How to Delegate Privileges to Safely Manage Domain Controllers and Active Directory

JUNE 2016

BY SECURITY EXPERT, RUSSELL SMITH & PRODUCT EXPERT, JASON SILVA

Sponsored by:

BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

It would be an understatement to say that welcoming a new member of the IT staff on board by adding them to the Active Directory *Domain Admins* group is a potential security hazard. And no matter what the longevity of a staff member or the seniority of their position, granting permanent access to privileged AD groups is always a bad idea.

But in spite of the well-understood risks of using administrative privileges, best practice advice from security experts, and the work Microsoft has undertaken to make Windows easier to use as a standard user, organizations often persist in granting administrative privileges to IT staff to expedite system access. However, with a little planning, Active Directory can be effectively managed without domain admin privileges.

It's worth remembering that there's no 'local administrator' account on a domain controller, and that access to Active Directory can be separated from administrative access to domain controllers. To get the equivalent of local administrator privileges on a domain controller, a user must be granted domain administrative privileges, which also gives unrestricted access to AD and to all DCs in a domain.

In this whitepaper, BeyondTrust looks at best practices on how to manage access to domain controllers (DCs) and Active Directory (AD) without permanently assigning domain administrative privileges to IT staff.

AUDIT PRIVILEGED AD GROUPS

If you are currently unaware of the extent of privileged AD access in your organization, the first step would be to establish which accounts have been added to the *Domain Admins, Enterprise Admins, and Schema Admins* groups in AD, and then to understand how these accounts are being used.

You should aim to have just a few accounts as permanent members of the above groups. Other built-in domain groups, such as *Backup Operators* and *Server Operators*, should also be used with caution as they give members enough privilege to disrupt DC operation and potentially elevate privileges beyond what is granted by group membership.

ISOLATE DOMAIN CONTROLLERS

Starting in Windows Server 2012, Microsoft supports the virtualization and cloning of domain controllers on hypervisors that support VM-Generation ID. Virtualization allows organizations to isolate DCs from other sever roles and applications, such as Exchange Server and fileservers, which in turn provides a more secure environment where true separation of administrative roles is easier to achieve.

Imagine a situation where a server acts as a DC and a fileserver. Privileges required by a fileserver administrator potentially give access to AD; there's no way to provide separate administrative access.

READ-ONLY DOMAIN CONTROLLERS

Read-Only Domain Controllers (RODCs) host read-only copies of the partitions of the AD database, and a read-only copy of the SYSVOL folder. Designed for improved security in environments where relatively few users are served by a DC that can't be physically secured, RODCs contact a writeable DC for user authentication as they don't store account credentials locally. Unidirectional replication means that if a RODC were compromised, no changes can be made and replicated to other DCs in the domain. Due to some of these restrictions, not all applications are compatible with RODCs.

RODCs can be set to allow or deny caching of passwords for faster logon of local users, object attributes filtered so that they're replicated to the RODC, and unlike writeable DCs, role separation allows organizations to assign local administrator privileges to individual RODCs.

MANAGING TEMPORARY PRIVILEGED ACCESS

It's reasonable to expect that at times IT staff will need administrative access to domain controllers to perform maintenance tasks. One way to achieve this is to set up a process for issuing access to a domain administrator account. Access should be given to a named account, for a specific period of time to perform an approved task, and when released for use, the name of the employee issued the account should also be recorded to ensure the user is accountable for actions performed while the account is in their care.

Because of the risks associated with privileged AD accounts, DCs should be managed and administered from workstations specially secured for this task. With that in mind, it's better to give support staff access to an account that's reserved exclusively for the purposes of DC support, rather than temporarily assign domain administrative privileges to an account that's used for everyday computing tasks.

POWERSHELL JUST-ENOUGH ADMINISTRATION (JEA)

The most secure way to administer Windows Server is using PowerShell. PowerShell Remoting constrained (JEA) endpoints allow organizations to granularly restrict access to servers, limiting the cmdlets, modules and parameters that can be executed. Users connected to JEA endpoints have the same privileges on the remote server as are assigned to their user account. However, it's also possible to configure endpoints to elevate privileges using a specially assigned administrator account on the remote server to which the connecting user never needs to know the password.

WINDOWS SERVER 2016 JUST-IN-TIME ADMINISTRATION (JIT)

A feature of Windows Server 2016, JIT administration requires Microsoft Identity Manager (MIM) to manage the workflow of this solution. JIT administration uses a separate bastion forest and new kind of cross-forest trust to isolate privileged accounts. Shadow groups are created in the bastion forest and users from the main AD environment are identified as potential members of these groups.

When access to a resource in AD is required, a secondary account for the user is added to the shadow group in the bastion forest and automatically removed after a given time period. Because the shadow group shares a SID with a group in the main AD environment, the user gets access to the required resource.

AD ADMINISTRATIVE MODEL

Organizational Units (OUs) allow organizations to group AD objects for management purposes. Each OU can be managed by a different set of Group Policy Objects or delegated permissions. With this in mind, it's possible to separate privileged AD accounts, service accounts, and other user and computer objects in different OUs so that they can be managed appropriately. Fine-grained password policies optionally allow different password policies to be assigned to groups of users in a domain.

PRIVILEGE DELEGATION

Employee user accounts can be managed by IT staff that don't have domain administrator or *account operator* privileges. The *Delegation of Control Wizard* in *Active Directory Users and Computers* (ADUC) allows privileges to be assigned to an AD group(s) for each OU - such as the ability to create, delete, and manage user accounts. The wizard provides an easy way to assign commonly used privileges, such as unlocking accounts and resetting passwords, but any privilege can be assigned by creating a custom task in the wizard.

RESTRICTED GROUPS

Group Policy *Restricted Groups* can be used to define and enforce membership of built-in AD groups, such as *Domain Admins* and *Account Operators*. When Group Policy is refreshed on a domain controller, restricted groups are re-evaluated and any accounts that aren't listed in the policy are removed, and any that are missing are added, making it harder for a rogue administrator to indefinitely remain a member of one of these groups.

AD MANAGEMENT BEST PRACTICES

Following the best practices outlined in this paper will significantly improve an organization's security posture with the minimum of administrative effort and outlay. Privileged Access Management (PAM) and auditing solutions can also aid in achieving the goals in this paper and help organizations meet compliance obligations.

USING BEYONDTRUST SOLUTIONS TO DELEGATE AD PRIVILEGES

While Microsoft has provided native features to delegate privileges within your enterprise, some of them can be confusing to use, or not available due to the requirements involved. In some cases, you may find your requirements exceed what is available with these features. In these cases, a third party solution geared toward security, compliance and auditing should be considered.

BeyondTrust is a leading cyber security company dedicated to preventing privilege misuse and stopping unauthorized access. With more than 30 years in the security space, and

4,000 customers, BeyondTrust has the experience to help organizations reduce risks, achieve compliance and simplify security operations. Specifically, several BeyondTrust solutions are designed to enforce least privilege, audit privileged activity and control access to AD and Windows assets.

Least Privilege and application control for Windows

Focused around the concept of least privilege, a security model of providing users Just Enough Rights (JER) to perform the tasks and duties related to their roles, PowerBroker for Windows works by installing an agent on a Windows Server or client. Using a centralized console, rules are delivered, (to all or a subset of nodes) that control the permissions and privileges a process has, or prevent it altogether.

But this model goes beyond typical application rights and control tools. Users log in and execute applications as a standard user. Based on policy, application reputation and other factors the respective application's security token is adjusted, not that of a user. This helps to protect against malicious software, ransomware, escalation attacks and unauthorized lateral movement with organizations.

Control and accountability over shared credentials

At times, true administrator (Local or Domain) access will be needed. Manually controlling which accounts have these rights, which users have the credentials for these accounts, and passwords for these accounts is highly prone to security and user error. Inevitably too many people have access beyond their needs,. What's more is there is no record of who is using these accounts.

PowerBroker Password Safe manages enterprise credentials by randomly generating and cycling them by schedule or upon release. Users are associated with access policies, determining under what situations they should be allowed a remote session to Windows, Unix/Linux or network devices. In addition, granting access to remote sessions can be done silently; without exposing passwords for these privileged accounts. In cases where the password needs to be exposed, users can request these with or without additional approvals via the same central portal used to request remote sessions.

Remote sessions can be recorded, providing a full video playback with keystroke logging. This not only provides a full record of which users had privileged access at a particular time, but a full audit of what was done during these times.

This technology helps to protect against issues around weak or shared credentials, poor records of privileged access, and unauthorized access within and between domains, a common theme in recently publicized breaches.

AUDIT AND RECOVERY OF CHANGES IN AD

Securing passwords and managing access are critical components to a proper security model. But they mean nothing without checks and balances. The PowerBroker Auditing & Security Suite maintains a constant, real-time audit of activities within Active Directory. This includes monitoring permissions, changes to structure, even protections against unauthorized changes. A full audit report is provided along with the ability to roll back changes made at any point in time.

CONCLUSION

In order to prevent data breaches, compliance violations or operational complexity, IT organizations must manage access to domain controllers (DCs) and Active Directory (AD) without permanently assigning domain administrative privileges to IT staff. Fortunately, there are both native and commercial options to help achieve this objective.

ABOUT THE AUTHORS

Russell Smith

Russell Smith specializes in the management and security of Microsoft-based IT systems. In addition to being a Contributing Editor at the Petri IT Knowledgebase and is an instructor at Pluralsight. Russell has more than 13 years of experience in IT, and has written a book on Windows security, co-authored one for Microsoft?s Official Academic Course (MOAC) series, and was a regular contributor at Windows IT Professional magazine.

Jason Silva

Jason Silva brings over 20 years of IT experience to BeyondTrust, the last ten with the company. Currently serving as Product Manager for BeyondTrust's Endpoint Security PAM products, he uses this knowledge to help design solutions that fill the critical and ever changing needs of our customers. Earlier in his career he found success as a software developer in a global consulting company and spent over four years managing IT and Regulatory Compliance in the banking industry.