Dell EMC SC Series and Active Directory Integration

Dell EMC Engineering
December 2017

A Dell EMC Best Practices Guide

Revisions

Date	Description
January 2013	Initial release
January 2017	Updated for new features and DSM
December 2017	Updated to reflect current branding

Acknowledgements

Author: Marty Glaser, Midrange Storage Technical Solutions

Table of contents

1 Introduction

Organizations of all sizes can benefit from consolidating user management and authentication into services such as Microsoft® Active Directory® (AD). The Active Directory service allows organizations to efficiently organize, manage, and control resources. Active Directory is a distributed, scalable database managed by Windows Server® domain controllers.

Dell EMC SC Series Active Directory integration provides a scalable solution for authentication that enables administrators to manage a potentially large number of accounts across many SC Series arrays from a central location. In addition, SC Series Active Directory integration simplifies account management for administrators by enabling them to leverage their existing native Active Directory infrastructure.

1.1 Audience

This document is for technology professionals who desire to learn more about how to manage SC Series user accounts with Active Directory.

1.2 Prerequisites

Understanding the material in this document requires advanced working knowledge of the following:

- Microsoft Windows Server
- Active Directory
- SC Series storage
- Operation of Dell Storage Manager (DSM) software

2 Introduction to SC Series Active Directory integration

2.1 Overview

Dell EMC Storage introduced Active Directory integration with the release of Storage Center Operating System (SCOS) 6.3.1. Since the initial release, improvements such as single sign on and automatic discovery make configuring and managing SC Series Active Directory integration seamless and intuitive.

Note: Active Directory integration is available on both the DSM Data Collector and SC Series arrays. However, AD integration on the Data Collector only applies to the Data Collector itself, and does not apply to any SC Series arrays managed by the Data Collector.

In environments with more than one SC Series array, enable AD integration individually on each array.

2.2 Authentication method

SC Series AD integration requires Kerberos v5 authentication. NTLMv2 authentication is not supported.

2.3 Single sign-on

The DSM client supports single sign-on (SSO) when connecting to a DSM Data Collector configured to use Active Directory integration, or when connecting directly to an SC Series array configured to use Active Directory integration. Prior to using SSO, the Active Directory user must be granted rights to the DSM Data Collector or SC Series array.

2.4 Active Directory functional levels

SC Series AD integration supports Windows 2016, 2012, 2008 R2, 2008, and 2003 R2 Active Directory functional levels, and will function in environments with domain controllers running a combination of any of the aforementioned server operating systems. The functional level of a domain or forest controls which advanced features are available in the domain or forest.

Note: The functional level of a domain or forest is determined by the domain controller running the oldest version of Windows Server in the domain or forest. For example, a configuration with Windows Server 2012 and a Windows Server 2008 R2 domain controller would run at a 2008 functional level. If possible, it is recommended to run at the latest functional level.

2.5 Read-only domain controllers (RODC)

SC Series AD integration supports the use of a combination of traditional domain controllers and read-only domain controllers for authentication.

2.6 Trusts and child domains

SC Series AD integration allows for the joining of SC Series storage to one AD domain. When joined to the domain, the SC Series array can authenticate users and groups in the local domain, as well as users and groups from child and trusted domains. A two-way transitive trust must exist between the local forest and any external forests in order for the SC Series array to authenticate trusted users. For more information about Active Directory trusts, refer to the Microsoft TechNet article, Understanding Trust Types.

For detailed information about configuring SC Series AD integration with child domains and forest trusts, see section 4.

3 Prerequisites

SC Series AD integration requires Active Directory Domain Services (AD DS) to be running and properly configured. As with any AD installation, the Domain Name System (DNS) must be running in a healthy state, and properly configured.

3.1 DNS/domain settings

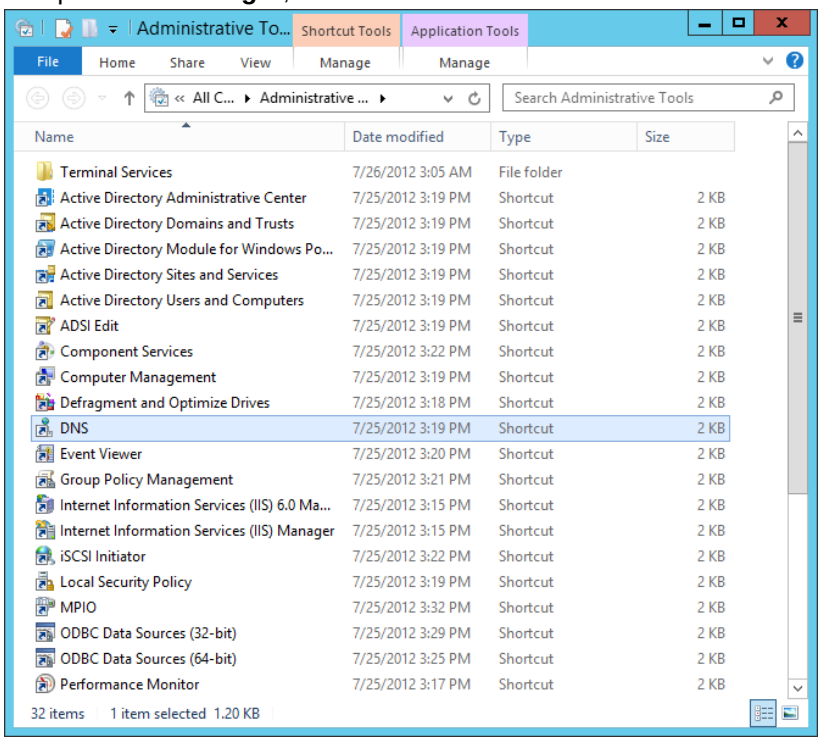
SC Series AD integration is heavily dependent upon a properly configured DNS environment. SC Series arrays and the domain controller(s) must be able to communicate with each other using fully qualified domain names (FQDN). In order to facilitate communication through FQDN between the SC Series array and the domain controller(s), a Host (A) record as well as a Pointer (PTR) record must exist for each SC Series array in DNS. In addition, SC Series AD integration automatic discovery uses service records (SRV records) to discover domain controllers and settings.

For more information about DNS records, refer to the Microsoft TechNet article, Domain Name System.

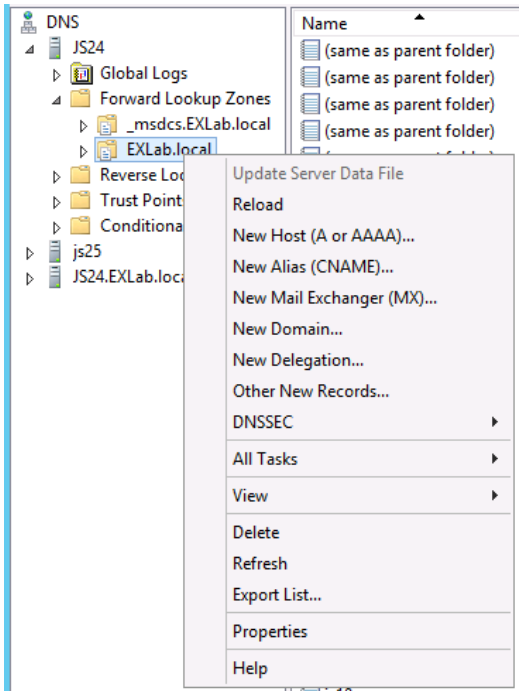
3.1.1 Create a Host (A) record

To create a Host (A) record for an SC Series array on Windows Server 2012 or above, perform the following steps:

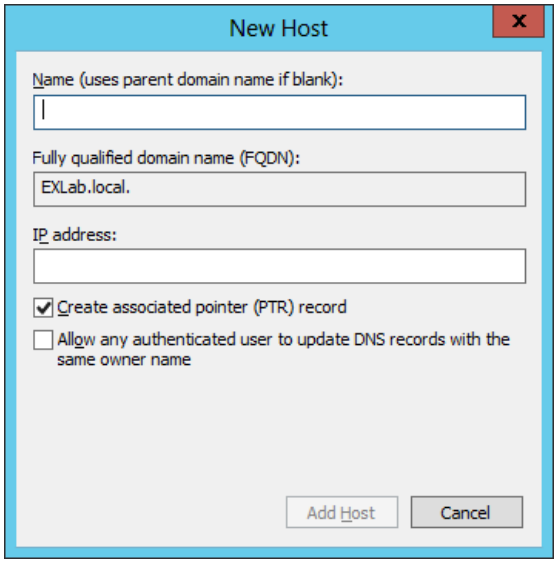
1. Open a console session to the primary DNS server. Log in as **Administrator**.
2. To open **DNS Manager**, at the start screen click **Administrative Tools** > **DNS**.



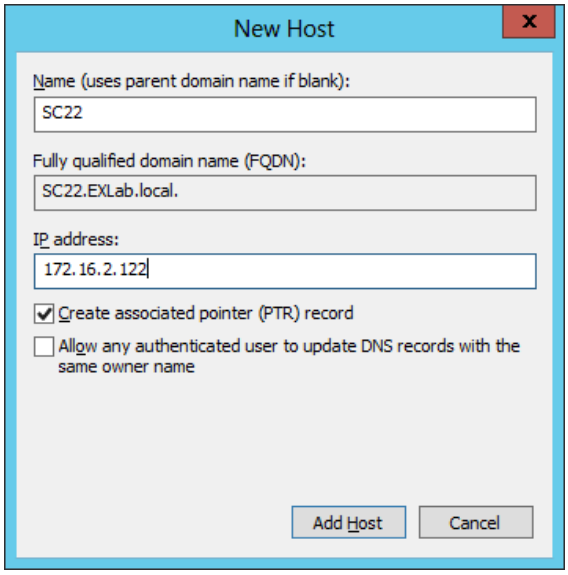
3. In DNS Manager, expand the domain controller, expand **Forward Lookup Zones**, right-click the domain, and select **New Host (A or AAAA)**.



4. The **New Host** window appears:

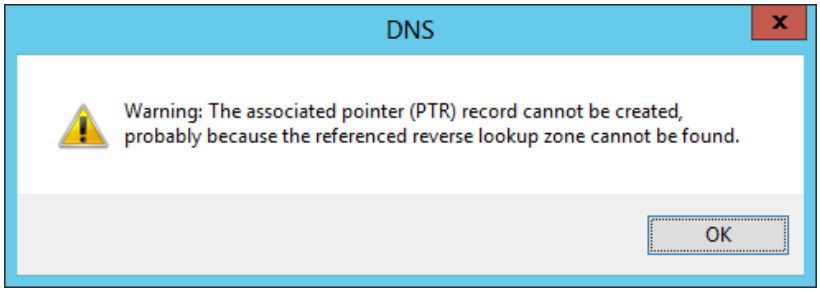


5. Enter the name of the SC Series array in the **Name** field, and provide the IP address of the SC Series array. For a single-controller SC Series array, enter the controller IP address. For a dual-controller SC Series array, enter the management IP address. Leave the **Create associated pointer (PTR) record** box checked. Click **Add Host**.

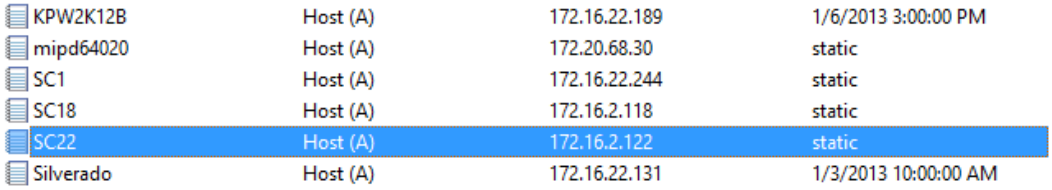


Note: Creating a pointer (PTR) record will fail if a reverse lookup zone has not been configured for the subnet where the SC Series array resides. Click **OK** to close the error message and continue creating the Host (A) record.

To create a reverse lookup zone and PTR record, refer to section 3.1.2 of this document.



6. Once the Host (A) record is created, verify that it is listed in the DNS Manager.



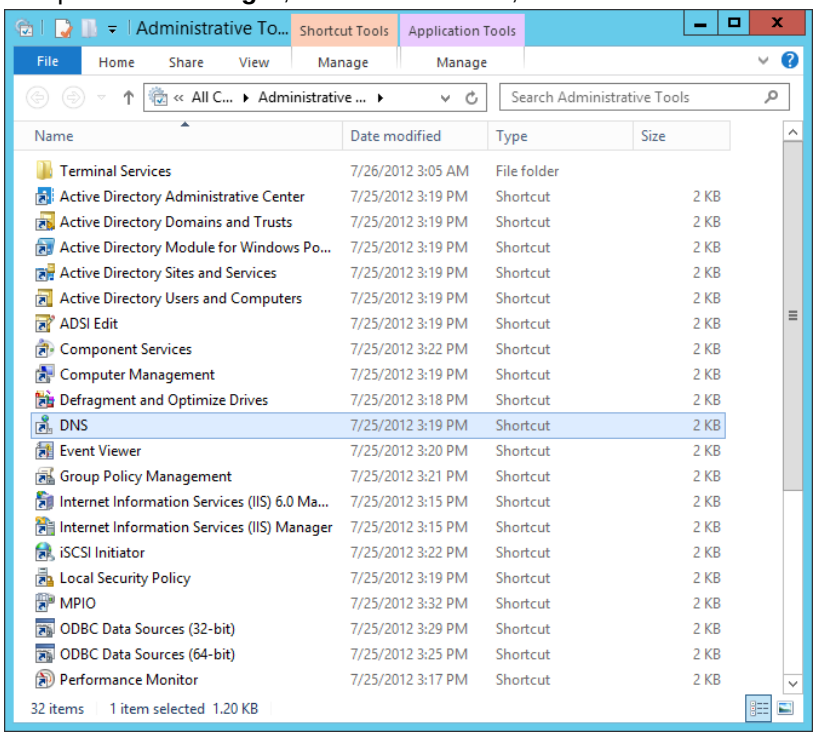
3.1.2 Reverse lookup zones and PTR records

A reverse lookup zone enables clients to use a known IP address during a name query and look up a computer name based on its address. PTR records map an IP to a hostname, whereas a host record maps a hostname to an IP. Reverse lookup zones are independent of the DNS installation and need to be manually created.

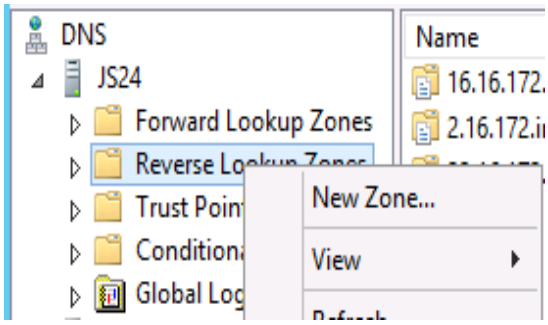
Note: Without host and PTR records for the SC Series array, the domain join operation will fail while configuring SC Series AD integration.

To create a reverse lookup zone:

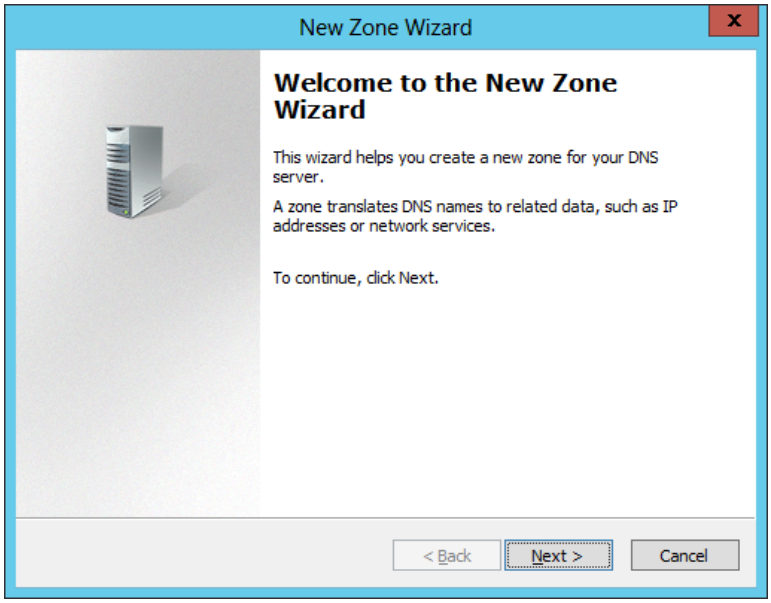
1. Open a console session to the primary DNS server. Log in as **Administrator**.
2. To open **DNS Manager**, at the start screen, click **Administrative Tools** > **DNS**.



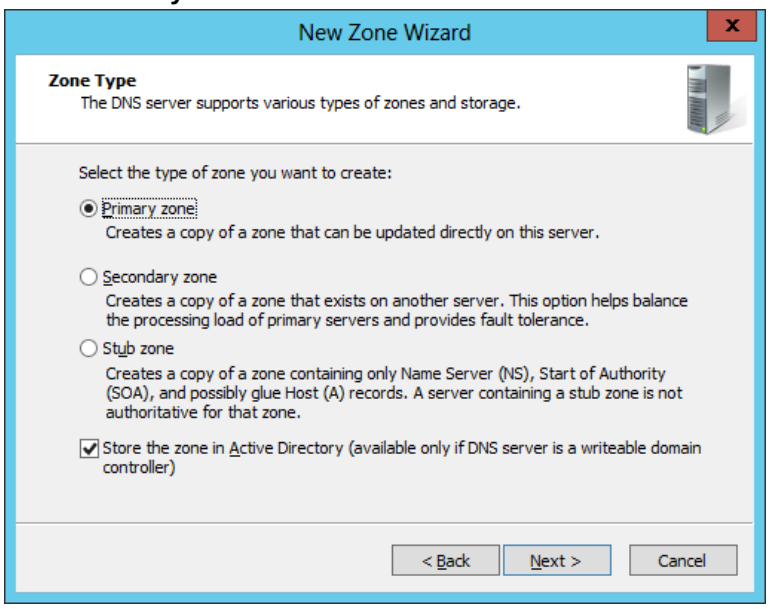
3. In DNS Manager, expand the domain controller, right-click **Reverse Lookup Zones** and select **New Zone**.



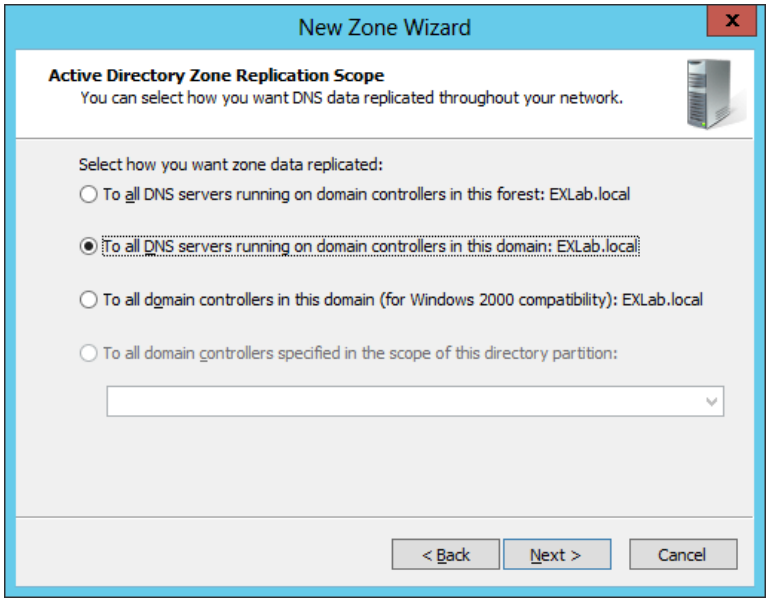
4. The **New Zone Wizard** window appears. Click **Next**.



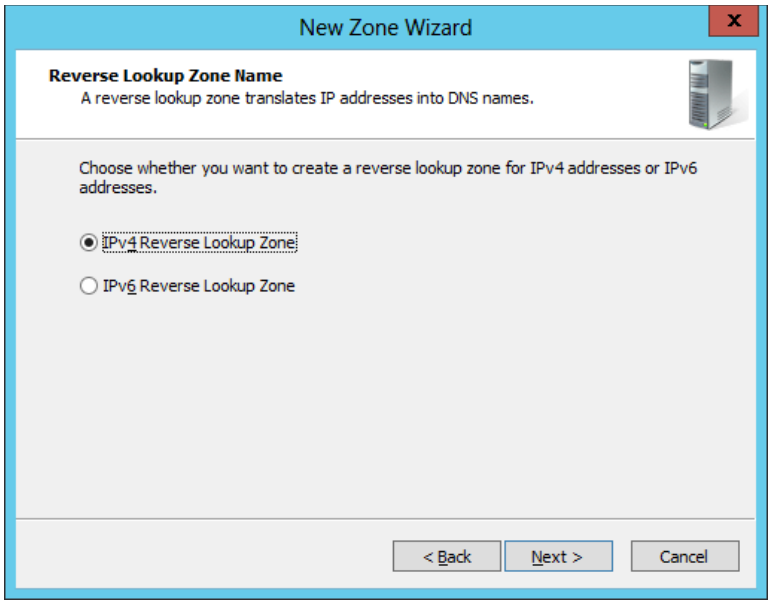
5. Select **Primary zone**. Click **Next**.



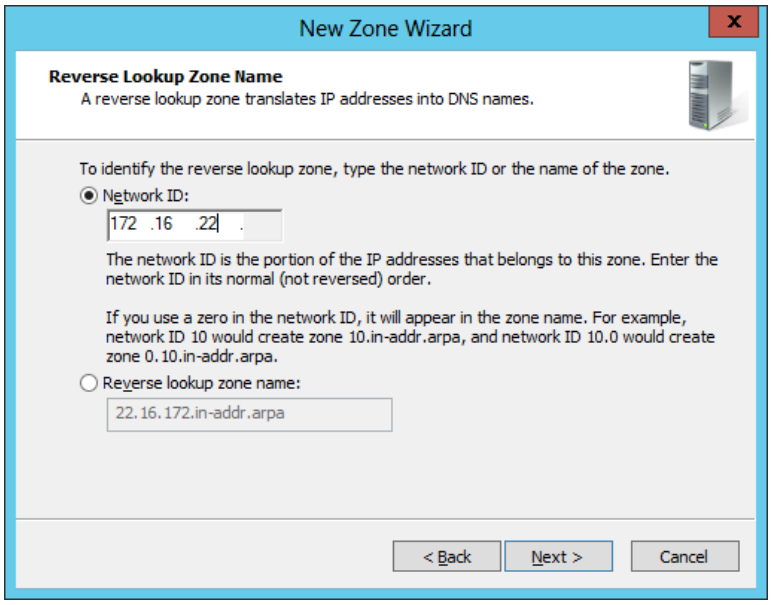
6. Select the zone replication scope. Click **Next**.



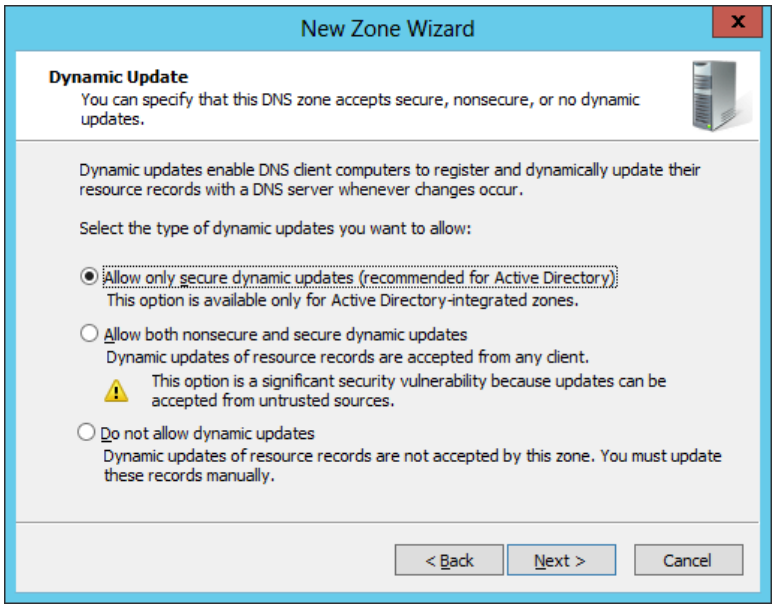
7. Select IPv4 Reverse Lookup Zone. Click Next.



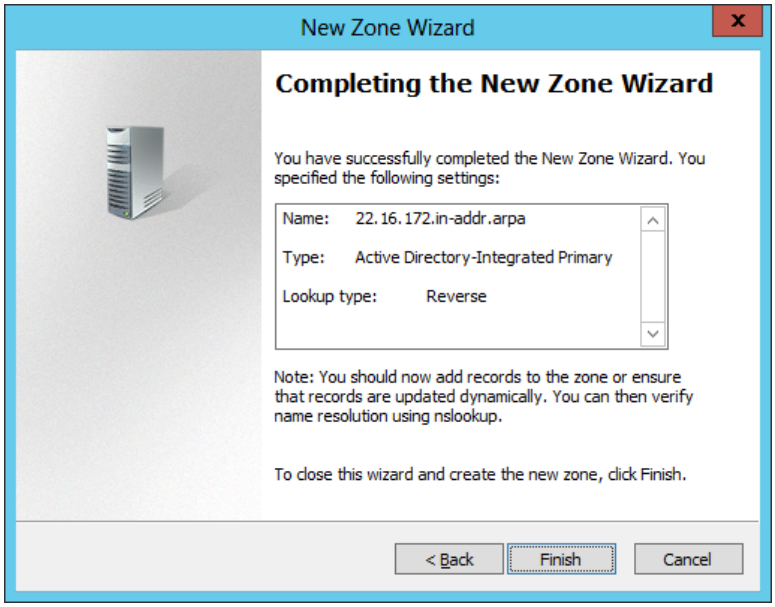
8. Enter the first three octets of the IP address for the SC Series array. For example, if the IP address is 172.16.22.122, enter 172.16.22. Click **Next**.



9. Select the dynamic update type. Click **Next**.



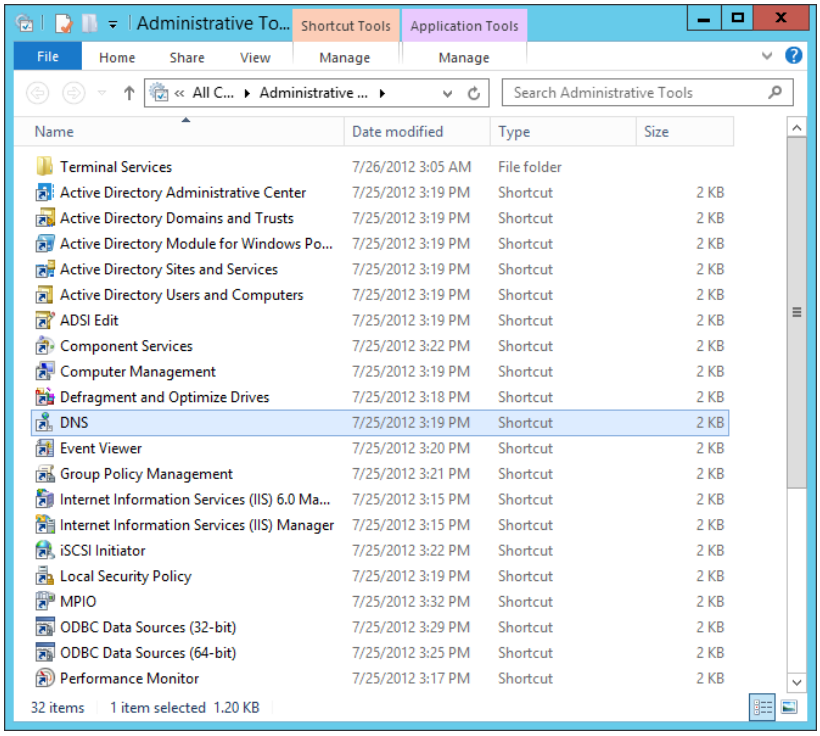
10. Click **Finish** to complete the New Zone Wizard.



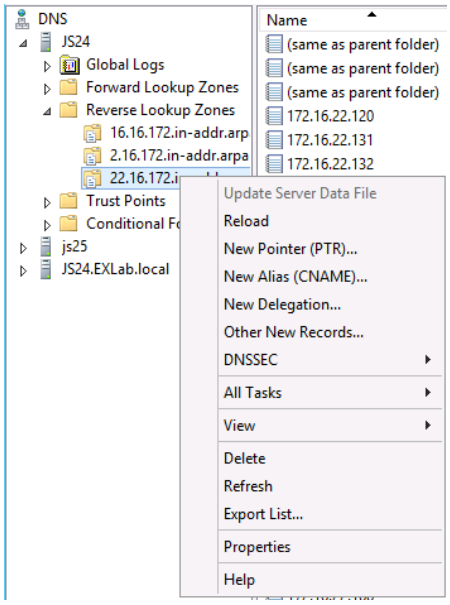
3.1.3 Creating a PTR record

To create a PTR record:

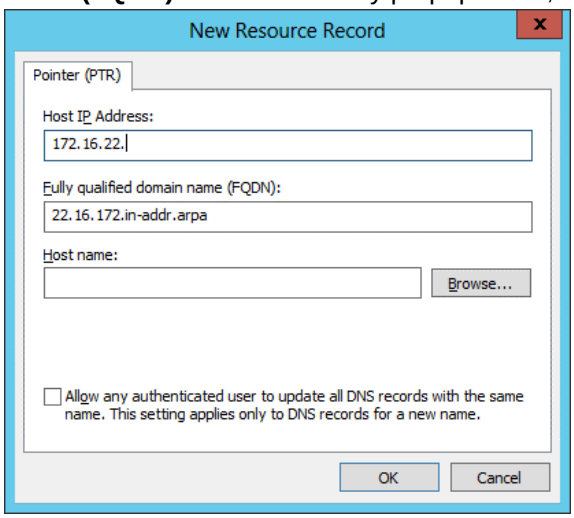
1. Open a console session to the primary DNS server. Log in as **Administrator**.
2. To open DNS Manager, at the start screen click **Administrative Tools** > **DNS**.



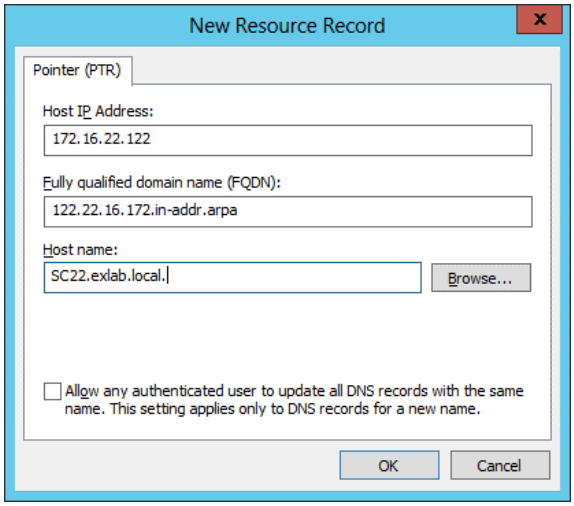
3. In DNS Manager, expand the domain controller, expand **Reverse Lookup Zones**, right-click the proper reverse lookup zone, and select **New Pointer (PTR)**.



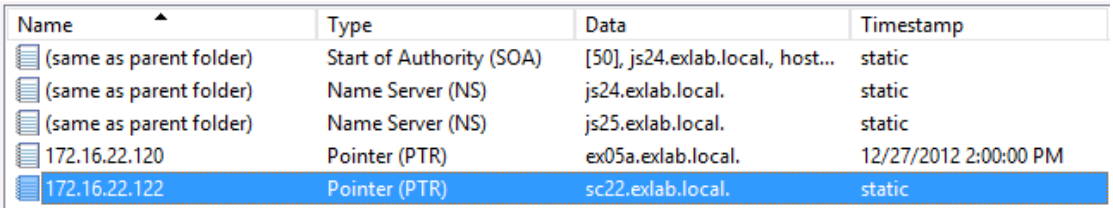
4. The **New Resource Record** window appears. The **Host IP Address** and **Fully qualified domain name (FQDN)** are automatically prepopulated, but will need modification in the following step.



5. Enter the **Host IP Address** for the SC Series array that matches the Host (A) record, the **Fully qualified domain name (FQDN)** of the SC Series array, and the **Host name** followed by a period. Leave the **Allow any authenticated user to update**… box unchecked. Click **OK**.



6. Verify that the Pointer (PTR) record displays in **DNS Manager**.

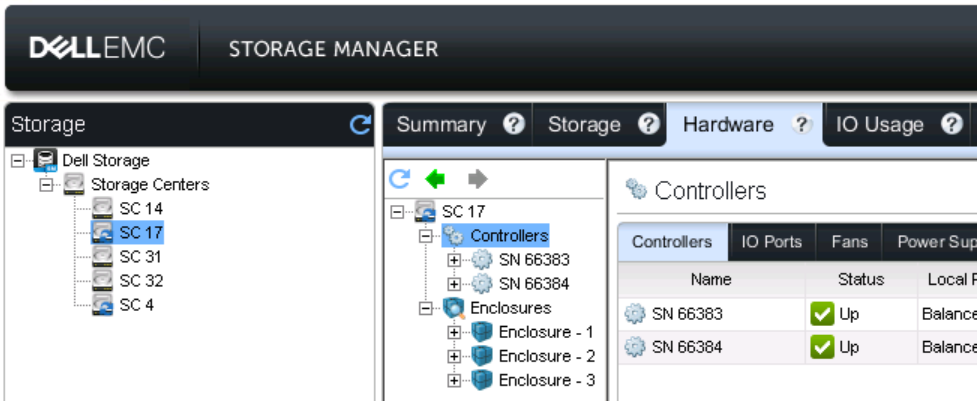


Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[50], js24.exlab.local., host...	static
(same as parent folder)	Name Server (NS)	js24.exlab.local.	static
(same as parent folder)	Name Server (NS)	js25.exlab.local.	static
172.16.22.120	Pointer (PTR)	ex05a.exlab.local.	12/27/2012 2:00:00 PM
172.16.22.122	Pointer (PTR)	sc22.exlab.local.	static

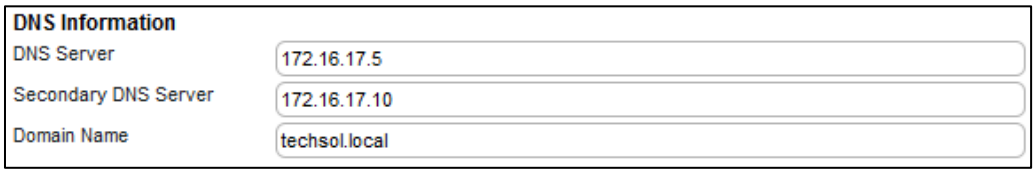
3.1.4 SC Series network settings

On the SC Series array, each controller's primary DNS server must be set to the primary DNS server used by Active Directory. If a secondary DNS server also exists, configure each controller to point to it. Each controller must also reflect the domain name where the SC Series array will exist and authenticate with. To modify the DNS/domain settings of the controller, perform the following steps:

1. Using the DSM client, connect directly to the SC Series array or to a DSM Data Collector that has the SC Series array added. If connected to a DSM Data Collector, select the SC Series array to manage.
2. Select the **Hardware** tab, and expand **Controllers**.



3. Right-click the first controller and select **Edit Settings**.
4. In the **DNS Information** section, enter the IP address of the primary **DNS Server**, the **Secondary DNS Server** (if applicable), and the **Domain Name**. Click **OK** when finished.



5. For a dual-controller SC Series array, repeat this process on the other controller.

4 Active Directory user and group access

For detailed information on granting access to directory users and groups, see the *Dell Storage Manager Administrator's Guide* for your version of DSM.

Consider the following when granting access to an Active Directory user:

- In the case a directory user has been given access to the SC Series array directly and also belongs to a directory group that has been granted access, the local user permissions will override the mapped group permissions.
- A directory group mapped to the SC Series array with Volume Manager or Reporter privileges must be mapped to a local SC Series group. The local SC Series group determines which folders the users in the mapped directory group have access to. A directory group mapped to the SC Series array with Administrator privileges does not require mapping to a local group because administrators have access to all folders in the SC Series array.
- SC Series supports authentication of a user in up to 16 nested groups.
- 64 AD groups can be mapped to a single SC Series group.

4.1 SC Series permissions

If a directory user has Administrator permissions to the SC Series array, the permissions level cannot be changed (downgraded) to Volume Manager or Reporter. However, user permissions can be changed from Volume Manager to Reporter or vice versa.

Like directory users, directory groups that have Administrator permissions to the SC Series array cannot be changed (downgraded) to Volume Manager or Reporter.

Permissions for a directly-mapped directory user can be changed, but not if the access is granted through membership in a group.

When a directory user is a member of more than one directory group with access to the SC Series array, the least restrictive permissions apply. For example, if a user is a member of Group 1 that grants Reporter access to the SC Series array (more restrictive), and is also a member of Group 2 that grants Volume Manager access in the SC Series array (less restrictive), the user is granted Volume Manager permissions when they log in.

4.2 Active Directory account maintenance

4.2.1 Granting access to user and group objects in a child or trusted domain

To allow access to users and groups from child or trusted domains, it is important to understand the three types of groups (universal, global, and domain local) within Active Directory.

A **universal group** can contain users and groups (global and universal) from any domain in the forest. Universal groups do not consider trust. Universal groups can be a member of domain local groups but not global groups. Because SC Series arrays requires a two-way trust in order to grant access to non-local users, using universal groups for SC Series access is not recommended.

A **global group** can contain users, computers and groups from the same domain, but not universal groups. A global group can be a member of global groups of the same domain, domain local groups, or universal groups of any domain in the forest or trusted domains.

A **domain local group** can contain users, computers, global groups, and universal groups from any domain in the forest and any trusted domain, and domain local groups from the same domain. Domain local groups can be a member of any domain local group in the same domain.

A user in a child domain can gain access to the SC Series array by being a member of a parent domain group that has access, or by being a member of a local child domain group that is a member of a parent domain group that has access. In this configuration, the parent domain group should be set to domain local because a global group cannot contain domain local or global groups from a child domain.

A user in a trusted domain can gain access to the SC Series array by being a member of a local domain group that has access, or by being a member of group on the trusted domain that is a member of the local domain group that has access. In this configuration, the local domain group should be set to domain local. The local domain group cannot be a global group because global groups cannot contain cross-domain members. Groups on the trusted domain should be created as global.

4.2.2 Account and group deletion

When an Active Directory user account is deleted, access to the SC Series array (whether access was granted directly or through group membership) is lost. The corresponding SC Series user account must be manually deleted.

When an Active Directory group is deleted, all the users of that AD group lose access to the SC Series array, unless the users have access granted directly. The group mapping and all user accounts that were part of that group must be manually deleted from the SC Series array.

4.2.3 Disabled or locked out accounts

Active Directory user accounts with access to the SC Series array (either directly or by group membership) will be unable to log in to the SC Series array if the user account is disabled or locked out in Active Directory. Access to the SC Series array is regained when the account is enabled.

5 Changing AD domains

SC Series AD integration can be changed to point to a different AD domain. DNS settings and SC Series networking settings must be updated to reflect the new AD domain information. To change to a new AD domain, run the Authentication Configuration wizard and enter the new AD domain settings.

When changing to a different AD domain, the original user and group mappings to the SC array from the previous AD domain configuration will no longer grant access to the SC array.

A Additional resources

A.1 Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

Dell TechCenter is an online technical community where IT professionals have access to numerous resources for Dell software, hardware and services.

Storage Solutions Technical Documents on Dell TechCenter provide expertise that helps to ensure customer success on Dell Storage platforms.

A.2 Related documentation

Table 1 Referenced or recommended resources

Vendor	Resource
Microsoft	Active Directory Domain Services Overview
Microsoft	Domain Name System (DNS) Overview