Microsoft Windows Server 2008R2 Directory Services (DS) on Amazon EC2

Introduction

This document has two main objectives. The first part of this paper will detail all the challenges and considerations to using Active Directory Domain Services in Amazon EC2 cloud and the next part will show you how to setup it up at a basic level.

Prerequisites

Organizations can use Active Directory Domain Services (AD DS) in Windows Server 2008R2 to simplify user and resource management while creating scalable, secure, and manageable infrastructures. You can use ADDS to manage your network infrastructure, including branch office, Microsoft Exchange Server, and multiple forest environments. There are many facets to a Windows Server 2008R2 Active Directory environment which should be understood before beginning your deployment. For more information on Windows Server 2008R2 and Active Directory refer to http://technet.microsoft.com/en-us/library/dd378801(WS.10).aspx

Before using this paper, you should be familiar with:

- Launching and terminating Windows instances
- Using RDP to connect to Windows instances
- Running tools from the Windows Command Prompt
- Administering Windows Server

For more information about launching and terminating Windows instances refer to the *Amazon Elastic Compute Cloud Getting Started Guide*

For this tutorial we are using the following Amazon EC2 AMI's:

- amazon/Windows-2008R2-SP1-English-Base
    - This is the Basic Microsoft Windows Server 2008R2 – 64bit
    - Used for the two Active Directory domain controllers

Challenges

Before getting further into the details, it is useful to understand the challenges to network 2 or more machines together using Active Directory on Amazon's Elastic Compute Cloud (EC2):

- All Amazon EC2 instances are assigned a dynamic private IP once they're started

- All Amazon EC2 instances are assigned a dynamic private host-name once they're started (which takes the form of "ip-[dynamic private ip].[region].compute.internal")
- All Amazon EC2 instances are assigned a dynamic public host-name once they're started

Use case scenarios

There are existing use case scenarios for using Microsoft Windows Server 2008R2 Directory Services (DS), this document captures some of the specific reasons to use Windows Server 2008R2 Directory Services in Amazon EC2.

The two use cases may be:

1. New Active Directory Directory Services (ADDS) Domain Controller in EC2
    a. There may be times when a customer has an application that they want to have a centralized, cloud-based authentication mechanism for their application By leveraging a new Directory Service implementation in Windows Server 2008R2 in Amazon EC2, the application in the Amazon EC2 cloud, can access the directory server in Windows Server.
2. Extending an Existing ADDS Corporate Environment in EC2

For more information on extend your existing IT infrastructure to create a Virtual Private Cloud (VPC) go to http://media.amazonwebservices.com/EC2_ADFS_howto_2.0.pdf

Planning

When planning your Active Directory deployment, you need to think about the following:

- Is this a stand-alone Active Directory environment or is it an extension of your existing Active Directory network?
- Choosing your DNS namespace
- Determine storage requirements
- IP address assignment

Choosing a DNS Namespace

Before setting up a domain, you should choose a DNS namespace for the domain. Currently, Amazon EC2 uses the internal DNS namespace *compute-1.internal* or *ec2.internal,* and they suggest you use this internal namespace plus a subdomain (yourdomain.compute-1.internal) when setting up your server. For your Active Directory Domain name, this may or may not be suitable, you can select the DNS namespace that is appropriate for your company's needs and requirements. This tutorial uses the DNS name aws.compute-1.internal.

To find the DNS suffix that was automatically assigned, enter the command >ipconfig/all

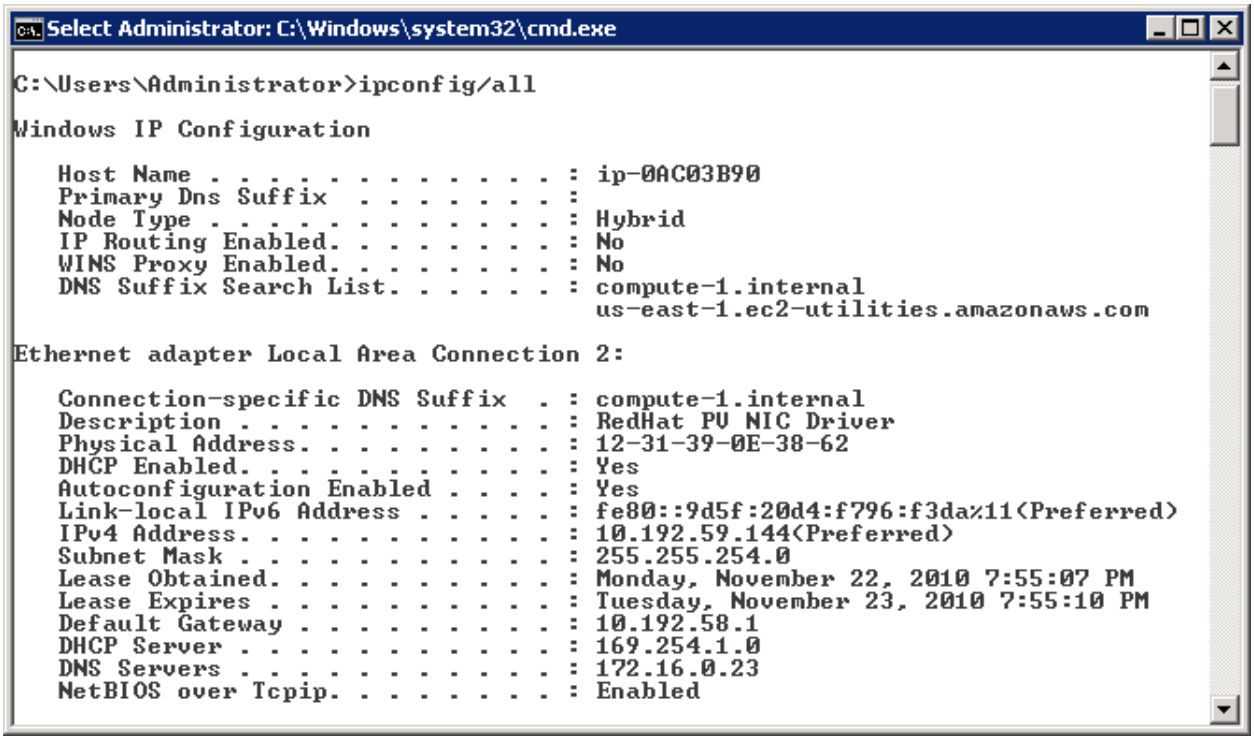


Figure 1 - IPCONFIG

Look for the value specified by the "Connection-specific DNS Suffix." This step is for information purposes only.

For general guidance on DNS namespace planning, see http://technet.microsoft.com/en-us/library/cc759036.aspx.

Storage

Before building your first Domain Controller, determine how much disk space you'll need for the Active Directory database, Active Directory log files, and the SYSVOL shared folder. For more guidance, go to http://technet.microsoft.com/en-us/library/cc754678%28WS.10%29.aspx.

After determining how much disk space you need, you must decide where to store your Active Directory data. We strongly recommend that you do not store the Active Directory data on the C: volume. The C: volume is limited to 20 GB and is not an appropriate choice for storing Active Directory data. If the volume housing the Active Directory database log files runs out of space AD will attempt to gracefully shutdown the instance. It is our recommendation that you add an additional EBS volume to your DC instance to store the Active Directory Database, logfiles and SYSVOL

> **Important:** Do not store Active Directory data under a reparse point hosted on the C: volume. A reparse point is a folder that redirects to a different location, possibly on a different volume. The Active Directory services cannot traverse reparse points and putting SYSVOL under one will cause Active Directory to fail in ways that that are likely to require reinstallation of the operating system.

This document uses the instance storage provided by the m1.large instance type. For more information about storage and instance types, go to http://docs.amazonwebservices.com/AWSEC2/2008-12-01/DeveloperGuide/index.html?instance-storage.html and http://docs.amazonwebservices.com/AWSEC2/2008-12-01/DeveloperGuide/index.html?instance-types.html. You can also use an Elastic Block Storage volume to store the data. For more information, go to http://aws.amazon.com/ebs/

> **Note:** Instance storage provides better disk IO performance than Amazon Elastic Block Storage (EBS). And, since AD is replicating the data to other DCs, the data is already stored redundantly.

If you want to store your Active Directory data files on a RAID 1 volume, you can use a larger instance type. For example, you can use an m1.large instance type and use a Windows mirrored volume.

Note: Amazon EBS is an excellent backup solution for your Active Directory backups. Amazon provides for taking snapshots of running instances. For a running Active Directory Directory Server, these snapshots are not a viable option for backup or restore of Active Directory, you should implement a standard backup solution for Active Directory.

IP Address assignment

By default all new instances are assigned a dynamic IP address (public and private). For reliable ADDS you need to have static private IP's assigned to each DC. To achieve this, Amazon provides their Virtual Private Cloud (VPC) service which allows you to utilize your own private IP addresses for your instances. For more information on VPC IP go to http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/

Replacement Instances

Do not bundle a running DC into an Amazon Machine Image (AMI) to launch replacement instances from that AMI. One reason is that a new security identifier is created during the instance launch process. Also, if the AMI used to launch the new instances is older than the tombstone lifetime, deleted objects can reappear in the directory. For information about AD tombstones see http://searchwinit.techtarget.com/tip/0,289483,sid1_gci1169756,00.html.

> **Note**: If you use replacement instances, you must still backup your DCs to ensure that the transaction logs are being cleaned up.

Security considerations

The security of a virtual domain controller must be managed just as carefully as that of a physical domain controller. A mismanaged virtual domain controller can allow the same types of attacks which could compromise all domains and forests.

For more information about securing domain controllers, see Best Practice Guide for Securing Active Directory Installations (http://go.microsoft.com/fwlink/?LinkID=28521).

Setup

Now that we have reviewed all the considerations, the following sections will detail the setup process.

Getting Started

After you have decided which environment this will be (stand-alone or an extension), you have chosen a DNS namespace, and determined your storage requirements, you are ready to begin with the sample. In the Getting Started task you will launch an instance and retrieve the Administrator password.

To get started:

1. Select the amazon/Windows-2008R2-SP1-English-Base from the Quick Start list
2. For the Instance Details use the following information:

    a. Number of Instances: (1)
    b. Availability Zone: choose one that makes sense for your region
    c. Instance Type: Large (m1.large, 7.5Gb)
    d. Select Launch Instances, then press Continue

3. Accept the defaults on the next screen and press Continue
4. Add a Tag to help simplify administration, then press Continue
5. Select Create a new Key Pair and enter a name for the pair
6. Press Create and Download your Key Pair and save it to a location on your hard drive you will remember

7. Create your Security Group then press Continue
    Note: All of your instances should be in the same security group.
8. Review your Instance information, if it correct press Launch, if not go back and make the necessary corrections
9. Once your Instance is running, you will need to wait approximately 15 minutes before the Administrator password generation happens.
10. Right click on the Running Status and select Get Windows Password from the list

NOTE: DO NOT turn off or reboot your instance until AFTER to have the Administrator password. If the instance is rebooted for any reason, the password generation utility will not provide a password and you are locked out of your image and will have to start over from the beginning.

11. Enter the data from your private key that you created earlier
12. Press Decrypt Password

NOTE: You may receive a Scripting error message asking if you want to stop running the script, press NO. You may need to do this multiple times before the password is provided

13. Right click on the Running Status and select Connect
14. You can download the Shortcut file or manually enter the Remote Desktop settings
15. Launch the Remote Desktop shortcut
16. Connect to the instance

Instance setup

After you have connected to an instance, you need to configure the instance.

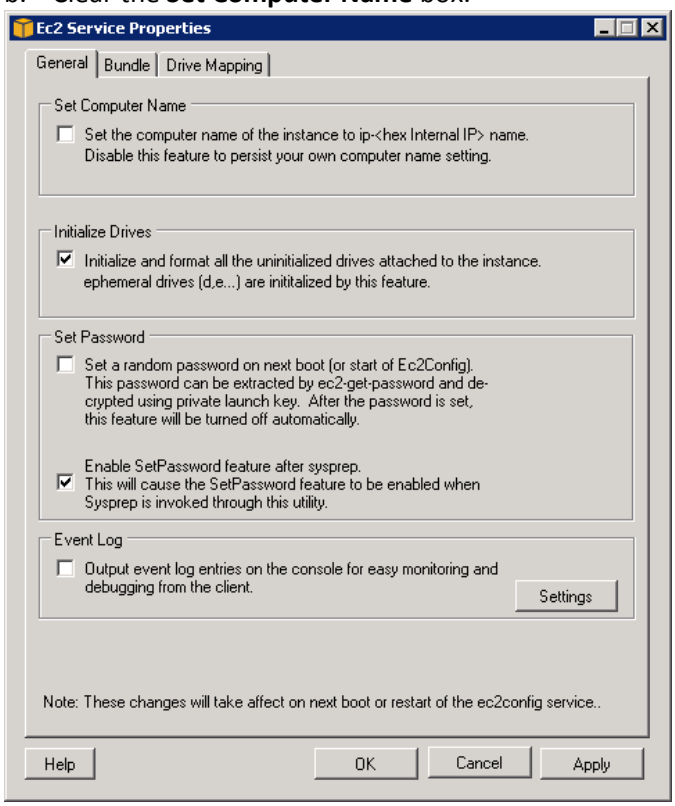
To set up your instance:

1. Change the administrator password (recommended). Standard Windows password policies would apply to your new password

>net user administrator <password>

2. Consider renaming the computer. In this tutorial, the DCs are renamed “DC1” and “DC2”. To rename your EC2 instance:

    a. From the Windows Desktop click **Start**, point to **All Programs**, and select **Ec2ConfigService Settings**.
    b. Clear the **Set Computer Name** box.



3. Rename the computer:
    a. From the Windows Desktop click **Start**, right-click **My Computer**, click **Properties,** and select the **Computer Name** tab.
    b. Change the computer name.

4. Install any utilities that you would like to have available on the instance and configure the instance. For example, you can set up a startup script to set environment variables to point to instance storage instead of the C: drive.

For more information, go to http://technet.microsoft.com/en-us/library/aa998306.aspx

5. We recommend that you setup an additional EBS volume now to be used for the Active Directory Database, logfiles, and SYSVOL.

For information on setting up additional EBS volumes go to http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/index.html?ebs-attaching-volume.html

Note: At this point, you should create an Amazon Machine Image of an instance to use as a DC. You will use this AMI to launch the remaining DCs in this tutorial.

If an instance running a DC fails, launch a new instance using this AMI. After the instance starts, run DCPROMO on it to create a new DC.

The remainder of this tutorial assumes you have a customized AMI.

With your first instance running, launch one more instance from your AMI. This will be the second DC for your AD Environment. You should have two instances running.

Promote the First Domain Controller

Before promoting the first domain controller, add Windows installation media to your DC.

To promote the first domain controller:

1. Configure your private static IP based on your VPC (see above) configuration
2. Add the Domain Controller role to you server.
   From the Windows Desktop click **Start** and **Manage Your Server**. This will launch the *Mange Your Server* wizard.
3. Select **Adding Roles to Your Server**
4. Select **Domain Controller (Active Directory).**
5. Click **Domain in a new forest.**
6. Name the domain using the DNS name you chose in the Planning section of this tutorial.
7. Enter a Domain NetBIOS name for the domain. For this tutorial the NetBIOS name will be "AWS."
8. Choose your additional EBS volume as the location for the Database folder and Log folder.
9. Choose your additional EBS volume as the location for the SYSVOL folder.
10. Click **Install and configure the DNS Server on this computer**, and set this computer to use this DNS server as its preferred DNS server.
11. Specify a directory services restore mode administrator password.
12. Cancel out of **Local Area Connection Properties** when prompted to change the NIC from DHCP to a static IP address.
13. Click **Finish** in the Manage Your Server Wizard.
14. Reboot the DC by clicking **Restart Now** in the Manage Your Server Wizard.

This installs DNS on the DC. Any computer that uses the DC as their DNS server will be able to resolve addresses in your domain (for us, this is the aws.compute-1.internal subdomain) and external DNS domains (for example: amazon.com, google.com, msn.com, yahoo.com). If you need to resolve DNS names for other Amazon EC2 instances outside this domain, configure conditional DNS forwarders utilizing Amazons EC2 DNS server which has the IP address of 172.16.0.23. For more information, go to http://technet.microsoft.com/en-us/library/cc773370.aspx.

Promote the Second Domain Controller

To promote the second domain controller:

1. (Optional) Rename the computer (e.g., “DC2”).
2. Configure your private static IP based on your VPC (see above) configuration
3. Point the instance at your DC for DNS.

   >netsh int ip set dns "local area connection" static <IP_Address> primary

4. Test DNS by running the following:

   >nslookup dc1.aws.compute-1.internal

   That should return the IP address of the DC.

To add the domain controller:

1. From the Windows Desktop click **Start** and **Manage Your Server**. This will launch the *Mange Your Server* wizard.
2. Select **Adding Roles to Your Server**
3. Select **Domain Controller (Active Directory).**
4. Click **Additional domain controller for an existing domain.**
5. Use the administrator username and password from DC1 and the full DNS name for the domain (e.g. aws.compute-1.internal)
6. Use the full DNS name for the domain
7. Specify your additional EBS volume as the location for the database folder and log folder.
8. Specify your additional EBS volume as the location for the SYSVOL folder.
9. Enter a directory services restore mode administrator password.
10. Click **Finish** in the AD Installation Wizard

You now have two domain controllers in your domain.

Launching a Replacement DC

If a DC fails, you can recover by launching a new DC. The domain will operate successfully as long as there is at least one DC remaining.

> **Tip:** To provide redundancy and business continuity, if all but one DC fails, add one or more additional DCs to the domain by simply repeating the steps in *Promote the Second Domain Controller.* .

Important: As with all disaster recovery plans, thoroughly test your recovery plans before going into production.