Micro Focus Security ArcSight SmartConnector

Software Version: 1.1.0

WiNC on Connector Hosting Appliance Installation Guide

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

Legal Notices

Copyright Notice

© Copyright 2020 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, “commercial computer software” is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation (“FAR”) and its successors. If acquired by or on behalf of any agency within the Department of Defense (“DOD”), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement (“DFARS”) and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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

Contents

Product Overview 4
Prerequisites 4
Enabling SSH to the Appliance 5
Checking the Appliance Version 5
Installing a Virtual Machine on CHA 5
Installing Windows on CHA 8
Installing WiNC 10
Installing WiNC Manually 10
Installing WiNC by Local ArcMC 10

Send Documentation Feedback 12

Product Overview

<description will be added later> .

Prerequisites

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

- PuTTY application
- Any of the VNC clients such as Tiger VNC Viewer, VNC Viewer, or TightVNC Viewer
- WiNC Hosting Appliance Package from Micro Focus
- Windows Server 2019 Core image in ISO format (preferably hardened) with a valid license
- WiNC installer
- RHEL version 7.7

For information about checking the RHEL version of your appliance, see Checking Appliance Version.

Note: In addition to the above prerequisites, ensure that you enable SSH.

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:
   a. Get 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.

   The RHEL successfully upgrades to 7.7 and restarts the CHA.

Installing a Virtual Machine on CHA

To install a virtual machine on CHA, perform the following steps:

1. Establish an SSH session to CHA using VNC (Virtual Network Computing) over an SSH tunnel by performing the following steps. This session is used to access Windows guest OS 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 **5900** 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 the **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. Run the following commands to allow VNC traffic to be forwarded by an SSHD (Secure Shell Daemon):

Command:

```
# getenforce
```

Output:

```
 Enforcing
```

Command:

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

Output:

```
#============= 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
```

3. Modify `sshd_config` to allow VNC traffic to be tunneled:

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

# vi /opt/local/openssh/config/sshd_config <---------------------- apply the below
changes

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

85c85

< AllowTcpForwarding no

---

> AllowTcpForwarding yes

102c102

< #PermitTunnel yes

---

> PermitTunnel yes
```

4. Restart SSHD service:

```
# systemctl restart arcsight_sshd.service
```

5. Install the dependencies for building a virtual machine:
   a. Get the WiNC Hosting Appliance Package from Micro Focus.
   b. Place the package to the `/opt` directory in CHA. The package contains following files:
      - Dependencies
      - WiNC_CHA_Installer.sh
   c. 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 WiNC Hosting Appliance Package the script exits with the following message:

      ```
      "Dependencies have installed successfully."

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

   d. Create the `WiNC_CHA_VM_Image.qcow2` image. Refer to Installing Windows on CHA for instructions.
   e. After creating an image, rerun the `WiNC_CHA_Installer.sh` script and choose **option 9** to back up the running Windows guest OS. Now, the WiNC Hosting Appliance Package contains following files:
      - Dependencies
      - WiNC_CHA_Installer.sh
      - WiNC_CHA_VM_Image.qcow2

   You can now use the WiNC Hosting Appliance Package as an original distribution, and the script to install and manage the virtual machine and Windows guest OS in any targeted CHA machine.

Installing Windows on CHA

To install Windows on CHA, perform the following steps:

1. Deploy Windows guest OS as follows:
   a. Copy the **Windows ISO** image to the /opt directory in CHA and then rename it to **WindowsServer2019.iso**:

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

   b. Assign the following variables with their respective values:

   ```
   # WINDOWS_VM_HOSTNAME="WiNC_CHA_HOST"
   # WINDOWS_VM_NAME="WiNC_CHA_VM"
   # WINDOWS_VM_NAME_SNAP="WiNC_CHA_VM_Snapshot"
   # WINDOWS_VM_VARIANT="win2k19"
   # WINDOWS_VM_IMAGE="WiNC_CHA_VM_Image.qcow2"
   # export ARCSIGHT_HOME=/opt/arcsight
   # RAM=16
   # CPUS=8
   ```

   c. Create a 60 GB file to store the Windows guest OS disk image:

   ```
   # mkdir -p $ARCSIGHT_HOME/connectors/WiNC_CHA/guests/images
   # time dd if=/dev/zero of=$ARCSIGHT_HOME/connectors/WiNC_
   CHA/guests/images/WindowsServer2019.img bs=1G count=60
   # qemu-img convert -f raw -O qcow2 $ARCSIGHT_HOME/connectors/WiNC_
   CHA/guests/images/WindowsServer2019.img $ARCSIGHT_HOME/connectors/WiNC_
   CHA/guests/images/$WINDOWS_VM_IMAGE
   # rm $ARCSIGHT_HOME/connectors/WiNC_CHA/guests/images/WindowsServer2019.img
   # ls -lh $ARCSIGHT_HOME/connectors/WiNC_CHA/guests/images/$WINDOWS_VM_IMAGE
   ```

   d. Create the VM instance:

   ```
   # virt-install=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.

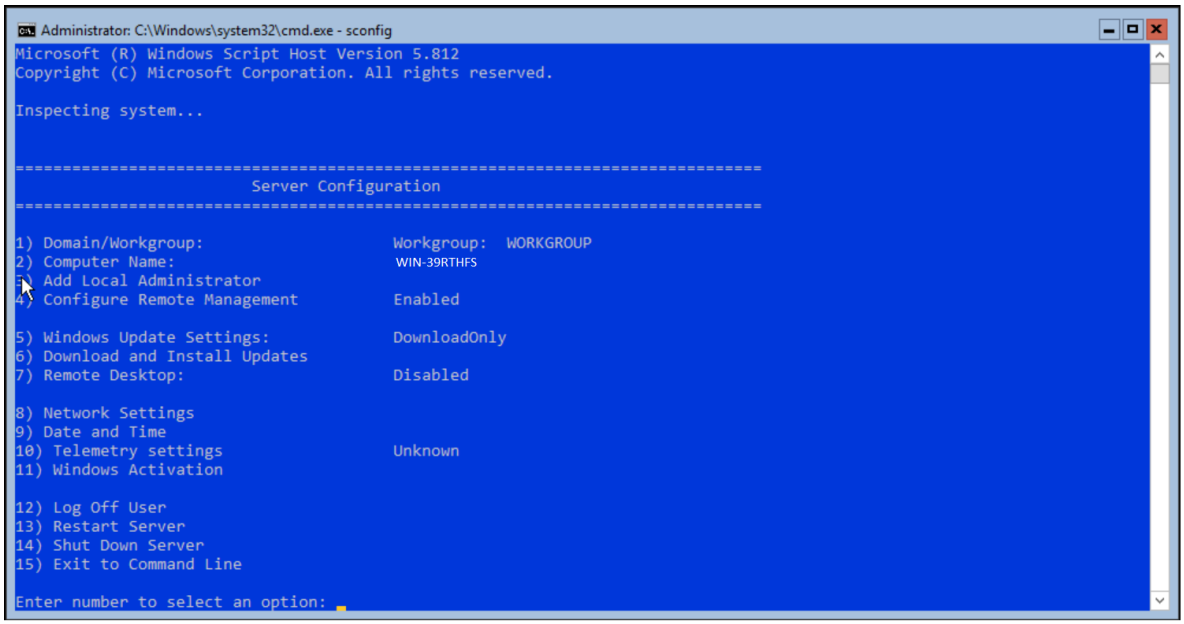
   ```
   --network default {we have two option for network 1. bridge 2. NAT , default
   reflect the NAT}
   ```

   Important: The `virt-install` command waits for the Windows installation to complete, therefore don't cancel it and proceed with the next steps.

2. Complete the Windows installation:
   a. Start VNC viewer on your system (such as TigerVNC) and connect to 127.0.0.1:5900.
   b. Follow the Windows installation steps.
   c. Re-establish the VNC connection to Windows guest OS if it drops because of the reboot.
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 then 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 the VNC. Refer to step 2 instructions mentioned above.
   e. On the command prompt, enter the following command to verify the hostname:

      ```
      hostname
      ```

4. Install WiNC instances as required. Refer to Installing WiNC for instructions.

Installing WiNC

You can install WiNC by using any of the following methods:

Installing WiNC Manually

1. Copy the WiNC Windows installer file to the /opt directory in CHA.
2. Open the VNC viewer and connect to Windows guest OS.
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 Windows guest OS:
   - `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 Windows guest OS hosted logs accordingly. 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:

1. Prepare the Windows guest OS for ArcMC to use as follows:
   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 Command 1 parameters from its output to the respective places 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`

Note: Port 9014 is available to use in ArcMC to deploy first WiNC instance.
Port 9015 is available to use in ArcMC 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.

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 WiNC on Connector Hosting Appliance Installation Guide (SmartConnector 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!