Hyper-V Installation Guide for Snare Server
Table of Contents
1. Introduction .................................................. 3
2. Creating the new virtual machine on Hyper-V ................. 4
3. Installing Snare Server on the Virtual Machine ............... 11
4. Starting the Snare Server ...................................... 22
1. Introduction

ℹ️ About this Guide
This user guide is aimed at users installing the Snare Server on Hyper-V. Please note for a successful installation that at least version 6.3.3 of the Snare Server is required.

ℹ️ Other guides that may be useful to read
- Installation Guide to the Snare Server
2. Creating the new virtual machine on Hyper-V

On your Hyper-V Manager create a new virtual machine and then follow the Wizard using the following screenshots for assistance.
Select Not Connected for now as the details will be removed and updated later.
Select the Snare Server .iso file.
Click Finish.

Select Settings... for your newly created Virtual Machine.

Select Add Hardware from the menu.

For version 6 Snare Server - From the options select Legacy Network Adapter and click Add.

For version 7 Snare Server - From the options select Virtual Switch Network Adapter and click Add.
Select the Virtual Switch and click Apply.
Specify the configuration of the network adapter or remove the network adapter.

**Virtual switch:**
- Intel(R) 82579LM Gigabit Network Connection - Virtual Switch

**VLAN ID**
- [ ] Enable virtual LAN identification

The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.

To remove the network adapter from this virtual machine, click Remove.

We recommend that you use a legacy network adapter only if you want to perform a network-based installation of the guest operating system, or if integration services are not installed in the guest operating system. Communications through a legacy network adapter are slower than through a network adapter.
Select the "Network Adapter - Not Connected". Click Remove, and click Apply.

Click OK to close the Settings window.

Start the Virtual Machine. It will boot the Snare Server installation file as selected above.
3. Installing Snare Server on the Virtual Machine

The screenshots below will aid you in installing the Snare Server, however it is recommended to follow the Installation Guide to the Snare Server for details.
Enter an IP address that is appropriate for your network.
Use a netmask that is appropriate for your network.
Use a domain name that is appropriate for your network.

I think we are missing a NTP screen in here need to check
Confirm your timezone details, usually this is detected during the install but you can override as needed.

Based on your present physical location, your time zone is Australia/South.

If this is not correct, you may select from a full list of time zones instead.

Is this time zone correct?

<Go Back>  <Yes>  <No>
This will just confirm your disk partition details for the virtual disk allocated to your virtual machine.

The sizing is automatically calculated based on the memory allocated to the vm and the size of the virtual disk.
Be sure to document your root password as if its lost it will be difficult to recover.
Your snare login will be your main login to the Snare Server remotely via SSH to use the configuration CLI for some server settings that cannot be set via the Web UI.

If you lose this password you will have to reset it from the root login from the console.
This administrator password is the main password used from the Web UI when you first login.
Make sure you document this or you will have to reset it from the Snare SSH CLI menu.
Your Snare Server is now up and running, now proceed to the Web UI to extract your hostids that are needed to load your new license key.

System reboot. Once the installation process has completed the Snare Server will automatically reboot and your server will be ready to connect to using a web browser.
4. Starting the Snare Server

1. Start a web browser and type in the Snare Server IP e.g. 10.1.1.100
2. A screen will appear that identifies the Host IDs. You will need to provide these Host IDs to your Snare support team so a permanent license can be provided to you.
3. For Snare Server evaluation users, load the temporary 30-day license that you were provided.

4. The Snare Server will present a login page. Enter the User Name Administrator and the password entered at installation time (or password generated by the installation process for Snare Server v7.0). Login into the Snare Server.
5. When the Snare Server is first accessed the Configuration Wizard will appear and assist you through the configuration process. Refer to the *Installation Guide to the Snare Server* for further details. Use the Next and Previous buttons to move between the sections.
5. System Intrusion Analysis & Reporting Environment

*DO NOT regenerate the SSL browser certificate if the server name has changed.

This name will be used to identify your SNAKE Server SSL Certificate, and will also be used to provide absolute links to the SNAKE Server in electronic mail. Note that if you have requested that the existing SSL certificate be overwritten, a new self-signed certificate will be created based on the server name you have entered.

If you have modified the server name, or recreated your SSL certificate, it is recommended that you restart the SNAKE web server. The option to restart the server will be provided to you at the end of this wizard.

The DNS Name for the SNAKE Server:

good.adp.org

SNAKE will attempt to synchronise the local clock to this server, every 24 hours.

The Port on which to contact SNAKE Agents:

8161

The Password to use to talk to SNAKE Agents:

This password, will be used by default, to contact SNAKE Agents. Alternatives can be specified in the SNAKE Agent management.

SNAKE Server authentication mode:

- Normal
  - LDAP / Active Directory
    - Server: [Server Name]
    - Domain: [Domain Name]

User password authentication can be delegated to an external Active Directory or LDAP server. Note that the user must still have a SNAKE account to log in.

If specified, the Domain will be added to the end of the username for authentication purposes (eg: A username of 'user' and a domain of 'test.local' will imply an LDAP/AD authentication at user@test.local).

Control optional SNAKE Services:

- FTP Daemon
- SSH Daemon
- NFS Services

Optional Services can be turned off, by modifying the service check-boxes.

Select the option to share the archive directory via a Windows Share:

Windows share access to Archive area:

Please set a password to access the share:

The archive directory is where the event logs are stored in compressed form. This area can be accessed as read only, via user name/password, and accessible via a Windows share. Note that if this is selected, the username is always 'snares' and the password is the one specified here. The Windows share can then be accessed as 'snares_server_IP_or_SSH/ShareName'.

**IMPORTANT**: Please ensure that the Windows host that is accessing this share is logged off. This will ensure that any changes to this share are not read by the Windows host.

Additional Login Controls:

Activate Enhanced Security for Operating System Accounts:

Many organisations need to abide by regulations that require enhanced operating system password controls.

Although the SNAKE Server includes some restrictions on password length and complexity by default, the administrative and file-transfer operating system accounts do not implement mandatory password rotation.

If you wish to force these accounts to rotate every 90 days, this setting can be activated. Please note that any authentication details included within accept that implement automated transfers to/from the SNAKE Server (particularly ftp or scp/ssh), will need to be updated in line with your choice.

**NOTE**: The following user accounts will be affected by this change: snares, snaresuser. The samba user, and the root user, will be unaffected.

User Interface Password Controls:

Activate Password Expiry in the SNAKE Server:

By default, SNAKE does not implement password expiry. If you wish to force SNAKE Server accounts to rotate passwords every 90 days, this setting can be toggled.

Password Security Controls:

Activate Enhanced Password Security:

© Intersect Alliance International Pty Ltd
Additional Login Controls

Activate Enhanced Security for Operating System Accounts

Many organisations need to abide by regulations that require enhanced operation-system password controls. Although the Snare Server includes some restrictions on password length and complexity by default, the administrator can enable this feature to further enforce password polices.

If you wish to force these accounts to rotate every 90 days, this setting can be activated. Please note that any authentication details included within scripts that implement automated transfers from the Snare Server (particularly file transfer protocols), will need to be updated in line with your choice.

NOTE: The following user accounts will be affected by this change: snare, snaredb. The snmp user, and the root user, will be unaffected.

User Interface Password Controls

Activate Password Expiry in the Snare Server

By default, Snare does not implement password expiry. If you wish to force Snare Server accounts to rotate passwords every 90 days, this setting can be toggled.

Password Security Controls

Activate Enhanced Password Security

If your organisation requires enhanced password controls, this setting can be toggled. Enhanced password controls include:

- Minimum password length (8 characters)
- Passwords must contain at least one letter, number, and special character
- Dictionary and similarity checks
- Password history (5 passwords)
- Last password similarity checks

Database Manager

Activate Database Manager Interface

In situations where your Snare Server support team needs to access the Snare Server configuration settings, the database manager may be required. Use this button to activate or deactivate the capability.

Snare Firewall

Deactivate Basic Snare Firewall

The Snare Server provides a basic IPv4 traffic firewall which blocks all but the commonly used Snare Server ports. This toggle simply enables and disables the firewall, using the default settings. It can be manually configured within the SSH console using the `ufw` command.

General Security Controls

Block external links from being clickable, when displayed by Snare

Some security scanners flag links to external web sites, as a security issue. Clickable links from the redirect page, can be disabled here.
6. Once configuration has finished, click on Return to the Snare Server button to return to the Snare Server.

7. Congratulations. The Snare Server is installed and ready for you to configure reports, create objectives and monitor your logs.