Table Of Contents

Table Of Contents 1
Applies To: 2
Background: 2
More Information: 2
Resolution: 2

How To: Isolate an AWS instance from Active Directory and Dynamic DNS until cutover

Reference Number: **AA-00409** Views: **3573** Created: **02-14-2017 13:19** Last Updated: **02-14-2017 14:34**

Applies To:

DynaCenter 6.5.0 and later

Background:

When migrating a Windows or Linux source server that has Dynamic DNS (DDNS or DynDNS) enabled, the newly deployed instance can take the DNS name of the source server if the newly deployed instance can reach the DNS server in the source environment. This might be an undesired outcome.

its Active Directory Domain Controller, which could cause a conflict with the source server.

More Information:

Security Groups for Your VPC

Network Ports Used by DNS

Active Directory and Active Directory Domain Services Port Requirements

Resolution:

To prevent a migrated server from taking the DNS name of the source server or from reporting to an Active Directory Domain Controller, apply a Security group that blocks outbound access from the new instance to the DDNS and Active Directory infrastructure.

Note: This solution cannot be used in scenarios where a deploy subnet is used for the migration operation as, in those scenarios, DynaCenter applies a standard security group that allows outbound access to DDNS and AD.

Follow these steps to prevent a deployed instance from accessing DDNS or AD infrastructure:

1. Verify the source server has a local user account, which will be needed to log in to the new instance before it is joined to an Active Directory domain.

2. Create a security group with the following settings:

Inbound Rules	Outbound Rules
3389 (TCP)	80 (TCP)
22 (SSH)	443 (TCP)
	123 (TCP)

3. If using the DynaCenter Console, assign only this security group in the migration template. If using the DynaCenter CLI, include only this security group in the deploy profile.

   Important: Assign only this security group during the migration; assigning additional security groups might allow premature access to DDNS or Active Directory.

4. After the server has been migrated to your Amazon environment, consider taking actions such as the following before you apply the production security group(s) to the instance so as to avoid DDNS or AD conflicts:

- Change the hostname of the deployed instance
- Change the IP address of the deployed instance
- Decommission the source server