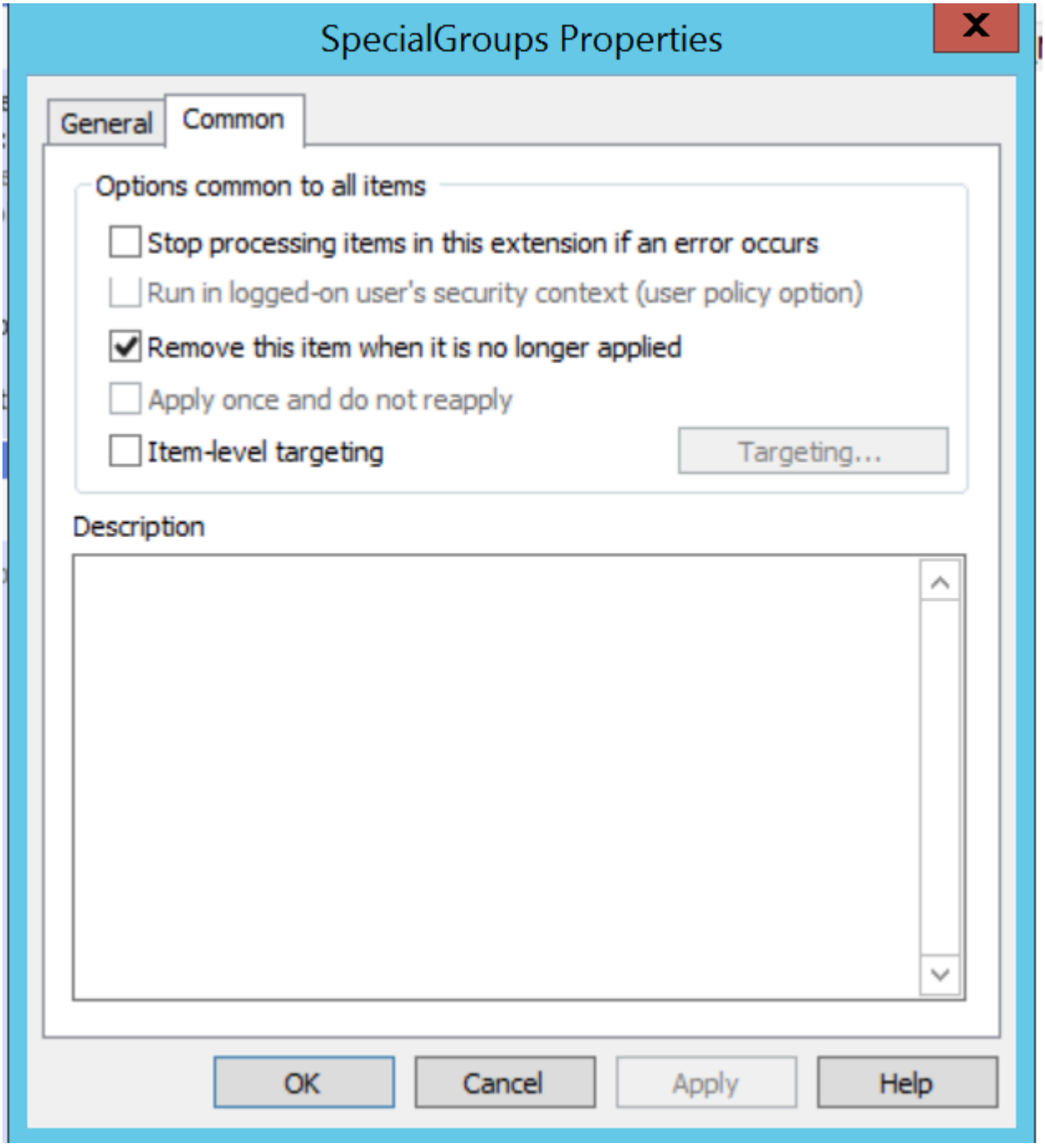
You can also use the power of https://support.microsoft.com/en-us/kb/243330 to know the Domain Admins SID is always S-1-5-21domain-512 and fill in the "domain" part based on another group in your domain, or you could logon on to a Domain Controller as a Domain Admin and run whoami /groups. If you pipe it out to a text file as shown, you can get the SID from there (useful trick for other stuff too.)



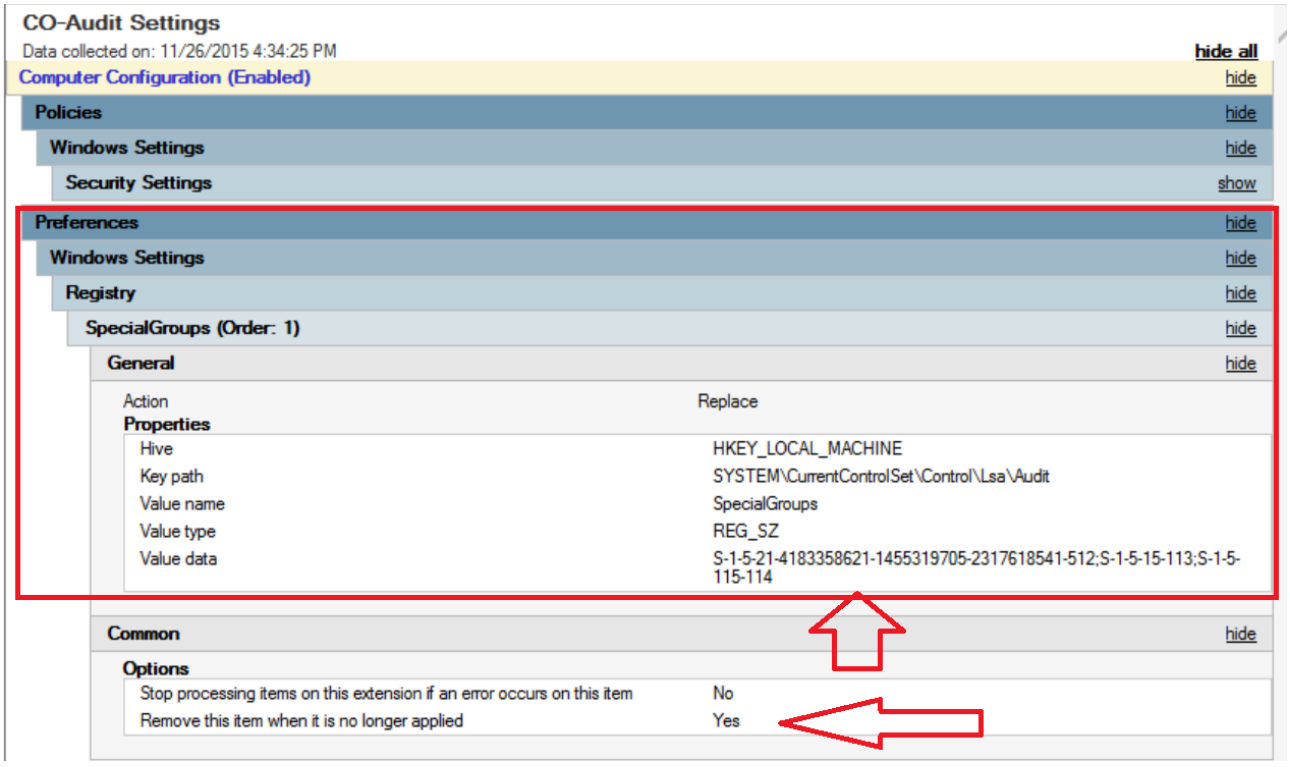
So now that we have our SIDs, either make a new GPO or edit one that applies where you need it (which, is pretty much everywhere. Except maybe Tier 0/Domain Controllers to reduce initial noise.) Navigate to Computer Configuration\Preferences\Windows Settings\Registry\ and create a New Registry Item. You'll want to fill it in like the screenshot below, with the key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Audit\SpecialGroups set to a REG_SZ (string) value that contains your SIDs of interest separated by ; (semi colons.)



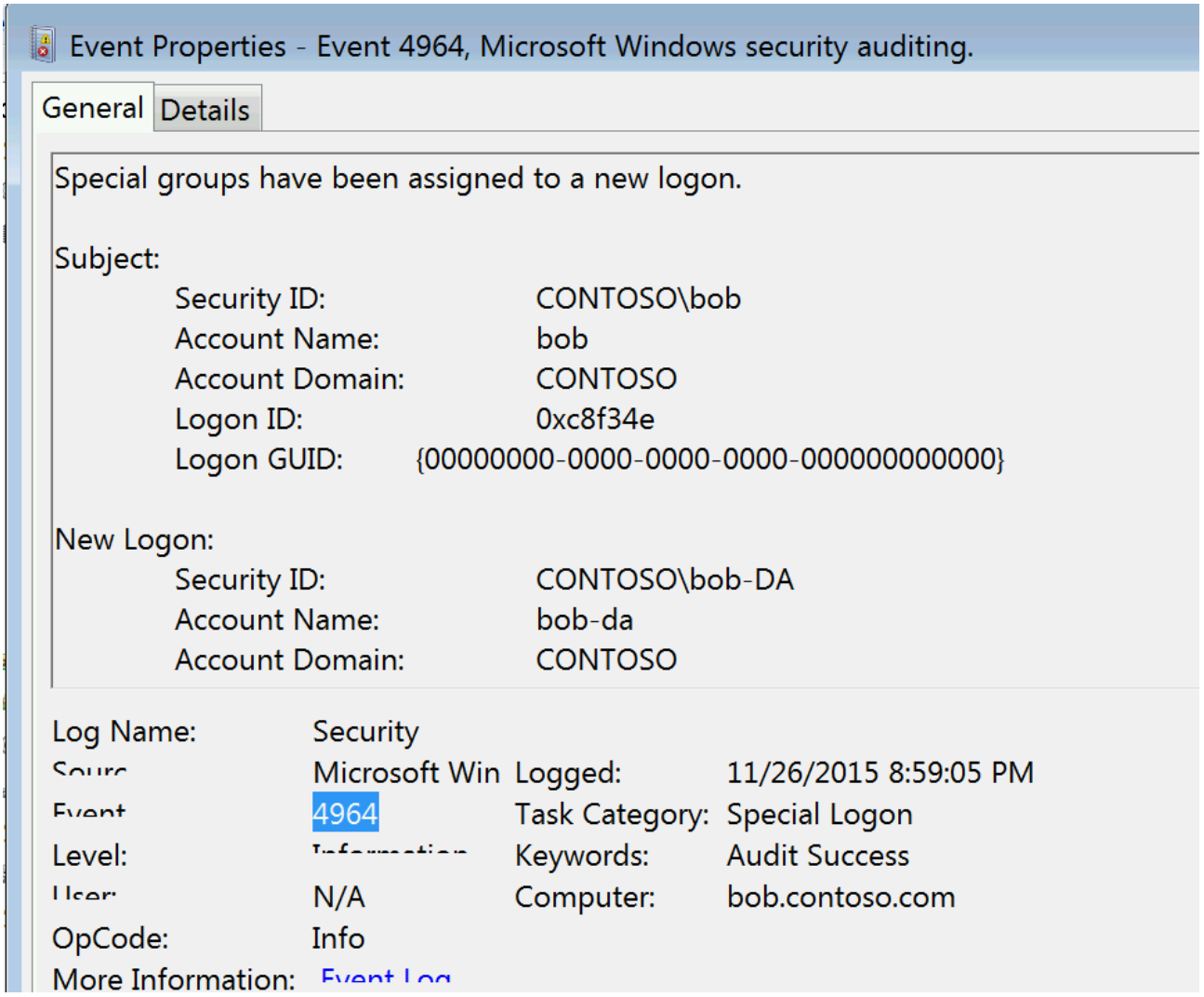
Public Service Announcement : whenever you're making a Group Policy Preference like a registry key, make sure to check the box on the Common tab for "Remove this item when it is no longer applied." This will make sure when you unlink the GPO the setting is cleaned up, otherwise you can sometimes get weird tattoos on your registry of settings you unlinked ages ago.



Once you're done, the GPO should look something like this.

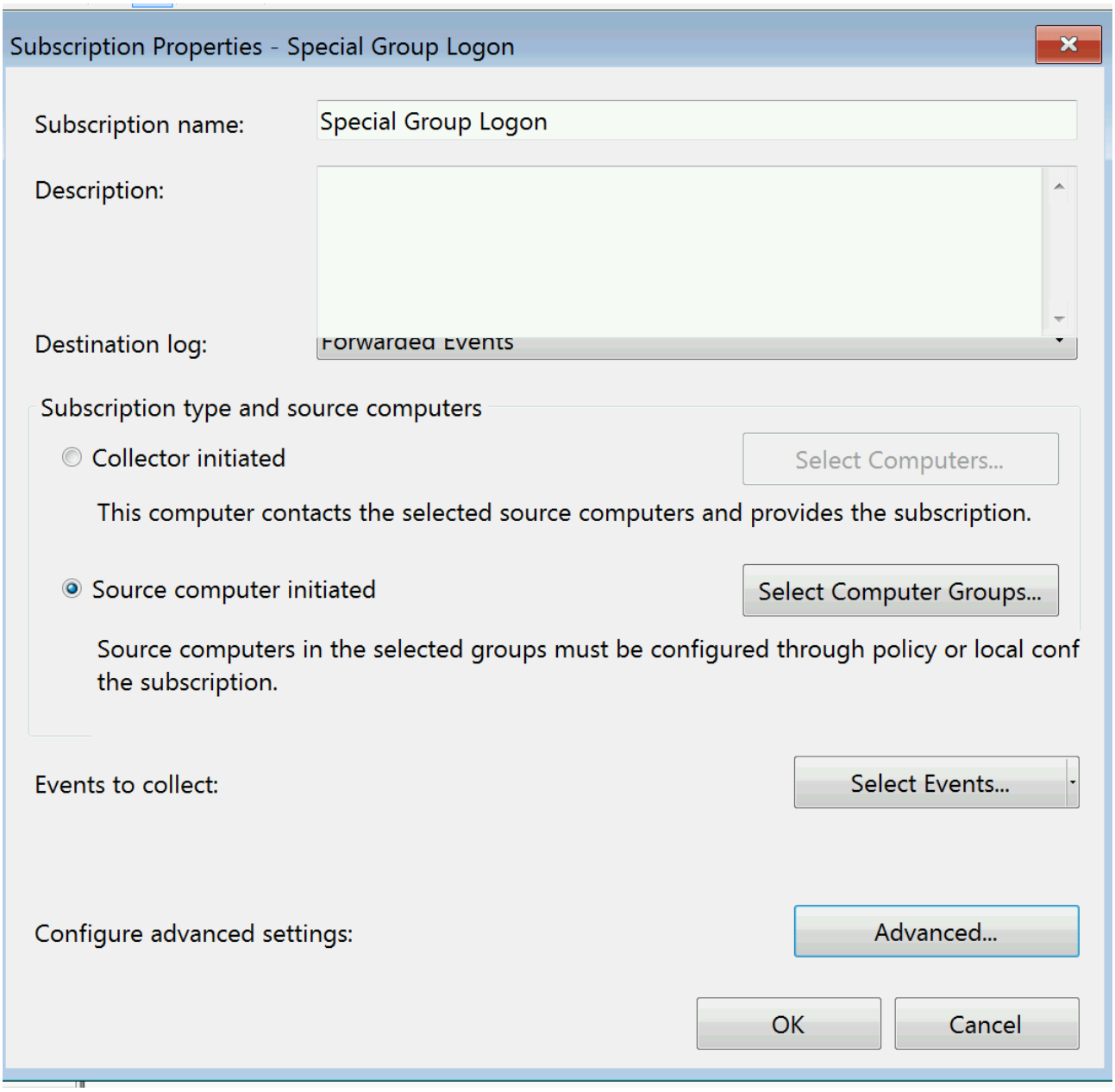


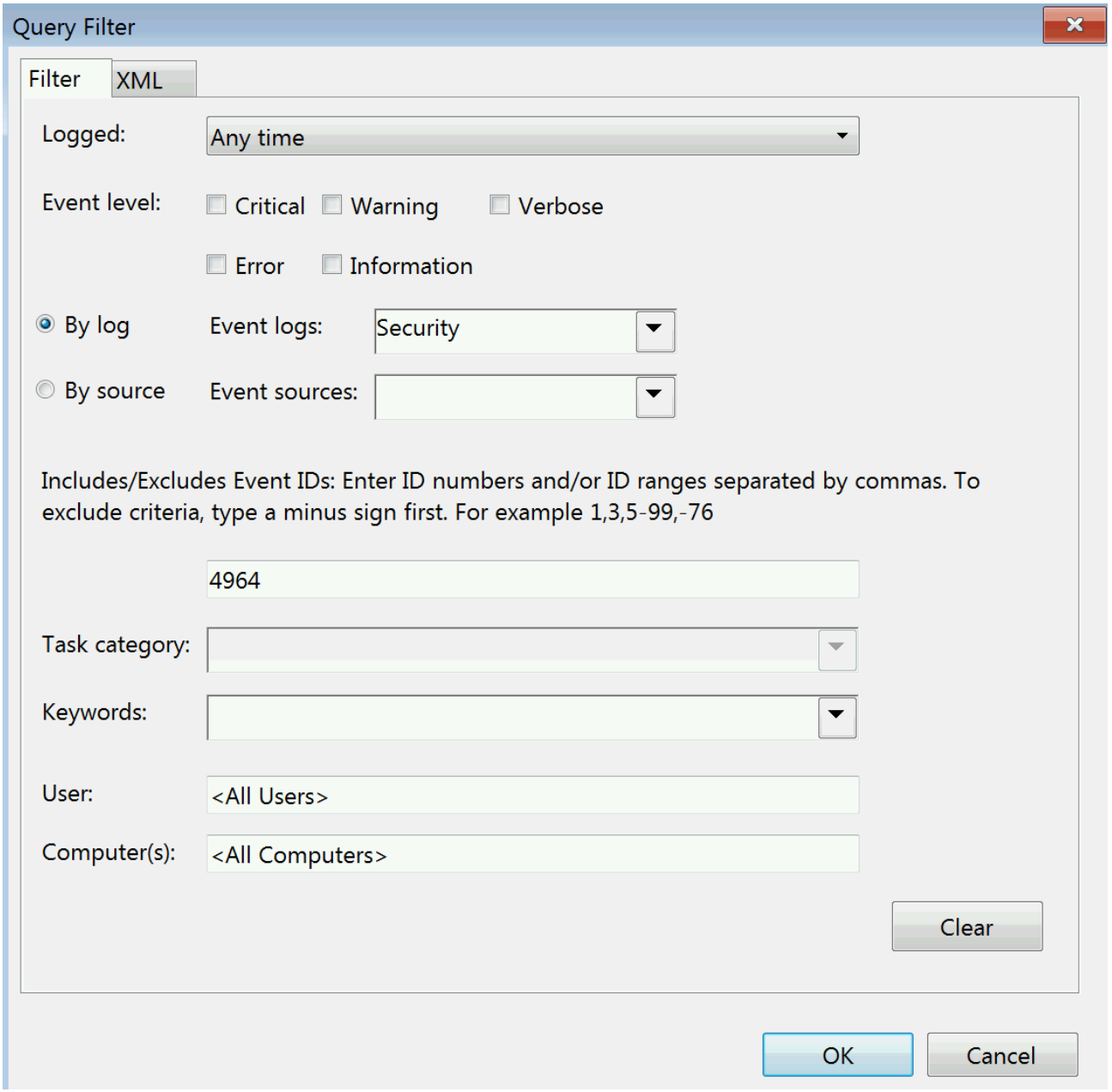
So now, when Bob the Domain Admin does the dangerous behavior of Shift+ Right Click +Run as Different User on his Bob the Regular User workstation we get a very descriptive alert telling us what Bob did and what group it was that triggered the alert.



Now that we have an Event ID, we can make a Subscription for this in Windows Event Forwarding. I already covered the basics of WEF in another post, so if you haven't read that go back to get the basics.

Our 4964 subscription can be quite simple :


Subscription Properties - Special Group Logon
Subscription name:
Special Group Logon
Description:
Destination log:
Forwarded Events
Subscription type and source computers
Collector initiated
Select Computers...
This computer contacts the selected source computers and provides the subscription.
Source computer initiated
Select Computer Groups...
Source computers in the selected groups must be configured through policy or local conf
the subscription.
Events to collect:
Select Events...
Configure advanced settings:
Advanced...
OK
Cancel



Now you have way more insight into what is happening on your network - both in preparation for Lateral Movement lockdowns and to keep track of Bad Guy Behaviors.

Another barrier to getting Lateral Account Movement lockdowns in place or removing Service Accounts from high privileged groups like Domain Admins is often the accounts are in those groups for legacy reasons, and have been for years. When nobody knows why the account is there, or what might break it can make even the very real and very easy to exploit threat of a Service Account in the Domain Admins difficult to mitigate for some customers. This is another case where Windows Event Forwarding can come to the rescue!

Creating a WEF subscription for "Where all did Service Account X log in" is very easy to do. I recommend making these subscriptions one or two accounts at a time, to make it easier to narrow down what it's doing, and I recommend making sure the subscription is targeted to both Domain Computers and Domain Controllers for visibility into any local/NTLM logons that might not hit the Domain Controllers.

I've covered the basics of Windows Event Forwarding in both an Ignite Session on Channel 9 and a previous blog post so we'll skip to just the Xpath filter you'll need to track down a specific account :

<QueryList>
<Query Id="0" Path="Security">
<Select Path="Security">
(*[EventData[Data[@Name="TargetUserName"] = "Interesting Account Name 1"]]) or
(*[EventData[Data[@Name="TargetUserName"] = "Interesting Account Name 2"]]) or
(*[EventData[Data[@Name="TargetUserName"] = "Interesting Account Name …."]])
and
(*[System[Provider[@Name='Microsoft-Windows-Security-Auditing'] and (EventID=4624 or EventID=4625 or EventID=4648)]])
</Select>
</Query>
</QueryList>

Replace Interesting Account name with the user names you're interested in. EventID 4624 will get you all of the logon types, service/batch/interactive so should go a long way to tracking down what is going on, but 4625 will track failed logons for you - which help not just with potential security issues but with troubleshooting after you reduce privileges/credential exposure. Event ID 4648 is for explicit credential logon, which is used by bad guys doing lateral movement and sysadmins doing things like runas/mapping drives, so it's definitely an Event ID you'll want. :)

Getting these monitors enabled in your domain will not only go a long way to helping you lock down and monitor Lateral Account Movement, they'll also be a huge help if you ever need an Incident Response.

Good luck and happy logging!

-Jessica @jepayneMSFT

- **Anonymous**
  November 28, 2015
  Last week at Ignite Australia I presented a session (available here) on something I don't think
- **Anonymous**
  December 14, 2015
  Hi there!
  In your GPO SO Audit Settings report you have specified Domain Admins SID and two strange looking SIDs:
  S-1-5-15-113
  S-1-5-115-114
  What's the purpose of that additional SIDs if their meaning is nowhere to be found?
- **Anonymous**
  December 14, 2015
  S-1-5-113 and S-1-5-114 are two new "well known SIDs" that came out with Windows 8.1 and 2012R2

that are the "Local Account" and "Local Account and member of administrators" groups. They also got backported to Windows 7 and 2008R2 with KB2871997, so you can use them in older environments as well! That's so you can block local accounts from being used as part of Lateral Movement, which is very valuable and highly recommended.

Well known SIDs : https://support.microsoft.com/en-us/kb/243330
KB2871997 overview : http://blogs.technet.com/b/srd/archive/2014/06/05/an-overview-of-kb2871997.aspx
Post on blocking local accounts : http://blogs.technet.com/b/secguide/archive/2014/09/02/blocking-remote-use-of-local-accounts.aspx

Thanks for reading!
-Jessica

- **Anonymous**
  December 14, 2015
  Excellent post, Jessica! I'm looking forward to part 2!
- **Anonymous**
  December 15, 2015
  "Pretty awesome" Like for sure... totally tubular Jess.
- **Anonymous**
  December 18, 2015
  There is a typo for these new SIDs, both in the article and in the comment from Jess.
  The right ones are S-1-5-113 and S-1-5-114.

  Well-Known SID Structures: https://msdn.microsoft.com/en-us/library/cc980032.aspx?f=255&MSPPError=-2147217396

- **Anonymous**
  December 18, 2015
  I don't know if there's an issue with the post versions but, I did Control+F/find from what Jean-Marc has and it's what's in the article and comment for me. But if you're seeing some old version, yes Jean-Marc's link is correct for the SIDs. Sorry if there's any confusion.
  -Jessica
- **Anonymous**
  December 28, 2015
  Hi, Jessica Payne from Microsoft Enterprise Cybersecurity Group's Global Incident Response and Recovery
- **Anonymous**
  July 29, 2016
  Great information, thanks! I can't seem to get "Local account with administrator" to work on Windows 7 hosts. When an account is local and an administrator, I don't get anything logged. Local account that is not an administrator works fine. I have a case open with support, so hoping to get it worked out.
  - **Anonymous**
    July 30, 2016

I'm helping out your support engineer - once we get it pinned down we'll make sure to update your case and I'll post to the blog post. Thanks for pointing it out to us! -Jessica

---