EnsureDR

www.ensuredr.com

# EnsureDR Quick Startup Guide for Microsoft Azure Site Recovery (ASR)

**Ver: 1.0 - 05/27/2022**

EnsureDR is a software solution that makes sure your data recovery (DR) site works when you need it. By running automatically every few days, DR testing is performed and used to reveal issues that need to be addressed - therefore keeping the business up to date with its DR state. EnsureDR supports DR solutions (data movers) such as AWS Elastic Disaster Recovery (AWS DRS), Carbonite Recover, Cohesity Helios, Microsoft Azure Site Recovery (ASR), NetApp storage, RecoverPoint for Virtual Machines, Veeam Backup & Replication, VMware vSphere Site Recovery Manager (SRM), Zerto, and more.

## Documents Description

In this quick startup guide, you will learn how to quickly set up the EnsureDR job to test VM's health check status in your DR environment. For advanced features, please refer to the full user guide. Please follow the instructions, and if you need additional help, please contact support@ensuredr.com.

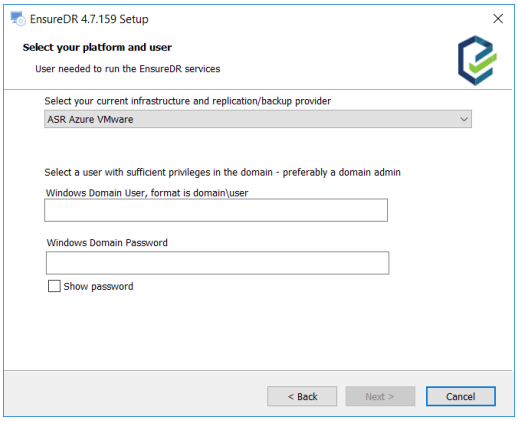
## Prerequisites

To make EnsureDR works properly, there are a few prerequisites to set up in advance.

| | |
|---|---|
| Servers and Console | One server with Windows 2016/2019 with 16 GB mem, 4 CPU, 250 GB disk, and single NIC.<br>EnsureDR management server (EDRM) must be located at the DR site in the Microsoft ASR environment.<br>Server must have only a single NIC.<br>Correct time zone set for the machines. |
| Domain Controller and DNS Server | Restored servers in Microsoft Azure ASR require a domain controller, the EDRM server must be joined to the same domain and point to the same DNS server before running the EDRM job.<br>In cases where a restored server in Microsoft Azure ASR does not need a domain controller, the EDRM servers do not need to be part of a domain.<br>If a domain controller is not used, the EDRM server must have correctly configured DNS server settings in order to be able to resolve restored server names in Microsoft Azure ASR. |
| Credentials | To be able to run services on the EDRM server, set up an account that is the local administrator on the EDRM server |
| Microsoft Azure ASR | Bubble/Isolated Virtual networks need to be created to avoid duplicate IP during testing |
| Microsoft Azure Network Connectivity & Firewall | EDRM server must be configured in the management Virtual network to be able to perform tests, EDRM machine Networking must be configured to allow access from EDRM to Microsoft Azure Cloud (Microsoft Public Cloud):<br>▪ *.aadcdn.microsoftonline-p.com<br>▪ *.aka.ms<br>▪ *.applicationinsights.io<br>▪ *.azure.com<br>▪ *.azure.net<br>▪ *.azure-api.net<br>▪ *.azuredatalakestore.net<br>▪ *.azureedge.net<br>▪ *.loganalytics.io<br>▪ *.microsoft.com<br>▪ *.microsoftonline.com<br>▪ *.microsoftonline-p.com<br>▪ *.msauth.net<br>▪ *.msftauth.net |

| | |
|---|---|
| | ▪ *.trafficmanager.net<br>▪ *.visualstudio.com<br>▪ *.asazure.windows.net (Analysis Services)<br>▪ *.core.windows.net (Azure Storage)<br>▪ *.database.windows.net (SQL Server)<br>▪ *.graph.windows.net (Azure AD Graph)<br>▪ *.kusto.windows.net (Azure Data Explorer/Kusto)<br>▪ *.search.windows.net (search)<br>▪ *.servicebus.windows.net (Azure Service Bus)<br><br>The EDRM networking must be configured to allow:<br>▪ Incoming/outgoing traffic between the EDRM server and recovered instances in Microsoft Azure Portal. If advanced tests are performed all ports must be specified depending on which tests the user is set in the EDRM job. (TCP 53, TCP 80, TCP 443, TCP 1433, etc.)<br>▪ Incoming traffic from the customer on-premise environment to the public IP address of the EDRM server in Microsoft Azure Portal for remote access (RDP 3389 and HTTPS 443).<br>▪ SMTP outgoing traffic should be open for sending email reports, from the EDRM server to the local mail server. Usually, the SMTP port number is 25 but can be different. Please ask your mail administrators for the correct port number. |
| Microsoft Azure App Registrations | Log into the Microsoft Azure portal, select “Azure Active Directory”, choose “Register an application”, select “Accounts in any organizational directory (Any Azure AD directory - Multitenant)”, and register the account. Save "Application (client) ID" and "Directory (tenant) ID" for future usage. Click on “Add a certificate or secret”, click on “New Client Secret”, put a description, and click on “Add” button. Immediately copy the "Value" and "Secret ID" to your password manager to store them in a safe place for future usage. |
| Antivirus | If you have antivirus software running inside the EnsureDR management server, add an exclusion for API.exe and EDRRunner.exe. |
| Reporting Mail | SMTP mail service available for the EnsureDR server to send the report via mail such as local exchange or Office365/Gmail. |
| Supported Version | Microsoft Azure Site Recovery - disaster recovery as a service (DRaaS) |
| Supported Browser | Google Chrome |

**Setup**

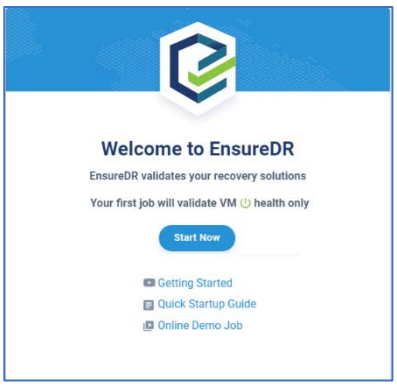



Prepare a server VM with a clean install of Windows server 2016/2019 (as described in the prerequisites table).

EnsureDR manager setup

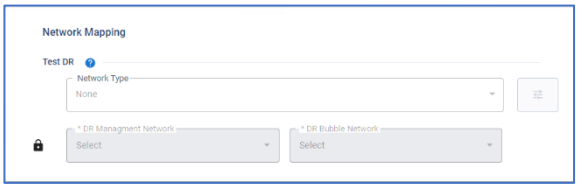
1. Log on with the service account you created in advance as described in the prerequisite document
2. Run the EnsureDRSetup.exe file as an administrator on the server you created upfront
3. Choose your data mover type and set a domain user credential that has local administrator rights on the EDRM server
4. Set up the default location for the installation, accept the license, and install the product
5. Wait for the installation to complete, depending on the environment and components, may take a few minutes

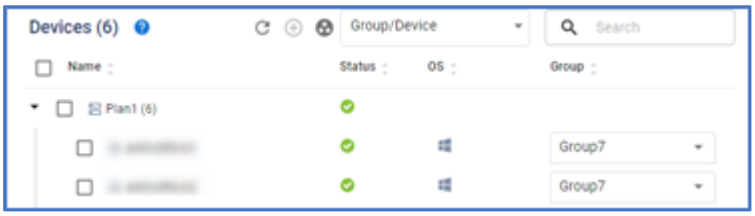
6. Save provided link for future access (used in the steps below)
7. When the installation is finished, restart the EDRM server




Creating the first job

1. Open the Google Chrome browser and navigate to the link you saved in the previous step
2. A welcome message pops up in the browser, click on “Start Now”
3. Fill in the necessary info in the first step to create the job
    - Enter a job name
    - Subscription ID
    - Tenant ID
    - Client ID
    - Client secret
    - Recovery Vault
    - Resource Group
    - Storage Name
    - Storage Connection String
    - Workflow user, set the credentials for windows user that has access right on servers that will be recovered to Microsoft ASR, set the credentials for Linux user that has access right on server recovered to Microsoft ASR




4. On the second step, network configuration, press next
    - Relevant for advance jobs only
5. For the third step, EnsureDR will fetch data from Microsoft ASR by collecting the list of available servers
    - Select the servers you want to test and click the blue arrow to move those servers to the job list in the right pane
6. Finally, define the e-mail address for the recipient of the report, and assign a time for the frequency of rerunning the job. Now you are ready to execute a job by clicking to "Save & Run" button