OpenVPN

All docs related to OpenVPN and OpenVPN Access Server (AS)

- OpenVPN AS Installation
  - [How-To] Install OpenVPN Access Server on Debian 12 VM
- OpenVPN AS Configuration
  - [How-To] Reset Default OpenVPN User Password via CLI
  - [How-To] Configure OpenVPN Access Server First Time
  - [How-To] Integrate Active Directory Authentication into OpenVPN AS

OpenVPN AS Installation

All OpenVPN AS Installation Docs

[How-To] Install OpenVPN Access Server on Debian 12 VM

Purpose

This document shows how to install OpenVPN Access Server on a Debian 12 VM.

Prerequisites

List of prerequisites:

- Root user or sudo user
- Debian 12 VM

OpenVPN AS Installation

Step 1: SSH To Server

First, SSH into your VM that will have OpenVPN AS installed on it. Once you've done that, verify you can sudo by executing the following:

```
sudo echo hello!
```

When you confirm you have sudo, sudo into the root user's profile with the following, as the installation needs to be done as root:

```
sudo su -l
```

Step 2: Update and Install Tools

Run the following command to update the system, as well as install needed tools for the install to run:

```
apt update && apt -y install ca-certificates wget net-tools gnupg
```

Step 3: Add Repository for OpenVPN AS

Run the following command to add the OpenVPN AS Repository to the server's list of repos:

```
wget https://as-repository.openvpn.net/as-repo-public.asc -qO /etc/apt/trusted.gpg.d/as-repository.asc
```

Now run this command to verify the repo is working normally:

```
echo "deb [arch=amd64 signed-by=/etc/apt/trusted.gpg.d/as-repository.asc] http://as-repository.openvpn.net/as/debian bookworm main">/etc/apt/sources.list.d/openvpn-as-repo.list
```

Step 4: Install OpenVPN AS

Run the following command to install OpenVPN AS:

```
apt update && apt -y install openvpn-as
```

After Installing, you'll get a blurb of text that give information about client and admin URLs as well as login information to get started that looks something like this:

```
++++++++++++++++++++++++++++++++++++++++++++++++++
Access Server has been successfully installed in /usr/local/openvpn_as
Configuration log file has been written to /usr/local/openvpn_as/init.log

Access Server Web UIs are available here:
Admin UI: https://192.168.102.130:943/admin
Client UI: https://192.168.102.130:943
Login as "openvpn" with "password" to continue
(password can be changed on Admin UI)
++++++++++++++++++++++++++++++++++++++++++++++++++
```

OpenVPN AS Configuration

All OpenVPN AS Configuration docs

[How-To] Reset Default OpenVPN User Password via CLI

Purpose

The purpose of this is to reset the default OpenVPN user password via the CLI when locked out and don't have other admin accounts to get in with.

Prerequisites

List of prerequisites:

- Root user or sudo user
- OpenVPN AS

CLI Commands to Reset Password

Step 1

Run these commands to reset the password for OpenVPN user:

```
sudo su -l
```

```
cd /usr/local/openvpn_as/scripts
```

```
./sacli --user "openvpn" --key "prop_superuser" --value "true" UserPropPut
```

```
./sacli --user "openvpn" --key "user_auth_type" --value "local" UserPropPut
```

```
./sacli --user "openvpn" --new_pass=<PASSWORD> SetLocalPassword
```

```
./sacli start
```

With these commands, and changing out <PASSWORD> for your desired password, you should be able to get back in.

Step 2: Reset/Remove 2FA From Account

Run these commands to remove 2FA from the default OpenVPN account.

```
sudo su -l
```

```
cd /usr/local/openvpn_as/scripts
```

```
./sacli --user "openvpn" --key "prop_deny" --value "false" UserPropPut
```

```
./sacli --user "openvpn" --key "prop_google_auth" UserPropDel
```

```
./sacli --user "openvpn" --lock 0 GoogleAuthRegen
```

```
./sacli start
```

Step 3: Reset the Password Lockout Policy

Run these commands to reset the password policy for the default OpenVPN account.

```
./sacli --key "vpn.server.lockout_policy.reset_time" --value "1" ConfigPut
```

```
./sacli start
```

```
sleep 2
```

```
./sacli --key "vpn.server.lockout_policy.reset_time" ConfigDel
```

```
./sacli start
```

https://openvpn.net/as-docs/reset-admin-access.html#notes-on-older-access-server-versions

[How-To] Configure OpenVPN Access Server First Time

Purpose

This document aims to walk through the initial confirmation of OpenVPN AS once OS is installed and up/running.

Prerequisites

List of prerequisites:

- Root user or sudo user
- OpenVPN AS

OpenVPN AS Configuration

Step 1: Log in with Default Credentials

If you don't have a public DNS record pointed to your OpenVPN Access Server, you can use its local IP address with port 943. Either way, you can browse to the login page and use the default OpenVPN username and the password generated during CLI installation. Once you've verified the default login works, add a /admin to the back of the URL at the base and login with the same default creds to get to the admin console.

Step 2: Licensing

Once logged in, you'll be presented with the Status Overview Page. Here, verify at the top that VPN Services are running. After you verify that, browse to configuration and then activation. Here is where you can apply for the license from your OpenVPN AS account. This isn't needed if you are using a free license but still good to apply for consistency's sake.

Step 3: Network Settings

Once your license is applied, browse down to the configuration and then the network settings section. Here we need to set a few things. First, change the Hostname/IP Address box from the server's local IP to the public DNS name for the website. If you don't have a public DNS record, use the local DNS record instead. But this should be set to what you want your VPN users to get redirected back to when connecting or having issues. Next, change the UDP port number to something that isn't he default 1194, like 1195 so that it's more secure. When finished, scroll to the bottom and click save settings. Then at the top after reloading, click Update running server.

Step 4: VPN Settings

In VPN Settings tab under Configuration, first change the network address settings under dynamic network address settings. Make this the IP range that you want users connecting to, like 102.168.10.0/24. Then, below see the section called routing. In the box with specify subnets accessible to VPN users section, add all subnets in the CIDR notation that you want accessible to the users when connected to this VPN. Enter down after each entry.

Step 5: Firewall Configuration

Now that the configuration section is done, log in to your network firewall solution and add a port forwarding nat rule on WAN to let in access to the port for your VPN and your web server on the local IP address of the server.

Step 6: Add Local User with 2FA

Now go to the user management and then the user permissions tab. This is where you'll need to change the default password for the OpenVPN user. Set it to something difficult as it has admin access. Save and update the running server. Then create a new local user with a strong password as well, allow it to admin access, and enable 2FA. Save and update the running server. Log out and log back in with the new local user. Add 2FA to your 2FA app on your phone and enter the code. Once working, go back to user permissions and enable 2fa for the OpenVPN user as well, and follow the same steps to add and test.

Step 7: Security Settings

As a final lockdown of security settings, you'll want to review all settings in the GUI as there are many related to security. The 2 we will focus on are allowing new users to auth for the first time and forcing 2FA on all users.

[How-To] Integrate Active Directory Authentication into OpenVPN AS

Purpose

The purpose of this how to is to show the process to add active directory authentication services to your OpenVPN access server.

Prerequisites

List of prerequisites:

- Root user or sudo user
- OpenVPN AS
- Domain Admin User
- Active Directory Domain

AD Integration Settings

Step 1: Prepare Active Directory Objects

You'll need to create a few things in Active Directory:

1. User Look Up OU:
    1. Determine the user lookup base for where it can find users, you can leave it open or at the root domain but it leaves more room for bad actors as well as slow lookups. Open the server manager and then open active directory users and computers.
    2. Find the OU that you want to use, right-click and select properties.
    3. Click the attribute editor, then find the Distinguished Name Entry. Copy this to the clipboard.
    4. Save this in your Password Manager as User Look Up OU for VPN Server AD Int.

2. Service Account to Read Users:
    1. We need a service account with regular domain user permissions that can read domain users from the domain directory. Open the server manager then open active directory users and computers.
    2. Find the OU where you want the service account for VPN to exist, then right-click on it and select new user.
    3. In the new user entry, enter an account name as well as a domain. Then click next.
    4. Set a password for the service account and repeat it. Then, remove the check for user must change password and check the boxes for password never expires as well as user cannot change password. Then click next, then finish.
    5. With the user created, right-click on it and select properties.
    6. Select the attribute editor and find the Distinguished Name Entry. Copy this to the clipboard.
    7. Save this information along with the password in your password manager as a Service Account to Read Users for VPN.
3. Security Group to Check Users Against:
    1. If extra security is desired, you'll need a security group for VPN users that ensures not all users in your user directory have the default ability to authenticate against VPN. Only users added to the group will. Start by opening the server manager and then opening active directory users and computers.
    2. Here, find the OU where you want the security group for VPN to exist, then right-click on it and select the new group.
    3. In the new group entry, verify that security and global are selected, then click next.
    4. Now enter the name of the security group. Then click next. Then click finish.
    5. With the group created, right-click on it and select properties.
    6. Select the attribute editor and find the Distinguished Name Entry. Copy this to the clipboard.
    7. Save this information in your password manager as Security Group to Check Users Against for VPN.

This concludes our Active Directory Preparation. You will use these entries in the next steps.

Step 2: Configure AD in OpenVPN AS

Now, log in to your Web UI Admin Instance of OpenVPN AS. Browse to the Authentication and the LDAP section. Then follow these steps to configure:

1. Under the LDAP Settings section, move the slider to yes for "Enable LDAP authentication". This enabled LDAP on the OpenVPN AS.
2. Verify that the correct settings are set for SSL and case-sensitive are correct for your active directory environment, normally they will both be set to "No".
3. Verify the "Re-verify autologin user on connect" is set to "Yes". This confirms that every time users connect to the Web UI or the VPN, their credentials are verified with the active directory domain and not using cached credentials on the AS.
4. In the "LDAP Server" Section, enter the IP addresses for the primary and secondary active directory servers.

5. Also in the "LDAP Server" Section, Set "Bind anonymously" to "No" and set "Use these credentials" to "Yes". Then, use the Bind DN and Password based on the "Service Account to Read Users" Created earlier.
6. For the "Base DN for User Entries", enter the "User Look Up OU" from earlier.
7. Leave "Username Attribute" set to "sAMAccountName".
8. If you decide to use extra security, fill in the "LDAP filter" with the value from "Security Group to Check Users Against". It is important to note the instruction in red, placing "memberOf=" before the security group.
9. Click Save Settings and then scroll to the top and select Update Running Server. This enabled the LDAP connection but it does not set it to the default auth type for new user creations. This means new LDAP users who have never authenticated will not pull in when they try for the first time.
10. To make LDAP the default for new users, browse to the Authentication and then Settings tab, and select LDAP as the default. Click Save Settings, and then Update Running Server at the top of the page.
11. An additional step would be to in Authentication Settings, Move the slider temporarily to "No" for "Deny New User logins" As you'll be registering new users in the test next. When done testing it is a good idea to re-enable that.

Step 3: Test AD Auth in Browser

We have to test the AD Auth in Web UI first as that is what creates the user profile. Browse to the main public DNS for the VPN and log in with AD Creds that are in the Security Group for the VPN. If you can log in, you'll be presented with a 2FA configuration. Add it to your 2FA app on your phone and verify with the code. Once logged in, download the agent for OpenVPN Connect and the profile as well.

Step 4: Test AD Auth in VPN Client

Launch OpenVPN Connect V3 and connect on the profile you just downloaded. Enter the password for that username and then the 2FA when asked. If it connects, you have been successful.