SMART Active Directory Migrator 9.0.2

Requirements

January 2016

Table of Contents

Requirements 3

SMART Active Directory Migrator Basic Installation Requirements 3
Workstation and Member Server System Requirements 5
Networking Requirements 5
SSL Certificate Requirements 6
Service Account Requirements 6
DNS SRV Record Requirement 7
SID History Synchronization Requirements 7
Password Requirements 9
SMART Directory Sync Requirement for Synchronize Passwords 9

About Binary Tree 10

Requirements

SMART Active Directory Migrator Basic Installation Requirements

The SMART Active Directory Migrator suite consists of Binary Tree's SMART Active Directory Migrator, which includes both the console and the Web service, and SMART Directory Sync software packages. Both packages will require access to Microsoft SQL Server. In most environments, all of these components will be installed on the same server.

Single Server Installation Requirements

Supported Operating Systems	o Windows Server 2008 R2 o Windows Server 2012 R2
SQL Server Requirements	o SQL 2008 R2 or SQL 2012 SP2 o SQL Express Editions are supported up to 5000 objects o SQL Management Studio must be installed o SQL must be configured to permit mixed authentication, and one local SQL authentication account must be created for SMART AD Migrator and SMART Directory Sync to share
Minimum Hardware Requirements	o 2 CPU/vCPU o 6GB RAM o 10 GB disk space, inclusive of the SQL install requirements
Additional Components	o If your server is not internet connected, you will be required to install the following components prior to installing SMART Active Directory Migrator: o **.NET Framework (Full) 4.5.2** or newer o **Visual C++ 2013 Redistributable** – BOTH the x64 and x86 versions must be installed, regardless of the fact that the Windows Operating system is 64-bit

Multi-Server Installation Requirements

SMART Active Directory Migrator 9.0.2 is scalable and supports segregating components and can be installed in a multi-server configuration to support larger or complex environments.

If required in larger installations, remote SQL Servers may be used for the primary database and the logging database. Additionally, the primary database and the logging database can be segregated onto separate SQL Server instances.

Each of the following roles/functions may be separated onto different servers as required in advanced configurations:

- AD Migrator Server Web Service
- AD Migrator Administrator Console
- SMART Directory Sync Software
- Directory Sync Database
- Directory Sync Logging Database

When installed independently, Binary Tree's components require the following resources:

Supported Operating Systems	o Windows Server 2008 R2 o Windows Server 2012 R2
AD Migrator Split Role Minimum Hardware Requirements	• 1 CPU/vCPU • 2GB RAM • 1 GB disk space
Directory Sync Hardware Requirements	• 2 CPU/vCPU • 4GB RAM • 5 GB disk space
SQL Server	• SQL 2008 R2 or SQL 2012 SP2 • SQL must be configured to permit mixed authentication, and one local SQL authentication account must be created for SMART AD Migrator and SMART Directory Sync to share. • SQL Management Studio must be installed • Express editions of SQL Server are supported as long as the express installation includes SQL Management Studio

Additional Components	• If your server is not internet connected, you will be required to install the following components prior to installing SMART Active Directory Migrator:
	  • **.NET Framework (Full) 4.5.2** or newer
	  • **Visual C++ 2013 Redistributable** – BOTH the x64 and x86 versions must be installed, regardless of the fact that the Windows Operating system is 64-bit

Workstation and Member Server System Requirements

Supported Operating Systems	o Windows XP SP3 o Windows Vista SP1 o Windows 7 SP1 o Windows 8 o Windows 8.1 o Windows 2003 SP2 o Windows 2008 o Windows Server 2008 R2 o Windows Server 2012 o Windows Server 2012 R2
PowerShell Requirements	o All client operating systems must have at least PowerShell 2.0 installed. o Please Note: Windows XP, Windows Vista, Windows 2003, and Windows 2008 do not natively contain PowerShell 2.0. It must be installed/deployed prior to installing the SMART Active Directory Migrator Agent.
.NET Framework Requirements	• All operating systems must have **.NET Framework 4.0 (Full Version)** or newer installed. This will appear as ".NET 4.0 Extended" in the add/remove programs list. • The "client" installation of the .NET Framework is not sufficient and must be upgraded to the full .NET Framework.

Networking Requirements

Domain Controller Access

For most scenarios, SMART AD Migrator requires access to at least one read/write domain controller running Windows 2003 SP2 or newer in each source and target Active Directory domain. For fault tolerance, Binary Tree recommends at least two domain controllers in each source and target domain.

If SID History will be synchronized, SMART Active Directory Migrator will require access to the domain controller holding the PDC Emulator Active Directory FSMO role in all source and target domains.

In limited scenarios, it is possible that SMART AD Migrator will not be responsible for creating or updating any accounts in the source or the target domains. In this scenario, SMART AD Migrator can be configured to communicate with Read Only Domain Controllers (RODCs).

Network/Firewall Requirements

SMART Active Directory Migrator requires the following network ports to enable full functionality:

Source	Target	Port/Protocol
Workstations and Member Servers	SMART AD Migrator Server	443 (TCP) or 80 (TCP)
SMART AD Migrator Server	Source and Target Domain Controllers running Windows 2003	135, 137, 389, 445, 1024-5000 (TCP) 389 (UDP)
SMART AD Migrator Server	Source and Target Domain Controllers running Windows 2008 or newer	135, 137, 389, 445, 49152-65535 (TCP) 389 (UDP)

SSL Certificate Requirements

SMART Active Directory Migrator does not require HTTPS (HTTP with SSL), and can operate using HTTP. However, Binary Tree strongly recommends implementing SMART AD Migrator using HTTPS to secure communications between the devices to be migrated and the AD Migrator Server. In order to activate HTTPS on the IIS component in Windows, the SMART AD Migrator system will require that a SSL certificate is present.

Binary Tree does not provide a SSL Certificate as part of the installation. For the most secure installation, Binary Tree recommends purchasing a SSL Certificate from a Windows supported 3rd party provider.

In scenarios where this is not possible, self-signed SSL Certificate can be generated in Windows following these directions: **https://technet.microsoft.com/en-us/library/cc753127(v=ws.10).aspx**

If using a self-signed certificate, it should be noted that Binary Tree's agent component would utilize the operating system's certificate trust list. Due to the security nature of Active Directory migrations, there is no method of implementing an override and forcing the agent to use an untrusted certificate. If a self-signed certificate is used, that certificate will need to be added to the trusted root certificate list for all computer objects to be migrated. This can be accomplished via group policy: **https://technet.microsoft.com/en-us/library/cc738131(v=ws.10).aspx**

Service Account Requirements

Binary Tree's SMART Active Directory Migrator requires the following user account permissions and privileges to support Active Directory Migrations:

- One service account with read/write access to all organizational units (OUs) containing user, group, and computer objects in the source Active Directory to be migrated to the target environment.
- One service account with administrative rights on the target domain(s)

- If administrative rights cannot be granted, the service account requires the following rights:
  - The ability to create and modify user objects in the desired OUs in the target Active Directory environment.
  - Read Permissions to the configuration container in Active Directory
  - User credentials with the delegated migrateSIDHistory extended right.
- A service account in each source and target domain with the ability to modify computer objects and add computers to the domain.

DNS SRV Record Requirement

In each source domain, a SRV DNS record must be created to enable autodiscover for SMART AD Migrator Agents.

- To enable autodiscover when HTTPS is desired
  - Record Name: _btadm._https.SourceDomainName.Local
  - Weight and Priority 0
  - Port Number 443
- To enable autodiscover when HTTP is desired
  - Record Name: _btadm._http.SourceDomainName.Local
  - Weight and Priority 0
  - Port Number 80

SID History Synchronization Requirements

In order to support synchronization of SID History from the source to the target domains, Windows requires that a specific domain local group exists and that account auditing is enabled.

Preparing the Source and Target Domains

To prepare each source and target domain for SID History Synchronization, the following configuration steps must be completed:

- In the source domain, create a local group called SourceDomain**$$$**, where SourceDomain is the NetBIOS name of your source domain. For example, if your domain's NetBIOS name is ADM, you must create a domain local group named ADM**$$$**.

  SID History synchronization will fail if members are added to this local group.

- Enable TCP/IP client support on the source domain PDC emulator:
  1. On the domain controller in the source domain that holds the PDC emulator operations master (also known as flexible single master operations or FSMO) role, click **Start**, and then click **Run**.
  2. In **Open**, type **regedit**, and then click **OK**.

3. In Registry Editor, navigate to the following registry subkey:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA

4. Modify the registry entry **TcpipClientSupport**, of data type **REG_DWORD**, by setting the value to 1.
5. Close Registry Editor, and then restart the computer.

- Enable auditing in the target domain:

1. Log on as an administrator to any domain controller in the target domain.
2. Click **Start**, point to All Programs, point to Administrative Tools, and then click **Group Policy Management**.
3. Navigate to the following node: Forest | Domains | Domain Name | Domain Controllers | Default Domain Controllers Policy
4. Right-click **Default Domain Controllers Policy** and click **Edit**.
5. In Group Policy Management Editor, in the console tree, navigate to the following node: Computer Configuration | Policies | Windows Settings | Security Settings | Local Policies | Audit Policy
6. In the details pane, right-click **Audit account management**, and then click **Properties**.
7. Click **Define these policy settings**, and then click **Success and Failure**.
8. Click **Apply**, and then click **OK**.
9. In the details pane, right-click **Audit directory service access** and then click **Properties**.
10. Click **Define these policy settings** and then click **Success**.
11. Click **Apply**, and then click **OK**.
12. If the changes need to be immediately reflected on the domain controller, open an elevated command prompt and type *gpupdate /force*.
13. Repeat the above steps in the source domain.

> It may also be necessary to reboot the domain controller to have auditing take effect.
>
> Even with group policy applied on the default domain controller for the domain audit, the server audit setting on the primary domain controller (PDC) may not be enabled. Please confirm this setting is enabled for the local security policy on the PDC server. If not enabled, use the local security policy to enable this setting.

Validate Cross-Domain Verification

A trust is not required to synchronize SID History in SMART AD Migrator. However, when a trust is present, it is necessary to ensure that the trust is properly configured to permit cross-domain verification. To do so, first identify if the trust between the source and target domain is an external trust or a forest trust. Next, following commands must be run from an administrative command prompt:

If the trust between the source and target is an external trust:

- From the source domain:
    - Netdom trust SourceDomain /domain: TargetDomain /quarantine:No /usero: *domainadministratorAcct /passwordo: domainadminpwd*
- From the target domain:
    - Netdom trust TargetDomain /domain: SourceDomain /quarantine:No /usero: *domainadministratorAcct /passwordo: domainadminpwd*

If the trust between the source and target is a forest trust:

- From the source domain:
    - Netdom trust SourceDomain /domain: TargetDomain /enablesIDHistory:Yes /usero: *domainadministratorAcct /passwordo: domainadminpwd*
- From the target domain:
    - Netdom trust TargetDomain /domain: SourceDomain /enablesIDHistory:Yes /usero: *domainadministratorAcct /passwordo: domainadminpwd*

Password Requirements

SMART Directory Sync does not validate the password policies present within your domains. Verify that the password entered as the Default Password complies with the password policy of your target environment. Objects will fail to be created if the password violates that policy.

SMART Directory Sync Requirement for Synchronize Passwords

If planning to use the Password Copy functionality of SMART Directory Sync, PsExec must be installed in the SMART Directory Sync program directory (C:\Program Files\Binary Tree\DirSync). Ignore the PSExec Installation Guide concerning the proper installation location. PsExec is available at: **https://technet.microsoft.com/en-us/sysinternals/bb897553**

About Binary Tree

Binary Tree is a singularly focused global provider of migration software and solutions for Lotus Notes, Microsoft Exchange, Active Directory, and Windows Server environments. Since 1993, Binary Tree has enabled more than 6,000 customers to migrate more than 35 million email users, and facilitated some of the most complex migrations on the planet. Its software solutions are available for migrating from Exchange 2003/2007/2010/2013 and Lotus Notes to on-premises and online versions of Microsoft Exchange, as well as migrations of Active Directory and Windows Server environments. Binary Tree is a Microsoft Gold Messaging Partner, an IBM Advanced Business Partner, and is one of Microsoft's preferred vendors for migrating to Microsoft Office 365. The Company is headquartered outside of New York City with offices in Hong Kong, London, Paris, Stockholm and Sydney. For more information, visit us at www.binarytree.com.

Binary Tree Social Media Resources