Governing GPOs with a Layered Security Framework

Written by Alvaro Vitta, principal solutions consultant, Quest

INTRODUCTION

Group Policy provides the centralized management and configuration of operating systems, applications and users' settings in a Microsoft Active Directory environment. Group Policy, in part, controls what users can and cannot do on a computer system. It enforces a password complexity system that prevents users from choosing an overly simple password, prevents or allows unidentified users from remote computers to connect to a network share, and restricts access to certain folders. Each set of such configurations is called a Group Policy Object (GPO).

Although GPOs are designed to streamline IT operations and provide centralized security policies across the Active Directory environment, like any other powerful system, they can be abused or infiltrated to circumvent security controls and gain access to sensitive data. Some midsize and large organizations have hundreds and sometimes thousands of GPOs deployed across widely distributed environments, creating not only a huge insider threat, but also a large surface attack area if the proper compensating security controls are not in place.

This white paper describes how GPOs can be abused or exploited when the proper security controls are not in place and explains how to implement a layered security architecture that allows you to detect, alert and prevent unauthorized access to GPOs.

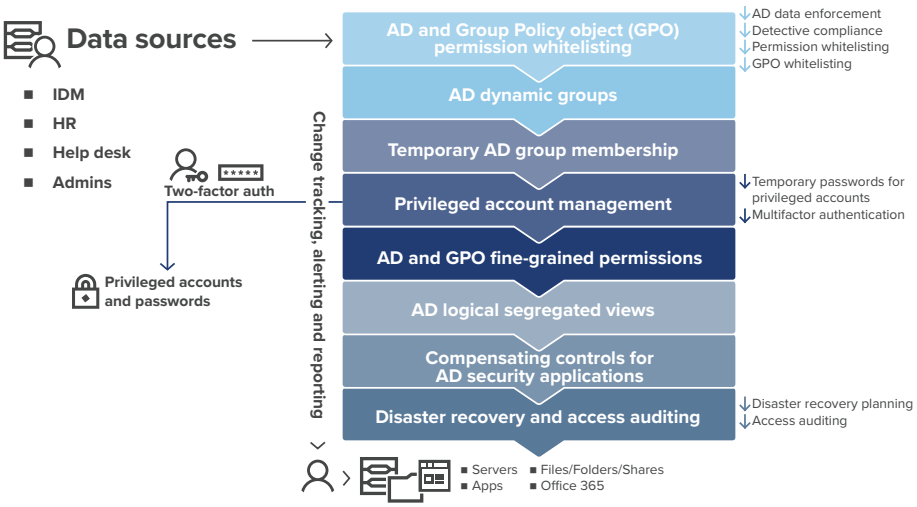

Figure 1. GPO layered-security framework

55 percent of security incidents involve internal actors abusing their access privileges.[1]

GPO PERMISSION EXPLOITATION

Sam Smith, a new IT admin at a manufacturing organization, needs to install a patch on a Windows-based database server containing a sensitive SQL database of confidential customer information. Sam is a domain admin and cannot log on to this SQL server because a GPO (**Deny log on locally**) has been set up specifically to prevent domain admins from logging on to this particular SQL server with the personal customer details. Instead of getting approval for the patch install and taking care of it during Saturday's change management window, Sam decides to change the GPO setting **Deny log on locally** to give himself access to the server. He disables the GPO that prevents admins from logging on and then logs on to install the patch. While there, he gets curious and decides to take a peek at some of the sensitive customer data — he even copies some of this information into a separate folder. He then changes the GPO back to its original setting. Because GPO setting changes are not tracked in native security logs, the unauthorized access isn't flagged until a database audit review is performed six weeks later.

HOW CAN SUCH A SECURITY LAPSE HAPPEN?

Unfortunately, similar scenarios occur more often than you might think — whether accidental or malicious in nature. Because of the way security permissions are designed around GPOs, any domain admin can modify any GPO security setting — even the settings that are supposed to prevent that very person from doing certain tasks. Also, because GPO setting changes are not tracked in the native security log, monitoring when such GPO setting changes happen is not possible, even if you are using security information and event management (SIEM) solutions. And you cannot prevent this from happening again in the future because you have no way of knowing what exact GPO setting changed (before and after values), and your domain admins can change GPO settings at will.

LAYERED SECURITY FRAMEWORK

One way to prevent breaches such as the one described above — and many other types, for that matter — is to take a layered approach to security. You need a cohesive set of security controls that allow administrators to make authorized

changes to GPO settings and, at the same time, prevent unauthorized changes to be made by external or internal sources (even by domain admins).

The following security layers act in unison to provide the proper security compensating controls for managing access to mission-critical GPO settings:

- GPO whitelisting in Active Directory
- GPO role-based access control (RBAC)
- Approval-based change control
- Locked-down access to GPO security applications
- Session-only access to GPO security applications

GPO WHITELISTING IN ACTIVE DIRECTORY

All sensitive GPOs — such as domain-wide GPOs, domain controller GPOs, mission-critical application GPOs and so on — are added to the Protection List of a third-party security application with whitelisting permissions capabilities for GPOs, such as Change Auditor for Active Directory. This Windows security solution provides functionality that allows for real-time permission whitelisting and monitoring of unauthorized change attempts to GPO settings.

Only a specific GPO service account, which is used by a third-party GPO (proxy) security solution such as GPOADmin, with rights to make changes to GPOs is listed as authorized to modify your most sensitive GPOs. All other accounts are automatically denied access to make GPO changes (including domain admins). Authorized changes can only happen via the GPOADmin interface, which provides a least-privilege access model and proper governance controls around GPO changes. Using a GPO whitelisting security application eliminates the risks associated with unauthorized day-to-day modifications.

GPO RBAC

Although native GPO permissions are designed to delegate permissions to GPOs, sometimes these permissions create a conflict of interest. For example, a member of the domain admin group can make changes at will to the same GPO security settings that are supposed to prevent him or her from doing certain tasks in the first place. Because of this, it's a good idea to implement a role-based access control model so that GPO permissions are externalized away from Active Directory and controlled by a third-party GPO (proxy) security solution such as GPOADmin. GPOADmin is a lifecycle governance solution for GPOs that provides a least-privilege access model and allows you to reduce the number of admins with excessive access to GPO settings.

APPROVAL-BASED CHANGE CONTROLS

Once you establish GPO whitelisting and a GPO RBAC model, you need to set up an automated process that allows for segregation of duties using approval workflows so that the person who edits a GPO setting is different from the person who approves the deployment of the GPO change into the production environment. It may seem obvious, but it is still something that needs to be formally addressed and implemented.

LOCKED-DOWN ACCESS TO GPO SECURITY APPLICATIONS

When you use third-party GPO security applications such as Change Auditor for Active Directory and GPOADmin to control changes made to GPOs, they become critical apps. It's then important to lock down these security solutions from unauthorized access as well. To add this layer of security, you simply add a GPO security policy to your whitelist and apply it to the servers hosting your security applications. Use the following settings:

Deny logon as a batch, Deny access from network, Deny logon as service, Deny logon locally, and Deny logon via RDP

69 percent of privileged users say security tools don't provide enough information on incidents.[2]

A layered security architecture allows you to detect, alert and prevent unauthorized access to GPOs.

SESSION-ONLY ACCESS TO GPO SECURITY APPLICATIONS

To create secure access for server admins to perform regular maintenance tasks on the third-party GPO security applications, you need to provide controlled access via an encrypted remote desktop connection from a jump server such as The Privileged Appliance and Modules (TPAM), which can also be front-ended by a two-factor authentication system such as Defender for extra security. From the jump server, which is a hardened appliance, once the time-based session has been approved by the appropriate approver(s), an authorized staff member can connect to the third-party GPO security application server to perform specific maintenance tasks. All session operations are recorded and can be replayed on demand to detail all operations performed on the server.

CONCLUSION

Unfortunately, GPO security incidents, whether accidental or malicious, can happen at any organization. Given that the built-in security logs don't provide enough information and native permissions are too inflexible, you need a layered security framework that incorporates capabilities from third-party GPO security solutions to detect, alert and prevent GPO security incidents from putting your organization's valuable data at risk.

ABOUT THE AUTHOR

Alvaro Vitta is a principal solutions consultant specializing in security for Quest. He has been assessing, designing, testing and deploying security solutions at large enterprises for on-premises and cloud-based platforms in the private and public sector for 15 years in the areas of identity and access management, Active Directory, and governance, risk and compliance. Vitta holds industry certifications, including CISSP, CISSO, MCSE and ITIL.

[1] "2015 Data Breach Investigations Report," Verizon, April 2015, http://www.verizonenterprise.com/DBIR/2015

[2] "Privileged User Abuse and the Inside Threat," Raytheon Company, May 2014, http://www.raytheoncyber.com/rtnwcm/groups/cyber/documents/content/rtn_257010.pdf.

ABOUT QUEST

Quest helps our customers reduce tedious administration tasks so they can focus on the innovation necessary for their businesses to grow. Quest® solutions are scalable, affordable and simple-to-use, and they deliver unmatched efficiency and productivity. Combined with Quest's invitation to the global community to be a part of its innovation, as well as our firm commitment to ensuring customer satisfaction, Quest will continue to accelerate the delivery of the most comprehensive solutions for Azure cloud management, SaaS, security, workforce mobility and data-driven insight.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (www.quest.com) for regional and international office information.