BINARY TREE™
Powering Enterprise Transformations™

Directory Sync Pro 5.1

Requirements

March 2017

Table of Contents

Section 1. Introduction

Directory Sync Pro features a new name and logo, but is the same, trusted product previously known as SMART Directory Sync.

This document details the requirements for implementing Binary Tree's Directory Sync Pro. These include the requirements for each of the servers needed to run Directory Sync Pro, as well as any environmental requirements.

If you are planning to use Active Directory Pro, please refer to the Active Directory Pro documentation for additional requirements.

Section 2. Prerequisites

2.1 Supported Environments

The following is a list of supported and unsupported environments. If implementing directory synchronization between Domino and Active Directory, you will need a Binary Tree Domino Server, a Binary Tree Windows Server and an SQL Server database server. If implementing directory synchronization between two Active Directory environments, you will need a Binary Tree Windows Server and an SQL Server database server.

	Supported	Not Supported
Binary Tree Domino Server	Windows Server 2008 R2 64-bit Domino 8.5.3 (32-bit version only) or Domino 9.0.1 (32-bit version only)	64-bit versions of Domino or versions prior to 8.5.3
Binary Tree Windows Server	Windows Server 2008 R2 64-bit, or Windows Server 2012 R2; US English Operating System	All other versions of Windows Server
SQL Server Database	SQL Server can be a new or existing database server in the customer's environment. The following SQL Server versions (English versions) are supported: • SQL Server 2008 R2 • SQL Server 2008 R2 Express with Advanced Services • SQL Server 2012 SP2 • SQL Server 2012 SP2 Express with Advanced Services • SQL Server 2014 • SQL Server 2014 Express with Advanced Services • SQL Server 2016 • SQL Server 2016 Express with Advanced Services	SQL Server 2008 or previous Reporting using SQL Server Reporting Services 2016 or SQL Server Express Reporting Services 2016
Exchange Environment	Exchange 2003, 2007, 2010, 2013, or 2016	Exchange 2000 or previous

Domain	At least one Windows Server 2003 SP2 Domain Controller in Source (if syncing from AD to AD or AD to Domino) and Target (if syncing from AD to AD or Domino to AD)
Domino Environment	Domino 7.x or higher

2.2 Binary Tree Domino Server Requirements

The Binary Tree Domino Server is responsible for the Directory Synchronization processes between Domino and SQL Server.

This server may also be running CMT for Coexistence (CMTC) which handles Free/Busy Look-up, Messaging, Calendaring, and Application Remediation between Domino and Exchange.

- This server should be dedicated to Domino and the Binary Tree solutions only.
- The Binary Tree Domino Server should be a separate server from the Domino Mail servers, and no user mail files should reside on it.
- Any Domino directory that will have entries synched to Active Directory must be replicated to this server.
- Directory Assistance must be configured on this server, with all Domino directories that should be searched for matches and collisions, as well as the AD target directory (Exchange.nsf)

2.3 Binary Tree Windows Server Requirements

- If using Windows Server 2008 R2 64-bit, if the server is also running the Binary Tree Free/Busy service between Domino and Exchange, it must also be running as a standalone IIS 7.0 server with the Web Server (IIS) Role installed. Please refer to the CMT for Coexistence Requirements document.
- .NET 4.5.2 or newer
- IPv4 Only
- The user running the BTDirsync service (full name BinaryTree.Coexistence.Dirsync.Exchange.exe) must have the following rights:
    - Administrator rights to SQL Server with sysadmin role (during installation).
    - Local administrative rights to the Binary Tree Windows server (during installation).
- Exchange cannot be installed on this server.
- The Binary Tree Windows Server must be a dedicated server for the Binary Tree solutions.
- If using the Password Copy functionality of Active Directory Migrator Synchronization, PsExec must be installed in the Directory Sync Pro program directory (C:\Program Files\Binary Tree\DirSync). Ignore the PSTools Installation Guide concerning the proper installation location. PsExec is available at: https://technet.microsoft.com/en-us/sysinternals/bb897553

2.4 SQL Server Database Requirements

- The IP address and either the default SQL port (1433) or an alternate port must be open to all Binary Tree servers.
- The ability to create and modify tables in the Dirsync database on the SQL Server database server.

- It is strongly recommended that the SQL Server database server is dedicated to SQL Server. This server can host other SQL databases, but should serve no other purpose than being a SQL Server database server.
- SQL Server must be configured using Mixed Mode authentication.
- Using the default system administrator SQL Server login account is not recommended. A Directory Sync SQL Server login account should be created. This account must have sysadmin and database owner rights to create the Dirsync database. The sysadmin right can be removed from this account once the install is complete.

2.5 General Requirements

If synchronizing between Domino and Exchange:

- All Lotus Domino Servers need to be at a release level currently supported by IBM/Lotus.
- All Domino entries to be synchronized with Exchange must have valid and unique SMTP addresses in the Domino Directory. This includes people, groups, mail-in databases, and rooms and resources.
- An Organizational Unit (OU) must be created in Active Directory (AD), with which the Domino objects will be synchronized. It is recommended that this directory be a direct subdirectory of the root in Active Directory (AD) to avoid exceeding character length limits in AD.
- At least one end-user workstation with a Lotus Notes Client (version 8.5.3 or higher), and one end-user workstation with a Microsoft Outlook Client (version 2010 or higher) should be available to represent end users. These workstations may run on physical or virtual machines and will be used to validate the end-user experience.
- At least one Microsoft Exchange Server version 2007 or higher with Send and Receive Connectors configured for communication with Domino for message routing between Domino and Exchange.
- All components of Directory Sync Pro are fully functional on physical as well as virtual machines. When setting up Proof of Concept or Pilot environments, Binary Tree fully supports, in fact, recommends the use of virtual machines as a means of lowering the expense of such projects. However, when it comes to production environments, Binary Tree has not yet gathered sufficient information to determine whether virtual environments have the same stability and performance characteristics as physical machines. Because a majority of production environments have been and are deployed on physical machines, Binary Tree advises potential customers of these facts, but defers to them to make the final decision. Binary Tree will provide product support in both physical and virtual environments. However, if either stability or performance issues are found in a virtual environment, Binary Tree may recommend switching to a physical one as a means of issue correction.
- Binary Tree Servers must be connected via a LAN (10MB or higher) connection. A high-speed WAN (5MB or higher) connection may be acceptable, but is not recommended. Where possible, it is recommended to have these servers, as well as Exchange and Domino on the same physical network.

2.6 Exchange Access Requirements

To deploy Directory Sync Pro on the Binary Tree Windows Server, an AD account with Server Administration rights must be able to log on to the server interactively. The account must be able to run programs with Administration-level access on the target Exchange Server and specifically be able to open the Exchange Management Shell (PowerShell).

Binary Tree recommends the following setup for the service account:

Active Directory

- Minimum membership of Domain Users (least privilege) built-in security group
- Read & List Contents rights to "Deleted Objects" container. You may follow these steps if your account is not a Domain Administrator or equivalent (see KB892806):

  Using a domain admin account, open a command prompt and confirm the successful execution of the following commands:

  ```
  dsacls "CN=Deleted Objects,DC=domain,DC=com" /takeownership
  dsacls "CN=Deleted Objects,DC=domain,DC=com" /g Domain\ServiceAccount:LCRP
  ```

- Full Control rights to destination OU in Active Directory

Exchange

- Administrative rights to Exchange

SQL Server

- Create a new login in the SQL Server Management Studio. In Server Roles, grant public and sysadmin rights (you may remove these rights after the **database** has been created). In User Mapping, select the Dirsync database and grant public and database owner rights.

Binary Tree Windows Server

- Member of local administrators group

2.7 Domino Access Requirements

- For program installation and restarts, if necessary, an AD account with remote logon and server administration rights to Windows Servers on which the Domino Servers reside.
- For the modification of the routing scheme in Domino, a Lotus Notes ID with a minimum of Editor rights to the Domino Directory is required. In addition, the ID must at a minimum have the following roles assigned:
  - NetCreator
  - NetModifier
  - ServerCreator
  - ServerModifier
- A Notes ID with greater administration rights is preferred for modification of the Domino routing scheme.

2.8 SID History and Password Synchronization Requirements

SID History Synchronization Requirements

Microsoft requires an administrative account in the source domain.

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.

SID History intra-forest migration is supported (with SMART AD Migrator 9.0.2.0) with the use of an out-of-the-box script available from Binary Tree.

The source and target domains must not have the same NETBIOS name to allow the required trust between the two environments.

Communication between a Source PDC and the configured Target GC is required for SID History Migration to successfully complete. Please note, there are additional ports that must be open between the Source PDC and the configured Target GC as defined in Section 3. Advanced Network Requirement's (Directory Sync Pro Profile with SID History Synchronization selected) of this document.

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

In order to receive the maximum benefit a trust should be in place. 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*

Domain Controller Access

If SID History will be synchronized, any Domain Controller listed in the Target DCs tab within a Directory Sync Pro profile will require access to the Domain Controller holding the PDC Emulator Active Directory FSMO role in the source. Keep in mind that even if the Domain Controller holding the PDC Emulator Active Directory FSMO role is not listed in the Source DCs tab, any SID History migration attempts will require a DC in the target to communicate with the PDC Emulator domain controller. For this reason, it is a best practice to ensure that all Domain Controllers specified in the Target DCs tab within a Directory Sync Pro profile has the appropriate networks access to communicate with the source Domain Controller holding the PDC Emulator Active Directory FSMO role before a SID History migration is attempted.

2.9 Password Requirements

Directory Sync Pro 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.

Section 3. Advanced Network Requirements

Directory Sync Pro to SQL Server Access

Source	Target	Ports	Protocol
Directory Sync Pro	SQL Server holding the primary database	1433	TCP & UDP
Directory Sync Pro	SQL Server holding the logging database	1433	TCP & UDP

Directory Sync Pro Profile Specific Scenario Requirements

Directory Sync Pro Match Only or Update Only Profile (no object creation)

Source	Target	Ports	Protocol
Directory Sync Pro	Source Domain controllers	389, 445*, 3268	TCP (all) UDP (389)
Directory Sync Pro	Target Domain controllers	389, 445, 3268	TCP (all) UDP (389)

* Port 445 only needs to be open to the Source Domain Controller during Directory Sync Pro Profile creation

Directory Sync Pro Profile with Create Only or Create/Update Matching Option

Source	Target	Ports	Protocol
Directory Sync Pro	Source Domain controllers	389, 445*, 3268	TCP (all) UDP (389)
Directory Sync Pro	Target Domain controllers	139, 389, 445, 3268	TCP (all) UDP (389)

* Port 445 only needs to be open to the Source Domain Controller during Directory Sync Pro Profile creation

Directory Sync Pro Profile with Synchronize Passwords selected

Source	Target	Ports	Protocol
Directory Sync Pro	Source or Target Domain controllers	139, 389, 445, 3268	TCP (all) UDP (389)

Directory Sync Pro Profile with SID History Synchronization selected

Source	Target	Ports	Protocol
Directory Sync Pro	Source or Target Domain controllers running Windows 2008 or newer	135, 137, 139, 389, 445, 3268 and 49152-65535	TCP (all) UDP (389)
Directory Sync Pro	Source or Target Domain controllers running Windows 2003	135, 137, 139, 389, 445, 3268 and 1024-5000	TCP (all) UDP (389)
Target GC	Source PDC	135, 138, 389, 445, 1027	TCP (all)

About Binary Tree

At Binary Tree, we power enterprise transformations. Our award-winning software and services help Enterprise businesses modernize their Microsoft email, directories and applications by moving and integrating them to the cloud. Binary Tree mitigates the risk of delays, downtime, and budget overruns for complex transformation projects for large organizations. We understand Enterprise migration requirements that go well beyond the needs of small companies. Since 1993, we've transformed more than 7,000 global clients and 40 million users, including 6 million to Office 365. Our business first approach helps plan, move and manage the transformation process from end-to-end. So, clients stay focused on their core business while our experts deliver a low-risk, successful IT transformation.

Binary Tree is a Microsoft Gold Partner and a globally preferred vendor for Offices 365. Our headquarters are located outside of New York City with global offices in the United Kingdom, France, Germany, Sweden and Singapore. For more, visit us at www.binarytree.com.

Binary Tree Social Media Resources