Micro Focus Security
WiNC on CHA

Software Version: 1.1.0

Installation Guide for WiNC on Connector Hosting Appliance

Document Release Date: 30 April, 2020
Software Release Date: 30 April, 2020

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

ArcSight Product Documentation on the Micro Focus Security Community

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Revision History

Date	Description
05/21/2020	First edition of this Installation Guide.

Contents

Product Overview 5

Prerequisites 7

Windows Server VM 7

Management Software 7

Setting up KVM to Host the Windows Server 2019 Core VM 8

Enabling SSH to the Appliance 8

Checking the Appliance Version 8

Enabling VNC to Manage the KVM-hosted VM 9

Installing KVM Dependencies on Appliance 10

Installing Windows Server 2019 on the KVM-hosted VM 12

Installing WiNC on the Windows Server 2019 VM 15

Installing WiNC Manually 15

Installing WiNC by Local ArcMC 15

Managing Windows Server 2019 VM 18

Replicating a VM in Other Systems 19

Send Documentation Feedback 20

Product Overview

Connector Hosting Appliance (CHA) is a hardened Linux-based hardware platform incorporating ArcSight Management Center (ArcMC) as well as on-board hosting of SmartConnectors. For more information, see ArcSight Management Center Administrator's Guide.

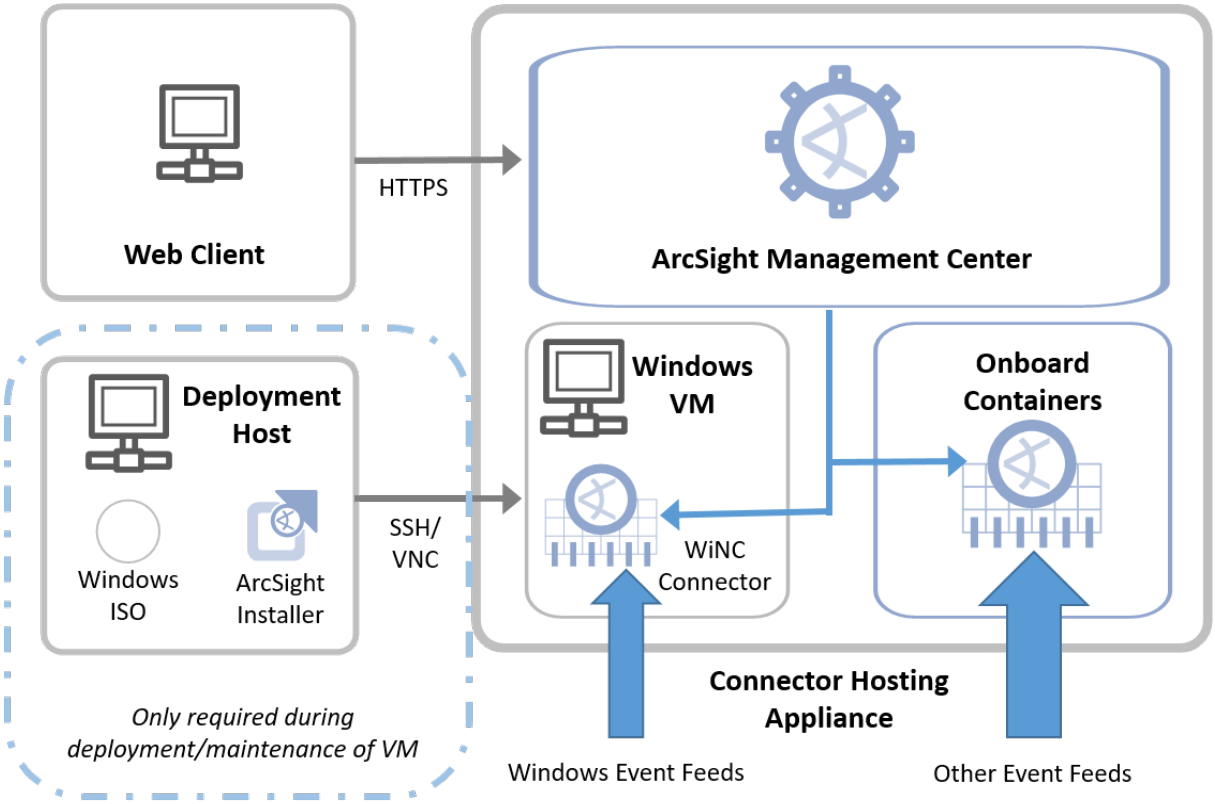
ArcSight SmartConnectors provide easy, scalable, and audit-quality collection of logs from event generating sources across the enterprise for real-time and forensic analysis. The SmartConnectors are optimized for remote event-collection from a large number of hosts without requiring the installation of a local agent. For more information, see ArcSight SmartConnector Users Guide.

SmartConnector for Microsoft Windows Event Log – Native (WiNC) helps to deliver critical Windows monitoring features, such as Operational Windows Event Logs and event collection and event filtering from IPv6 hosts. It leverages native Microsoft platform technology and provides the best support for Windows event features and capabilities (including collection for all Windows log types). For more information, see SmartConnector for Microsoft Windows Event Log - Native Configuration Guide.

As the WiNC SmartConnector requires a native Windows Server platform for installation, there is now a scalable mechanism to deploy the WiNC on the Linux-based CHA hardware appliance by leveraging standard Virtual Machine (VM) technology and function-based scripting to effectively deploy and manage the WiNC running a VM on the CHA platform.

Once deployed, the WiNC instance(s) can be fully monitored and managed like any other remote or embedded SmartConnector through the ArcMC User Interface.

The following diagram helps you understand the WiNC on CHA installation architecture:



WiNC on Connector Hosting Appliance

By leveraging the CHA appliance in this way, no additional physical host system need be provisioned for the successful deployment of the WiNC SmartConnector. It is installed into the VM hosted in the physical CHA system.

This guide provides information about deploying the WiNC SmartConnector on the ArcSight G9 C6600 CHA.

Prerequisites

Windows Server VM

The ArcSight administrator is responsible for building the Windows 2019 Server Core VM image, hardening it, and keeping it up-to-date with OS patches and other ongoing maintenance. This document describes how to create the initial image and the functions provided in the management scripts supporting installation and overall VM management. How the image is hardened, patched and otherwise kept up-to-date is determined by the administrator according to enterprise's requirements.

The Kernel-based Virtual Machine (KVM) hypervisor hosts and manages this VM image. After the Windows Server 2019 VM is booted into KVM, the WiNC software is installed and configured into this VM.

Management Software

Ensure that you have the following software applications and operating system (OS) before installing WiNC on CHA:

- G9 C6600 CHA appliance with RHEL 7.7 and ArcMC 2.9.x

  Note: By default, G9 C6600 CHA appliance comes with RHEL 7.5 and ArcMC 2.9.0. Therefore, you must upgrade RHEL 7.5 to 7.7. See Checking the Appliance Version.

- Windows Server 2019 Core image in ISO format (preferably hardened)
- A customer-provided and valid Windows Server 2019 license key
- WiNC appliance installer from Micro Focus
- The WiNC on CHA deployment script
- PuTTY or similar SSH client application
- A VNC client application such as Tiger VNC Viewer, VNC Viewer, or TightVNC Viewer, which is used to manage the KVM hypervisor
- ArcSight SmartConnector 7.15.0

Note: The required Linux packages for managing this environment on Gen9 CHA are provided with the installation materials and will be installed automatically.

Setting up KVM to Host the Windows Server 2019 Core VM

This section provides information for setting up KVM to host the Windows 2019 Server Core VM. Eventually the Windows Server 2019 Core VM will have WiNC SmartConnector setup.

Before setting up KVM, ensure that you complete the following prerequisites:

- Enable SSH to your appliance
- Check RHEL Version

Enabling SSH to the Appliance

You can enable SSH access to the appliance. By default, SSH access to your appliance is disabled. For optimal security purposes, enable SSH access only when necessary. For example, when troubleshooting.

Enable SSH access to your appliance:

1. Log in to the **ArcSight Management Center** console.
2. Click **Administration** > **Setup** > **System Admin**.
3. In the left navigation pane, under **System**, click **SSH**.
4. In the **SSH Configuration** page, under **SSH Status**, select **Enabled**.
5. In the **Change SSH Status** dialog, select **Yes**.

Checking the Appliance Version

Perform the following steps to check your appliance version:

1. Log in to PuTTy application as the **root** user by using your SSH key.
2. Enter the following command:

   ```
   cat /etc/os-release
   ```

3. If the RHEL version is not 7.7, upgrade RHEL OS to RHEL 7.7:

   Important: You cannot upgrade to RHEL OS 7.7 from earlier versions directly. It is mandatory to upgrade all prior versions of RHEL OS individually till RHEL 7.7. For example: To upgrade RHEL 7.5 to 7.7, you must upgrade RHEL 7.5 to RHEL 7.6, and then to RHEL 7.7

a. Download the tarball OS upgrade rpms from Micro Focus.
b. Go to the **ArcSight Management Center** console.
c. On the **Management Center** dashboard page, click **Administration** > **Setup** > **System Admin**.
d. In the left navigation pane, under **System**, click **License & Upgrade**.
e. Browse and upload respective rpms.

After the upgrade, appliance restarts.

Enabling VNC to Manage the KVM-hosted VM

This section describes about enabling Virtual Network Computing (VNC) to manage the KVM hosted Windows system after installation.

To enable VNC:

1. Establish an SSH session to CHA using VNC over an SSH tunnel by performing the following steps. This session is used to access WiNC appliance subsequently:
   a. Connect to your required SSH client such as PuTTY. Create a session with the CHA appliance (C6600 or C6700).
   b. In the PuTTY Configuration window, under **Category**, go to **Connection** > **SSH** > **Tunnels**.
   c. In the **Source port** field, enter **5901** to configure a tunnel for VNC on the port 5900. (5900 is the default port used by VM to forward VNC traffic. If this is the first time you are installing a VM, the 5900 port will be used, else contiguous port will be used.)
   d. In the **Destination** field, enter **127.0.0.1:5900**, and then click **Add**.
   The created tunnel appears in the left pane, under **SSH** list.
   e. In the left pane, select **Session**. Enter **Hostname (or IP address)** of the CHA appliance and enter **22** for the **Port** field.
   f. Select the **Connection Type** as **SSH** and click **Open** to start the SSH terminal.
   g. Connect and log in to the CHA appliance as the **root** user.
2. Modify `sshd_config` to allow VNC traffic to be tunneled:

Commands:

```
cp /opt/local/openssh/config/sshd_config /opt/local/openssh/config/sshd_config.ori
vi /opt/local/openssh/config/sshd_config
```

Modify the following parameters:

From **`AllowTcpForwarding no`** to **`AllowTcpForwarding yes`**

From **`#PermitTunnel no`** to **`PermitTunnel yes`**

Verify the following parameters:

Command:

```
diff /opt/local/openssh/config/sshd_config{.ori,}
```

Output:

```
85c85
< AllowTcpForwarding no
---
> AllowTcpForwarding yes
102c102
< #PermitTunnel yes
---
> PermitTunnel yes
```

3. Run the following command to restart SSHD service:

```
systemctl restart arcsight_sshd.service
```

Installing KVM Dependencies on Appliance

Linux RHEL 7.7 comes with the default capabilities of KVM. To manage the additional capabilities, install the following dependencies before you proceed with the Windows installation on KVM:

- Dependencies
- WiNC_CHA_Installer.sh

Note: Before installing all Dependencies, ensure you have WiNC appliance installer from Micro Focus that contains **Dependencies** and **WiNC_CHA_Installer.sh** files.

To install all dependencies:

1. Place the WiNC appliance installer to the `/opt` directory in CHA.
2. Run the **WiNC_CHA_Installer.sh** script and choose **option 1** to install all dependencies. Since you do not have a pre-installed image in the installer, the script exits with the following exception:

```
"Error: Image file WiNC_CHA_VM_Image.qcow2 does not exist. Please use the
original distribution that contains all the required files."
```

3. Create the **WiNC_CHA_VM_Image.qcow2** image. Refer to Installing Windows Server 2019 on the KVM-hosted VM for instructions.
4. After creating an image, rerun the **WiNC_CHA_Installer.sh** script and choose **option 9** to back up the running WiNC appliance. Now, WiNC appliance installer contains the following files and folder:
   - Dependencies
   - WiNC_CHA_Installer.sh
   - WiNC_CHA_VM_Image.qcow2

   Now, the KVM and Windows setup is ready and available to replicate in any other required systems. For more information, see Replicating a VM in Other Systems.

Installing Windows Server 2019 on the KVM-hosted VM

To install Windows Server 2019 into the KVM-hosted VM, perform the following steps:

1. Deploy WiNC appliance as follows:
   a. Open the PuTTy session.
   b. Copy the **Windows ISO** image to the /opt directory in CHA and then rename it to **WindowsServer2019.iso** by using the following command:

```
mv /opt/CURRENT_ISO_NAME /opt/WindowsServer2019.iso
```

   c. Assign the following variables with their respective values by using the following commands:

```
export WINDOWS_VM_NAME="WiNC_CHA_VM"
export WINDOWS_VM_VARIANT="win2k19"
export WINDOWS_VM_IMAGE="WiNC_CHA_VM_Image.qcow2"
export WINDOWS_VM_IMAGE_RAW="WiNC_CHA_VM_Image.img"
export ARCSIGHT_HOME=/opt/arcsight
export RAM=16384
export CPUS=8
export HARD_DISK=60
```

   d. Create a 60 GB file to store the WiNC appliance disk image:

```
mkdir -p $ARCSIGHT_HOME/connectors/WiNC_CHA/guests/images
time dd if=/dev/zero of=$ARCSIGHT_HOME/connectors/WiNC_
CHA/guests/images/$WINDOWS_VM_IMAGE_RAW bs=1G count=$HARD_DISK
qemu-img convert -f raw -O qcow2 $ARCSIGHT_HOME/connectors/WiNC_
CHA/guests/images/$WINDOWS_VM_IMAGE_RAW $ARCSIGHT_HOME/connectors/WiNC_
CHA/guests/images/$WINDOWS_VM_IMAGE
rm -rf $ARCSIGHT_HOME/connectors/WiNC_CHA/guests/images/$WINDOWS_VM_IMAGE_RAW
ls -lh $ARCSIGHT_HOME/connectors/WiNC_CHA/guests/images/$WINDOWS_VM_IMAGE
```

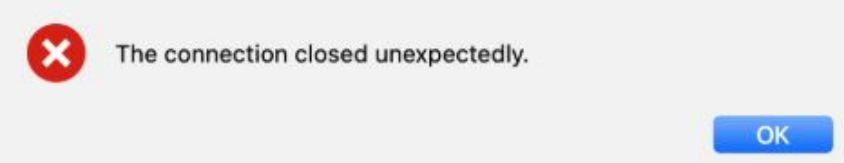
   e. Create the VM instance:

```
timeout 10 virt-install --virt-type=kvm --name $WINDOWS_VM_NAME --
cdrom=/opt/WindowsServer2019.iso --network default --memory ${RAM} --vcpus
${CPUS} --rng /dev/urandom --disk $ARCSIGHT_HOME/connectors/WiNC_
CHA/guests/images/$WINDOWS_VM_IMAGE --os-variant=$WINDOWS_VM_VARIANT --graphics
vnc
```

   Parameters mentioned in the commands above are used as inputs for the `virt-install` command and each parameter is self-explanatory.

```
--network default {we have two option for network 1. bridge 2. NAT , default
reflect the NAT}
```

2. Complete the Windows installation:
   a. Start VNC viewer on your system (such as TigerVNC) and connect to 127.0.0.1:5901. The following exception is displayed. Click **OK**.



   Go to PuTTy session and run the following commands to resolve the above exception:

Command:

```
getenforce
```

Output:

```
 Enforcing
```

Command:

```
grep vnc_port_t /var/log/audit/audit.log | audit2allow
```

Output:

```
s ============= sshd_t ==============
 !!!! This avc is allowed in the current policy
 allow sshd_t vnc_port_t:tcp_socket name_connect;
```

Commands:

```
grep vnc_port_t /var/log/audit/audit.log | audit2allow -M WiNC_CHA_vnc
semodule -i WiNC_CHA_vnc.pp
systemctl restart arcsight_sshd.service
semodule -i WiNC_CHA_vnc.pp
```

Important: You must re-establish the PuTTy session with tunnel to connect the VM through VNC viewer.

   b. Follow the Windows installation steps and select **Windows Server 2019 Standard**.
   c. After installation, the VNC connection drops because of the reboot.
   d. Go to PuTTy session and run the following command to check whether the Windows has successfully rebooted:

```
virsh list --all
```

If the WiNC_CHA_VM is not running, run the following command:

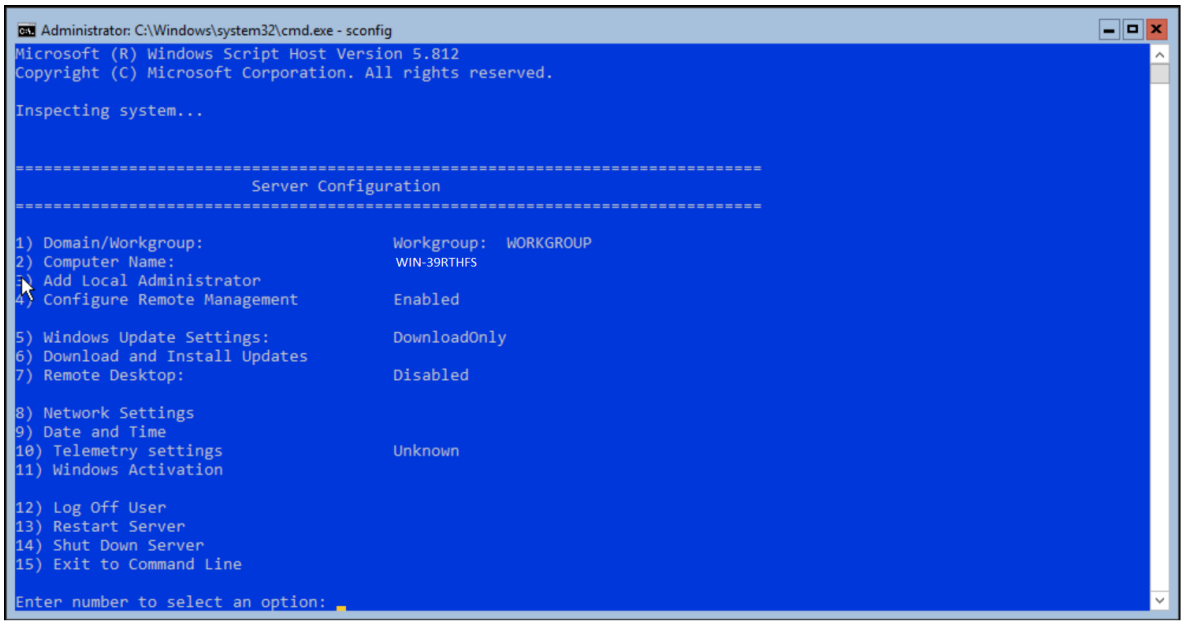
```
virsh WiNC_CHA_VM start
```

   e. Re-establish the VNC connection to WiNC appliance.

3. Change the Windows hostname:
   a. Open the command prompt in Windows and enter the following command:

      ```
      sconfig
      ```

      The **Server Configuration** details display in the command-line window as shown in the following image:



   a. For **Enter number to select an option:** type **2** and press **Enter**.
   b. For **Enter new computer name:** type **`WiNC_CHA_HOST`** and press **Enter**.
   c. Restart Windows to apply changes by entering **13**.
   d. Reconnect VNC. Refer to step 2 instructions mentioned above.
   e. On the command prompt, enter the following command to verify the hostname:

      ```
      hostname
      ```

4. To restart VM automatically when the system reboots, run the following commands:

   ```
   export WINDOWS_VM_NAME="WiNC_CHA_VM"
   virsh autostart $WINDOWS_VM_NAME
   ```

5. Install WiNC SmartConnector instances as required. Refer to Installing WiNC on the Windows Server 2019 VM for instructions.

Installing WiNC on the Windows Server 2019 VM

This section provides information about installing the WiNC SmartConnector into the Window Server 2019 VM by using any of the following methods:

Installing WiNC Manually

1. Copy the WiNC Windows installer file to the /opt directory on CHA.
2. Open the VNC viewer and connect to WiNC appliance.
3. On the command prompt, enter the following command to access the Windows PowerShell command-line editor:

   ```
   powershell
   ```

4. Enter the following command to copy the WiNC installer from CHA to WiNC appliance:

   ```
   scp
   For example: scp root@CHA_IP:/opt/WiNC_Installer C:\Your_Location
   ```

5. You can install multiple instances of WiNC to gather local and other WiNC appliance hosted logs. For more information about installing WiNC, refer to the MS Windows Event Log–Native SmartConnector (WiNC) Configuration guide available on the Micro Focus Community page.

Installing WiNC by Local ArcMC

Local ArcMC is the ARcMC running on the same CHA.

To install the WiNC SmartConnector into the Windows Server 2019 VM through local ArcMC:

1. Prepare the WiNC appliance for ArcMC to use:
   a. Open the command prompt using the VNC viewer and enter the following command to access the Windows PowerShell command-line editor:

      ```
      powershell
      ```

   b. Verify whether port 5986 is enabled:

      ```
      WinRM e winrm/config/listener
      ```

c. If port 5986 is not enabled:

Command 1:

```
New-SelfSignedCertificate -DnsName "WiNC_CHA_HOST" -CertStoreLocation
Cert:\LocalMachine\My
```

Output:

```
PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My
Thumbprint -------Subject
---------- -------
BF5C63693DB069911532E510140506BD6CXXXXXX CN= WiNC_CHA_HOST
```

Command 2: Copy the Command 1 parameters from its output to the respective places (as shown below) in the following command:

```
winrm create winrm/config/Listener?Address=*+Transport=HTTPS '@{Hostname="WiNC_
CHA_HOST"; CertificateThumbprint=" BF5C63693DB069911532E510140506BD6CXXXXXX "}'
```

Output:

```
ResourceCreated
Address = http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
ReferenceParameters
ResourceURI = http://schemas.microsoft.com/wbem/wsman/1/config/listener
SelectorSet
Selector: Address = *, Transport = HTTPS
```

Command 3:

```
Enable-WSManCredSSP -Role Server
```

d. Run the following commands to open the firewall ports:

```
New-NetFirewallRule -name WiNC_WinRM_OUT -DisplayName "WiNC_WinRM_OUT" -Enable
True -Direction Outbound -Action Allow -Protocol TCP -LocalPort 5986
New-NetFirewallRule -name WiNC_RM1_OUT -DisplayName "WiNC_RM1_OUT" -Enable True
-Direction Outbound -Action Allow -Protocol TCP -LocalPort 9014
New-NetFirewallRule -name WiNC_RM2_OUT -DisplayName "WiNC_RM2_OUT" -Enable True
-Direction Outbound -Action Allow -Protocol TCP -LocalPort 9015
New-NetFirewallRule -name WiNC_WinRM_IN -DisplayName "WiNC_WinRM_IN" -Enable
True -Direction Inbound -Action Allow -Protocol TCP -LocalPort 5986
New-NetFirewallRule -name WiNC_RM1_IN -DisplayName "WiNC_RM1_IN" -Enable True -
Direction Inbound -Action Allow -Protocol TCP -LocalPort 9014
New-NetFirewallRule -name WiNC_RM2_IN -DisplayName "WiNC_RM2_IN" -Enable True -
Direction Inbound -Action Allow -Protocol TCP -LocalPort 9015
```

Note: Port 9014 is available to deploy first WiNC instance.
Port 9015 is available to deploy second WiNC instance.

2. Go to the **ArcSight Management Center** console and install WiNC using the One Click / Instant deployment feature.

   For more information, refer to the *Instant Connector Deployment* section in the *ArcSight Management Center Administrator's* Guide, available on the Micro Focus Community page.

Managing Windows Server 2019 VM

WiNC Connector Management script is a configuration file that enables you to install WiNC on CHA and also manage the Windows server VM.

This section provides information about understanding all the installer script options and their capabilities. The following table provides information about the different options the script provides:

Option	Description
Install WiNC Appliance	Installs the **Dependencies** directory from the current location where you are running the script. Installs the WiNC appliance as per your inputs. If the WiNC appliance is already installed it displays the WiNC appliance details on the console. It also, enables local ArcMC to manage the WiNC connector on WiNC appliance.
Enable remote ArcMC to manage WiNC (DISABLED)	This option is disabled. Do not use it.
Reset to factory settings	Resets the WiNC appliance to factory settings. You can back up this image by using the relevant option in the script before resetting to factory settings.
Create a snapshot of WiNC appliance	Creates a snapshot. If a snapshot already exists it displays the details of it. You can create only one snapshot.
View an existing WiNC appliance snapshot	Displays the snapshot details, if available.
Revert WiNC appliance to an existing snapshot	Reverts the VM from an existing snapshot.
Uninstall WiNC appliance	Uninstalls the WiNC appliance and deletes all the created files.
Increase C drive size in Windows VM (DISABLED)	This option is disabled. Do not use it.
Backup your VM image, if you have setup the VM manually without using the script	Backs up the VM image as **WiNC_CHA_VM_Image.qcow2** in the folder where you are running the **WiNC_CHA_Installer.sh** script.
Exit	Terminates the installer script.

Replicating a VM in Other Systems

Perform the following steps to automatically replicate the KVM and Windows setup in any targeted machine using the installer script:

To prepare package for the VM replication:

1. Run the **WiNC_CHA_Installer.sh** installer script.
2. After setting up the Windows Server 2019 Core VM, rerun the **WiNC_CHA_Installer.sh** script and choose **option 9** to back up the VM. The backup VM image is created as as **WiNC_CHA_VM_Image.qcow2** in the folder where you are running the **WiNC_CHA_Installer.sh** script. Ensure the following files and folder are present in this folder:
   - Dependencies
   - WiNC_CHA_Installer.sh
   - WiNC_CHA_VM_Image.qcow2
3. Choose **option 10** to exit the script.
4. Create a zipped folder of the following files:
   - Dependencies
   - WiNC_CHA_Installer.sh
   - WiNC_CHA_VM_Image.qcow2

To replicate the VM in another G9 appliance:

1. Copy the zipped folder to any other ArcMC appliance.
2. Enable SSH to your appliance.
3. Enable VNC to Manage the KVM-hosted VM.
4. Unzip the folder.
5. Run the **WiNC_CHA_Installer.sh** installer script.
6. Choose **option 1** from the installer script to start the installation.

   Now, the VM is ready and available to setup the WiNC connector.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Installation Guide for WiNC on Connector Hosting Appliance (WiNC on CHA 1.1.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arcsight_doc@microfocus.com.

We appreciate your feedback!