One Identity Active Roles

Active Roles on Azure and AWS User Guide

Copyright 2022 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (http://www.OneIdentity.com) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at http://www.OneIdentity.com/legal/patents.aspx.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

Active Roles Active Roles on Azure and AWS User Guide
Updated - July 2022
Version - 7.6

Contents

Marketplace images **4**
Hardware requirements 4
Supported configurations 5

Creating virtual machines on the cloud **8**
Prerequisites 8
Communication ports 8
Opening ports in Azure 9
Opening ports in AWS 9
Creating Azure virtual machine 9
Creating EC2 instance on AWS cloud platform 10

Supported environment configurations **12**
Cloud-only setup 12
Cloud-only setup on Azure 13
Cloud-only setup on AWS 13
Cross-cloud setup 13
Cross-cloud setup between Azure and AWS 14
Hybrid on-premises setup 15
Site-to-Site VPN connection on Azure 16
Site-to-Site VPN connection on AWS 17

About us **18**
Contacting us 18
Technical support resources 18

1

Marketplace images

Active Roles supports AWS and Azure cloud platforms. You can utilize Active Roles Marketplace images available on Azure or AWS Marketplace using the available organization subscription. The below images contain Active Roles 7.6 preinstalled but not configured with different Active Roles components:

- Active Roles Service on Windows Server 2016
- Active Roles Web on Windows Server 2016
- Active Roles Service and Web on Windows Server 2016
- Active Roles Service on Windows Server 2019
- Active Roles Web on Windows Server 2019
- Active Roles Service and Web on Windows Server 2019

IMPORTANT:

- Above mentioned images contain specific components of Active Roles 7.6 according to their respective configurations, such as, Service, Web, or both. For additional Active Roles components, you should modify the Active Roles installation. For more information on modifying Active Roles installation, see the *Active Roles Quick Start Guide*.
- To install the relevant hotfix along with the Active Roles Marketplace image, see the **Software Downloads** section on the One Identity support site.

CAUTION: Currently, AWS EC2 instances that are preinstalled with Active Roles are not available on AWS Marketplace. However, with the AWS subscription you can create virtual machines or EC2 instances, install Active Roles, and configure them using the prerequisites and the procedure provided in the document.

Hardware requirements

This section briefs about the minimum hardware requirements to ensure optimal performance.

- A server with Microsoft Windows Server 2016, 4 Core vCPUs , and 8GB RAM- Used as a Domain Controller with ADFS services that connects to Azure hosted AD.
- A server with Microsoft Windows Server 2016, 4 Core vCPUs, and 8GB RAM- Used as an Exchange Server
- A server with Microsoft Windows Server 2016, 1 Core vCPUs, and 2GB RAM- Used for Administration activity
- A server with Microsoft Windows Server 2016, 1 Core vCPUs, 2GB RAM- Used for ARS Administrator portal, Self-Service portal, and Help desk portal.
- A server with Microsoft Windows Server 2016 R2, SQL Server 2012 SP4, 1 Core vCPUs, and 2GB RAM- Used as a Database Server.
- A server with Microsoft Windows Server 2016, 8 Core vCPUs, and 16GB RAM- Used for Synchronization services.

NOTE: The minimum hardware requirement specified here is applicable for small environments. For a more detailed information about the recommended configuration on small and medium environment, see Supported configurations.

Supported configurations

This topic briefs about the supported configurations in Azure and AWS Marketplace images.

Before choosing a type of Azure VM or AWS EC2 instance, see the links available here, that help in selecting the suitable configuration based on the requirement.

- For Azure- https://azure.microsoft.com/en-us/pricing/details/virtual-machines/windows/
- For AWS- https://aws.amazon.com/ec2/instance-types/

The following examples briefly outline the types of environments supported by Active Roles on Azure and AWS Virtual machine configurations:

- **Small**
  - Active Directory environment with 15000 AD accounts.
  - Dynamic Groups with 3000 Users.
  - Group Families on Department/location attributes.
  - 10 Virtual Attributes on the User Objects.
  - Managed Units with 10 Virtual Attributes.
  - Enable Mailbox provisioning on Exchange server.
  - Script Policies for Provisioning Home Folders, set attributes such Description, Manager, property generation policy, de-provisioning policy.
  - Quest Authentication Services Add-ON.

- **Medium**
  - Active Directory environment with 50000 AD accounts.
  - Dynamic Groups with 10000 Users.
  - Group Families on Department/location attributes.
  - 10 Virtual Attributes on the User Objects.
  - Managed Units with 10 Virtual Attributes.
  - Enable Mailbox provisioning on Exchange server.
  - Script Policies for Provisioning Home Folders, set attributes such Description, Manager, property generation policy, de-provisioning policy.
  - Workflows to modify the user objects.
  - Quest Authentication Services Add-ON.

IMPORTANT: One Identity recommends to use the Azure-F4s series for environment with 30 to 50 concurrent users for optimal performance. For more information on the supported configurations, see the table below.

CAUTION:

- **Currently, AWS EC2 instances that are preinstalled with Active Roles are not available on AWS Marketplace. However, with the AWS subscription you can create virtual machines or EC2 instances, install Active Roles, and configure them using the prerequisites and the procedure provided in the Active Roles on Azure and AWS Marketplace User Guide.**
- **The configurations mentioned here have limited support depending on the quantity of Dynamic Groups (DG), Managed Units (MU), policies, scripts, workflows, and other infrastructural considerations. One Identity reserves the right to withhold support until the customer moves the configuration inline with the Supported configurations.**

Legend:

- **W**- Web service
- **S**- Active Roles service
- **WS**- Web service and Active Roles service

Table 1: Fully Supported Platforms for Active Roles Deployments

Environment	VM Configuration	Concurrent Users	Active Roles Components					
			Windows 2016			Windows 2019		
			W	S	WS	W	S	WS
Small	Azure- B4ms (4 vCPU 16GB)	50	No	No	No	No	No	Yes
	Azure-B2ms (2vCPU 8GB)	50	Yes	Yes	Yes	Yes	Yes	No
	Azure-B2s(2vCPU 4GB)	30	Yes	Yes	Yes	Yes	Yes	No
	Azure-B2s(2vCPU 4GB)	10	No	No	No	No	No	
	AWS-t2.large (2vCPU 8GB)	50	No	Yes	Yes	Yes	Yes	No
	AWS-t2.xlarge (4vCPU 16GB)	50	Yes	No	No	No	No	Yes
	AWS-t2.medium (2vCPU 4GB)	50	Yes	Yes	Yes	Yes	Yes	Yes
Medium	Azure-B2s (2vCPU 4GB)	10	Yes	Yes	Yes	Yes	Yes	Yes
	Azure-B2 series	30	Yes	Yes	Yes	Yes	Yes	No
	Azure-F4s series	30	Yes	Yes	Yes	Yes	Yes	Yes
	Azure-F4s series	50	Yes	Yes	Yes	Yes	Yes	Yes
	AWS- t2.xlarge (4vCPU 16GB)	50	Yes	Yes	Yes	Yes	Yes	Yes
	AWS-t3a.medium (2vCPU 4GB)	10	Yes	Yes	Yes	Yes	Yes	Yes

Creating virtual machines on the cloud

This topic briefs about creating virtual machines on the cloud. Before creating virtual machines on the cloud, ensure that the prerequisites are met.

Prerequisites

- Configure the domain controller before deploying the Active Roles virtual machine on the cloud.
- Configure the SQL server before deploying the Active Roles virtual machine on the cloud.
    - The health of the Active Roles Administration service depends on the access permissions the Administration service has on the SQL Server. For the list of required permissions see, SQL Server permissions in the Active Roles Quick Start Guide. For additional SQL Server port requirements, see https://docs.microsoft.com/en-us/sql/sql-server/install/configure-the-windows-firewall-to-allow-sql-server-access?view=sql-server-ver15.
- The domain controller and SQL server must be accessible to the Active Roles virtual machine on cloud.
- In the case of the on-premises hybrid configuration, add a domain controller and connect Active Roles to it.
- In case of an hybrid on-premises or cross-cloud configuration, network must be setup with the domain controller and SQL server should be accessible to Active Roles virtual machine on the cloud.

Communication ports

If the environment managed by Active Roles is protected by a firewall, then the applicable ports must be open between the Active Roles Administration Service and the managed

environment. For example, if there is a firewall between Active Roles and DNS, then port 15172 must be open (Inbound/Outbound) on the Active Roles host (or the firewall between Active Roles and Exchange) and port 53 must be open on the DNS server (or the firewall between Active Roles and DNS).

For the list of communication ports, see *Active Roles Administration Guide*. For additional information on communication ports, see https://support.oneidentity.com/kb/30256/communication-ports-for-active-roles-service-and-clients.

Opening ports in Azure

Create a network filter on a subnet or a VM network interface to open a port or create an endpoint to a virtual machine (VM) on Azure. You select the filters to control both inbound and outbound traffic, on a network security group attached to the resource that receives the traffic.

For more information on opening ports for Azure virtual machine, see https://docs.microsoft.com/en-us/azure/virtual-machines/windows/nsg-quickstart-portal.

Opening ports in AWS

A security group acts as a virtual firewall that controls the traffic for one or more instances. You can add rules to each security group that allow traffic to or from its associated instances. If you have requirements that are not met by the security groups, you can maintain your own firewall on any of your instances apart from using the security groups.

Ensure for Windows-based AMIs an RDP port (3389) by default is open. WINRM (port 5985) must be open to the required IP address. For more information on opening ports for AWS instance, see https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ec2-security-groups.html#adding-security-group-rule.

Creating Azure virtual machine

1. Log on to the Azure portal with appropriate credentials.
2. On the search bar, enter **Marketplace**.
3. In Marketplace, search for the **One Identity Active Roles** offer.
4. Select the required Active Roles component configuration image.
    - Service Only
    - Web Only

- Service + Web

5. Create an Azure virtual machine by providing appropriate inputs.

   For Active Roles Service only or Web only Components, the recommended configuration **F4s series** or any other equivalent configuration.

6. After the virtual machine is created and running, join the virtual machine into your already configured domain as mentioned in the prerequisites topic. For more information on joining a virtual machine to a domain, see https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/join-a-computer-to-a-domain.

   NOTE: You can also use Azure artifact to join virtual machine to a domain.

7. Refer the *Active Roles Administration Guide* and the *Active Role Quick Start Guide* to proceed further with the configuration steps, as the process is similar to that of the on-premises environment.

Creating EC2 instance on AWS cloud platform

CAUTION: Currently, AWS EC2 instances that are preinstalled with Active Roles are not available on AWS Marketplace. However, with the AWS subscription you can create virtual machines or EC2 instances, install Active Roles, and configure them using the prerequisites and the procedure provided in the document.

1. Log on to the AWS Console with appropriate credentials.
2. On the search bar, enter **AWS Marketplace** and click **Discover Products**..
3. Search for the **One Identity Active Roles** offer.
4. Select the required Active Roles component configuration image.
   - Service Only
   - Web Only
   - Service + Web
5. Launch an AWS EC2 instance with required configuration.
6. For Active Roles Service only, Web only, or Service + Web Components, the minimum recommended configuration is **General purpose t2.xlarge – 4vCPUs, 16 GB RAM with Moderate Network Performance** or any other equivalent configuration.
7. After the virtual machine is created and running, join the virtual machine into your already configured domain as mentioned in the prerequisites topic. For more information on joining a virtual machine to a domain, see

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/join_windows_instance.html.

8. Refer the *Active Roles Administration Guide* and the *Active Role Quick Start Guide* to proceed further with the configuration steps, as the process is similar to that of the on-premises environment.

3

Supported environment configurations

Active Roles support the following environment configurations.

- **Cloud only**- All required resources for Active Roles to function exist on the same cloud platform.
- **Cross-cloud**- Some of the resources for Active Roles to function can be on another cloud platform. For example, AWS with Azure.

  NOTE: Currently, Active Roles support AWS with Azure or Azure with AWS cloud platforms.
- **Hybrid on-premises**- Some of the resources for Active Roles to function can be on cloud and on the on-premises environment.

CAUTION:

- **One Identity does not support or assist in configuring or troubleshooting network connectivity or performance issues related to network.**
- **Currently, AWS EC2 instances that are preinstalled with Active Roles are not available on AWS Marketplace. However, with the AWS subscription you can create virtual machines or EC2 instances, install Active Roles, and configure them using the prerequisites and the procedure provided in the document.**

Cloud-only setup

In the cloud-only setup, all the resources required for Active Roles must be on same cloud platform.

Cloud-only setup on Azure

CAUTION: Ensure that the virtual network is setup and virtual machines on Azure with the required resources, such as Active Directory, Exchange, and SQL are installed and configured. The Azure environment setup must be in same region for better performance.

Configuring Azure VM with Active Roles

1. Log on to the Azure portal with appropriate credentials.
2. Search for Active Roles Marketplace offer and create a virtual machine by providing required details.
3. Join the Active Roles installed virtual machine into the already created domain.
4. Configure Active Roles using the **Active Roles Configuration Center**.

For more information on configuring, see *Active Role Quick Start Guide* to proceed further with the configuration steps are similar to the on-premises configuration process.

Cloud-only setup on AWS

CAUTION: Ensure that VPC (virtual private cloud), subnets, and route tables are already setup. EC2 Instances with Active Directory, Exchange and SQL are already installed and configured.

Cconfiguring AWS EC2 instance with Active Roles

1. Log into AWS Management Console.
2. Create an instance using Active Roles Marketplace AMI.
3. Join the Active Roles installed virtual machine into the already created domain.
4. Configure Active Roles using the **Active Roles Configuration Center**.

For more information on configuring, see *Active Role Quick Start Guide* to proceed further with the configuration steps are similar to the on-premises configuration process.

Cross-cloud setup

In Cross-cloud setup, some of the resources for Active Roles can be on another cloud platform. Example, AWS with Azure.

NOTE:

- Currently, Active Roles support AWS with Azure or Azure with AWS cloud platforms.
- One Identity recommends to use Active Roles and SQL Server on the same region.
- One Identity recommends to setup a Site-to-Site VPN between Azure and AWS.

Cross-cloud setup between Azure and AWS

This topic briefs about creating a Site to Site VPN connection between Azure and AWS cloud platforms. However, you can also create a VPN connection between Azure and AWS cloud platforms through any other alternative methods.

IMPORTANT: The IP Addresses mentioned in the steps below are used as an example. You can choose the IP addresses based on specific requirements.

Primary settings to be performed on Azure

1. Create a virtual network. For example:
    - Address space: For example 10.0.0.0/16.
    - Subnet Address range: For example 10.0.0.0/24.
2. Create gateway subnet. For example 10.0.254.0/24.
3. Create a Public IP Address.
4. Create a virtual network gateway:
    a. In the **Gateway Type** field, select VPN.
    b. In the **VPN Type** field, select Route-based.
    c. In the **Public IP Address** field, use the IP address created earlier.

    NOTE: The deployment of the Azure Virtual Network Gateway may take several minutes to complete.

Primary settings to be performed on AWS side

1. Create a VPC.
2. Create a subnet. For example, 192.168.0.0/24.
3. Create an Internet gateway.
4. Attach the Internet gateway to the VPC.
5. Specify the Internet gateway at 0.0.0.0/0 in the route table.
6. Create a customer gateway. Check and enter the Public IP Address from Azure's virtual network gateway.
7. Create a Virtual Private Gateway and attach it to the VPC that is already created.
8. Create a Site-to-Site VPN connection by choosing Customer Gateway and Virtual Private Gateway created above and select Static from the Routing options and provide a static IP Prefix, for example, 10.0.0.0/24.

9. After the VPN connection is available, click **Download Configuration** to download the configuration. Download the file with the following options:
    - Vendor- Generic
    - Platform- Generic
    - Software- Vendor Agnostic

    NOTE: The file is downloaded as a .txt file with the network details.

Final steps to create tunnel between two sites

1. On Azure, create a local network gateway. Provide the **IP Address** available in the downloaded configuration file from AWS. You can find it in **Outside IP Address | Virtual Private Gateway**.
2. Provide the **Address space**. For example, 192.168.0.0/24 (AWS IPv4 subnet CIDR details).
3. Navigate to **Local network gateway | Connections**.
4. Click **Add Connections**.
    - Select Site-to-Site (IPsec) as the **Connection type**.
    - Validate if the **Virtual network gateway** and **Local network gateway** details are populated.
    - Copy the **Pre-Shared Key** value from the **IPSec Tunnel #1** available in the downloaded configuration file to the **Shared key (PSK)** field.
5. On AWS, add a virtual private gateway to the routing table. For example, 10.0.0.0/24 in Subnet Routing table.
    - Optionally on Azure, create another local network gateway and have **IPSec Tunnel #2**. If a connection expires due to time signature or other factors, the connection still continues with the other gateway.
6. Ensure that **Azure Connection** and **Connection Status** is updated and the status **Connected** is displayed. AWS Site-to-Site VPN connection Tunnel status displays UP.
7. Ping the systems from both AWS and Azure to ensure successful communication.

Hybrid on-premises setup

In the Hybrid on-premises setup, some of the resources for Active Roles can be on cloud and on-premises.

NOTE:

- Currently, Active Roles support AWS or Azure with on-premises platforms.
- One Identity recommends to use Active Roles and SQL Server to be in the same region.

- One Identity recommends to setup a Site-to-Site VPN between the cloud (Azure or AWS) and on-premises. A Site-to-Site VPN gateway connection is used to connect your on-premises network to a cloud virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. This type of connection requires a VPN device located on-premises that has an externally facing public IP address assigned to it.

Site-to-Site VPN connection on Azure

Before you begin to create a Site-to-Site VPN connection on Azure, ensure the following aspects:

- A compatible VPN device is available and the administrator can configure it.
- An externally facing public IPv4 address is available for the VPN device.
- Familiarity with the IP address ranges located on the on-premises network configuration.
- Choose the same location or region for all Azure resources.

Configuring a Site-to-Site VPN

1. Create a resource group in desired region
2. Create a virtual network with required address space
3. Create a Gateway subnet in the above virtual network
4. Create a Public IP address
5. Create the VPN gateway using the above Public IP address
6. Create the local network gateway using the Public IP Address of on-premises and mention the IP address space of on-premises network
7. Configure your VPN device
8. Create the VPN connection under Local network Gateway created above
9. Ensure Shared Key provided in Connection matches with on-premises
10. Verify the VPN connection status shows Connected

For more information on creating a Site-to-Site VPN gateway connection from the on-premises network to the Azure VNet, see https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal.

Configuring Active Roles with on-premises domain controller

After the Site-to-Site VPN connection is set and running, configure Active Roles with on-premises domain controller.

Site-to-Site VPN connection on AWS

Before you begin to create a Site-to-Site VPN connection on AWS, ensure the following aspects:

- A compatible VPN device is available and the administrator can configure it.
- An externally facing public IPv4 address is available for the VPN device.
- Familiarity with the IP address ranges located on the on-premises network configuration.
- Choose the same location or region for all AWS resources.

Configuring a Site-to-Site VPN

1. Create a Customer Gateway using the Public IP address of on-premises network
2. Create a Virtual Private Gateway and attach it to the VPC.
3. Enable Route Propagation in the route table.
4. Update the Security Group.
5. Create a Site-to-Site VPN connection by choosing Customer Gateway and Virtual Private Gateway created above.
6. After the VPN connection is available, click Download Configuration to download the configuration. Download the file with the following options:
    - Vendor- Generic
    - Platform- Generic
    - Software- Vendor Agnostic
7. Configure the Customer Gateway/VPN Device.
8. Ensure the AWS Site-to-Site VPN connection Tunnel status displays UP.

For more information on creating a Site-to-Site VPN gateway connection from the on-premises network to AWS, see https://docs.aws.amazon.com/vpn/latest/s2svpn/SetUpVPNConnections.html.

After the Site-to-Site VPN is created and running configure Active Roles with the on–premise domain controller.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product