Enhance Your Disaster Recovery Strategy

Barracuda Backup and Barracuda SecureEdge unlock the power of cloud recovery.

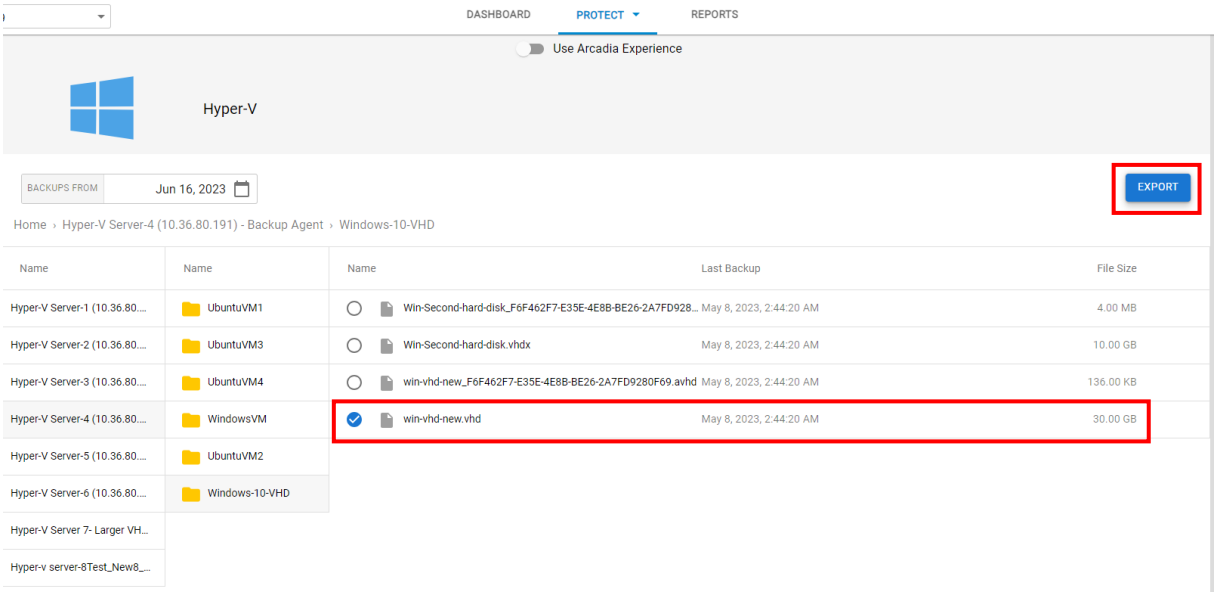
In today's digital-first environment, the ability to quickly recover from data loss and ensure continuous operations is paramount for any organization. Integrating Barracuda Backup with its Export to Azure feature and Barracuda SecureEdge offers a seamless and robust solution for virtual machine recovery and secure connectivity in the cloud. This solution brief explores how the synergy between these solutions not only enhances an organization's disaster recovery strategy but also fortifies data security and business continuity. By leveraging Barracuda's cutting-edge solutions, businesses can minimize downtime, protect against data breaches, and maintain operational resilience in the face of unexpected disruptions.

Cloud Recovery with Barracuda Backup

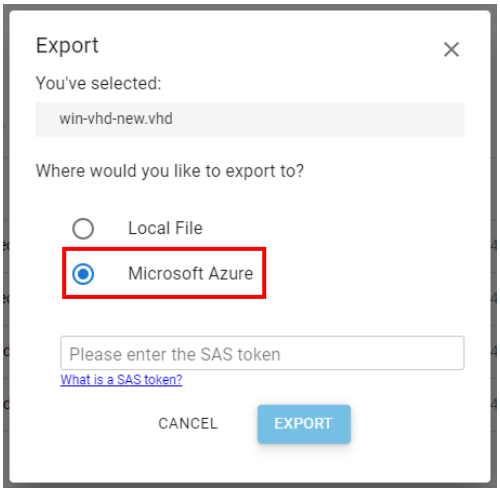
The Barracuda Backup Export to Azure feature allows organizations to recover VMware and Hyper-V virtual machine disks to a Microsoft Azure storage account. From Azure, the virtual machine disks can be used to create Azure virtual machine instances. This is an easy method for recovering on-premises virtual workloads to the cloud for recoverability testing, cloud migration, or as part of a disaster recovery strategy.

Step 1: Exporting Data to Microsoft Azure

Browse to any VMware or Hyper-V virtual machine backup in the Barracuda Backup restore interface. You can select entire virtual machines or select individual virtual machine disks to export. Once you have made a selection, click the **Export** button.



The export dialog box will appear, with two options. Select the option to export to **Microsoft Azure**. Selecting the Local File option will give you the ability to download the selected data to your local system.



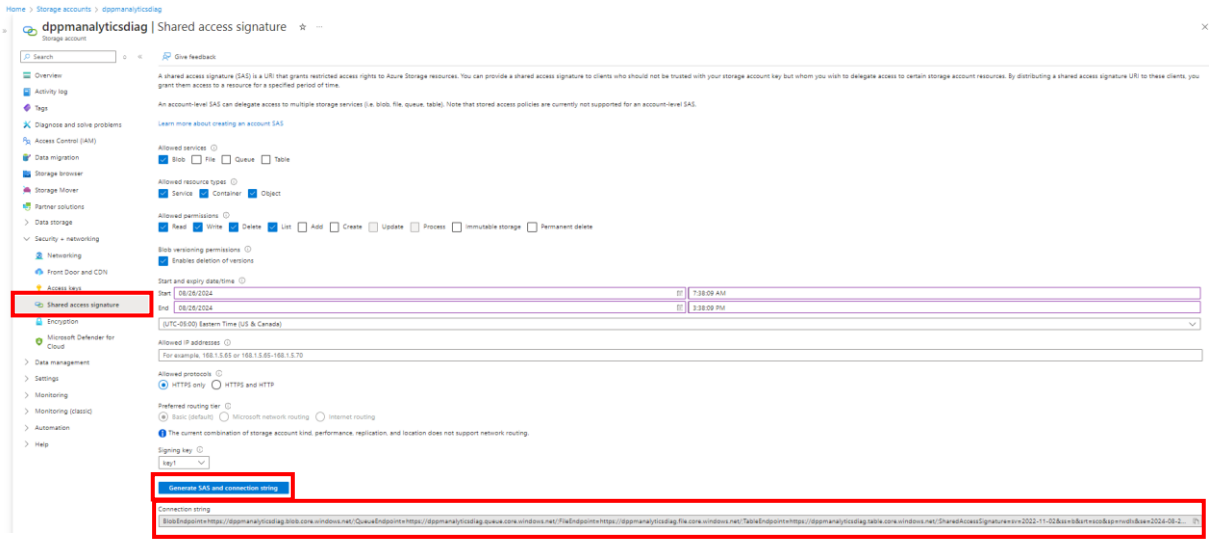
After selecting the Microsoft Azure option, you'll be asked to enter a Shared Access Signature or SAS token. A shared access signature (SAS) provides secure delegated access to resources in your Azure storage account. With a SAS, you have granular control over how a client can access your data. For example:

- What resources the client may access
- What permissions they have to those resources
- How long the SAS is valid

To generate a shared access signature, follow the steps below:

1. Log into your Microsoft Azure account and navigate to **Storage accounts**.

2. Select your desired Azure storage account.
3. Select **Shared Access Signature** from the left-hand menu, under the **Security + networking** section.
4. The Export to Azure feature requires the following services, resource types, and permissions:
    a. **Allowed services** – Blob
    b. **Allowed resource types** – Service, Container, Object
    c. **Allowed permissions** – Read, Write, Delete, List
5. Set a **start and expiry date/time** for the shared access signature. (We recommend setting the expiration for 3-7 days, but it will depend on the size of the data being exported and the length of time to do so)
6. Click the **Generate SAS and connection string** button.
7. Copy the **Connection string**.



8. **Paste** the connection string into the SAS token field in the Export to Azure dialog box.
9. Click the **Export** button.
10. The export to Azure job will begin. To view the status of your export job, navigate to the **Dashboard** or **Reports** page.

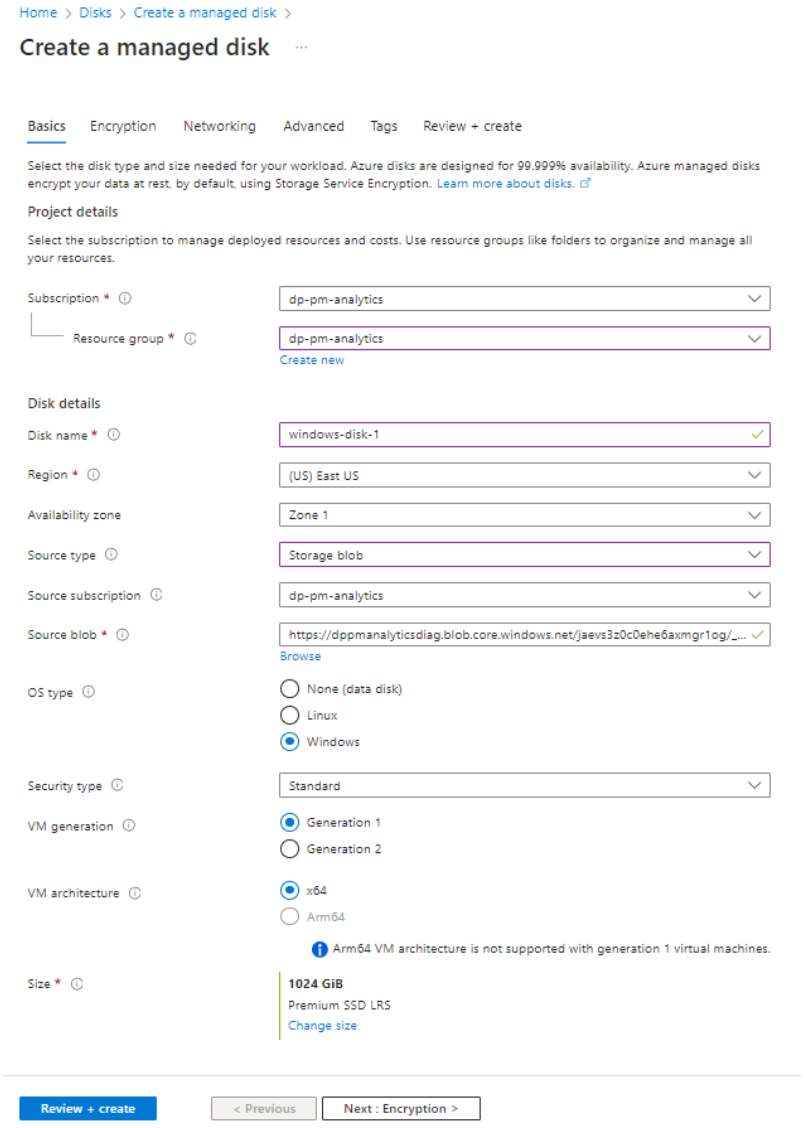
Step 2: Creating an Azure Managed Disk

Once a VMware (.VMDK) or Microsoft Hyper-V (.VHD) disk file has been exported to Azure you can create an Azure Managed Disk, which can then be used to create an Azure virtual machine instance.

1. From the Azure portal, navigate to the **Disks** service.
2. Click the **Create** button.
3. Fill in the required information in **Create a managed disk**. In Source type, select **Storage blob**. Click **Browse**, then navigate to the newly created page blob and

select it. Make sure you select the correct OS type, VM generation, and VM architecture that matched the VM's original state on-premises.

4. Click **Review + create**.
5. If validation passes, click **Create**.

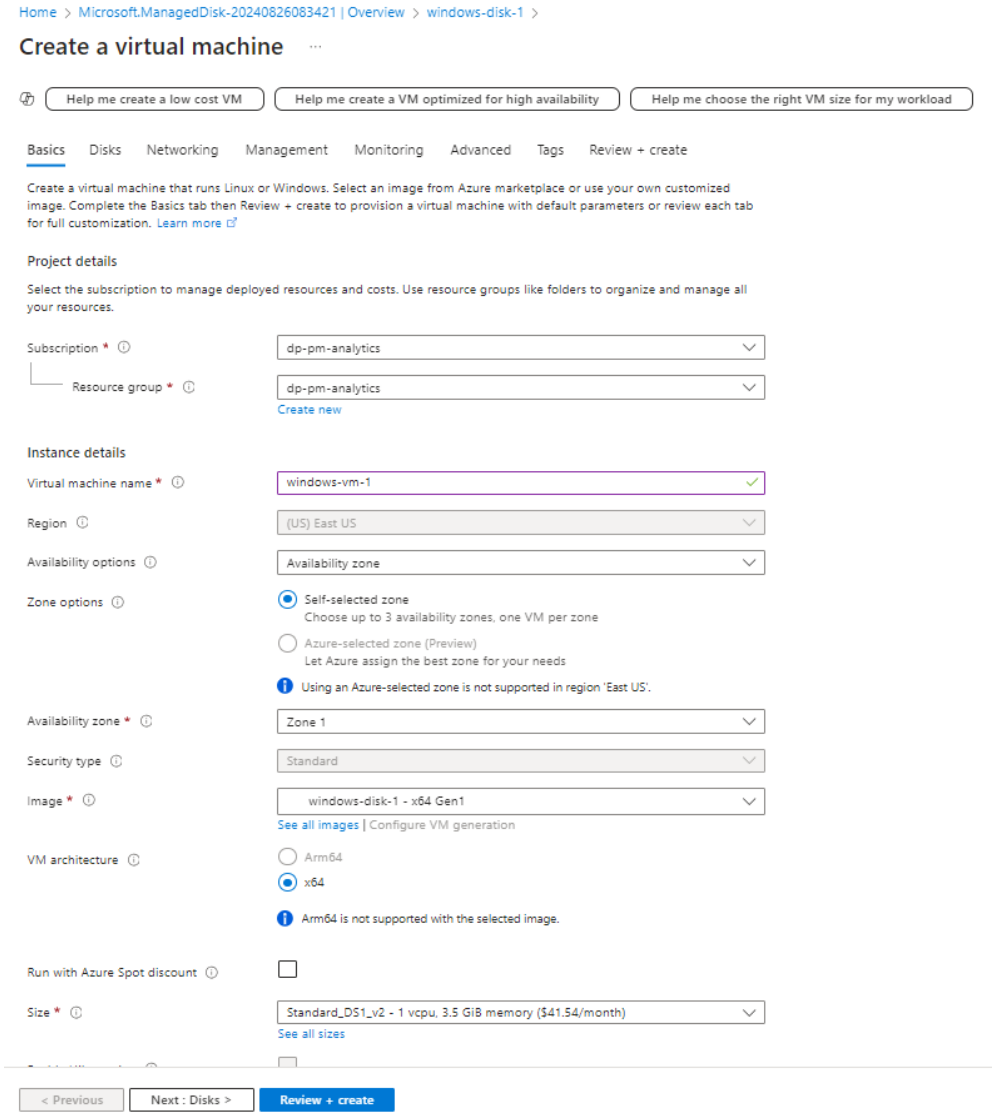


Step 3: Creating a New Azure Virtual Machine

Now that an Azure Managed Disk has been created out of your original .VMDK or .VHD disk file, you can use it with an existing or new Azure virtual machine.

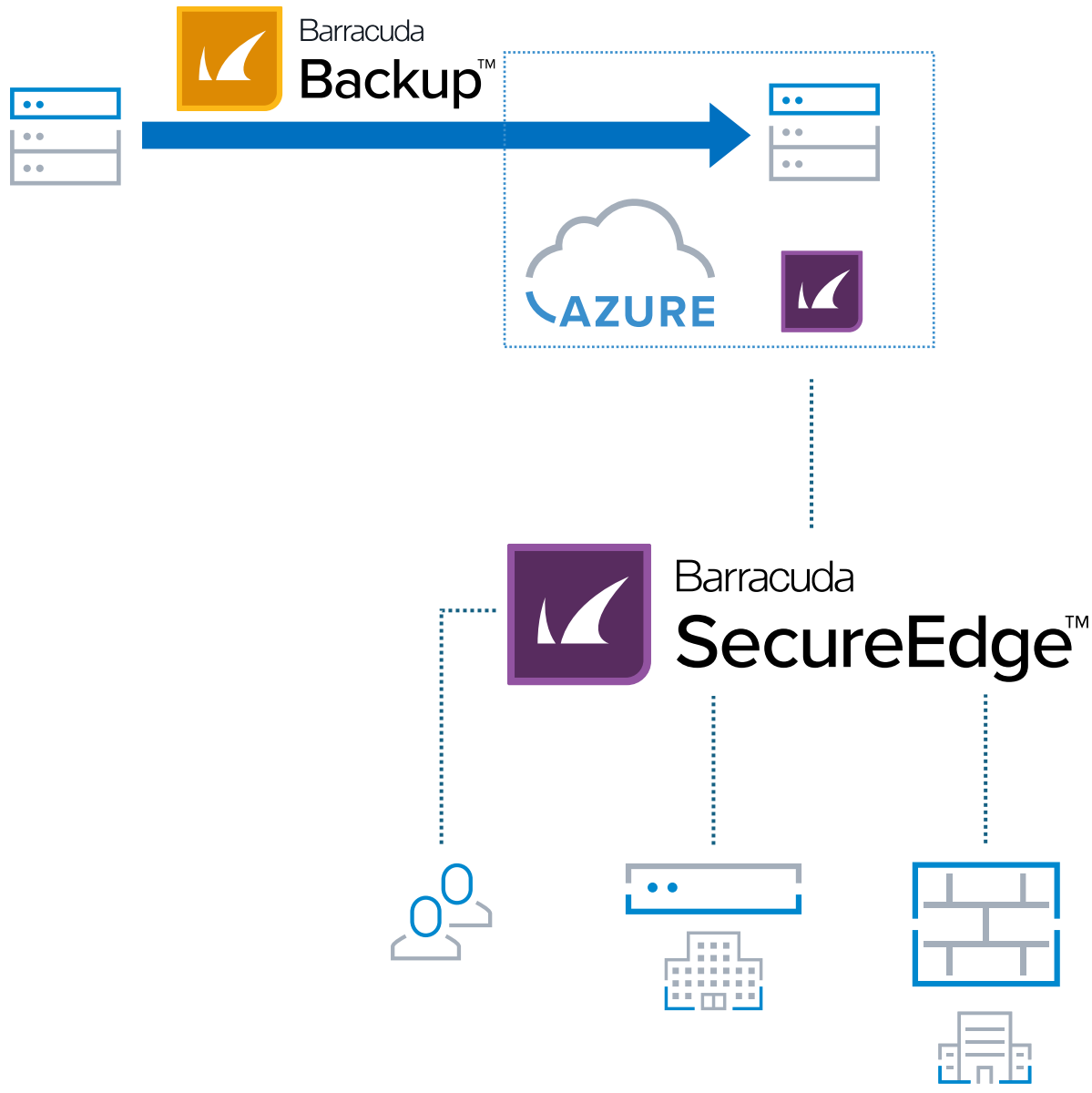
1. Select your newly created Azure managed disk to view the details.
2. Click **Create VM** and create a new Azure virtual machine.
3. Fill in all required information in **Create a virtual machine**. The image should list your newly created managed disk.
4. If your virtual machine has multiple disks, the secondary disks must first be converted to Azure Managed Disks. Then when creating your Azure virtual

machine, under the **Disks** section, click **Attach an existing disk** and select your secondary disk(s).



Secure Cloud Connectivity with Barracuda SecureEdge

Once the Virtual Machine has been successfully restored, you can connect the restored instance by using the Connector which is a little piece of software that establishes a secure connection to a SecureEdge SASE-environment. If no account is available, a trial account for SecureEdge can be used to access the resource temporarily via a secure VPN tunnel to the SASE environment or by utilizing the installable SecureAccess Agent on clients to access the resource (ZTNA).



How to connect a resource with SecureEdge

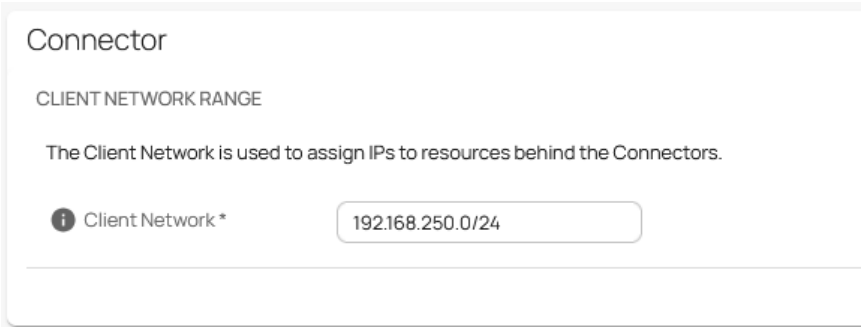
SecureEdge

Trial of SecureEdge (optional)

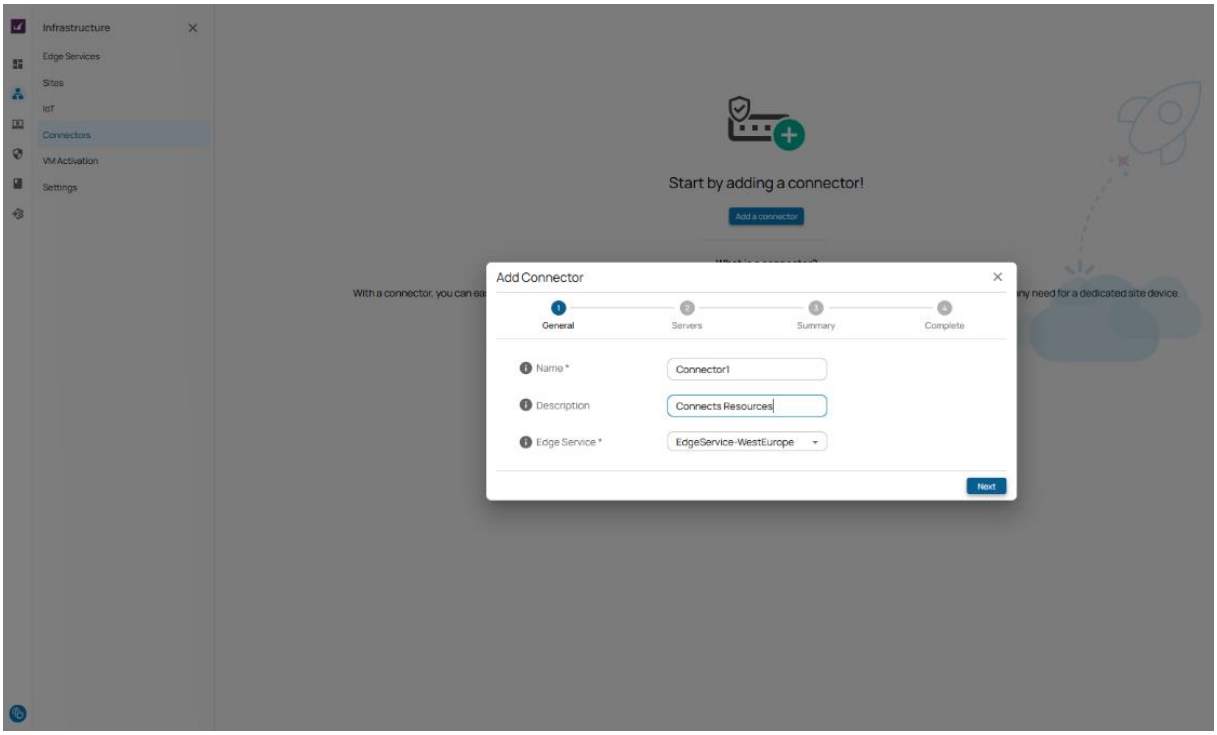
1. Get a Barracuda Cloud Control account (if not already present)
2. Go to https://se.barracudanetworks.com/
3. Create New User to start a trial
4. Deploy a new Edge Service
    - Infrastructure > Edge Services > New Edge Service (Edge Service)
        - Campus Documentation: Create an EdgeService

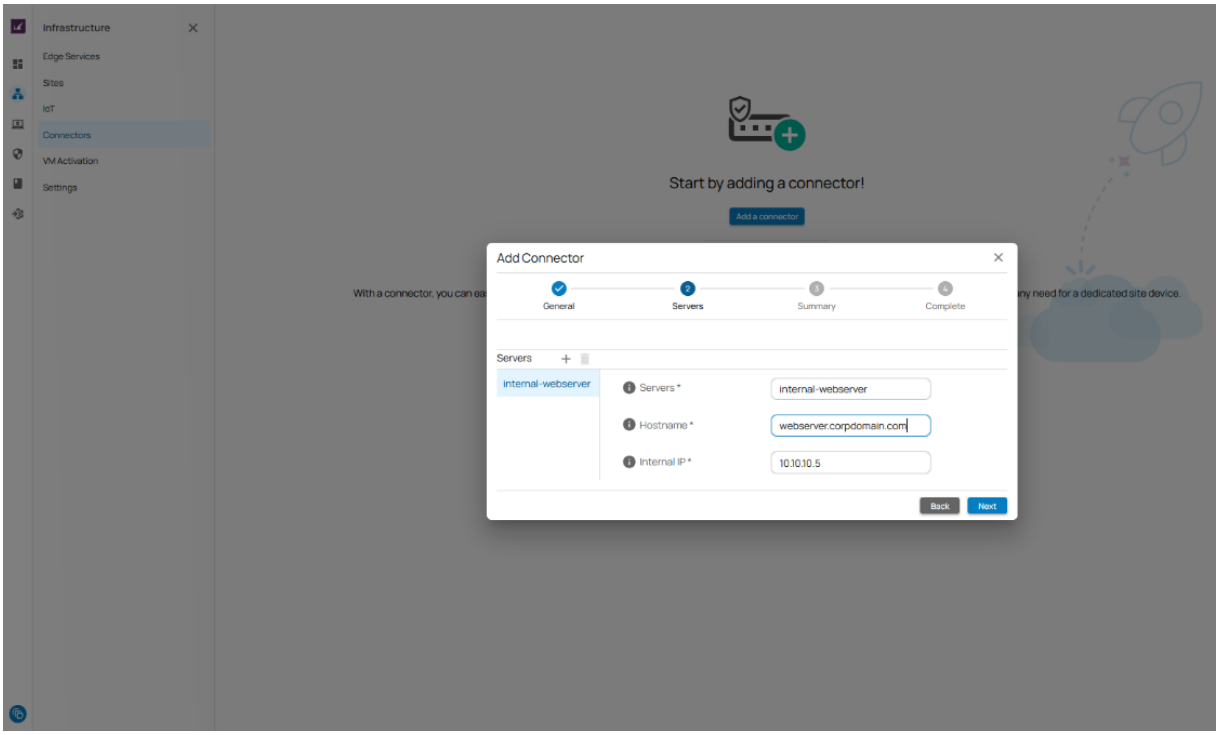
Set up the Connector

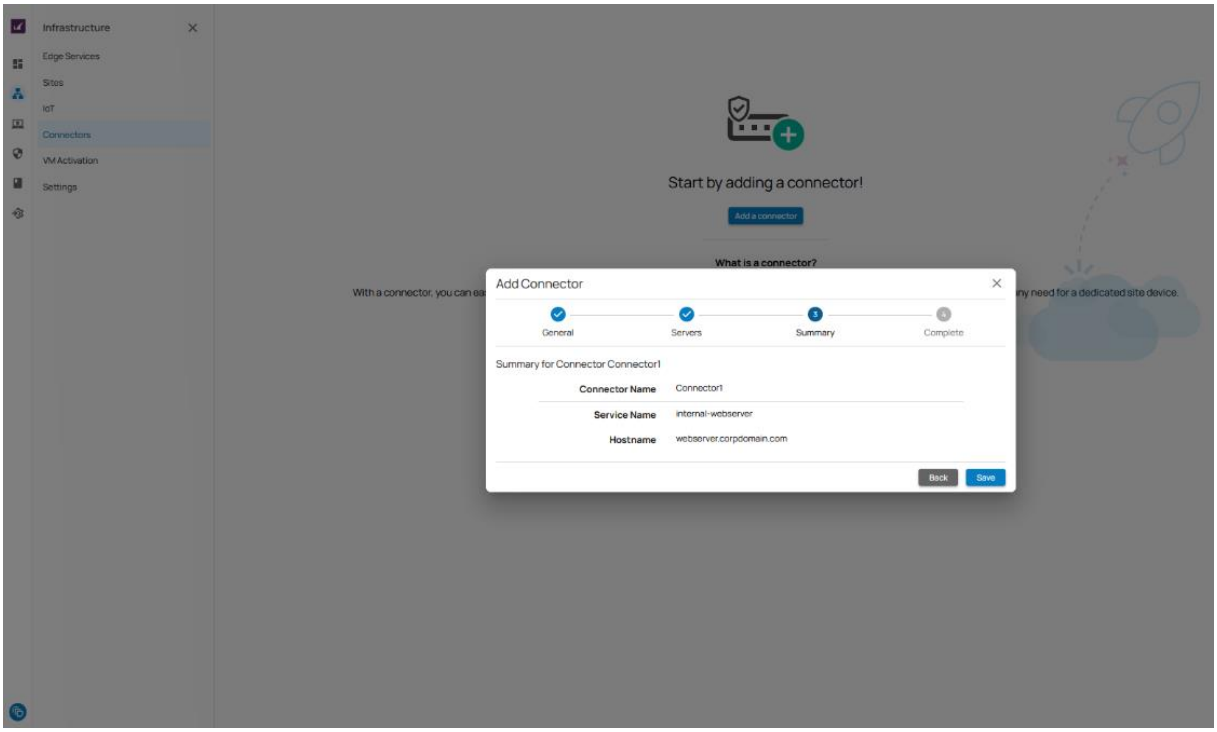
1. Login to SecureEdge
    - https://se.barracudanetworks.com/
2. Set up the SecureEdge Connector
    - Campus Documentation: How to Configure the SecureEdge Connector
5. Define an IP-Range for the Connectors
    - Infrastructure > Settings > Connector
        - Client Network in CIDR
        - Choose a Network that is not used in your current infrastructure

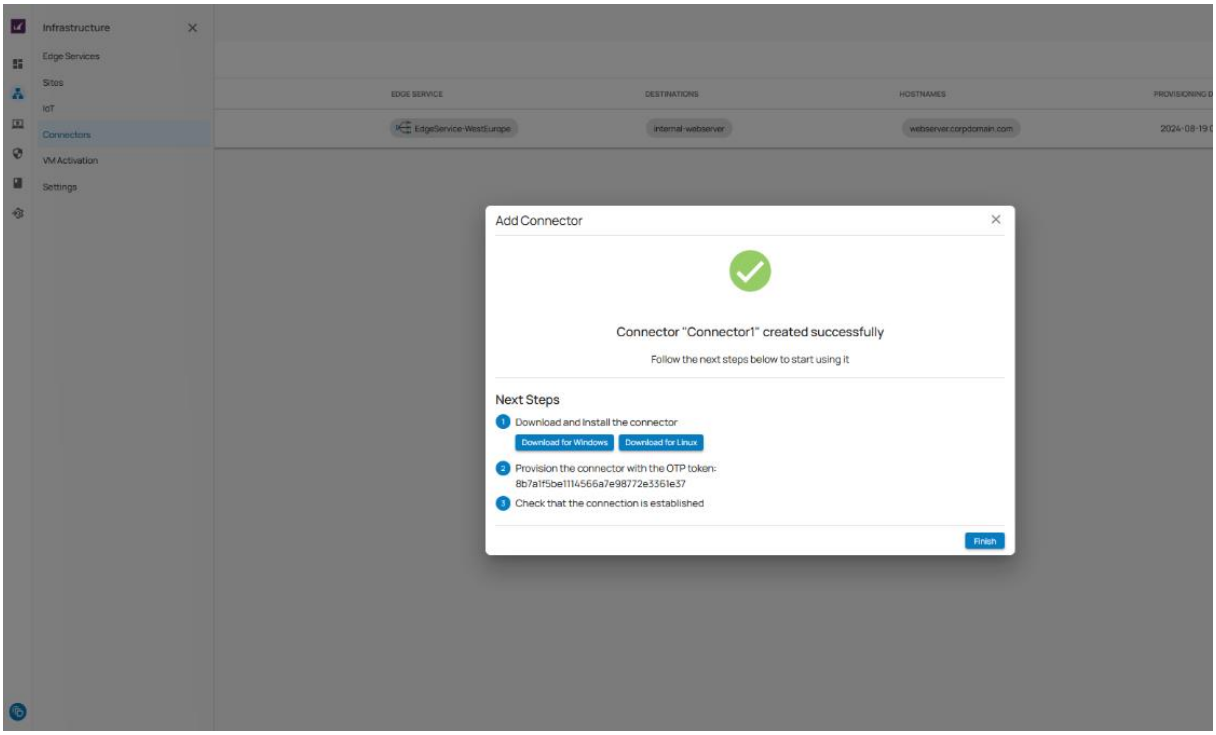


6. Add a Connector
    - Infrastructure > Connectors > Add
        - Name: <Name of the Connector>
        - Description: <Description of the Connector>
        - Edge Service: <Edge Service>
        - Servers: <Unique name for of the restored VM>
        - Hostname: <Resolved name in the SecureEdge environment>
        - Internal IP: <Internal IP of the VM>


Infrastructure
Edge Services
Sites
IoT
Connectors
VM Activation
Settings
Start by adding a connector!
Add a connector
Add Connector
General
Servers
Summary
Complete
Name *
Connector1
Description
Connects Resources
Edge Service *
EdgeService-WestEurope
Next


Infrastructure
Edge Services
Sites
IoT
Connectors
VM Activation
Settings
Start by adding a connector!
Add a connector
Add Connector
General
Servers
Summary
Complete
Servers
internal-webserver
Servers *
internal-webserver
Hostname *
webserver.corpdomain.com
Internal IP *
10.10.10.5
Back
Next


Infrastructure
Edge Services
Sites
IoT
Connectors
VM Activation
Settings
Start by adding a connector!
Add a connector
What is a connector?
Add Connector
General
Servers
Summary
Complete
Summary for Connector Connector1
Connector Name
Connector1
Service Name
internal-webserver
Hostname
webserver.corpdomain.com
Back
Save


Infrastructure
Edge Services
Sites
IoT
Connectors
VM Activation
Settings
EDGE SERVICE
DESTINATIONS
HOSTNAMES
EdgeService-WestEurope
internal-webserver
webserver.corpdomain.com
Add Connector
Connector "Connector1" created successfully
Follow the next steps below to start using it
Next Steps
1 Download and install the connector
Download for Windows
Download for Linux
2 Provision the connector with the OTP token:
8b7a1f5be1114566a7e98772e3561e37
3 Check that the connection is established
Finish

Azure (portal.azure.com):

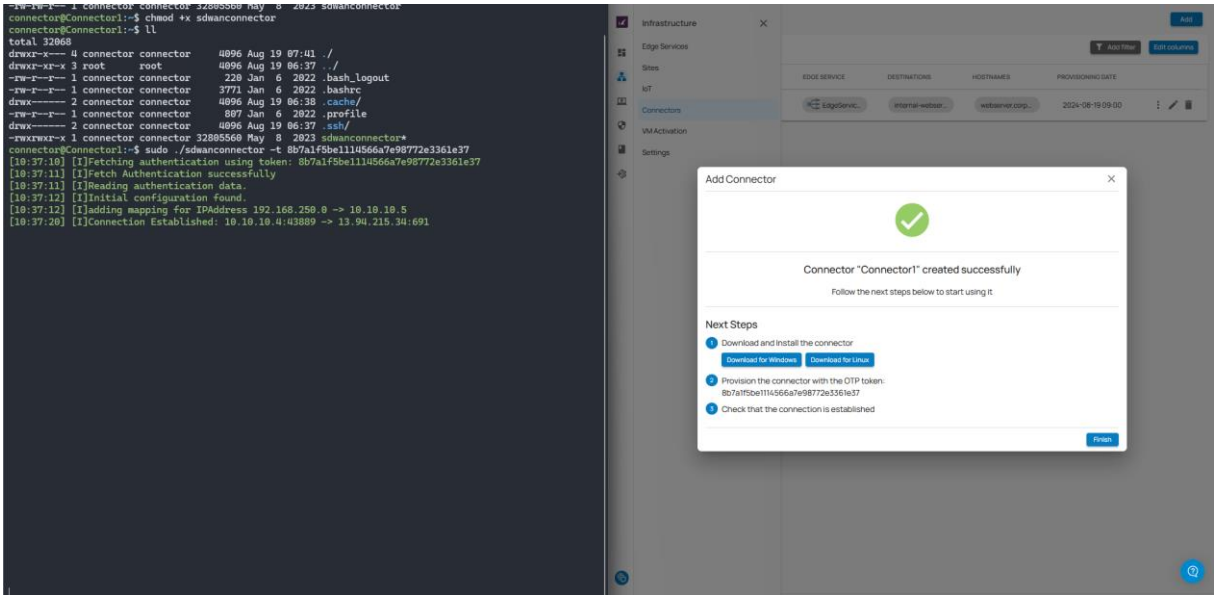
Install the agent directly on the restored virtual machine.
Alternatively, the connector can be installed on a dedicated virtual machine in the same network.

- Install the connector directly on the restored virtual machine
  - Transfer the Connector to the related virtual machine
  - Make the connector executable (if not already the case)
  - Register the connector with the OTP token

Campus Documentation:

- How to Configure the SecureEdge Connector (Windows)
- How to Configure the SecureEdge Connector (Linux)

Example of a restored Linux machine:



Access the Resource

There are three options to make the resource accessible.

1. With the SecureEdge Access Agent
   Enables enrolled clients with the installed Agent to access the resource
   - Enroll users with ZTNA
     - Campus Documentation: SecureEdge Access
2. IPsec IKEv2 VPN
   Enables your corporate network to access the resource
   - Connect your Corporate firewall to the EdgeService by using IPSec VPN (IKEv2)
     - Integration > IPsec VPN > Add IPsec Tunnel
     - Campus Documentation: How to Configure a Site-to-Site IPsec IKEv2 VPN Tunnel on SecureEdge Using Static Routing
3. T/VT Sites
   The resource is automatically available for T/VT Sites deployed in the SecureEdge environment connected to the related EdgeService