What's new in Active Directory

New features in Active Directory Domain Services in Windows Server 2012, Windows Server 2012 R2 and Windows Server 2016

Sander Berkouwer

MCSA, MCSE & Microsoft Most Valuable Professional (MVP) on Directory Services

AVAILABILITY
for the Always-On Enterprise™

Contents

Introduction . . . 3

New scalability boundaries . . . 4

RID and DNT improvements . . . 4

RID Pool Artificial Ceiling . . . 5

Thirty-first bit of the RID Pool . . . 5

Exposed DNTs . . . 6

Resource SID compression . . . 6

New deployment and migration features . . . 7

Deferred Index Creation . . . 7

Virtualization safeguards . . . 8

Domain Controller Cloning . . . 8

New promotion process . . . 9

New upgrade process . . . 10

New security features . . . 11

Group Managed Service Accounts (gMSAs) . . . 11

Kerberos Armoring (FAST) . . . 12

Protected Users . . . 13

Authentication Policies and Policy Silos . . . 14

Dynamic Access Control . . . 14

Privileged access management . . . 15

New manageability features . . . 16

Active Directory Recycle Bin GUI . . . 16

Fine-grained Password Policy GUI . . . 17

PowerShell History Viewer . . . 17

Mobility features . . . 18

Azure AD Join . . . 18

References . . . 20

About the Author . . . 22

About Veeam Software . . . 22

Introduction

While Active Directory has been around since Windows 2000 Server, Microsoft has been making adjustments and introducing new features in newer releases of Windows Server, especially in Windows Server 2012.

I would even go as far as saying that Windows Server 2012 is as big a milestone for Active Directory as Windows 2000 Server. Virtualization-safe(r) Active Directory, Domain Controller Cloning and the overhauled Active Directory Administrative Center usher in a new era for Active Directory.

Revisiting Active Directory in (Windows Server) 2016, however, painted a different picture with Active Directory playing a different role after Hybrid Identity took center stage.

I'll discuss most of the new features in this whitepaper and I'll show you how to unlock them and put them to good use. This whitepaper, however, is not a complete list of all the new features in Active Directory Domain Services in Windows Server 2012, Windows Server 2012 R2 and Windows Server 2016.

New scalability boundaries

With all the talk on Active Directory multi-master replication, you'd think the sky is the limit for Active Directory. Actually, scalability boundaries exist for all versions of Active Directory.

However, in Windows Server 2012, Microsoft has made two big changes that allow Active Directory environments to grow more easily beyond the limitation encountered by some Active Directory admins today.

RID and DNT improvements

Every object in Active Directory is identified by a Security Identifier (SID). The SID consists of the domain name space and the relative identifier. These attributes are replicated to all Domain Controllers in scope of replication. In the database itself, objects are identified through Distinguished Name Tags (DNTs). DNTs are local to Domain Controller and are not replicated. You can see these as record identifiers.

An Active Directory environment can run out of Relative Identifies (RIDs). This situation is called RID Pool exhaustion or RID Pool depletion. This is a serious problem since no new objects can be created after the local RID Pool blocks of the Domain Controllers are used up. The obvious way out would be to migrate the Active Directory environment to a new environment, but, alas, for such an endeavor an Active Directory trust is needed between the two environments and trust creation requires an RID.

In an Active Directory domain, $2^{30}-1$ (1,073,741,823 or roughly 1 billion) RIDs are available, resulting in a maximum of 2 billion objects, including users, computers, groups, domain trusts, fine-grained password policies and Managed Service Accounts (MSAs).

A couple of scenarios have been identified in previous versions of Active Directory, where RID Pool blocks and thus the RID Pool is used up fast. In these scenarios an RID is taken from an RID Pool block, but is not used to create an object. A prime example is user creation, where the user didn't meet the policies set in the domain. An example of such a policy would be a password policy. Also, when a Domain Controller computer object was deleted and subsequently reanimated or restored, it would ask for a new RID Pool block every 30 seconds because of a missing rIDSetReference attribute and thus depleting the RID Pool in roughly 2 years.

In addition to fixing the scenarios leading to unusual fast RID pool depletion, in Windows Server 2012 and up, the following improvements have been made:

RID Pool Artificial Ceiling

Requirements:

The Domain Controller holding the RID Pool master FSMO role needs to run Windows Server 2012 or up.

When an Active Directory environment reaches RID Pool depletion, warnings will appear in the System log of the Domain Controller holding the RID Pool Master FSMO role. When the Domain Controller holding the RID Pool Master FSMO role has handed out RID Pool blocks corresponding to 90% of the RID Pool, it will stop handing out RIDs and RID Pool blocks.

Domain Admins can override the ceiling by setting the msDS-RIDPoolAllocationEnabled attribute on the RID Manager$ object in the System container of the domain to true.

Thirty-first bit of the RID Pool

Requirements:

All Domain Controllers in the Active Directory domain need to run Windows Server 2012 or up. You do not need to raise the functional level to Windows Server 2012, though.

The thirty-first bit of the RID Pool can be enabled, enabling organizations to create a billion more objects, in addition to the original billion RIDs. Unlocking the 2^{31} bit increases the RID Pool to 2,147,483,647.

Unlocking the thirty-first bit of the RID Pool can be achieved by setting **sidCompatibilityVersion** to **1** using a RootDSE Modification with **ldp.exe**:

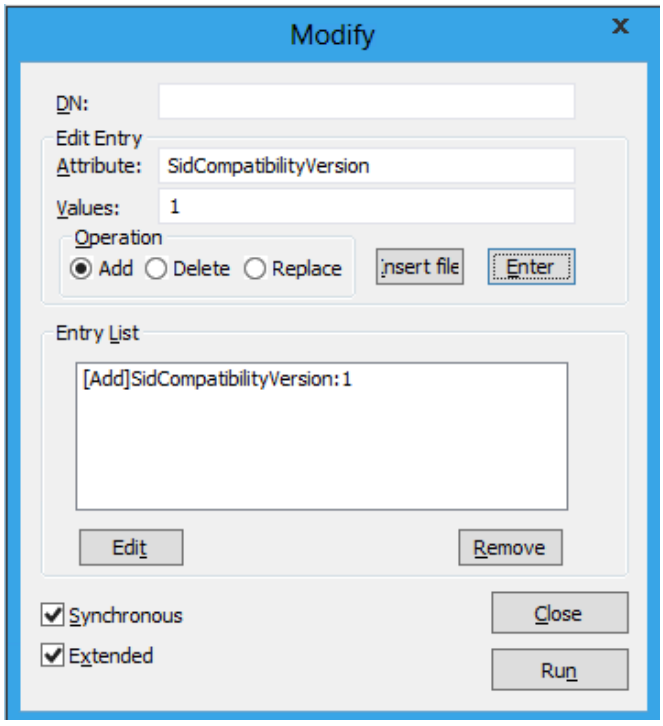

Figure 1: Performing a RootDSE mod to enable the 31st bit of the RID Pool

Exposed DNTs

Requirements:
Domain Controllers for which you want to investigate the DNTs used need to run Windows Server 2012 or up.

In its lifetime a Domain Controller is limited to creating a maximum of approximately two billion DNTs over its lifespan. To be exact, a maximum of 2^{31}–255 DNTs can be created. This amounts to 2,147,483,393 DNTs. Since DNTs don't get re-used, re-claimed or re-serialized, a Domain Controller faces its end when it reaches this limit. Since Windows Server 2012, this limit is suddenly in sight, since the maximum amount of RIDs can now also grow to this limit.

In previous versions of Windows Server it was hard to see the amount of DNTs created; it required dumping the database or programmatically interrogating the database. These options are time consuming and impact performance and disk space.

In Windows Server 2012 and up, admins can more easily see the amount of DNTs using Performance monitor.

Resource SID compression

Requirements:
None. This feature is enabled by default when Kerberos tickets are used by a Domain Controller running Windows Server 2012 and up.

Kerberos tickets can become large in larger Active Directory environments. Domain Admins for these kinds of environments have experience with a problem called Token Bloat. This problem occurs when the amount of data representing the group memberships in the authorization data field (PAC) of Kerberos tickets exceeds the maximum size of the tickets allowed.

In earlier versions of Active Directory Domain Services in Windows Server, this problem was mitigated through SID Compression. This feature would replace the Domain SID Namespace with a relative identifier for the following two kinds of group memberships:

1. Global groups in the user's account domain
2. Universal groups in either of the user's account domains

All other group SIDs remained uncompressed. This includes Domain Local Groups, SIDs from any other groups outside the Active Directory domain the user account is a member of (like sIDhistory) and SIDs for well-known groups.

Along with other Kerberos Token logic, in Windows Server 2012 a new SID Compression scheme is used. This feature is called Resource SID Compression. It is enabled by default.

SID Compression can now also be used to compress Kerberos Service Tickets (STs), not just Kerberos Ticket Granting Tickets (TGTs), enabling the compression of SIDs for Domain Local Groups for the Active Directory domain the user account is a member of and any resource domains.

The following extra group SIDs will be compressed by default in Windows Server 2012 and up:

1. Universal groups in either the user's account or resource domain
2. SID history groups in either the user's account or resource domain

This helps in reducing the Kerberos ticket size.

New deployment and migration features

Deferred Index Creation

Requirements:
Domain Controllers on which you want to (manually) enable Deferred Index Creation need to run Windows Server 2012 or up.

Although Deferred Index Creation in Active Directory borders another scalability boundary, I want to introduce this as the first new migration feature. In larger Active Directory environments, changes in the indexability of objects and their attributes may sometimes have a big effect on the Availability of Domain Controllers to serve clients and replicate changes. Sometimes, index creation even results in a Denial of Service (DoS) of Active Directory, when all Domain Controllers are semi-simultaneously busy (re)creating indices in the database. Isn't that ironic? These indices were built into Active Directory to speed up the performance in the first place.

One of the biggest scenarios in which changes in indexability of objects and attributes occur is the scenario of the Active Directory schema update. It is one of the first steps of a migration to newer versions of Active Directory.

Deferred Index Creation can help in large Active Directory environments to prevent unavailable Domain Controllers due to the building of indices after schema updates.

Deferred Index Creation allows for greater control over which Domain Controller will build indices at a specific moment in time, but as an Active Directory admin, you will need to signal each Domain Controller to create indices or reboot them before they will.

Virtualization safeguards

Requirements:

- *The virtualization platform used to run virtual Domain Controllers needs to support the VM-GenerationID feature.*
- *Virtual Domain Controllers need to run Windows Server 2012 or up. Virtual Domain Controllers need to be installed with the Integration Components/Tools and these need to be configured and running.*

Virtualizing Domain Controllers in previous versions of Windows Server was a daunting task. Domain Controllers running Windows Server 2012 and up can now detect that they are running as virtual machines when the virtualization platform supports the VM-GenerationID feature. Hyper-V on Windows 8 and up, Windows Server 2012 and up, VMware vSphere 5.1 and up and Citrix XenServer 6.2 and up all support this feature.

Domain Controllers can work with the virtualization platform to prevent two possible scenarios for data loss when virtualizing Domain Controllers:

1. USN Rollbacks
2. Lingering objects

The virtualization safeguards will be automatically enabled when the requirements are met.

Domain Controller Cloning

Requirements

- *The Domain Controller holding the Primary Domain Controller emulator (PDCe) Flexible Single Master Operations (FSMO) role needs to run Windows Server 2012 or up.*
- *The source Domain Controller needs to run on a VM-GenerationID-capable virtualization platform and the Integration Components/Tools need to be installed and running.*
- *The source Domain Controller needs to run Windows Server 2012 or up.*
- *The source computer needs to be a member of the Cloneable Domain Controllers group or needs to be granted the* ***DS-Clone-Domain-Controller*** *extended right.*
- *The source Domain Controller cannot be assigned Managed Service Accounts (MSAs), unless these accounts are group Managed Service Accounts (gMSAs).*
- *Applications that are incompatible with cloning should be uninstalled or added to* ***CustomDCCloneAllowList.xml****.*
- *The information specified in DcCloneConfig.xml should be unique.*

Building on the virtualization safeguards in Active Directory, Domain Controllers can be safely cloned:

Figure 2: Domain Controller cloning in Windows Server 2012 and up

Domain admins can use Domain Controller cloning to quickly create a replica Domain Controller when the current Domain Controllers are burdened, but they can also use it as a Disaster Recovery method. Combining Domain Controller Cloning with only a backup copy of one pre-prepped Domain Controller in each domain within an Active Directory environment allows for fast and easy re-creation of the environment.

New promotion process

Requirements:
None. This feature is available by default on Windows Servers running Windows Server 2012 and up. This feature is also available on Windows workstation installations equipped with the Remote Server Administration Tools (RSAT) installed.

Of course, in addition to cloning Domain Controllers, the old-fashioned method of promoting Domain Controllers is still available. However, it has somewhat changed.

We've been trained to use **dcpromo.exe** through the years, but from Windows Server 2012 onwards this tool can only be used to promote Windows Server installations to Domain Controllers when scripted. In the foreseeable future, even this functionality might come to its end, due to the new powerful PowerShell Cmdlets **New-ADForest**, **New-ADDomain** and **New-ADDomainController**.

To promote a Domain Controller using the Graphical User Interface, we use the standardized Server Manager interface. After installing the Active Directory Domain Services (AD DS) role, promotion is done with the **Active Directory Domain Services Configuration Wizard**:

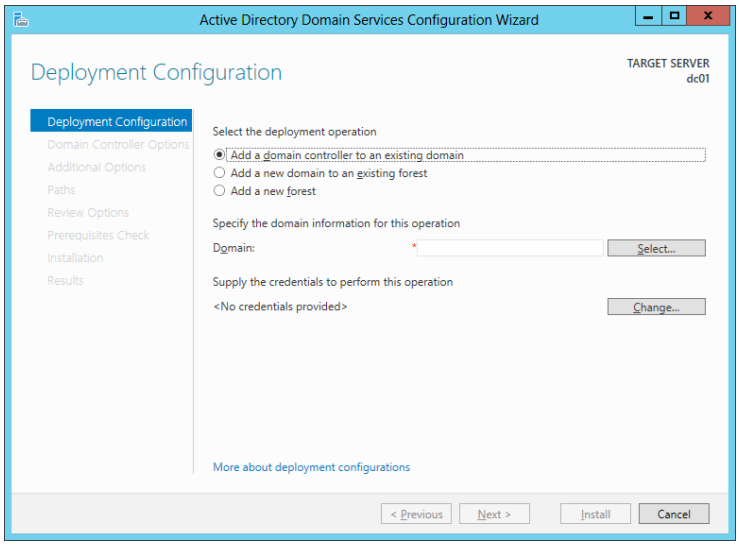

Figure 3: Active Directory Domain Services Configuration Wizard

In contrast to **dcpromo.exe**, this tool allows for remote promotion, allowing Domain Admins to promote a server remotely using either a Windows Server installation with the role installed or a Windows workstation with the Remote Server Administration Tools (RSAT) installed. Or to promote ten Domain Controllers in one action.

Additionally, the new promotion wizard adds prerequisites checking, allowing for a smoother promotion process.

New upgrade process

A third feature of the **Active Directory Domain Services Configuration Wizard** is the ability to automatically prepare the Active Directory domain and forest for new versions of Windows Server for Domain Controllers.

In previous versions of Windows Server, when you would upgrade or transition the Active Directory environment, a couple of manual actions needed to be performed on the old Domain Controllers: You first had to prepare the Active Directory.

Microsoft provided two tools to facilitate this preparation: adprep.exe for 64bit (x64) Domain Controllers and adprep32.exe for 32bit (x86) Domain Controllers. To make things more complex, you needed to run the following commands on typical Domain Controllers in your current Active Directory environment: You needed to run the Forest Preparation (**adprep.exe /forestprep**) on the Schema Master, run the Domain Preparation (**adprep.exe /domainprep**) on the Infrastructure Master, and run the (optional) Read-only Domain Controller preparation (**adprep.exe /rodcprep**) on the Domain Naming Master, etc. After you were done you needed to check proper replication before you set your next migration step. Long story short — it was a pain.

When you promote the first host with a newer Windows Server version to a Domain Controller, the **Active Directory Domain Services Configuration Wizard** will determine if preparation is needed, as part of prerequisites checking. When it is triggered to perform preparation, the wizard will check afterwards for proper replication of these changes.

Of course, for larger or more stringently managed Active Directory environments, **adprep.exe** is still available. And even this tool has seen a nice improvement; it is now multi-lingual. Unfortunately, the catch is that there's no longer a 32bit version available.

Note:
Microsoft has announced the deprecation of the Windows Server 2003 Functional levels. You will not be able to promote Windows Servers running the next version beyond Windows Server 2016 as Domain Controllers in Active Directory Domain Services environments running the Windows Server 2003 Domain Functional Level. You will first, manually, have to upgrade the functional levels to at least Windows Server 2008 and migrate SYSVOL replication to DFS-R manually, if your environment has ever begun life before the advent of Windows Server 2008.

New security features

In Windows Server 2012 and Windows Server 2012 R2, a couple of features have been introduced to enable domain admins to further lock down their Active Directory environments:

Group Managed Service Accounts (gMSAs)

Requirements:

- *At least one Domain Controller running Windows Server 2012 or up*
- *Active Directory PowerShell module installed on either a Windows Server 2012-based management server or up, or a Windows 8 management workstation or up.*
- *For automatic password and SPN management, the Active Directory environment needs to be running the Windows Server 2008 R2 Domain Functional Level or up.*

Managed Service Accounts (MSAs) allow you to securely run a service on domain-joined Windows and Windows Server installation. MSAs solve most of the headaches involved with using 'regular' service accounts; passwords for MSAs are not stored in the registry, passwords for MSAs are changed automatically every 30 days and MSAs cannot be misused to log on interactively.

The drawback of MSA objects, introduced with Windows Server 2008 R2, is that they can only be configured for one host. When a service resides on multiple hosts, multiple MSAs need to be used or domain admins need to resort to the 'regular' unsafe service accounts.

Group Managed Service Accounts (gMSAs) solve this latter problem. gMSAs provide a single identity solution for services running on server farms, or on systems behind Network Load Balance. By using gMSAs, services can be configured for the new gMSA object and the password management is handled by Windows.

After you've created and targeted a gMSA to a group of servers, you can configure services to use the gMSA as easy as you would use the built-in NETWORK service.

Kerberos Armoring (FAST)

Requirements for enabling Kerberos Armoring:

- *Strategically placed Domain Controllers running Windows Server 2012 or up.*
- *The environment no longer contains Domain Controllers running Windows Server 2003.*
- *Clients need to be running Windows 8 or up.*

Requirements for requiring Kerberos Armoring:

- *All Domain Controllers in domains the client uses are running Windows Server 2012 or up. (Including transited referral domains)*
- *All domains the client uses are running the Windows Server 2012 Domain Functional Level, or up.*
- *Clients need to be running Windows 8 or up*

A whole new security feature in Active Directory Domain Services in Windows Server 2012 listens to the name Flexible Authentication Secure Tunneling (FAST). This new feature solves common security problems with Kerberos and also makes sure clients do not fall back to less secure legacy protocols or weaker cryptographic methods.

Note: *Sometimes, this feature is referred to as Kerberos Armoring, but Flexible Authentication Secure Tunneling (FAST) is its official name defined by the April 2011 RFC 6113.*

Kerberos Armoring can be deployed in stages through Group Policy Objects (GPOs). The Group Policy setting **KDC support for claims, compound authentication and Kerberos armoring** was designed for this purpose. There are options corresponding to the deployment stages.

The first stage is **Supported**. You will have Kerberos Armoring (FAST) on your network between domain-joined Windows 8 clients and up and Windows Server 2012-based Domain Controllers and up, after the next Group Policy refresh cycle.

Requiring Kerberos Armoring (FAST) is the next step. Group Policy remains the deployment method, but you will need to configure additional settings. It starts with configuring the **Fail authentication requests when Kerberos armoring is not available** in the Group Policy setting on Domain Controllers. Then above the mentioned Group Policy **KDC support for claims, compound authentication and Kerberos armoring**, located in Computer Configuration, Administrative Templates, System, KDC needs to be configured with the Fail unarmored authentication requests setting.

Protected Users

Requirements for client-side protection:

- *The Active Directory schema version needs to be upgraded to at least Windows Server 2012 R2 (69).*
- *The Domain Controller with the Domain Controller emulator (PDCe) Flexible Single Master Operations (FSMO) role needs to run Windows Server 2012 R2 or up.*
- *Users need to authenticate on Windows 8.1-based devices (or up) or Windows Server 2012 R2-based servers (or up) to a Domain Controller that runs at least Windows Server 2012 R2.*

Requirements for Domain Controller protection:

- *The Active Directory schema version needs to be upgraded to at least Windows Server 2012 R2 (69).*
- *The Domain Controller with the Domain Controller emulator (PDCe) Flexible Single Master Operations (FSMO) role needs to run Windows Server 2012 R2 or up.*
- *Users need to authenticate on Windows 8.1-based devices (or up) or Windows Server 2012 R2-based servers (or up) to a Domain Controller that runs at least Windows Server 2012 R2.*
- *The Active Directory domain needs to operate on the Windows Server 2012 R2 Domain Functional Level (DFL) or up.*

From a security point of view, accounts and devices can also be more sensitive than others. Stricter password policies to user accounts and groups with the Fine-Grained Password Policies functionality and Group Policies to disallow interactive logons and network logons to user accounts and groups in Active Directory on Organizational Units (OUs) on certain domain-joined devices were considered solutions to these challenges.

However, there was no way to restrict sensitive accounts in terms of the lifetime of the Ticket Granting Tickets (TGTs), restricting more vulnerable authentication protocols (like NTLM), encryption standard to use in the pre-authentication process, the ability to be (constrainedly) delegated, or criteria for the devices sensitive accounts log on.

The **Protected Users** global security group in the **Users** container triggers non-configurable protection on devices and servers running Windows Server 2012 R2 and Windows 8.1 and on Active Directory Domain Controllers in domains running the Windows Server 2012 R2 Domain Functional Level (DFL).

These protections come in two stages:

1. Client-side protection, disabling the ability to authenticate using digest authentication and CredSSP and restricting the maximum lifetime for user tickets and user ticket renewal to 240 minutes (4 hours).
2. Domain Controller protection, disabling the ability to authenticate using NTLM, disabling caching of password hashes and disabling Kerberos pre-authentication encryption with DES and RC4.

Note: *When authenticating devices with Operating Systems prior to Windows 8.1 or servers with Operating Systems prior to Windows Server 2012 R2, no protections apply.*

Authentication Policies and Policy Silos

Requirements:

- *All Domain Controllers in the Active Directory domain must be running at least Windows Server 2012 R2 or up.*
- *The Active Directory Domain Functional Level (DFL) must be Windows Server 2012 R2 or up.*
- *Domain Controllers need to be configured with the* ***KDC support for claims, compound authentication and Kerberos armoring*** *group policy setting.*
- *Clients in scope for authentication policies and authentication policy silos need to be configured with the* ***Kerberos client support for claims, compound authentication and Kerberos armoring*** *group policy setting.*

When the **Protected Users** group isn't granular enough to cater to the needs of the environment, **Authentication Policies** and **Authentication Policy Silos** can be used.

Authentication policy silos tie user objects and computer objects together using a claim with the name of the silo to apply the authentication policy. When the requirements set in the authentication policy are met, the policy applies to Kerberos Ticket Granting Ticket (TGT) lifetime and renewal. When they are not met, no (TGT) is issued and thus, logon is denied.

Dynamic Access Control

Requirements:

- *At least one Domain Controller needs to run Windows Server 2012 or up.*
- *File Servers, where you want to use claims-based access control, need to be running Windows Server 2012 or up. Third-party storage vendors may also support the feature.*
- *The Active Directory Forest Functional Level needs to be Windows Server 2003.*
- *Kerberos Armoring (FAST) is required for* ***Compound Identity*** *(Compound ID).*

The same claims can be used for Claims-based Access Control (CBAC) to files and folders, named Dynamic Access Control (DAC), where these claims are placed in tokens. Claims within Dynamic Access Control can be based on any attribute of a user object. Claims can also be based on attributes for computer objects, but this requires Kerberos Armoring (FAST). When the user claims and the device claims are combined, this forms the **Compound Identity** (Compound ID).

Dynamic Access Control can be scoped to specific file servers using **Central Access Policies**. These Central Access Policies contain **Central Access Rules**, applying to files and folders, targeted using file and folder **Property lists** containing file and folder **Resource properties**.

When a file or folder in scope of the Central Access Policy corresponds with the resource properties, the access is granted as defined in the Central Access Policy. Even when a file or folder is moved, but the properties remain the same, the same access policy applies.

Privileged access management

Requirements:

- *The Active Directory Forest Functional Level needs to be Windows Server 2008 R2, or up.*
- *A Microsoft Identity Manager 2016 implementation running on Windows Server 2012 R2 or Windows Server 2016, configured as Domain Controllers or members of a Privileged Access Management Active Directory Forest, running at least the Windows Server 2012 R2 Domain and Forest Functional Level.*
- *Expiring links on linked values and the corresponding Kerberos Key Distribution Center (KDC) enhancements require the Windows Server 2016 Forest Functional Level and the Optional Feature to be enabled (but not necessarily in the compromised forest in a PAM scenario).*
- *Shadow Security Principals (groups) require the Windows Server 2016 Forest Functional Level (in the privileged forest in a PAM scenario).*

One of the new associated features for Active Directory in Windows Server 2016 is the Privileged Access Management (PAM) feature. This feature builds upon three new features in Windows Server 2016:

1. Shadow Security Principles (groups)
2. Expiring links on linked values, like group memberships
3. Kerberos Key Distribution Center (KDC) enhancements

Together with the new PAM Forest and PAM components in Microsoft Identity Manager 2016, this enables an admin to regain control over a compromised Active Directory environment.

The new Shadow Security Principals in Windows Server 2016 allow security groups of the Privileged Access Management (PAM) forest to be referenced to privileged groups in the compromised forest, without requiring changes to access control lists (ACLs). These references can subsequently be provided with a time-to-live value, so that they expire automatically. This solves the greater part of the problem surrounding always-on admin accounts. The KDC enhancements in Windows Server 2016 limit the Kerberos tickets to the shortest remaining time-to-live value for any of the linked values.

This is all governed through Microsoft Identity Manager 2016, that includes a Privileged Access Management REST API, portal, client and monitoring service, as well as the PowerShell cmdlets to manage the new PAM Forest type.

New manageability features

The Active Directory Administrative Center (**dsac.exe**) that was introduced with Windows Server 2008 R2, has had a serious overhaul in Windows Server 2012. In addition to providing Graphical User Interfaces (GUIs) to the new features discussed above, it was expanded with the functionality to manage features that were previously only manageable on the command line:

Active Directory Recycle Bin GUI

Requirements:

- *At least one Windows 8 or up installation, or Windows Server 2012 or up installation, with the Remote Server Administration Tools (RSAT) and the Active Directory Domain Servers management tools installed.*
- *The Active Directory Forest Functional Level needs to be Windows Server 2008 R2 or up.*

The Active Directory Recycle Bin was introduced in Windows Server 2008 R2 and the Windows Server 2008 R2 Forest Functional Level (FFL). It enables administrators to restore (accidentally) deleted objects without booting into Directory Services Restore Mode (DSRM) or reanimating objects (with loss of attributes).

Unfortunately, the only way to manage the Active Directory Recycle Bin in Windows Server 2008 R2 is to use PowerShell. PowerShell is useful for repeating tasks, but its strength is not in performing one-time actions like enabling the Active Directory Recycle Bin and undeleting accidentally deleted objects with PowerShell.

Using the Active Directory Administrative Center (**dsac.exe**) on Windows Server 2012 and up, you can enable the Active Directory Recycle Bin. After enabling the feature and after replication has occurred, you can undelete objects from the **Deleted Objects** container:

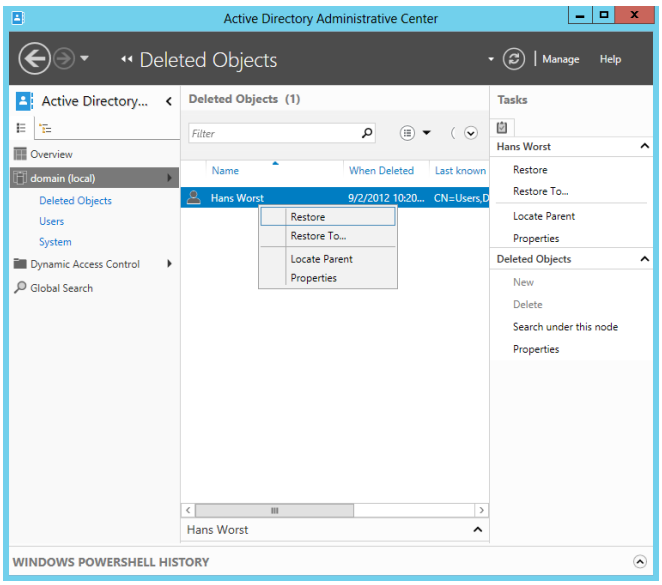

Figure 4: Undeleting a deleted user object using the Active Directory Administrative Center

Fine-grained Password Policy GUI

Requirements:

- *At least one Windows 8 or up installation, or Windows Server 2012 installation, or up with the Remote Server Administration Tools (RSAT) and the Active Directory Domain Servers management tools installed.*
- *The Active Directory Domain Functional Level needs to be Windows Server 2008 or up.*

Additionally, using the Active Directory Administrative Center (**dsac.exe**) on Windows Server 2012 and up, you can now define and apply fine-grained password policies.

Microsoft introduced the concept of Fine-grained Password Policies in Active Directory back in Windows Server 2008. From that day on, Active Directory admins could granularly roll out Password and Account Lockout Policies to groups and individual users. It was, however, such a painful experience, that many books suggested to use the free SpecOps Password Policy Basic tool to set fine-grained password policies, instead of using the built-in PowerShell commands.

Fine-grained password policies are located in the **Password Settings container.**

PowerShell History Viewer

Requirements:

- *At least one Windows 8 installation, or up or Windows Server 2012 installation, or up with the Remote Server Administration Tools (RSAT) and the Active Directory Domain Servers management tools installed.*

A third and perhaps the most useful improvement to the Active Directory Administrative Center (**dsac.exe**) in Windows Server 2012 is the **PowerShell History Viewer**.

The contents of this pane, which flicks up when you press the up arrow in the right bottom corner on the bar that reads PowerShell History Pane, show you the equivalent PowerShell commands to actions you perform in the Graphical User Interface (GUI).

The Active Directory PowerShell History Viewer makes it easy to learn the Active Directory PowerShell Cmdlets. It's a useful addition to the Active Directory Administrative Center (**dsac.exe**), since Windows Server 2012 contained 145 Active Directory Domain Services-related PowerShell Cmdlets and it would take you over three years to learn them otherwise.

Mobility features

Azure AD Join

Requirements:

- ***Scenario 1***

At least Windows 10 RTM or up, for Azure AD Join during the Out-of-the-Box Experience (OOBE) and through PC Settings.

- ***Scenario 2***

At least Windows Vista with the WorkPlace Join for non-Windows 10 clients package installed, Windows 7 and/or Windows 8.1 clients in environments with:

- *Active Directory Domain Services (AD DS) prepared for Windows Server 2012 R2, or up. Your Active Directory schema must read at least version 69.*
- *Active Directory Federation Services (AD FS) running Windows Server 2012 R2 or up, with the Device Registration Service enabled.*
- *Devices in scope for Workplace Join need to be domain-joined.*
- *Devices in scope for Workplace Join need to be in scope of a Group Policy Object with the* ***Automatically workplace join client computers*** *Group Policy setting enabled.*
- *The AD FS Global Primary Authentication Policy must be configured to allow Windows Integrated Authentication for the Intranet.*
- *Multi-factor Authentication must not be configured for the Device Registration Service or in the Global Primary Authentication Policy in AD FS for devices, connected as an inside device (on the Intranet).*
- *The Federation server used needs to see the devices in scope to be connected as an inside device (on the Intranet). You cannot automatically WorkPlace Join through a reverse proxy solution, such as the Web Application Proxy.*
- *Internet Explorer on devices in scope must use the following (default) settings for the Local intranet security zone:*
  - *Don't prompt for client certificate selection when only one certificate exists: Enable*
  - *Allow scripting: Enable*
  - *Automatic logon only in Intranet zone: Checked*

A Service Connection Point (SCP) configured and AD FS Claims Transformation Rules configured as per the instruction on How to setup automatic registration of Windows domain joined devices with Azure AD.

- ***Scenario 3***

At least Windows Vista with the WorkPlace Join for non-Windows 10 clients package installed Windows 7, Windows 8.1 and/or Windows 10 domain-joined clients running in an environment with:

- *Active Directory Domain Services running at least the Windows Server 2003 Forest Functional Level.*
- *Azure AD Connect version 1.1.108.0 or up, installed on Windows Server 2008 R2, or up, with the Sync Domain Joined Computers Sync feature enabled through the ADSyncPrep PowerShell Module*

The rapid adoption of Azure Active Directory has sparked organizations to embrace a Hybrid Identity approach. In this approach, the on-premises Active Directory Domain Services still acts as the Identity Provider (IdP) for the organization, but not just for single sign-on access to on-premises applications, systems and services, but also to cloud-based applications and services.

Because it is not the brightest idea to use Kerberos or NTLM over the Internet, in recent years new protocols have been developed; open, web-ready protocols, based on the principles of identity federation. Active Directory Federation Services (AD FS) has played a key role for many organizations, but AD FS is not strictly needed to achieve Hybrid Identity.

Microsoft's free 'identity bridge' product, **Azure AD Connect**, is capable of enabling Hybrid Identity in Same Sign-On and Single Sign-On scenarios. One of the most interesting scenarios is the way Windows devices can be Azure AD-joined and be written-back to the on-premises Active Directory environment, but also how domain-joined devices can automatically be Azure AD-joined, through Domain Join ++.

When joined to Azure AD, every user account in the Azure AD tenant can be used to interactively log on to the device.

Scenario 1

Windows 10 can be joined to Azure Active Directory during the Out-of-the-Box Experience (OOBE) and through PC Settings > Accounts. In environments with Hybrid Identity, Azure AD Connect can write the corresponding objects in Azure AD back to the on-premises Active Directory environment as registered devices.

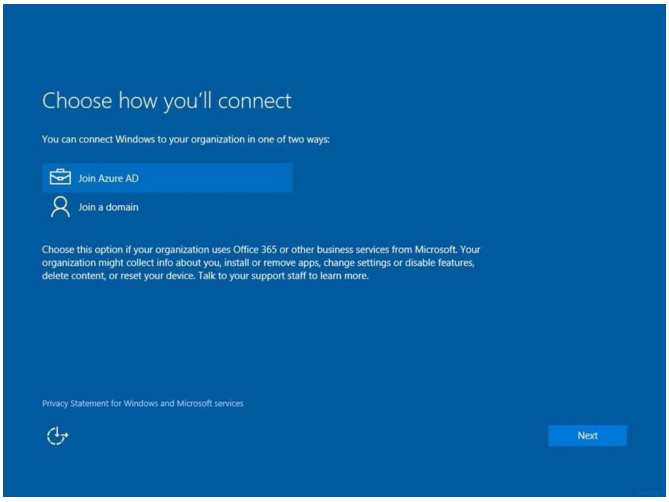

Figure 5 Out-of-the-Box Experience for Azure AD Join in Windows 10

Note:

Since this scenario is particularly suitable for Bring-Your-Own and Choose-Your-Own scenarios, the user account used to join the device to Azure AD this way is automatically granted local admin rights.

Scenario 2

In Hybrid Identity scenarios with Active Directory Federation Services (AD FS), domain-joined devices can be instructed through Group Policy to register with Azure AD.

Scenario 3

In Hybrid Identity scenarios without AD FS, Azure AD Connect can take care of the sync of computer objects in Active Directory Domain Services to device objects in Azure Active Directory. Because Password Hash Sync is needed for Same Sign-On in this scenario, the Active Directory environment needs to run at least the Windows Server 2003 Forest Functional Level and Azure AD Connect needs to be installed on Windows Server 2008 R2 or up.

References

Microsoft TechNet — What Are Active Directory Functional Levels?

Microsoft TechNet — How Active Directory Functional Levels Work

Microsoft TechNet — How the Active Directory Schema Works

Microsoft TechNet — Operations master roles

What's New in Active Directory Domain Services (AD DS) in Windows Server 2012

Microsoft TechNet — Active Directory Maximum Limits - Scalability

The things that are better left unspoken — RID improvements

Microsoft TechNet — Managing RID Issuance

The things that are better left unspoken — DNTs exposed

Microsoft KB article 2774190 — Resource SID Compression in Windows Server 2012 may cause authentication problems on NAS devices

The things that are better left unspoken — Resource SID Compression

The things that are better left unspoken — Deferred Index Creation

Microsoft TechNet — Introduction to Active Directory Domain Services (AD DS) Virtualization

The things that are better left unspoken — Virtualization-safe Active Directory

The things that are better left unspoken — Domain Controller Cloning

Microsoft TechNet — What's New in Active Directory Domain Services Installation and Removal

Microsoft TechNet — Upgrade Domain Controllers to Windows Server 2012

The things that are better left unspoken — New Promotion Process

The things that are better left unspoken — New Upgrade Process

Microsoft TechNet — Group Managed Service Accounts Overview

The things that are better left unspoken — Group MSAs (gMSAs)

Microsoft TechNet — What's New in Kerberos Authentication

The things that are better left unspoken — Kerberos Armoring

Microsoft TechNet — Protected Users Security Group

The things that are better left unspoken — Protected Users Group

Microsoft TechNet — Authentication Policies and Authentication Policy Silos

The things that are better left unspoken — Dynamic Access Control

Microsoft TechNet — Introduction to Active Directory Administrative Center Enhancements

The things that are better left unspoken — PowerShell History Viewer

The things that are better left unspoken — Recycle Bin GUI

The things that are better left unspoken — Fine-grained Password Policy GUI

Microsoft TechNet — Introduction to Active Directory Management Using Windows PowerShell

The things that are better left unspoken — New PowerShell Cmdlets

Microsoft TechNet — What's New in Active Directory Domain Services in Windows Server 2016

Microsoft TechNet — Privileged Access Management for Active Directory Domain Service

How to set up automatic registration of Windows domain joined devices with Azure AD

About the Author

Sander Berkouwer is an MCSA, MCSE, MCT, Microsoft Most Valuable Professional (MVP) and Veeam Vanguard. Working for SCCT, a Dutch IT services provider, he has ample experience with deploying and maintaining Microsoft technologies in hundreds of environments, ranging from four to four hundred thousand seats, both on-premises and in the cloud.

You can read more from Sander in his blog.

About Veeam Software

Veeam® recognizes the new challenges companies across the globe face in enabling the Always-On Business™, a business that must operate 24.7.365. To address this, Veeam has pioneered a new market of *Availability for the Always-On Enterprise*™ by helping organizations meet recovery time and point objectives (RTPO™) of less than 15 minutes for all applications and data, through a fundamentally new kind of solution that delivers high-speed recovery, data loss avoidance, verified protection, leveraged data and complete visibility. Veeam Availability Suite™, which includes Veeam Backup & Replication™, leverages virtualization, storage, and cloud technologies that enable the modern data center to help organizations save time, mitigate risks, and dramatically reduce capital and operational costs.

Founded in 2006, Veeam currently has 43,000 ProPartners and more than 230,000 customers worldwide. Veeam's global headquarters are located in Baar, Switzerland, and the company has offices throughout the world. To learn more, visit www.veeam.com.


VEEAM
AVAILABILITY
for the Always-On Enterprise™
IT'S HERE
NEW Veeam
Availability Suite 9.5
AVAILABILITY for the Always-On Enterprise
go.veeam.com/v9-5