

Using Microsoft Active Directory

with

FlashNAS ZFS

Table of Contents

Product Models Covered by This Document	3
FlashNAS ZFS Family of Unified Storage Systems	4
Using Microsoft Active Directory (AD) with FlashNAS ZFS Systems in	
Windows Server	5
Step 1: Preparing the Environment	6
Step 2: Verifying AD Server DNS	8
Step 3: Configuring AD User Account Settings for Import into FlashNAS	16
Step 4: Adding AD server to FlashNAS	17
Step 5: Importing Users from AD Server	20
Step 6: Allowing Users to Access Folders	
Appendix	23
FlashNAS System Recovery Procedure	23
Troubleshooting	23

Product Models Covered by This Document

This document applies to the following product models:

- FlashNAS ZX2U12 Series
- FlashNAS ZX3U16 Series
- FlashNAS Desktop Series

For more information about compression, virtualization, snapshot, remote replication, ZFS, backup, storage, network-attached-storage, file-sharing and WORM (Write Once, Read Many), please visit <u>www.winsys.com</u>

FlashNAS Family of Unified Storage Systems

IT environments often feature multiple types of storage infrastructures to accommodate various types of data and achieve different service levels. The scattered boxes for DAS (Direct-Attached Storage), SAN (Storage Area Network) and NAS (Network-Attached Storage) configurations lead to poor utilization and complicated management.

Winchester Systems FlashNAS simultaneously serves file and block-based applications with a unified storage platform, and features easy management, optimized resource utilization, high availability, flexible scalability and competitive price/performance. In addition, FlashNAS offers a comprehensive set of advanced software features at no additional costs. FlashNAS systems help businesses effectively meet diverse and changing data demand while staying within budget.



4

Using Microsoft Active Directory (AD) with FlashNAS ZFS Systems in Windows Server

Microsoft Active Directory (AD) in Windows Server environments is a directory service designed for data management and resource distribution on network environments. Microsoft AD allows storing and sharing data, configuring storage parameters, and managing account information from a central location.

Using Microsoft AD with FlashNAS systems offers the following benefits:

• Simplified account management

The same Microsoft AD account name and password can be used for FlashNAS; there is no need to manage separate sets of account information.

Consolidated access control

Read/write rights to shared directories on the network can be controlled from the FlashNAS.

• Enhanced security

FlashNAS can also benefit from the enhanced data protection protocol integrated in Microsoft AD.

The FlashNAS systems are compatible with Microsoft AD for the following versions of Windows OS:

- Windows Server 2003, 2003 R2
- Windows Server 2008, 2008 R2
- Windows Server 2012

1.1 Confirm the FlashNAS software version.

The procedure described in this application note is applicable to software version 1.2.46 or later. To check the software version follow these steps:





Check the software version in the Currently Installed Software Package corner.

(if the software version is not at an acceptable level, please contact Winchester Systems support)

1.2 Take a FlashNAS system snapshot.

This snapshot image will be of use in case errors are encountered during the user import.

Go to Maintenance > System > Backup System Setting.

Maintenance System Backup System Setting				
status Configuration	Backup/Restore Settings			
E Storage	Backup System Settings			
± 🥪 Folder ∃ 🔒 Account	Save basic system settings, including network configurations and user accounts, to a local file			
🗄 🧕 Backup				
🗆 💥 Maintenance				
C III Pustam				
System				
Software Update				
System Software Update Backup System Setting				
System System Software Update Backup System Setting Dower Schedule				
Software Update Software Update Backup System Setting Power Schedule	Restore System Settings			

Click on *Backup*. When prompted, save the backup file to a location of your choice.



In the event this system backup has to be used (system recovery), this recovery will require a short amount of downtime in the form of a FlashNAS system reboot. Make sure to properly plan this recovery so that the reboot downtime does not interfere with business applications.

<u>1.3</u> The FlashNAS and AD server should be synchronized with a time difference of no more than 5 minutes. To check the date/time settings of the FlashNAS, go to *Configuration* > *System* > *Date/Time*.

Configuration System Date/Time		
Status Configuration	Date/Time	ne / NTP Servers
Service System	Adjust the date an	d time to your local environment or synchronize
Host Settings	Date/Time	
Admin Password	Date	2015-03-02
Certificates	Time	13:08:47
 	Timezone	e.g. 17:00:00 (GMT-05:00) America/New_York
≆ 🧐 Storage ≇ 🥧 Folder	Daylight Sav	ving Time Settings
Account Backup Maintenance		

1.4 Conduct a Test Run

Prepare a test AD server to conduct a practice run before doing the configurations on the operational AD server. In this way, users can ensure that the configurations highlighted in this document work in their specific environments and avoid any damage from unexpected errors that may occur when doing these configurations for the first time.

- This AD server should include all user accounts.
- This AD server will be the target server for FlashNAS.

Step 2: Verifying AD Server DNS

2.1 Open DNS Manager.

(Windows Server 2003/2008) Go to Start > Administrative Tools > DNS.



(Windows Server 2012) Open DNS Manager by going to Tools > DNS.



<u>2.2</u> Check the forward lookup zone.

The DNS Manager will appear. Locate the DNS server and expand the tree in the sidebar.



Check the AD server IP settings in the *Forward Lookup Zones*. In this example, the IP address is *172.18.4.164*.

🛓 DNS Manager				
File Action View Help				
🗇 🔿 🞽 🖬 🗐 🙆 😹 🚺				
	Name	Туре	Data	Timestamp
Global Logs	iii _msacs			
Forward Lookup Zones	🚊 _tcp			
	🚞 _udp			
E Everse Lookup Zones	DomainDnsZones			
📋 4. 18. 172. in-addr. arpa	(same as parent folder)	Start of Authority (SOA)	[62], win-uehnbcsvhe2.test	static
+ Conditional Forwarders	same as parent folder)	Name Server (NS)	win-uehnbcsvhe2.test.com.	static
	(same as parent folder)	Host (A)	172.18.4.164	2012/7/3 上午 11:00:00
	win-uehnbcsvhe2	Host (A)	172.18.4.164	static

- Start of Authority (SOA): Make sure this item is included in the list.
- Name Server (NS): Make sure this item is included in the list.
- Host (A): The IP address must match that of the AD server.

2.3 Add a reverse lookup zone.

Add a zone in *Reverse Lookup Zones* by right-clicking and selecting *New Zone*, as shown below.



The New Zone Wizard will appear. Click Next to proceed.

New Zone Wizard		X
	Welcome to the New Zone Wizard This wizard helps you create a new zone for your DNS server. A zone translates DNS names to related data, such as IP addresses or network services. To continue, dick Next.	
	< Back Next > Cance	

Select the following options and click Next:

- Primary zone
- Store the zone in Active Directory

Zone Th	Type ne DNS server supports various types of zones and storage.
Se	lect the type of zone you want to create:
•	Primary zone Creates a copy of a zone that can be updated directly on this server.
C	Secondary zone Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
C	Stub zone Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.
	Store the zone in Active Directory (available only if DNS server is a writeable domain

Select the following option and click Next.

• To all domain controllers in this domain

/ Zone Wizard		
Active Directory Zone Replication So	ope	
Tou can select now you want bits date	a replicated all bughout your network.	
Select how you want zone data replica	ated:	
C To all DNS servers running on doma	ain controllers in this forest: test.com	
C To all DNS servers running on doma	ain controllers in this domain: test.com	
		-
To all domain controllers in this dom	nain (for Windows 2000 compatibility): test.	.com
C To all domain controllers specified i	n the scope of this directory partition:	
		X
1		
	(Bal) News	Connel
	< Back Next >	Cancel

(For Windows Server 2008/2012) Select the following option and click Next:

• IPv4 Reverse Lookup Zone

New Zone Wizard	×
Reverse Lookup Zone Name A reverse lookup zone translates IP addresses into DNS names	s.
Choose whether you want to create a reverse lookup zone for addresses.	IPv4 addresses or IPv6
IPv4 Reverse Lookup Zone	
O IPv6 Reverse Lookup Zone	
< Back	Next > Cancel

Enter the first three portions of the server's IP address as the Network ID and click *Next*.

101	identify the reverse lookup zone, type the network ID or the name of the zone.
•	Network ID: AD server's IP:172.18.4.164(Example)
	172 .18 .4 . =>Network ID:172.18.4
	In enetwork ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order. If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.in-addr.arpa.
C	Reverse lookup zone name:

Select the following option and click Next:

• Allow only secure dynamic updates

New Zon	e Wizard	×
Dyna Yr uj	amic Update You can specify that this DNS zone accepts secure, nonsecure, or no dynamic pdates.	
D' re Se	ynamic updates enable DNS dient computers to register and dynamically updat esource records with a DNS server whenever changes occur. elect the type of dynamic updates you want to allow:	e their
G	 Allow only secure dynamic updates (recommended for Active Directory) This option is available only for Active Directory-integrated zones.]
c	 Allow both nonsecure and secure dynamic updates Dynamic updates of resource records are accepted from any dient. This option is a significant security vulnerability because updates can b accepted from untrusted sources. Do not allow dynamic updates Dynamic updates of resource records are not accepted by this zone. You must these records manually. 	e st update
	< Back Next >	Cancel

The reverse lookup zone will appear in the DNS Manager. Confirm the settings on the screen.

Using Microsoft Active Directory with FlashNAS ZFS

DNS Manager File Action View Help Image: State				
	Name	Type	Data	Timestamp
 WIN-UE-INBCSVHE2 ♥ [ii] Global Logs ♥ Forward Lookup Zones ♥ [ii] _msdcs.test.com ♥ [ii] test.com 	(same as parent folder)	Start of Authority (SOA) Name Server (NS)	[8], win-uehnbcsvhe2.test win-uehnbcsvhe2.test.com.	static static

- Start of Authority (SOA): Make sure this item is included in the list.
- Name Server (NS): Make sure this item is included in the list.

<u>2.4</u> Create a host record in the reverse lookup zone.

Right-click on the newly created reverse lookup zone and select *Other New Records*.



Select the following option and click Create Record:

- Host (A or AAAA): Windows Server 2008/2012
- Host (A): Windows Server 2003

source Record Type		×
elect a resource record type	2:	
AFS Database (AFSDB)		
Alias (CNAME)		
ATM Address (ATMA)		
DHCID		
Domain Alias (DNAME)		
Host (A or AAAA)		
escription:		
32-bit IP version 4 address address (RFC 1886).	(RFC 1035) or a 128-bit IP version 6	
		P

Enter the IP address of the AD server and check "Update associated pointer (PTR) record." Click OK.



Restart the AD server, and then check that the reverse lookup zone setting has been updated.

🍰 DNS Manager				
File Action View Help				
🗢 🔿 📶 🔚 🖬 🖄 📾				
DNS	Name	Туре	Data	Timestamp
 WIN-UEHNBCSVHE2 Image: Global Logs Forward Lookup Zones Forward Lookup Zones Image: Structure Structure Image: Struct	(same as parent folder) (same as parent folder) (same as parent folder) 172.18.4.164	Start of Authority (SOA) Name Server (NS) Host (A) Pointer (PTR)	 [13], win-uehnbcsvhe2.test win-uehnbcsvhe2.test.com. 172.18.4.164 4.18.172.in-addr.arpa. 	static static static static

- Start of Authority (SOA): Make sure this item is included in the list.
- Name Server (NS): Make sure this item is included in the list.
- Host (A): The IP address must match that of the AD server.
- Pointer (PTR): The Data column should show the IP address of the AD server.

Make sure that the AD user accounts meet the following criteria:

• AD user logon name needs to be the same as the full name.

New Object - User		×
Create in:	nas-test.ad/Users	
<u>F</u> irst name:	Bart <u>I</u> nitials: YH	
Last name:	Hsiao	
Full n <u>a</u> me:	Bart YH. Hsiao	
<u>U</u> ser logon name: Bart YH, Hsiao	@nas-test.ad	
User logon name (pre- NAS-TEST\	Windows 2000): Bart YH, Hsiao	
J		
	< Back Next > Cancel	

 The user logon name can not include the following invalid characters: \[]:;|=,+*?<>@"
 Using Microsoft Active Directory with FlashNAS ZFS Step 4: Adding AD server to FlashNAS

<u>4.1</u> In the FlashNAS GUI, go to *Configuration* > *Network* > *DNS* and click on *Add* in the DNS Server section. Enter the Windows AD server's IP address and click on *OK*.

d New DNS Server	
DNS Server Address	172.18.4.164 e.g. 172.16.80.5
	OK Cance

Confirm that the DNS server has been added.

Status Configuration	DNS
E Service	DNS Server
🗉 🔛 System	The DNS server translates
🖃 🚅 Network 🖏 Basic Settings	DNS Server
DNS DNS	172.18.4.164
Pouting Interpretation in the second sec	

4.2 Go to Configuration > Service > Share and make sure that the CIFS service

has been enabled (Online). If it has been disabled, click the 😃 icon to enable it.

Status Gonfiguration	Share	
E Service	File Sharing Protocols	
Share Understand	Activate and configure file service pr Linux (NFS).	rotocols to provide shared access to y
Miscellaneous	Service Name	Status
E System	CIFS	😑 Online
Basic Settings	FTP	🖯 Disabled
DNS DNS	NFS	🖯 Disabled
💣 Routing	AFP	🖯 Disabled
Trunking	ISCSI	O Disabled

<u>4.3</u> Go to *Configuration > Service > Directory*, select the LDAP service and click on *Edit*. Configure the settings and click *OK* after finishing the settings.

Status	Directory	
E Service	Directory Protocols	
B Share	Activate and configure directory protocols to edit directories and sys	stem configuratio
Directory	Service Name Status	
E System	LDAP O Disable	ed
🖃 🚅 Network	NIS O Disable	ed
Basic Settings	LDAP Client Settings	×
 Pouting Trunking Jumbo Frame Peripheral Notification 	LDAP Server IP Address 172.18.4.164 Domain Name LDAP Server Port 389 Proxy Username Administrator	
 Storage Folder Account Backup 	Proxy User Password	Cancel

- LDAP Server IP Address / Domain Name: Enter either the IP address or the domain name of the AD server to specify it. Example: (IP Address) 172.18.4.164 (Domain Name): test.com
- LDAP Server Port: Specifies the server port. This parameter will be assigned automatically according to the IP address.
- Proxy Username: Enter the AD server admin username.
- Proxy User Password: Enter the AD server admin password.

When LDAP configuration is successful, the AD has been added to the FlashNAS system.



The LDAP service has been configured. Joining the domain has been completed.

<u>4.4</u> Go to *Configuration* > *Network* > *DNS* to check the DNS Suffix setting and confirm the Windows domain name. It should appear automatically if the LDAP configuration has been done correctly.



<u>4.5</u> Go to *Configuration* > *Service* > *Share* to check CIFS settings and confirm the Windows domain name. It should appear automatically if the LDAP configuration has been done correctly.



Go to *Account* > *User* and click on *Import*.

Account User					Welcome admin	🛃 Logout	🔒 Links 🔻
Status Configuration Storage Folder Account	User Accounts User Accounts Create user accounts for accessing shared volumes or files with unique usernames and passwords. Configure their access rights: read/write or read only.						
User ∰ Group ∰ Backup ☆ Maintenance	Name ✓ Page 0 ▼ / Tot	Home Directory ↓ al 0 Pages Total 0 User(Type 💌 S)	Group 🗸	Quota 🗸	Description Delete	on v Import

Ensure the AD users are imported from the AD server.

1005	/home/1005	LdapUser	10000	none
1006	/home/1006	LdapUser	10000	none
1007	/home/1007	LdapUser	10000	none
1008	/home/1008	LdapUser	10000	none
1009	/home/1009	LdapUser	10000	none
101	/home/101	LdapUser	10000	none
1010	/home/1010	LdapUser	10000	none
1011	/home/1011	LdapUser	10000	none
1012	/home/1012	LdapUser	10000	none
1013	/home/1013	LdapUser	10000	none
1014	/home/1014	LdapUser	10000	none
1015	/home/1015	LdapUser	10000	none
1016	/home/1016	LdapUser	10000	none
1017	/home/1017	LdapUser	10000	none
1018	/home/1018	LdapUser	10000	none
1019	/home/1019	LdapUser	10000	none
102	/home/102	LdapUser	10000	none
1020	/home/1020	LdapUser	10000	none
1021	/home/1021	LdapUser	10000	none
The 1	💌 page / Total 145 pages	Total 30 records	0	

Step 6: Allowing Users to Access Folders

<u>6.1</u> Go to *Explorer* in the FlashNAS GUI and select the folder to be shared. Click on *Share*.

lume/Folder/File Managem	ent				
ld, delete, or upload files the	rough this explorer window. Use	the sidebar to expand the volu	me/file hierarchy.		
FlashNAS_6	/Pool-1	888			
Pool-1	Name	Available	Used	Туре	Last Update
disshare	UserHome	377GB	43.4KB	filesystem	2012-02-07 10:09
	Cfsshare	377GB	43.4KB	filesystem	2012-02-08 10:41
п.					

<u>6.2</u> Add users that will have permission to access this folder by clicking on *Add*. Make sure that the CIFS/FTP/SFTP share protocol has been checked.

Folder Path /	Pool-1/test2			
Share Name t	est2			
Description				
Access F	lights			
🕵 everyone		Access	Allow	Forbid
		Full Control	~	
		Modify	~	
		Read and Execute	~	
		List folder contents	•	
		Read	~	
		Write	~	
Add	Delete			
Share				
CIFS/FTF	/SFTP			
□ NFS			5	etting
AFP				

<u>6.3</u> To add users and/or groups, move them to the right-side boxes using the arrow signs.

Available Users	Select All		Added Users	Select All
S guest			‰test	
8 Administrator			🏡 krbtgt	
Suest		>		
		<		
Available Groups	Select All		Available Groups	- Select All
Allowed RODC Password Rep Group	lication			
Cert Publishers				
Certificate Service DCOM Acce	ss			
Cloneable Domain Controllers	;	<		
Scryptographic Operators	~			
<	>			

<u>6.4</u> After configuring the share settings, click *OK* button to apply the modifications.

Informati	ion	×
	The sharing settings have been configured.	
	ОК	

<u>6.5</u> After that, go back to Windows Server and verify whether the share folder access rights are the same as on the FlashNAS system. To do so, find the relevant network disk, right-click and select *Properties*. The share folder access settings can be found in the *Security* tab.

Appendix

FlashNAS System Recovery Procedure

If the system encounters errors during import, recover (rollback) the system as follows using the system snapshot image mentioned above.

Go to *Maintenance* > *System* > *Backup System Setting*. Select the restore image for recovery and click on *restore*.

WINCHESTERSYSTEMS* Purpose-Built Strage		Background Job	e. Alert	Pala Shortcut	Explorer	di Home
Maintenance System Backup System	Setting		_	2015-03-02 15:44:11	Welcome admin ¥	Links
Generation	Backup/Restore Settings					?
E Storage	Backup System Settings					
E 😏 Folder	Save basic system settings, including network configurations and user accounts, to a local file.					
🗉 🚑 Backup						sackup
Maintenance Maintenance System Software Update Backup System Setting Power Schedule						
📴 Diagnostic Report	Restore System Settings					
😡 High Availability 🏭 Log	Reators system configurations from a previously saved sating like					
						testore

Troubleshooting

If joining Windows AD fails after configuring everything, check the following items again to make sure the configurations are correct.

• FlashNAS DNS Server IP Address

It should be the same as the Windows AD server's IP address.

• The Time Difference between FlashNAS and Windows AD Server It should be less than 5 minutes.