AWS Directory Service

Administration Guide

Version 1.0

AWS Directory Service: Administration Guide

Table of Contents

What is AWS Directory Service? 1
- New to Amazon EC2? 1

Setting Up 2
- AWS Account 2
- Create an IAM User 2
  - Controlling Access 4
- Prerequisites 4
  - Simple AD 5
  - AD Connector 5

Getting Started 9
- Creating a Directory 9
  - Creating a Directory 9
  - Details 10
- Connecting to a Directory 11

Managing a Directory 12
- Console Management 12
  - Directories 12
  - Console Access 17
  - IAM Roles 18
- Directory Administration 33
  - Join a Directory 33
  - Install AD Tools 36
  - Creating Users and Groups 39

Troubleshooting 42
- I receive a "DNS unavailable" error when I try to connect to my on-premises directory 42
- I receive a "Connectivity issues detected" error when I try to connect to my on-premises directory 42
- I receive an "SRV record" error when I try to connect to my on-premises directory 43

Tutorials 44
- Tutorial: Creating a Simple AD Directory 44
  - Prerequisites 44
  - Notes 44
  - Step 1: Create and Configure Your VPC 45
  - Step 2: Create the Directory 46

Limits 48

Document History 49

What is AWS Directory Service?

The AWS Directory Service is a managed service that makes it easy to connect to your existing on-premises Microsoft Active Directory, or set up and operate a new directory in the AWS cloud, making it easy to deploy and manage Windows workloads in the AWS cloud. Your directory users and groups can access the AWS Management Console, and AWS applications, such as Amazon WorkSpaces and Amazon Zocalo, using their existing credentials.

New to Amazon EC2?

If you are new to Amazon EC2, there are some concepts you should be familiar with to use AWS Directory Service. We recommend that you begin by reading the following topics:

- What is Amazon EC2? in the *Amazon EC2 User Guide for Microsoft Windows Instances*.
- Launching EC2 Instances in the *Amazon EC2 User Guide for Microsoft Windows Instances*.
- Security Groups in the *Amazon EC2 User Guide for Microsoft Windows Instances*.
- What is Amazon VPC? in the *Amazon VPC User Guide*.
- Adding a Hardware Virtual Private Gateway to Your VPC in the *Amazon VPC User Guide*.

Setting Up AWS Directory Service

The following topics discuss how to get started using AWS Directory Service.

Topics

- AWS Account (p. 2)
- Create an IAM User (p. 2)
- Prerequisites (p. 4)

AWS Account

Your AWS account gives you access to all services, but you are charged only for the resources that you use.

If you do not have an AWS account, use the following procedure to create one.

To sign up for AWS

1. Open http://aws.amazon.com and click **Sign Up**.
2. Follow the on-screen instructions.

Your root account credentials identify you to services in AWS and grant you unlimited use of your AWS resources, such as your WorkSpaces. To allow other users to manage AWS Directory Service resources without sharing your security credentials, use AWS Identity and Access Management (IAM). We recommend that everyone work as an IAM user, even the account owner. You should create an IAM user for yourself, give that IAM user administrative privileges, and use it for all your work.

Create an IAM User

The AWS Management Console requires your username and password so that the service can determine whether you have permission to access its resources. However, we recommend that you avoid accessing AWS using the credentials for your root AWS account; instead, we recommend that you use AWS Identity and Access Management (IAM) to create an IAM user and add the IAM user to an IAM group with administrative permissions. This grants the IAM user administrative permissions. You then access the AWS Management Console using the credentials for the IAM user.

If you signed up for AWS but have not created an IAM user for yourself, you can create one using the IAM console.

To create the Administrators group

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, click **Groups** and then click **Create New Group**.
3. In the **Group Name** box, type `Administrators` and then click **Next Step**.
4. In the **Select Policy Template** section, click **Select** next to the **Administrator Access** policy template.
5. Click **Next Step** and then click **Create Group**.

Your new group is listed under **Group Name**.

To create the IAM user, add the user to the Administrators group, and create a password for the user

1. In the navigation pane, click **Users** and then click **Create New Users**.
2. In box **1**, type a user name and then click **Create**.
3. Click **Download Credentials** and save your access key in a secure place. You will need your access key for programmatic access to AWS using the AWS CLI, the AWS SDKs, or the HTTP APIs.

   > **Note**
   > You cannot retrieve the secret access key after you complete this step; if you misplace it you must create a new one.

   After you have downloaded your access key, click **Close**.
4. In the content pane, under **User Name**, click the name of the user you just created. (You might need to scroll down to find the user in the list.)
5. In the content pane, in the **Groups** section, click **Add User to Groups**.
6. Select the **Administrators** group and then click **Add to Groups**.
7. In the content pane, in the **Security Credentials** section (you might need to scroll down to find this section), under **Sign-In Credentials**, click **Manage Password**.
8. Select **Assign a custom password** and then type and confirm a password. When you are finished, click **Apply**.

To sign in as this new IAM user, sign out of the AWS Management Console, then use the following URL, where *your_aws_account_id* is your AWS account number without the hyphens (for example, if your AWS account number is `1234-5678-9012`, your AWS account ID is `123456789012`):

```
https://your_aws_account_id.signin.aws.amazon.com/console/
```

Enter the IAM user name and password that you just created. When you're signed in, the navigation bar displays "*your_user_name @ your_aws_account_id*".

If you don't want the URL for your sign-in page to contain your AWS account ID, you can create an account alias. From the IAM dashboard, click **Customize** and enter an alias, such as your company name. To sign in after you create an account alias, use the following URL:

```
https://your_account_alias.signin.aws.amazon.com/console/
```

For more information about using IAM policies to control access to your AWS Directory Service resources, see Controlling Access to AWS Directory Service Resources (p. 4).

Controlling Access to AWS Directory Service Resources

By default, IAM users don't have permission to AWS Directory Service resources. To allow IAM users to manage AWS Directory Service resources, you must create an IAM policy that explicitly grants IAM users permission to create and manage AWS Directory Service and Amazon EC2 resources, and attach the policy to the IAM users or groups that require those permissions. For more information about IAM policies, see Permissions and Policies in the *Using IAM* guide.

The following policy statement grants a user or group permission to manage all AWS Directory Service resources. The access to IAM resources is needed so that AWS Directory Service can read and create IAM roles on your behalf. Access to some Amazon EC2 resources is necessary to allow AWS Directory Service to create, configure, and destroy its directories.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:*",
        "iam:PassRole",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

For more information about IAM, see the following:

- Identity and Access Management (IAM)
- Using IAM

Prerequisites

To use AWS Directory Service, you must satisfy the following prerequisites.

Topics

- Simple AD Prerequisites (p. 5)

- AD Connector Prerequisites (p. 5)

Simple AD Prerequisites

To create a directory with Simple AD, you need an VPC with an Internet gateway and at least two subnets. Each of the subnets must be in a different Availability Zone. For more information, see the following topics in the *Amazon VPC User Guide*:

- What is Amazon VPC?
- Subnets in Your VPC

AD Connector Prerequisites

The following topics explain how to prepare to use AD Connector to connect AWS Directory Service to your on-premises directory.

Topics

- Requirements (p. 5)
- Delegating Connect Privileges (p. 6)
- Multi-factor Authentication Prerequisites (p. 8)

Requirements

To connect to your on-premises directory, you need the following:

- A VPC, with an Internet gateway and at least two subnets. Each of the subnets must be in a different Availability Zone. The VPC must also be connected to your on-premises network through a virtual private network (VPN) connection or AWS Direct Connect. For more information, see the following topics in the *Amazon VPC User Guide*:
  - What is Amazon VPC?
  - Subnets in your VPC
  - Adding a Hardware Virtual Private Gateway to Your VPC

  For more information about AWS Direct Connect, see the AWS Direct Connect User Guide.
- An on-premises network with an Active Directory domain. The functional level of this domain must be `Windows Server 2003` or higher.
- Credentials for an account in the on-premises directory with the following privileges. For more information, see Delegating Connect Privileges (p. 6).
  - Read users and groups
  - Create computer objects
  - Join computers to the domain
- The IP addresses of two DNS servers or domain controllers in your on-premises directory.
- For AWS Directory Service to communicate with your on-premises directory, the firewall for your on-premises network must have the following ports open to the CIDRs for both subnets in the VPC.
  - TCP 53
  - TCP 88
  - TCP 135
  - TCP 389
  - TCP 445

- TCP 464
- TCP 636
- TCP 1024-65535
- UDP 53
- UDP 88
- UDP 123
- UDP 138
- UDP 389
- UDP 445
- UDP 464

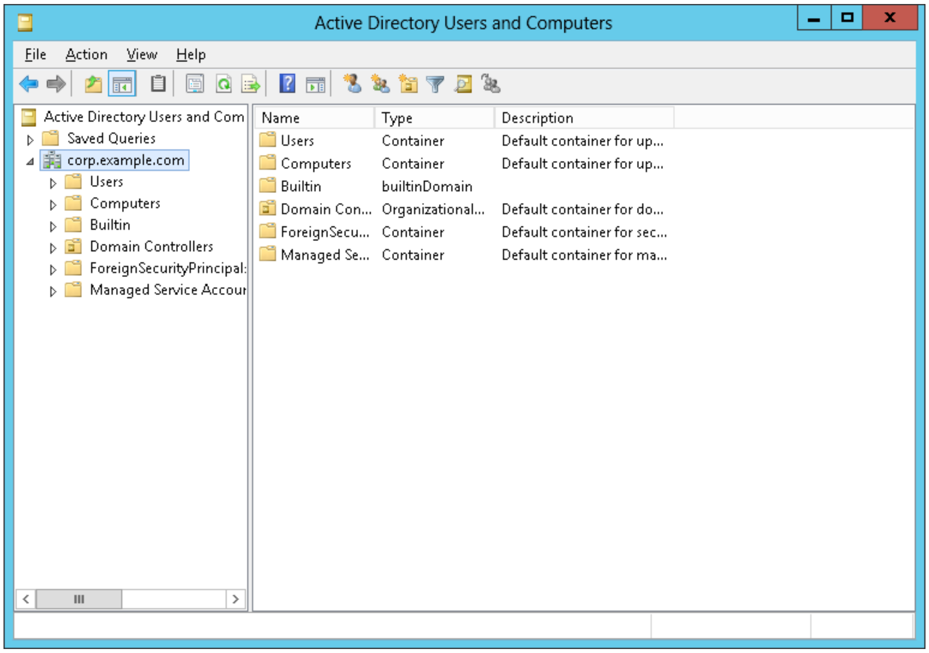
Delegating Connect Privileges

To connect to your on-premises directory, you must have the credentials for an account in the on-premises directory that has certain privileges. While members of the **Domain Admins** group have sufficient privileges to connect to the directory, as a best practice, you should use an account that only has the minimum privileges necessary to connect to the directory. The following procedure demonstrates how to create a new group called `Connectors`, and delegate the privileges to this group that are needed to connect AWS Directory Service to the directory.

This procedure must be performed on a machine that is joined to your directory and has the **Active Directory User and Computers** MMC snap-in installed. You must also be logged in as a domain administrator.

To delegate connect privileges

1. Open **Active Directory User and Computers** and select your domain root in the navigation tree.



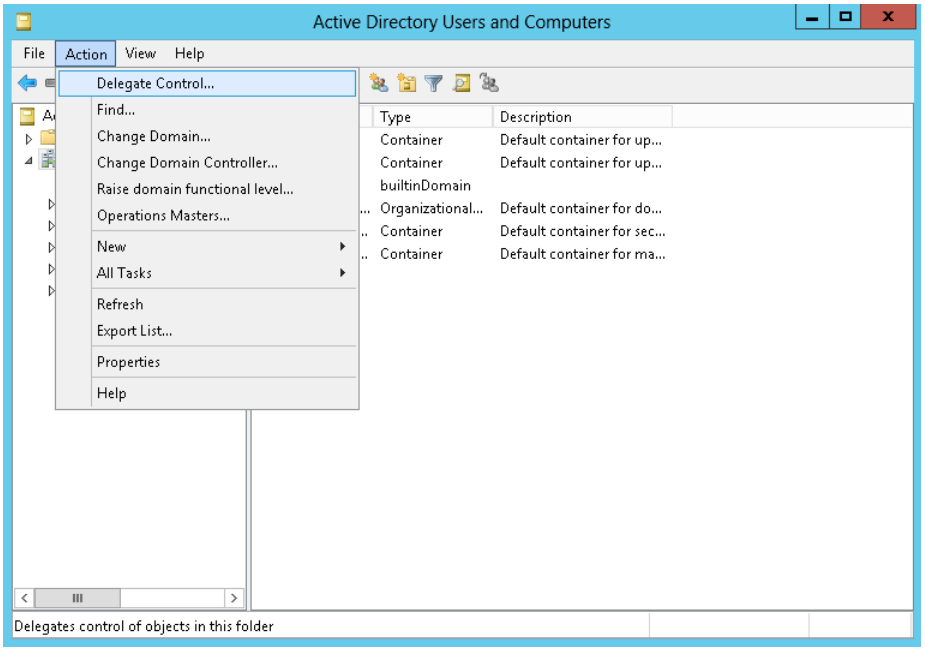
Name	Type	Description
Users	Container	Default container for up...
Computers	Container	Default container for up...
Builtin	builtinDomain	
Domain Con...	Organizational...	Default container for do...
ForeignSecu...	Container	Default container for sec...
Managed Se...	Container	Default container for ma...

2. In the list in the left-hand pane, right-click **Users**, select **New**, and then select **Group**.

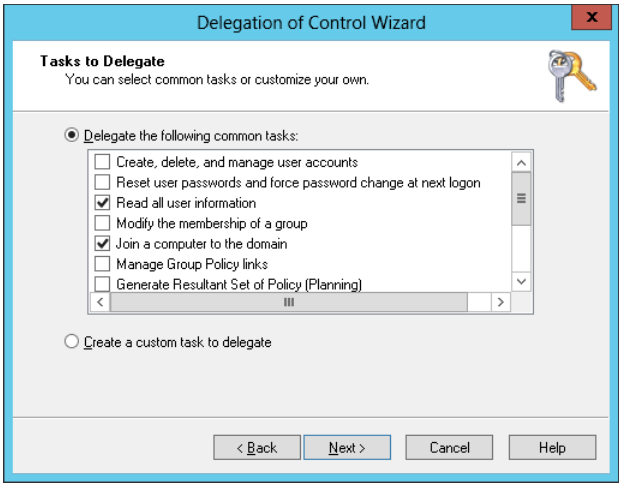
3. In the **New Object - Group** dialog box, enter the following and click **OK**.

Field	Value/Selection
Group name	`Connectors`
Group scope	**Global**
Group type	**Security**

4. In the **Active Directory User and Computers** navigation tree, select your domain root. In the menu, select **Action**, and then **Delegate Control**.


Active Directory Users and Computers
File
Action
View
Help
Delegate Control...
Find...
Change Domain...
Change Domain Controller...
Raise domain functional level...
Operations Masters...
New
All Tasks
Refresh
Export List...
Properties
Help
Type
Description
Container
Default container for up...
Container
Default container for up...
builtinDomain
Organizational...
Default container for do...
Container
Default container for sec...
Container
Default container for ma...
Delegates control of objects in this folder

5. On the **Delegation of Control Wizard** page, click **Next**, then click **Add**.
6. In the **Select Users, Computers, or Groups** dialog box, enter `Connectors` and click **OK**. If more than one object is found, select the `Connectors` group created above. Click **Next**.
7. On the **Tasks to Delegate** page, select only **Read all user information** and **Join a computer to the domain**, then click **Next**.



Delegation of Control Wizard

Tasks to Delegate
You can select common tasks or customize your own.

● Delegate the following common tasks:

- □ Create, delete, and manage user accounts
- □ Reset user passwords and force password change at next logon
- ☑ Read all user information
- □ Modify the membership of a group
- ☑ Join a computer to the domain
- □ Manage Group Policy links
- □ Generate Resultant Set of Policy (Planning)

○ Create a custom task to delegate

8. Verify the information on the **Completing the Delegation of Control Wizard** page, and click **Finish**.
9. Create a user with a strong password and add that user to the `Connectors` group. The user has sufficient privileges to connect AWS Directory Service to the directory.

Multi-factor Authentication Prerequisites

To support multi-factor authentication with your AD Connector directory, you need the following:

- A Remote Authentication Dial In User Service (RADIUS) server in your on-premises network that has two client endpoints. The RADIUS client endpoints have the following requirements:
  - To create the endpoints, you need the IP addresses of the AWS Directory Service servers. These IP addresses can be obtained from the **Directory IP Address** field of your directory details.
  - Both RADIUS endpoints must use the same shared secret code.
- Your on-premises network must allow inbound traffic over the default RADIUS server port (1812) from the AWS Directory Service servers.
- The usernames between your RADIUS server and your on-premises directory must be identical.

For more information about enabling multi-factor authentication with your AD Connector directory, see Multi-factor Authentication (p. 16).

Getting Started with AWS Directory Service

You can get started with AWS Directory Service in one of two ways. You can either create a directory in the cloud using Simple AD, or connect AWS Directory Service to your on-premises directory using AD Connector.

Topics

- Creating a Directory with Simple AD (p. 9)
- Connecting to Your Existing Directory with AD Connector (p. 11)

Creating a Directory with Simple AD

Simple AD creates a fully managed, Samba-based directory in the AWS cloud. When you create a directory with Simple AD, AWS Directory Service creates two directory servers and DNS servers on your behalf. The directory servers are created in different subnets in a VPC, which is done for redundancy so that your directory remains accessible even if a failure occurs.

Topics

- Creating a Directory (p. 9)
- Details (p. 10)

Creating a Directory

To create a directory with Simple AD, perform the following steps. Before starting this procedure, make sure you have completed the prerequisites identified in Simple AD Prerequisites (p. 5).

To create a directory with Simple AD

1. In the AWS Directory Service console navigation pane, select **Directories** and click **Set up Directory**.
2. In the **Create a Simple AD** area, click **Create Simple AD**.
3. Enter the following fields:

Directory DNS
The fully-qualified name for the directory, such as corp.example.com.

NetBIOS name
The short name for the directory, such as CORP.

Administrator password
The password for the directory administrator. The directory creation process creates an administrator account with the username Administrator and this password. For password requirements, see the note following the table.

The directory administrator password is case-sensitive and must be between 8 and 64 characters in length, inclusive. It must also contain at least one character from three of the following four categories:

- Lowercase letters (a-z)
- Uppercase letters (A-Z)
- Numbers (0-9)
- Non-alphanumeric characters (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Confirm password
Re-enter the administrator password.

Description
An optional description for the directory.

Directory Size
Select the size of the directory.

4. Enter the following fields in the **VPC Details** section and click **Next Step**.

   VPC
   The VPC for the directory.

   Subnets
   Select the subnets for the directory servers. The two subnets must be in different Availability Zones.

5. Review the directory information and make any necessary changes. When the information is correct, click **Create Simple AD**.

It takes several minutes for the directory to be created. When it has been successfully created, the **Status** value changes to Active.

Details

When you create a directory with Simple AD, AWS Directory Service performs the following tasks on your behalf:

- Sets up a Samba-based directory within the VPC.
- Creates a directory administrator account with the username Administrator and the specified password. You use this account to manage your directory.
- Creates a security group for the directory controllers.

Connecting to Your Existing Directory with AD Connector

AD Connector allows you to connect AWS Directory Service to your existing enterprise directory. When connected to your on-premises directory, all of your directory data remains on your directory servers. AWS Directory Service does not replicate any of your directory data.

To connect to your on-premises directory with AD Connector, perform the following steps. Before starting this procedure, make sure you have completed the prerequisites identified in AD Connector Prerequisites (p. 5).

To connect with AD Connector

1. In the AWS Directory Service console navigation pane, select **Directories** and click **Set up Directory**.
2. In the **Connect using AD Connector** area, click **Create AD Connector**.
3. Enter the following fields:

   Directory DNS
   The fully-qualified name of your on-premises directory, such as `corp.example.com`.

   NetBIOS name
   The short name of your on-premises directory, such as `CORP`.

   Connector Account Username
   The username of a user in the on-premises directory. For more information about this account, see the Requirements (p. 5) section.

   Connector Account Password
   The password for the on-premises user account.

   Confirm password
   Re-enter the password for the on-premises user account. This is required to prevent typing errors before the directory is connected.

   DNS address
   The IP address of at least one DNS server in your on-premises directory. These servers must be accessible from each subnet specified below.

   Description
   An optional description for the directory.

   Directory Size
   Select the size of the directory.

4. Enter the following fields in the **VPC Details** section and click **Next Step**.

   VPC
   The VPC for the directory.

   Subnets
   Select the subnets for the directory servers. The two subnets must be in different Availability Zones.

5. Review the directory information and make any necessary changes. When the information is correct, click **Create AD Connector**.

It takes several minutes for your directory to be connected. When it has been successfully extended, the **Status** value changes to `Active`.

Managing a Directory

You use the AWS Directory Service management console to perform certain directory-related actions, such as creating a new directory or deleting an existing directory. After a directory is created, most administrative functions are performed with directory management tools, such as the Active Directory Administration Tools.

Topics

- Console Management (p. 12)
- Directory Administration (p. 33)

Console Management

The following operations can be performed from the AWS Directory Service console.

Topics

- Managing Directories (p. 12)
- Managing Console Access for AWS Directory Service (p. 17)
- Managing IAM Roles (p. 18)

Managing Directories

The following topics discuss how to manage your AWS Directory Service directories.

Topics

- Viewing Directory Information (p. 13)
- Creating an Access URL (p. 13)
- Managing Directory Apps & Services (p. 13)
- Simple AD Directory Management (p. 14)
- AD Connector Directory Management (p. 15)

Viewing Directory Information

You can view basic information about a directory within the directories page, or more detailed information in the directory details page.

Topics

- Basic Information (p. 13)
- Detailed Information (p. 13)

Basic Information

To view basic information about a directory, perform the following steps:

To view basic directory information

1. In the AWS Directory Service console navigation pane, select **Directories**.
2. Click the arrow button next to your directory. Basic information about the directory is displayed below the directory entry in the list.

Detailed Information

To view more detailed information about a directory, perform the following steps:

To view detailed directory information

1. In the AWS Directory Service console navigation pane, select **Directories**.
2. Click the directory ID link for your directory. Information about the directory is displayed in the **Directory Details** section.

Creating an Access URL

You can create an access URL for your directory by performing the following steps.

> **Warning**
> After an access URL has been created, it cannot be deleted or reused, so this procedure should only be used when absolutely necessary.

To create an access URL

1. In the AWS Directory Service console navigation pane, select **Directories**.
2. Click the directory ID link for your directory.
3. In the **Access URL** section, if an access URL has not been assigned to the directory, the **Create Access URL** button is displayed. Enter a directory alias and click **Create Access URL**. If an **Entity Already Exists** error is returned, the specified directory alias has already been allocated. Choose another alias and repeat this procedure.

   Your directory URL is changed to `<alias>.awsapps.com`.

Managing Directory Apps & Services

AWS Directory Service provides the ability to give other AWS applications and services, such as Amazon WorkSpaces, access to your directory users.

To display the applications and services that can work with your AWS Directory Service directory, perform the following steps.

To display the apps and services for a directory

1. In the AWS Directory Service console navigation pane, select **Directories**.
2. Click the directory ID link for your directory.
3. Select the **Apps & Services** tab.

The management of access to your directories is performed in the console of the application or service that you want to give access to your directory. To enable or disable access to your directories, click on the link for the application or service that you want to modify. The following applications and services can be used with AWS Directory Service:

Amazon WorkSpaces
: For more information, see the Amazon WorkSpaces Administration Guide.

Amazon Zocalo
: For more information, see the Amazon Zocalo Administration Guide.

AWS Management Console
: For more information, see Managing Console Access for AWS Directory Service (p. 17).

Simple AD Directory Management

The following topics explain the different management actions you can perform on a Simple AD directory.

Topics

- Managing Snapshots (p. 14)
- Deleting a Simple AD Directory (p. 15)

Managing Snapshots

AWS Directory Service provides the ability to take manual snapshots of data for a Simple AD directory. These snapshots can be used to perform a point-in-time restore for your directory.

> **Note**
> You cannot take snapshots of AD Connector directories.

Topics

- Creating a Snapshot of Your Directory (p. 14)
- Restoring Your Directory From a Snapshot (p. 15)
- Deleting a Snapshot (p. 15)

Creating a Snapshot of Your Directory

A snapshot can be used to restore your directory to what it was at the point in time that the snapshot was taken. To create a manual snapshot of your directory, perform the following steps.

> **Note**
> You are limited to 5 manual snapshots for each Simple AD directory. If you have already reached this limit, you must delete one of your existing manual snapshots before you can create another.

To create a manual snapshot

1. In the AWS Directory Service console navigation pane, select **Snapshots**.

2. Click **Create Snapshot**.
3. In the **Create directory snapshot** dialog box, select the directory to take a snapshot of. You can also apply a description to the snapshot, if desired. When ready, click **Create Snapshot**.

Depending on the size of your directory, it may take several minutes to create the snapshot. When the snapshot is ready, the **Status** value changes to `Completed`.

Restoring Your Directory From a Snapshot

Restoring a directory from a snapshot is equivalent to moving the directory back in time.

> **Warning**
> When you restore a directory from a snapshot, any changes made to the directory after the snapshot date are overwritten.

To restore your directory from a snapshot, perform the following steps.

To restore a directory from a snapshot

1. In the AWS Directory Service console navigation pane, select **Snapshots**.
2. Select the snapshot to restore from.
3. Click **Restore**, review the information in the dialog box, and click **Restore**.

It takes several minutes for the directory to be restored. When it has been successfully restored, the **Status** value of the directory changes to `Active`.

Deleting a Snapshot

To delete a snapshot

1. In the AWS Directory Service console navigation pane, select **Snapshots**.
2. Select the snapshot to delete.
3. Click **Delete**, verify that you want to delete the snapshot, and click **Delete**.

Deleting a Simple AD Directory

When a Simple AD directory is deleted, all of the directory data and snapshots are deleted and cannot be recovered. After the directory is deleted, all instances that are joined to the directory remain intact. You cannot, however, use your directory credentials to log in to these instances. You need to log in to these instances with a user account that is local to the instance.

For information about deleting an AD Connector directory, see Deleting an AD Connector Directory (p. 17).

To delete a directory

1. In the AWS Directory Service console, select only the directory to be deleted.
2. Click **Delete**. It takes several minutes for the directory to be deleted. When the directory has been deleted, it is removed from your directory list.

AD Connector Directory Management

The following topics explain the different management actions you can perform on an AD Connector directory.

Topics

- Update Directory Credentials (p. 16)
- Multi-factor Authentication (p. 16)
- Deleting an AD Connector Directory (p. 17)

Update Directory Credentials

The AD Connector directory credentials represent the account that is used to access your on-premises directory. You can modify these account credentials by performing the following steps.

To modify the directory account credentials

1. In the AWS Directory Service console navigation pane, select **Directories**.
2. Click the directory ID link for your directory.
3. Select the **Connector Account** tab.
4. Enter the new user name and password, and click **Update Directory**.

Multi-factor Authentication

You can enable multi-factor authentication for your AD Connector directory by performing the following procedure. For more information about using multi-factor authentication with AWS Directory Service, see Multi-factor Authentication Prerequisites (p. 8).

To enable multi-factor authentication

1. In the AWS Directory Service console navigation pane, select **Directories**.
2. Click the directory ID link for your directory.
3. Select the **Multi-Factor Authentication** tab.
4. Enter the following values and click **Update Directory**.

   Enable Multi-Factor Authentication
   Check to enable multi-factor authentication.

   RADIUS server IP address(es)
   The IP addresses of your RADIUS server endpoints, or the IP address of your RADIUS server load balancer. You can enter multiple IP addresses by separating them with a comma (e.g., `192.0.0.0,192.0.0.12`).

   Port
   The port that your RADIUS server is using for communications. Your on-premises network must allow inbound traffic over the default RADIUS server port (1812) from the AWS Directory Service servers.

   Shared secret code
   The shared secret code that was specified when your RADIUS endpoints were created.

   Confirm shared secret code
   Confirm the shared secret code for your RADIUS endpoints.

   Protocol
   Select the protocol that was specified when your RADIUS endpoints were created.

   Server timeout
   The amount of time, in seconds, to wait for the RADIUS server to respond. This must be a value between 1 and 60.

   Max retries
   The number of times that communication with the RADIUS server is attempted. This must be a value between 0 and 10.

Multi-factor authentication is available when the **RADIUS Status** changes to **Enabled**.

Deleting an AD Connector Directory

When an AD Connector directory is deleted, your on-premises directory remains intact. All instances that are joined to the directory also remain intact and remain joined to your on-premises directory. You can still use your directory credentials to log in to these instances.

For information about deleting a Simple AD directory, see Deleting a Simple AD Directory (p. 15).

To delete a connected directory

1. In the AWS Directory Service console, select only the directory to be deleted.
2. Click **Delete**. It takes several minutes for the directory to be deleted. When the directory has been deleted, it is removed from your directory list.

Managing Console Access for AWS Directory Service

AWS Directory Service allows you to grant members of your directory access to the AWS Management Console. By default, your directory members do not have access to any AWS resources. You assign IAM roles to your directory members to give them access to the various AWS services and resources. The IAM role defines the services, resources, and level of access that your directory members have.

Before you can grant console access to your directory members, your directory must have an access URL. For more information about how to view directory details and get your access URL, see Viewing Directory Information (p. 13). For more information about how to create an access URL, see Creating an Access URL (p. 13)

For more information about how to create and assign IAM roles to your directory members, see Managing IAM Roles (p. 18).

Topics

- Enabling AWS Management Console Access (p. 17)
- Disabling AWS Management Console Access (p. 18)

Enabling AWS Management Console Access

By default, console access is not enabled for any directory. To enable console access for your directory users and groups, perform the following steps:

To enable console access

1. In the AWS Directory Service console navigation pane, select **Directories**.
2. Click the directory ID link for your directory.
3. In the **Directory Details** page, select the **Apps & Services** tab.
4. In the **Services** area, click the **Manage Access** link for **AWS Management Console**.
5. In the **Enable AWS Management Console** dialog box, click **Enable Application**. Console access is now enabled for your directory.

After the IAM roles have been assigned to your directory members, they can access the console at the following URL:

```
https://<directory URL>/console
```

For example, if your directory's access URL is `example-corp.awsapps.com`, the URL to access the console is `https://example-corp.awsapps.com/console`.

Disabling AWS Management Console Access

To disable console access for your directory users and groups, perform the following steps:

To disable console access

1. In the AWS Directory Service console navigation pane, select **Directories**.
2. Click the directory ID link for your directory.
3. In the **Directory Details** page, select the **Apps & Services** tab.
4. In the **Services** area, click the **Manage Access** link for **AWS Management Console**.
5. In the **Manage access to AWS Resources** dialog box, click **Disable Access**.

Managing IAM Roles

AWS Directory Service provides the ability to give your directory users and groups access to AWS services and resources, such as access to the Amazon EC2 console. To provide this access, assign IAM roles to your AWS Directory Service users and groups. For more information, see Roles in the *Using IAM* guide.

Topics

- Editing the Trust Relationship for an Existing Role (p. 18)
- Creating a New Role (p. 19)
- Assigning a Role (p. 20)
- Viewing Role Details (p. 20)
- Removing a Role (p. 20)
- Removing a Role From a User or Group (p. 21)
- AWS Directory Service Role Policies (p. 21)

Editing the Trust Relationship for an Existing Role

You can assign your existing IAM roles to your AWS Directory Service users and groups. To do this, however, the role must have a trust relationship with AWS Directory Service. When you use AWS Directory Service to create a role using the procedure in Creating a New Role (p. 19), this trust relationship is automatically set. You only need to establish this trust relationship for IAM roles that are not created by AWS Directory Service.

To establish a trust relationship for an existing role to AWS Directory Service

1. In the navigation pane of the IAM console, click **Roles**.

   The console displays the roles for your account.
2. Click the name of the role that you want to modify, and open the **Trust Relationships** section in the details page.
3. Click **Edit Trust Relationship**.
4. Enter the following for the **Policy Document** field and click **Update Trust Policy**.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ds.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
    }
  ]
}
```

Creating a New Role

In addition, AWS Directory Service provides a set of predefined templates for common access needs. You can use these templates to create roles for your AWS Directory Service users. During this process, AWS Directory Service creates an IAM role in your account on your behalf. Because AWS Directory Service is using the IAM service to create the role on your behalf, you must provide explicit permission for this action in step 9.

> **Note**
> The user performing this task must have permission to perform the following IAM actions. For more information, see Controlling Access to AWS Directory Service Resources (p. 4).
>
> - iam:PassRole
> - iam:GetRole
> - iam:CreateRole
> - iam:PutRolePolicy

To create a new role from an AWS Directory Service template

1. In the AWS Directory Service console navigation pane, select **Directories**.
2. Click the directory ID link for your directory.
3. In the **Directory Details** page, select the **Apps & Services** tab.
4. In the **Services** area, click the **Manage Access** link for **AWS Management Console**.
5. In the **Manage Access to AWS Resource** dialog box, click **Continue**.
6. In the **AWS Management Console Access** page, click **New Role**.
7. In the **Select Role Type** page, click **Create New Role**.
8. In the **Select Role Template** page, select the template to create the role from and click **Next Step**. For more information about the templates provided by AWS Directory Service, see AWS Directory Service Role Policies (p. 21).
9. Review the information and click **Allow** to allow AWS Directory Service to create the IAM role on your behalf. When the role has been created, you will be taken to step 9 of Assigning a Role (p. 20) to select the users to apply the role to.

Assigning a Role

You can assign an existing IAM role to an AWS Directory Service user or group. The role must have a trust relationship with AWS Directory Service. For more information, see Editing the Trust Relationship for an Existing Role (p. 18).

To assign a role to an AWS Directory Service user or group

1. In the AWS Directory Service console navigation pane, select **Directories**.
2. Click the directory ID link for your directory.
3. In the **Directory Details** page, select the **Apps & Services** tab.
4. In the **Services** area, click the **Manage Access** link for **AWS Management Console**.
5. In the **Manage Access to AWS Resource** dialog box, click **Continue**.
6. In the **AWS Management Console Access** page, click **New Role**.
7. In the **Select Role Type** page, click **Use Existing Role**.
8. In the **Select Existing Role** page, select the role to add, and click **Next Step**.
9. In the **Select Users/Groups** page, select the users and groups to apply the role to. You can search for the user or group by typing all or part of the name in the text box. When enough context has been entered, a list of possible matches is displayed. Select the desired user or group and the user or group will is added to the list. Click **Next Step** when the list of users and groups to apply the role to is complete.
10. Review the information and click **Create Role Assignment** to apply the selected role to the selected AWS Directory Service users and groups.

Viewing Role Details

To view the details for a role, perform the following steps:

To view details for a role

1. In the AWS Directory Service console navigation pane, select **Directories**.
2. Click the directory ID link for your directory.
3. In the **Directory Details** page, select the **Apps & Services** tab.
4. In the **Services** area, click the **Manage Access** link for **AWS Management Console**.
5. In the **Manage Access to AWS Resource** dialog box, click **Continue**.
6. In the **AWS Console Access** page, click the role. The **Role Detail** page is displayed.

Removing a Role

To remove a role from all AWS Directory Service users or groups, perform the following steps.

To remove a role

1. In the AWS Directory Service console navigation pane, select **Directories**.
2. Click the directory ID link for your directory.
3. In the **Directory Details** page, select the **Apps & Services** tab.
4. In the **Services** area, click the **Manage Access** link for **AWS Management Console**.
5. In the **Manage Access to AWS Resource** dialog box, click **Continue**.
6. In the **AWS Console Access** page, select the role to remove, and click **Remove Role**.

7. In the **Remove Role Access** dialog box, verify that you want to remove the role and click **Remove**. The role is removed from all users and groups that the role is assigned to, but the role is not removed from your account.

Removing a Role From a User or Group

To remove a role from specific AWS Directory Service users or groups, perform the following steps.

To remove a role from a user or group

1. View the details for the role to remove as shown in Viewing Role Details (p. 20).
2. In the **Role Detail** page, in the **Assigned Users and Groups** section, select the users or groups to remove the role from and click **Remove**.
3. In the **Remove Role Access** dialog box, verify that you want to remove the role from the selected users and/or groups, and click **Remove**. The role is removed from the specified users and groups, but the role is not removed from your account.

AWS Directory Service Role Policies

AWS Directory Service provides the following role policies that allow you to quickly and easily create IAM roles for use with AWS Directory Service.

Topics

- Read Only Role (p. 21)
- Power User Role (p. 23)
- Amazon EC2 Full Access Role (p. 24)
- Amazon EC2 Read Only Role (p. 24)
- Amazon VPC Full Access Role (p. 25)
- Amazon VPC Read Only Role (p. 27)
- Amazon RDS Full Access (p. 27)
- Amazon RDS Read Only (p. 28)
- DynamoDB Full Access (p. 28)
- DynamoDB Read Only (p. 29)
- Amazon S3 Full Access (p. 29)
- Amazon S3 Read Only (p. 30)
- CloudTrail Full Access (p. 30)
- CloudTrail Read Only (p. 31)
- CloudWatch Full Access (p. 31)
- CloudWatch Read Only (p. 32)
- CloudWatch Logs Full Access (p. 32)
- CloudWatch Logs Read Only (p. 32)

Read Only Role

This role provides an AWS Directory Service user or group with read-only access to the following AWS services and resources.

- Auto Scaling
- Elastic Load Balancing

- AWS CloudFormation
- Amazon CloudFront
- AWS CloudTrail
- Amazon CloudWatch
- AWS Direct Connect
- Amazon DynamoDB
- Amazon Elastic Compute Cloud
- Amazon ElastiCache
- AWS Elastic Beanstalk
- Amazon Elastic Transcoder
- AWS Identity and Access Management
- Amazon Kinesis
- AWS OpsWorks
- Amazon Route 53
- Amazon Redshift
- Amazon Relational Database Service
- Amazon Simple Storage Service
- Amazon SimpleDB
- Amazon Simple Email Service
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- AWS Storage Gateway
- AWS Trusted Advisor

The following is the policy for this role.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "appstream:Get*",
        "autoscaling:Describe*",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:GetTemplate",
        "cloudformation:List*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "directconnect:Describe*",
        "dynamodb:GetItem",
        "dynamodb:BatchGetItem",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:Describe*",
        "elasticache:Describe*",
        "elasticbeanstalk:Check*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:RequestEnvironmentInfo",
        "elasticbeanstalk:RetrieveEnvironmentInfo",
        "elasticloadbalancing:Describe*",
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
        "iam:List*",
        "iam:Get*",
        "kinesis:Describe*",
        "kinesis:Get*",
        "kinesis:List*",
        "opsworks:Describe*",
        "opsworks:Get*",
        "route53:Get*",
        "route53:List*",
        "redshift:Describe*",
        "redshift:ViewQueriesInConsole",
        "rds:Describe*",
        "rds:ListTagsForResource",
        "s3:Get*",
        "s3:List*",
        "sdb:GetAttributes",
        "sdb:List*",
        "sdb:Select*",
        "ses:Get*",
        "ses:List*",
        "sns:Get*",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "sqs:ReceiveMessage",
        "storagegateway:List*",
        "storagegateway:Describe*",
        "trustedadvisor:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Power User Role

This role provides an AWS Directory Service user or group with full access to AWS services and resources, but does not allow management of IAM users and groups. The following is the policy for this role.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "NotAction" : "iam:*",
      "Resource" : "*"
    }
  ]
}
```

Amazon EC2 Full Access Role

This role provides an AWS Directory Service user or group with full access to the following Amazon EC2 services and resources.

- Amazon Elastic Compute Cloud
- Elastic Load Balancing
- Amazon CloudWatch
- Auto Scaling

The following is the policy for this role.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "ec2:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:*",
      "Resource" : "*"
    }
  ]
}
```

Amazon EC2 Read Only Role

This role provides an AWS Directory Service user or group with read only access to the following Amazon EC2 services and resources.

- Amazon Elastic Compute Cloud
- Elastic Load Balancing
- Amazon CloudWatch
- Auto Scaling

The following is the policy for this role.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:Describe*",
      "Resource" : "*"
    }
  ]
}
```

Amazon VPC Full Access Role

This role provides an AWS Directory Service user or group with full access to Amazon VPC services and resources. The following is the policy for this role.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AttachVpnGateway",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDhcpOptions",
        "ec2:CreateInternetGateway",
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:CreateVpcPeeringConnection",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:DeleteCustomerGateway",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcPeeringConnection",
        "ec2:DeleteVpnConnection",
        "ec2:DeleteVpnGateway",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DetachInternetGateway",
        "ec2:DetachVpnGateway",
        "ec2:DisassociateAddress",
        "ec2:DisassociateRouteTable",
        "ec2:ModifyVpcAttribute",
        "ec2:RejectVpcPeeringConnection",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Amazon VPC Read Only Role

This role provides an AWS Directory Service user or group with read only access to Amazon VPC services and resources. The following is the policy for this role.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcPeeringConnection",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

Amazon RDS Full Access

This role provides an AWS Directory Service user or group with full access to Amazon RDS services and resources. The following is the policy for this role.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:*",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcs",
        "sns:ListSubscriptions",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Amazon RDS Read Only

This role provides an AWS Directory Service user or group with read only access to Amazon RDS services and resources. The following is the policy for this role.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:Describe*",
        "rds:ListTagsForResource",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "cloudwatch:GetMetricStatistics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

DynamoDB Full Access

This role provides an AWS Directory Service user or group with full access to DynamoDB services and resources. The following is the policy for this role.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "dynamodb:*",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "sns:CreateTopic",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

DynamoDB Read Only

This role provides an AWS Directory Service user or group with read only access to DynamoDB services and resources. The following is the policy for this role.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "dynamodb:BatchGetItem",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:ListTables",
        "dynamodb:Query",
        "dynamodb:Scan",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Amazon S3 Full Access

This role provides an AWS Directory Service user or group with full access to Amazon S3 services and resources. The following is the policy for this role.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3:*",
      "Resource" : "*"
    }
  ]
}
```

Amazon S3 Read Only

This role provides an AWS Directory Service user or group with read only access to Amazon S3 services and resources. The following is the policy for this role.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

CloudTrail Full Access

This role provides an AWS Directory Service user or group with full access to CloudTrail services and resources. The following is the policy for this role.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:AddPermission",
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:GetTopicAttributes",
        "sns:ListPlatformApplications",
        "sns:ListTopics",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketNotification",
        "s3:GetBucketPolicy",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketVersioning",
        "s3:GetObject",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListBucketVersions",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudtrail:*",
      "Resource" : "*"
    }
  ]
}
```

CloudTrail Read Only

This role provides an AWS Directory Service user or group with read only access to CloudTrail services and resources. The following is the policy for this role.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

CloudWatch Full Access

This role provides an AWS Directory Service user or group with full access to CloudWatch services and resources. The following is the policy for this role.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "logs:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

CloudWatch Read Only

This role provides an AWS Directory Service user or group with read only access to CloudWatch services and resources. The following is the policy for this role.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "autoscaling:Describe*",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "logs:Get*",
        "logs:Describe*",
        "logs:TestMetricFilter",
        "sns:Get*",
        "sns:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

CloudWatch Logs Full Access

This role provides an AWS Directory Service user or group with full access to CloudWatch Logs services and resources. The following is the policy for this role.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "logs:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

CloudWatch Logs Read Only

This role provides an AWS Directory Service user or group with read only access to CloudWatch Logs services and resources. The following is the policy for this role.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:TestMetricFilter"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Directory Administration

You use the AWS Directory Service management console to perform certain directory-related actions, such as creating a new directory or deleting an existing directory. For more information, see Console Management (p. 12). After a Simple AD directory is created, most administrative functions are performed with third-party directory management tools, such as the Active Directory Administration Tools. To use these tools, you need a Windows EC2 instance that is joined to your directory domain. The following topics explain how to launch a Windows EC2 instance, join the instance to your directory domain, and install the Active Directory Administration Tools.

Topics

- Joining an Instance to an AWS Directory Service Directory (p. 33)
- Installing the Active Directory Administration Tools (p. 36)
- Creating Users and Groups (p. 39)

Joining an Instance to an AWS Directory Service Directory

To join an EC2 instance to a directory, you must launch the instance in the proper region and security group or subnet, then join the instance to the directory.

Topics

- Launching an Instance (p. 33)
- Joining an Instance (p. 34)

Launching an Instance

To launch an instance to be joined to a directory in a VPC

1. Sign in to the AWS Management Console and open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. From the region selector in the navigation bar, select the same region as the existing directory.
3. From the Amazon EC2 console dashboard, click **Launch Instance**.
4. Select the appropriate AMI.
5. In the **Configure Instance Details** page of the launch wizard, make the following selections:

Network

Select the VPC that your directory was created in.

Subnet

Select one of the public subnets in your VPC. The subnet you select must have all external traffic routed to an Internet gateway. If this is not the case, you won't be able to connect to the instance remotely.

Auto-assign Public IP

The instance must have a public IP address. Set this to **Enable** to assign a public IP address automatically, or assign an Elastic IP address to the instance after it is launched.

6. The security group you select for the instance must allow remote access to the instance from your network.

Joining an Instance

The following topics explain how to join different types of Amazon EC2 instances to an AWS Directory Service directory.

Topics

- Get the DNS Server Addresses (p. 34)
- Joining a Windows Instance to an AWS Directory Service Directory (p. 34)

Get the DNS Server Addresses

To join an Amazon EC2 instance to your directory, you need the IP addresses of the DNS servers in the AWS Directory Service directory. To obtain these IP addresses, in the AWS Directory Service console navigation pane, click **Directories**, and click the directory ID. In the **Directory Details** section, note the **DNS IP Address** values.

Joining a Windows Instance to an AWS Directory Service Directory

To join an existing Amazon EC2 Windows instance to an AWS Directory Service directory, the instance must be launched as specified in Launching an Instance (p. 33).

To join a Windows instance to an AWS Directory Service directory

1. Connect to the instance using any Remote Desktop Protocol client.
2. Open the TCP/IPv4 properties dialog box on the instance.

   a. Open **Network Connections**.

      Tip

      You can open **Network Connections** directly by running the following from a command prompt on the instance.

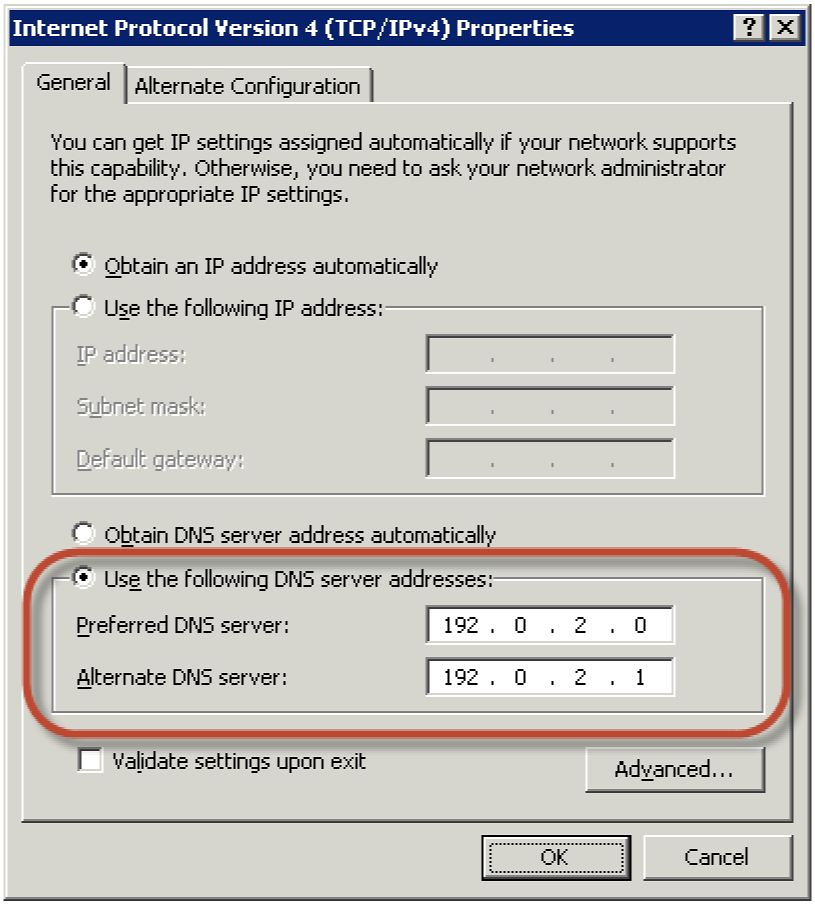
      ```
      %SystemRoot%\system32\control.exe ncpa.cpl
      ```

   b. Right-click any enabled network connection and select **Properties**.

   c. In the connection properties dialog box, double-click **Internet Protocol Version 4**.

3. Select **Use the following DNS server addresses**, change the **Preferred DNS server** and **Alternate DNS server** addresses to the IP addresses of the AWS Directory Service-provided DNS servers,

and click **OK**. For more information about how to obtain the DNS server IP address, see Get the DNS Server Addresses (p. 34).



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 0 . 2 . 0

Alternate DNS server: 192 . 0 . 2 . 1

□ Validate settings upon exit

4. Open the **System Properties** dialog box for the instance, select the **Computer Name** tab, and click **Change**.

   Tip
   You can open the **System Properties** dialog box directly by running the following from a command prompt on the instance.

   ```
   %SystemRoot%\system32\control.exe sysdm.cpl
   ```

5. In the **Member of** field, select **Domain**, enter the fully-qualified name of your AWS Directory Service directory, and click **OK**.
6. When prompted for the name and password for the domain administrator, enter `Administrator` for the name and the password specified when the AWS Directory Service directory was created.
7. After you receive the message welcoming you to the domain, restart the instance to have the changes take effect.

Now that your instance has been joined to the domain, you can log into that instance remotely and install utilities to manage the directory, such as adding users and groups.

Installing the Active Directory Administration Tools

To manage your directory from an EC2 Windows instance, you need to install the Active Directory Domain Services and Active Directory Lightweight Directory Services Tools on the instance.

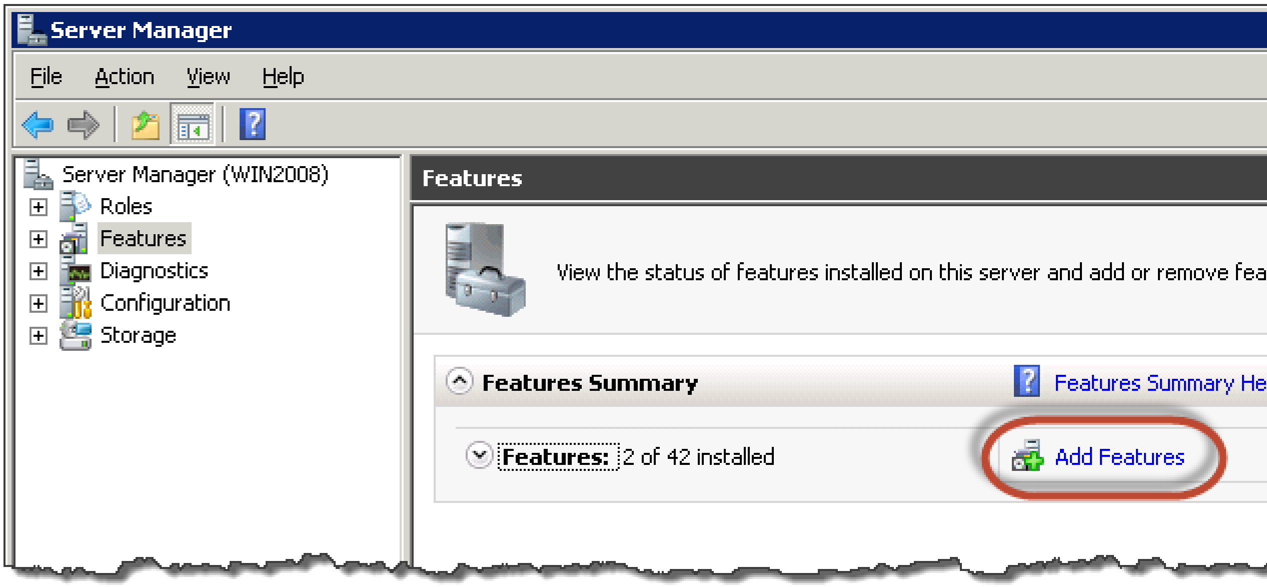
Topics

- Install the Active Directory administration tools on Windows Server 2008 (p. 36)
- Install the Active Directory administration tools on Windows Server 2012 (p. 37)

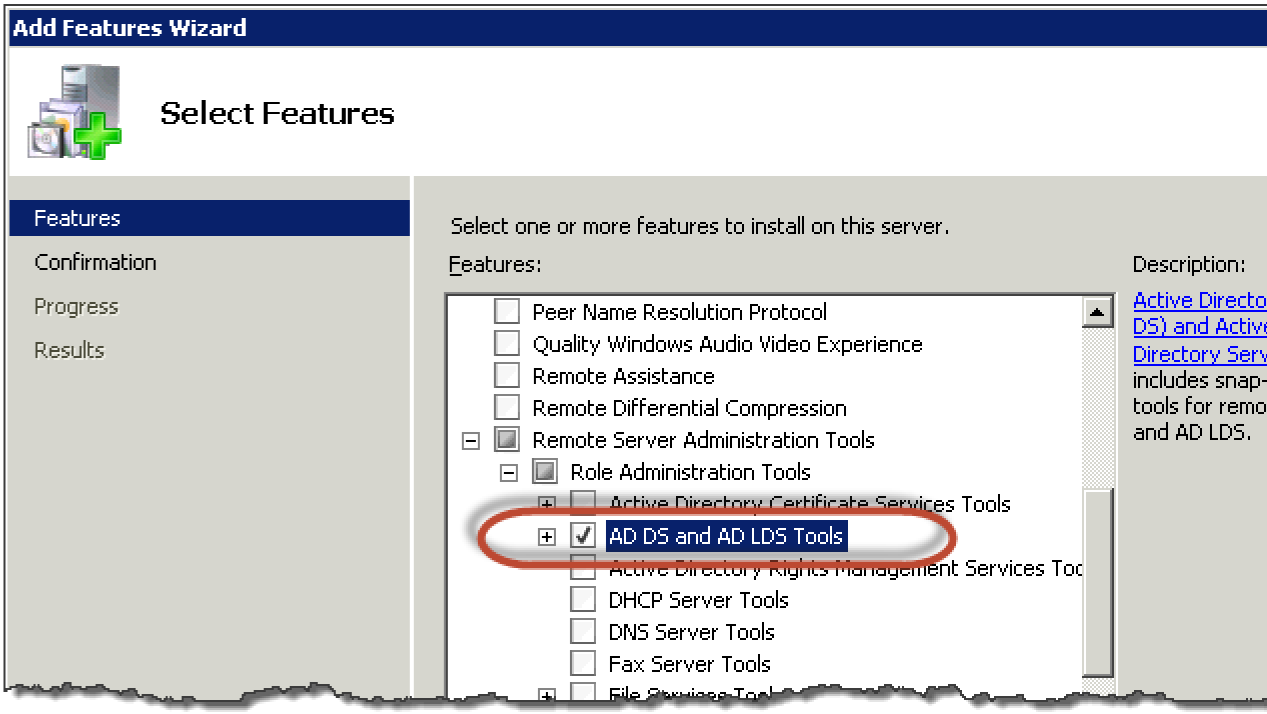
Install the Active Directory administration tools on Windows Server 2008

To install the Active Directory administration tools on Windows Server 2008

1. Open Server Manager by clicking **Start**, **Administrative Tools**, **Server Manager**.
2. In the **Server Manager** tree pane, select **Features**, and click **Add Features**,



3. In the **Add Features Wizard**, open **Remote Server Administration Tools**, **Role Administration Tools**, select **AD DS and AD LDS Tools**, and click **Next**.



Select one or more features to install on this server.

Features:

- ☐ Peer Name Resolution Protocol
- ☐ Quality Windows Audio Video Experience
- ☐ Remote Assistance
- ☐ Remote Differential Compression
- ⊟ ▣ Remote Server Administration Tools
  - ⊟ ▣ Role Administration Tools
    - ⊞ ☐ Active Directory Certificate Services Tools
    - ⊞ ☑ AD DS and AD LDS Tools
    - ☐ Active Directory Rights Management Services Toc
    - ☐ DHCP Server Tools
    - ☐ DNS Server Tools
    - ☐ Fax Server Tools
    - ⊞ ☐ File Services Tool

Description:

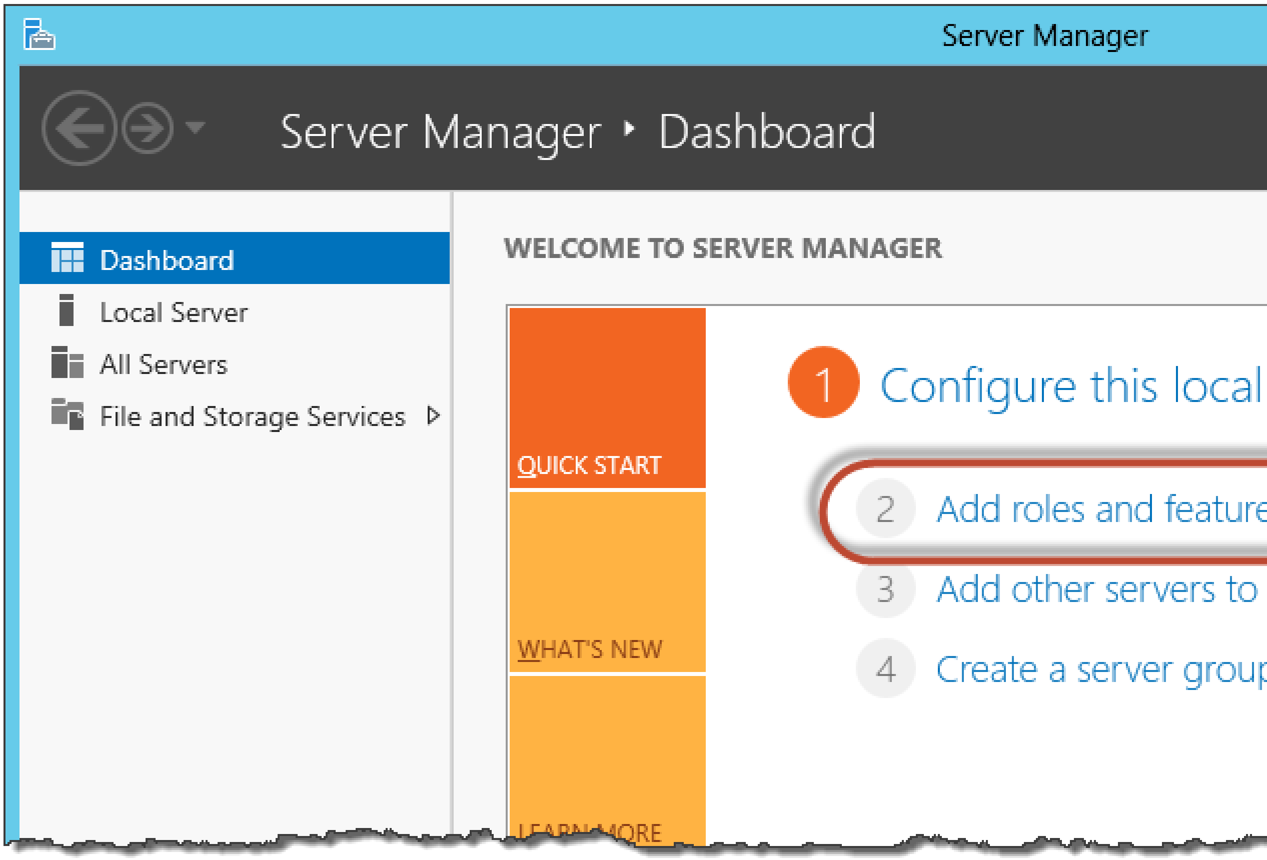
Active Directo
DS) and Active
Directory Serv
includes snap-
tools for remo
and AD LDS.

4. Review the information and click **Install**. The feature installation requires that the instance be restarted. When the instance has restarted, the Active Directory Domain Services and Active Directory Lightweight Directory Services Tools are available on the **Start** menu, under **All Programs** > **Administrative Tools**.

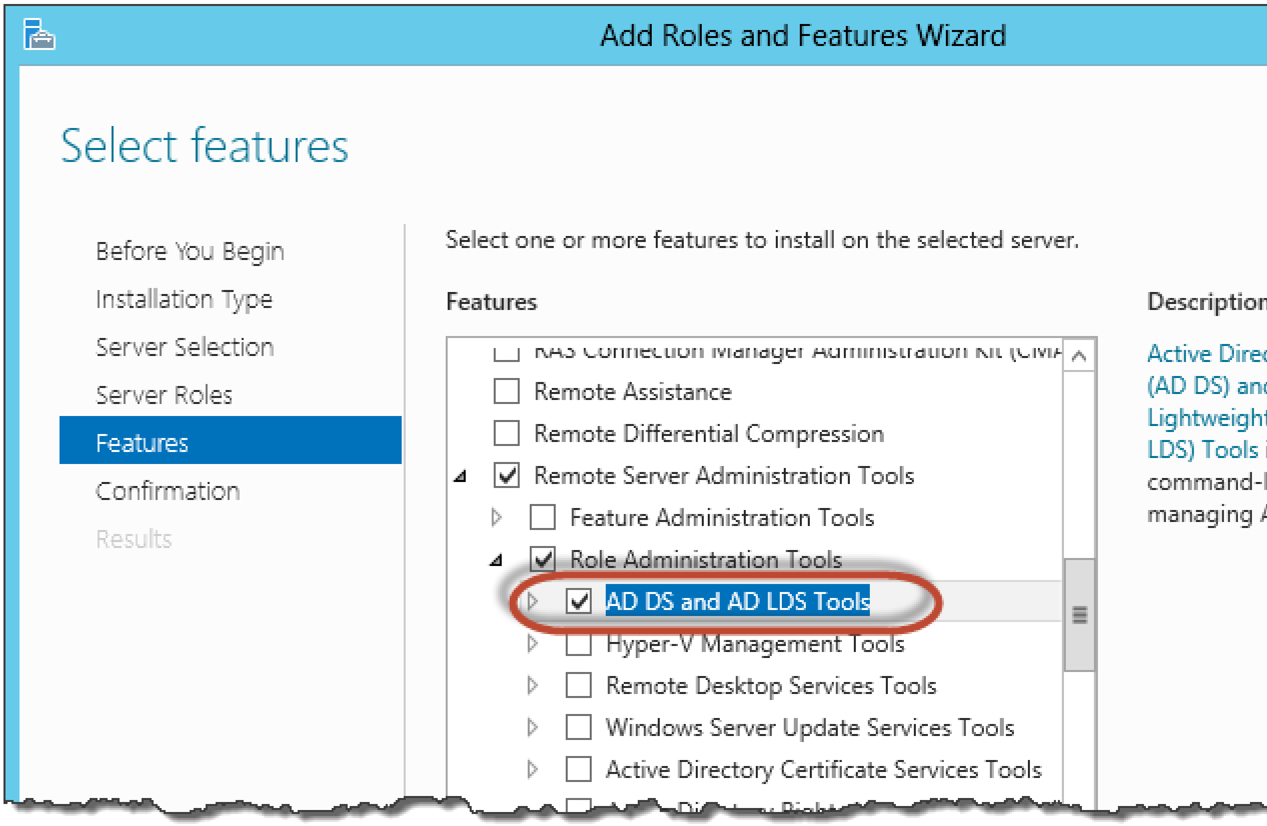
Install the Active Directory administration tools on Windows Server 2012

To install the Active Directory administration tools on Windows Server 2012

1. Open Server Manager by from the Start screen by clicking **Server Manager**.
2. In the **Server Manager Dashboard**, click **Add roles and features**,



3. In the **Add Roles and Features Wizard** click **Installation Type**, select **Role-based or feature-based installation**, and click **Next**.
4. Under **Server Selection**, make sure the local server is selected, and click **Features**.
5. In the **Features** tree, open **Remote Server Administration Tools**, **Role Administration Tools**, select **AD DS and AD LDS Tools**, and click **Next**.



Select one or more features to install on the selected server.

- ☐ RAS Connection Manager Administration Kit (CMA
- ☐ Remote Assistance
- ☐ Remote Differential Compression
- ☑ Remote Server Administration Tools
  - ☐ Feature Administration Tools
  - ☑ Role Administration Tools
    - ☑ AD DS and AD LDS Tools
    - ☐ Hyper-V Management Tools
    - ☐ Remote Desktop Services Tools
    - ☐ Windows Server Update Services Tools
    - ☐ Active Directory Certificate Services Tools
    - ☐ Active Directory Rights

Active Direc
(AD DS) and
Lightweight
LDS) Tools i
command-l
managing A

6. Review the information and click **Install**. When the feature installation is finished, the Active Directory Domain Services and Active Directory Lightweight Directory Services Tools are available on the Start screen in the **Administrative Tools** folder.

Creating Users and Groups

You can create users and groups with the Active Directory Users and Computers tool, which is part of the Active Directory Domain Services and Active Directory Lightweight Directory Services tools. Users represent individual people or entities that have access to your directory. Groups are very useful for giving or denying privileges to groups of users, rather than having to apply those privileges to each individual user. If a user moves to a different organization, you move that user to a different group and they automatically receive the privileges needed for the new organization.

The following examples demonstrate how to create a user, create a group, and add the user to the group. To create users and groups in a AWS Directory Service directory, you must be connected to a Windows instance that is a member of the AWS Directory Service directory, and be logged in as a user that has privileges to create users and groups.

To create a user

1. Open the Active Directory Users and Computers tool. There is a shortcut to this tool in the **Administrative Tools** folder.

   Tip
   You can run the following from a command prompt on the instance to open the Active Directory Users and Computers tool box directly.

```
%SystemRoot%\system32\dsa.msc
```

2. In the directory tree, open your directory and select the **Users** folder.
3. On the **Action** menu, click **New**, and then click **User** to open the new user wizard.
4. In the first page of the new user wizard, enter the following values and click **Next**.

   First name
   `Mary`

   Last name
   `Major`

   User logon name
   `marym`

5. In the second page of the new user wizard, enter a temporary password for **Password** and **Confirm Password**. Make sure the **User must change password at next logon** option is selected. None of the other options should be selected. Click **Next**.
6. In the third page of the new user wizard, verify that the new user information is correct and click **Finish**. The new user will appear in the **Users** folder.

To create a group

1. Open the Active Directory Users and Computers tool. There is a shortcut to this tool in the **Administrative Tools** folder.

   Tip
   You can run the following from a command prompt on the instance to open the Active Directory Users and Computers tool box directly.

   ```
   %SystemRoot%\system32\dsa.msc
   ```

2. In the directory tree, open your directory and select the **Users** folder.
3. On the **Action** menu, click **New**, and then click **Group** to open the new group wizard.
4. Enter **`Division Managers`** for the **Group name**, select **Global** for the **Group scope**, and select **Security** for the **Group type**. Click **OK**. The new group, **Division Managers**, appears in the **Users** folder.

To add a user to a group

1. Open the Active Directory Users and Computers tool. There is a shortcut to this tool in the **Administrative Tools** folder.

   Tip
   You can run the following from a command prompt on the instance to open the Active Directory Users and Computers tool box directly.

   ```
   %SystemRoot%\system32\dsa.msc
   ```

2. In the directory tree, open your directory, select the **Users** folder, and select the **Division Managers** group.
3. On the **Action** menu, click **Properties** to open the properties dialog box for the **Division Managers** group.

4. Select the **Members** tab and click **Add...**.
5. For **Enter the object names to select**, enter `marym` and click **OK**. **Mary Major** is displayed in the **Members** list. Click **OK** again to update the group membership.
6. Verify that Mary Major is now a member of the **Division Managers** group by selecting **Mary Major** in the **Users** folder, click **Properties** in the **Action** menu to open the properties dialog box for Mary Major. Select the **Member Of** tab. **Division Managers** is in the list of groups that Mary Major belongs to.

Troubleshooting AWS Directory Service Administration Issues

Topics

- I receive a "DNS unavailable" error when I try to connect to my on-premises directory (p. 42)
- I receive a "Connectivity issues detected" error when I try to connect to my on-premises directory (p. 42)
- I receive an "SRV record" error when I try to connect to my on-premises directory (p. 43)

I receive a "DNS unavailable" error when I try to connect to my on-premises directory

You receive an error message similar to the following when connecting to your on-premises directory:

```
DNS unavailable (TCP port 53) for IP: <DNS IP address>
```

AD Connector must be able to communicate with your on-premises DNS servers via TCP and UDP over port 53. Verify that your security groups and on-premises firewalls allow TCP and UDP communication over this port. For more information, see AD Connector Prerequisites (p. 5).

I receive a "Connectivity issues detected" error when I try to connect to my on-premises directory

You receive an error message similar to the following when connecting to your on-premises directory:

```
Connectivity issues detected: LDAP unavailable (TCP port 389) for IP: <IP ad
dress>
```

```
Kerberos/authentication unavailable (TCP port 88) for IP: <IP address>
Please ensure that the listed ports are available and retry the operation.
```

AD Connector must be able to communicate with your on-premises domain controllers via TCP and UDP over the following ports. Verify that your security groups and on-premises firewalls allow TCP and UDP communication over these ports. For more information, see AD Connector Prerequisites (p. 5).

- 88 (Kerberos)
- 389 (LDAP)

I receive an "SRV record" error when I try to connect to my on-premises directory

You receive an error message similar to one or more of the following when connecting to your on-premises directory:

```
SRV record for LDAP does not exist for IP: <DNS IP address>

SRV record for Kerberos does not exist for IP: <DNS IP address>
```

AD Connector needs to obtain the `_ldap._tcp.<DnsDomainName>` and `_kerberos._tcp.<DnsDomainName>` SRV records when connecting to your directory. You will get this error if the service cannot obtain these records from the DNS servers that you specified when connecting to your directory. Make sure that your DNS servers contains these SRV records. For more information about SRV records, go to SRV Resource Records on Microsoft TechNet.

Tutorials

The following tutorials will help you perform detailed tasks using the AWS Directory Service service.

Topics

- Tutorial: Creating a Simple AD Directory (p. 44)

Tutorial: Creating a Simple AD Directory

The following tutorial walks you through all of the steps necessary to set up an AWS Directory Service Simple AD directory. This tutorial explains how to complete the following tasks:

- Create a VPC for use with AWS Directory Service.
- Create a Simple AD directory in your VPC.

Topics

- Prerequisites (p. 44)
- Notes (p. 44)
- Step 1: Create and Configure Your VPC (p. 45)
- Step 2: Create the Directory (p. 46)

Prerequisites

This tutorial assumes the following:

- You have an active AWS account.
- Your account has not reached its limit of VPCs for the region in which you want to use AWS Directory Service.
- You do not have an existing VPC in the region with a CIDR of 10.0.0.0/16.

Notes

This tutorial is intended to get you started with AWS Directory Service quickly and easily, but is not intended to be used in a large-scale production environment. The following notes provide additional information.

- For more information about Amazon VPC, see the following topics in the *Amazon VPC User Guide*:
  - What is Amazon VPC?
  - Subnets in Your VPC
- For more information about managing your directory, see Console Management (p. 12).

Step 1: Create and Configure Your VPC

The following sections demonstrate how to create and configure a VPC for use with AWS Directory Service.

Topics

- Create a New VPC (p. 45)
- Add a Second Subnet (p. 46)

Create a New VPC

This tutorial uses one of the VPC creation wizards to create the following:

- The VPC
- One of the subnets
- An Internet gateway

To create your VPC using the VPC wizard

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, click **VPC Dashboard**. If you do not already have any VPC resources, locate the **Your Virtual Private Cloud** area of the dashboard and click **Get started creating a VPC**. Otherwise, click **Start VPC Wizard**.
3. Select the second option, **VPC with a Single Public Subnet**, and then click **Select**.
4. Enter the following information into the wizard and click **Create VPC**.

   IP CIDR block
   `10.0.0.0/16`

   VPC name
   `ADS VPC`

   Public subnet
   `10.0.0.0/24`

   Availability Zone
   No Preference

   Subnet name
   `ADS Subnet 1`

   Enable DNS hostnames
   Leave default selection

   Hardware tenancy
   Default

5. It takes several minutes for the VPC to be created. After the VPC is created, proceed to the following section to add a second subnet.

Add a Second Subnet

AWS Directory Service requires two subnets in your VPC, and each subnet must be in a different Availability Zone. The VPC wizard only creates one subnet, so you must manually create the second subnet, and specify a different Availability Zone than the first subnet.

Create the second subnet by perform the following steps:

To create a subnet

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, select **Subnets**, select the subnet with the name `ADS Subnet 1`, and select the **Summary** tab at the bottom of the page. Make a note of the Availability Zone of this subnet.
3. Click **Create Subnet** and enter the following information in the **Create Subnet** dialog box and click **Yes, Create**.

   Name tag
   `ADS Subnet 2`

   VPC
   Select your VPC. This is the VPC with the name `ADS VPC`.

   Availability Zone
   Select any Availability Zone other than the one noted in step 2. The two subnets used by AWS Directory Service must reside in different Availability Zones.

   CIDR Block
   `10.0.1.0/24`

Step 2: Create the Directory

To create your AWS Directory Service Simple AD directory, perform the following steps. For more information about this process, see Creating a Directory with Simple AD (p. 9).

To create a Simple AD directory

1. Open the AWS Directory Service console for your desired region.
2. In the navigation pane, select **Directories**, click **Set up Directory**, then select **Create Simple AD**.
3. Enter the following fields.

   Directory DNS
   The fully-qualified name for the directory, such as `corp.example.com`.

   NetBIOS name
   The short name for the directory, such as `CORP`.

   Administrator password
   The password for the directory administrator. The directory creation process creates an administrator account with the username `Administrator` and this password.

   The directory administrator password is case-sensitive and must be between 8 and 64 characters in length, inclusive. It must also contain at least one character from three of the following four categories:

   - Lowercase letters (a-z)
   - Uppercase letters (A-Z)
   - Numbers (0-9)
   - Non-alphanumeric characters (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Confirm password
Re-enter the administrator password.

Description
An optional description for the directory.

Directory Size
Select the size of the directory.

4. Enter the following fields in the **VPC Details** section and click **Next Step**.

   VPC
   The VPC for the directory.

   Subnets
   Select the subnets for the directory servers. The two subnets must be in different Availability Zones.

5. Review the directory information and make any necessary changes. When the information is correct, click **Create Simple AD**.

   It takes several minutes for the directory to be created. When it has been successfully created, the **Status** value changes to `Active`.

AWS Directory Service Limits

The following are the default limits for AWS Directory Service. Each limit is per region unless otherwise noted.

AWS Directory Service Limits

Resource	Default Limit
Simple AD directories	2
AD Connector directories	2
Manual snapshots	5 per Simple AD

If you need to increase your limit in a region, you can request a limit increase.

To request a limit increase

1. Go to the AWS Support Center page, sign in, if necessary, and click **Open a new case**.
2. Under **Regarding**, select **Service Limit Increase**.
3. Under **Limit Type**, select **AWS Directory Service**.
4. Fill in all of the necessary fields in the form and click the button at the bottom of the page for your desired method of contact.

Document History

The following table describes the important changes since the last release of the *AWS Directory Service Administrator Guide*.

- **Latest documentation update:** October 21st, 2014

Change	Description	Date Changed
New guide	This is the first release of the *AWS Directory Service Administrator Guide*.	October 21st, 2014