Windows IT Pro

The Keys to the Kingdom: Limiting Active Directory Administrators

By Sean Deuby

Contents

QUEST SOFTWARE®
Simplicity At Work™

The Keys to the Kingdom: Limiting Active Directory Administrators

By Sean Deuby

The practice of allowing data center server operators to be Active Directory domain administrators is the most common—and the most potentially damaging—security risk in the Active Directory infrastructure. The challenge for the Active Directory administrator is to adequately secure their directory, while still delegating enough domain controller administration rights to allow effective daily operations. This white paper explains the domain controller security model and the security risks associated with simple implementations of the model—and presents best practices for separating the role of domain controller administration from domain administration using native tools.

Domain Controller Security

When you're looking at the Active Directory security model it's important to distinguish between data administrator and service administrator roles, though these roles are often lumped together. **Data administrators** are responsible for the content of Active Directory. This role can encompass a wide range of jobs, from centralized account operators that create, modify and delete user accounts to client hardware technicians that create computer accounts as they build new PCs or notebooks for employees and join them to an Active Directory domain. Delegated business unit administrators are also data administrators, although with a smaller scope (such as an OU) than overall data administrators.

Service administrators have a different role, which is the care and feeding of the directory service itself. Regardless of whether the directory service has five users or 500,000, the essentials of the role are the same: define and maintain the Active Directory logical configuration (such as its site and replication topology) and administer its domain controllers, which are the distributed network of Windows servers running the directory service.

A maxim of information security states that if a hacker has full administrative access to a computer, sooner or later they can gain logical access to all the data it contains. This

basic security premise is at the heart of Microsoft's domain controller security model, and is the most difficult aspect of designing your own implementation of the model. That is, how do you delegate administrators of domain controllers without also making them administrators of the domain? To understand why this question is so important, let's examine the way identity is managed in an Active Directory domain.

Member servers in a domain have both a SAM (security accounts manager) database for local account logon and the ability to use domain-wide accounts from Active Directory. Because a domain controller has no local SAM database (only the Active Directory database), it has no local accounts. Therefore, you can only logon to a DC with a domain account. As a result, by default an account with rights to fully administer a domain controller (a member of the Administrators security group) also has rights to fully administer a domain and the data inside it. This issue is known as *administrative role separation*. Microsoft's position on this problematic situation points back to that information security rule: Because domain controller administrators have full access to the system, they can—with the necessary tools, skills, and time—gain access to the data. Therefore, it's folly to set up a security model that pretends they don't have access.

Real-World Risks

Although this principle is correct—and Microsoft must design for it—in the real world it creates a serious security problem. Why? Because the lowest-effort domain controller operational security model is to simply make all server operators members of the Administrators group. And that's what most Active Directory administrators do when they first deploy Active Directory. Microsoft's *Best Practices for Delegating Active Directory Administration* is a 209-page document that details the Active Directory delegation model and provides recommended approaches for creating roles that delegate both service (i.e., the directory service itself) and data (the information stored inside the service) management. However, its recommendation for creating a domain-controller administration role simply by creating a Domain Controller Admins security group in each domain and adding it to the built-in Administrators group does not address the administrative role separation issue. This effectively gives front-line operations staff elevated rights in the domain of the DCs they administer, creating the risk of accidental or malicious alteration or deletion of data, or data structures in the domain. In large enterprises, using this type of configuration can grant literally hundreds of people administrative rights to domains.

As if compromising domain security by using the out-of-the-box configuration isn't bad enough, this vulnerability extends beyond the local domain boundary to the entire forest. All domain owners in a forest must trust each other, because, although the domain partition is the best-known logical structure in Active Directory, it's not the only one. Two directory partitions, schema and configuration extend across the entire Active Directory forest and are therefore on every domain controller in the forest. A user with Domain Admin rights on a domain controller in one domain also has access to the forest-wide schema and configuration partitions on that DC. If the user alters, deletes or otherwise corrupts his local copy of either partition, the changes will replicate to the other copies of the partition on every DC in the forest—and thus impact the entire forest.

For example, a common configuration for a multinational company (Contoso) headquartered in the United States is to have the root domain in the U.S. and child domains for Asia-Pacific (APAC) and Europe (EUR). A server operator in Hong Kong, granted Domain Admin rights in the APAC domain to administer their DCs, has writeable access to the configuration partition for the CONTOSO forest. They can, for example, interfere with site definitions and their NTDS settings to cause Active Directory replication failure across the forest—even though they have elevated privileges in only the APAC domain.

This scenario is an example of why, when designing Active Directory forests, domains and organizational units (OUs), the forest owner must trust all domain owners in a forest. The only true security boundary is at the forest level. If you have operations staff from different major organizations managing domain controllers in different geographies, the most secure configuration dictates that you have separate forests for each. This is explained in detail in Achieving Autonomy and Isolation with Forests, Domains and Organizational Units (http://bit.ly/dWbKls) on Microsoft TechNet.

Best Practices for Delegating Active Directory Administration

So what is the best way to delegate needed rights to domain controller administrators without compromising the domain's security? To effectively delegate domain controller administration using only native tools requires a combination of read-only domain controllers (RODCs), Group Policy and automated software installation.

The RODC, introduced in Windows Server 2008, has three features that mitigate the challenges of administrative role separation on domain controllers. First, as the name implies, it contains a read-only copy of the directory partitions it hosts. No replication occurs from an RODC to a traditional read-write DC (RWDC), so a compromised RODC cannot affect the rest of the domain or forest. RWDCs treat an RODC as an untrusted member of the domain; if a workstation or member server that has a session with an RODC needs to write to the directory (for example, to register a DNS record in an AD-integrated DNS zone), the RODC forwards the request to an RWDC.

Second, by default an RODC stores no passwords. Authentication requests, which require the password hash stored in Active Directory, are forwarded to RWDCs. If an RODC is compromised and the database is run through a password-cracking program like "L0phtcrack," you can't steal what doesn't exist. In a branch office scenario, for example, you can cache authenticated users' passwords locally to speed logon time, while still excluding all administrative accounts from the cache if you wish. This is not a perfect solution, however, since a hacked directory partition still contains useful information such as user account names, server names and DNS records.

Third, Microsoft feels that the read-only nature of these DCs is secure enough to allow delegated, local administrative accounts that do not require any elevated rights in the domain. The accounts using the appropriately named "administrative role separation" feature must be created on the target RODC using the DSMGMT command-line utility.

Because of these features, RODCs provide the only out-of-the-box separation between domain-controller administration and domain administration. Microsoft now suggests a two-tiered domain-controller administration model, with a core of relatively few RWDCs in hub sites surrounded by a greater number of RODCs in branch offices and perimeter networks. Although this configuration doesn't eliminate the original administrative role-separation problem, it lessens the number of domain controllers affected by it.

Group Policy is the primary method for delegating domain-controller administration rights to non-administrative accounts in the domain. Although you must define your own requirements for domain-controller administration, many of the rights needed to delegate this task are found in the "Computer Configuration\Windows Settings\Security settings\Local Policies\User Rights Assignment" section of the Default Domain Controllers GPO. Avoid the temptation to use built-in groups such as Account Operators, Server Operators and Backup Operators because their rights might be more broadly defined than necessary.

Software installation on a domain controller cannot be delegated to a non-administrative user. The best method to delegate this administrative task is to use an automated software-deployment solution, such as System Center Configuration Manager.

Forest-wide service operations cannot and should not be delegated to domain-controller administrators. Site and schema changes, for example, involve writing to the configuration and schema partitions and should only be used by the top-tier directory service administrators.

Finally, take into consideration the effect of virtualization on domain-controller security and administration. Many enterprises have virtualized some or all of their Active Directory infrastructure. Remember that the virtualized domain controller resides on a host, and any operators who have administrative rights on the host can potentially gain administrative access to that domain controller's domain or forest. Therefore, host administrators must also be included in the trusted chain of Active Directory administrators.

Conclusion

Separating the tasks of domain-controller administrators from overall domain administration is the

most important step you can take to secure your Active Directory forest. Using out-of-the-box groups is not sufficient. You must use a combination of read-only domain controllers, Group Policy and software automation to securely delegate day-to-day operations to users that do not have elevated domain privileges. Working through this delegation process will ensure that you keep the number of highly trusted individuals with domain and forest privileges to an absolute minimum.

Sean Deuby, technical director for *Windows IT Pro* and *SQL Server Magazine*, has over 25 years of experience in enterprise IT. He began his IT career running Texas Instruments' IBM VM systems, then helped design, deploy and support TI's first Windows NT 3.5 worldwide infrastructure. He spent 10 years with Intel Corporation, where he was one of the architects of Intel's corporate Active Directory forest and the design engineer of the directory services team. A longtime contributing editor before joining the magazine, Sean is the author of many articles as well as a book on Windows Server and Active Directory. He also speaks on these topics at conferences around the world. Microsoft has recognized Sean as a directory services MVP every year since 2004.