Micro Focus Security
WiNC on CHA

Software Version: 8.1.0

Installation Guide for WiNC on Connector Hosting Appliance

Document Release Date: December 3, 2020
Software Release Date: December 3, 2020

MICRO FOCUS

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
12/03/2020	Added support for G10 C6700 Connector Hosting Appliance.
07/31/2020	First edition of this guide.

Contents

About This Guide

This guide provides information about deploying the WiNC SmartConnector on the ArcSight G9 C6600 or G10 C6700 CHA.

Product Overview

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

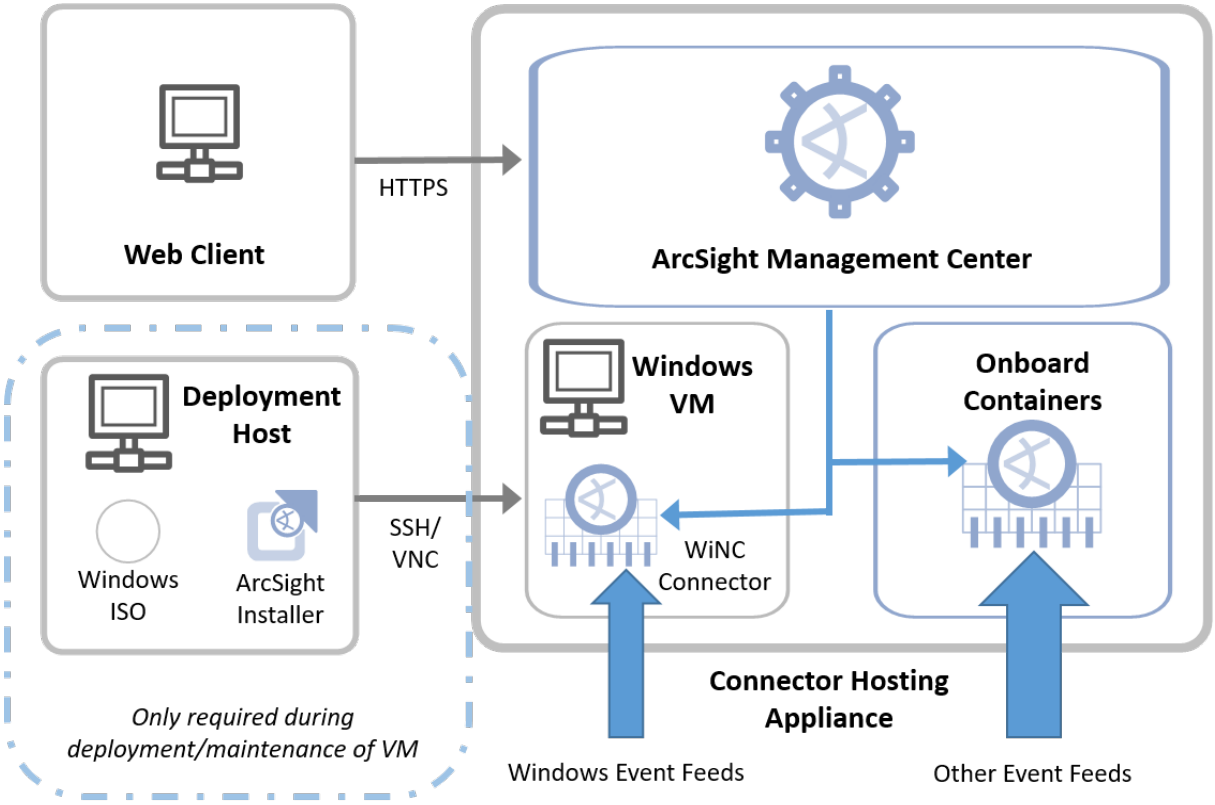
ArcSight SmartConnectors provide easy, scalable, and audit-quality collection of logs from event generating sources across the enterprise for real-time and forensic analysis. The SmartConnectors are optimized for remote event-collection from a large number of hosts without requiring the installation 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 needs be provisioned for the successful deployment of the WiNC SmartConnector. It is installed into the VM hosted in the physical CHA system.

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 or G10 C6700 CHA with RHEL 7.7 and ArcMC 2.9.x

  Note: By default, the G10 C6700 CHA comes with RHEL 7.7. However, G9 C6600 CHA comes with RHEL 7.5, which you must manually upgrade to 7.7.

- Windows Server 2019 Core image in ISO format (preferably hardened)
- Windows Server 2019 license key
- WiNC appliance installer from Micro Focus
- 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 Windows VM
- ArcSight SmartConnector package version 7.15.0 or later

Setting Up the Windows Server 2019 VM on the Appliance

This section provides information for setting up the Windows Server 2019 as a Core VM on the appliance. Ultimately, the Windows Server 2019 Core VM will have WiNC SmartConnector setup.

Enabling SSH on the Appliance

Before setting up the Windows Server 2019 as a VM, ensure that you enable SSH access on 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.

To enable SSH access on your appliance:

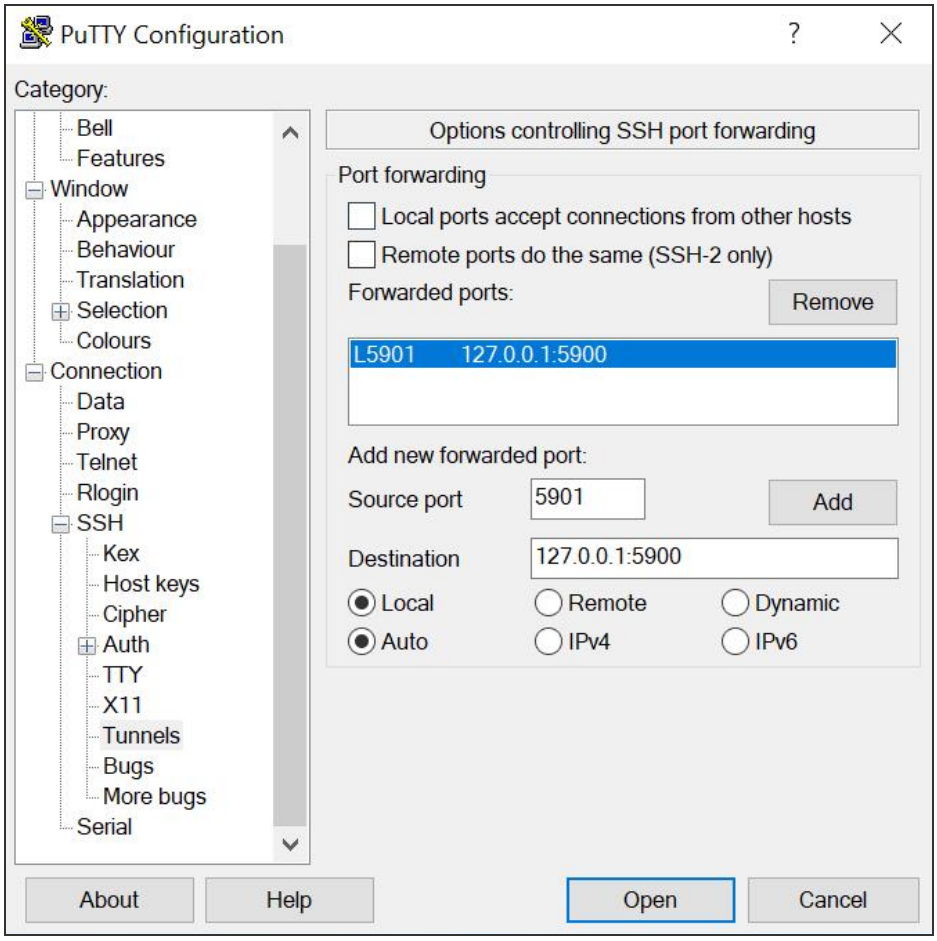
1. Log in to the **ArcSight Management Center** console.
2. Click **Administration** > **Setup** > **System Admin**.
3. In the left navigation pane, under **System**, click **SSH**.
4. In the **SSH Configuration** page, under **SSH Status**, select **Enabled**.
5. In the **Change SSH Status** dialog,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

Connecting to VNC to Manage the Windows VM

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

To connect to VNC, establish an SSH session to CHA using VNC over an SSH tunnel by performing the following steps. This session is used to access the WiNC appliance subsequently:

1. Connect to your required SSH client such as PuTTY. Create a session with the CHA appliance (C6600 or C6700).



2. In the left pane, select **Session**. Enter the **Hostname (or IP address)** of the CHA appliance and enter **22** for the **Port** field.
3. Select the **Connection Type** as **SSH** and click **Open** to start the SSH terminal.
4. Connect and log in to the CHA as the **root** user.
5. After logging in to the CHA, right-click the SSH window header and select **Change Settings** from the window menu.
6. In the PuTTY Configuration window, under **Category**, go to **Connection** > **SSH** > **Tunnels**.
7. In the **Source port** field, enter **5901** to configure a tunnel for VNC on the port 5900.
8. 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.

Setting Up the Appliance for Windows Installation

RHEL 7.7 comes with the default capabilities of KVM.

To manage the additional capabilities and install all the dependencies provided in the installer script:

1. Log in to the appliance and download the appliance build: `ArcSight_WiNC_Hosting_Appliance.8.1.0.xxxxx.0.tgz`.
2. Extract the `ArcSight_WiNC_Hosting_Appliance.8.1.0.xxxxx.0.tgz` zip file to the `/opt` directory. This directory contains the following files and folder:
   - arcmcConfig.ps1
   - Dependencies
   - WiNC_CHA_Installer.sh
3. Run the `./WiNC_CHA_Installer.sh` script. Choose **option 1** to install the WiNC appliance and follow the instructions provided in the script. After the installation is complete, re-establish the PuTTY session.
4. Connect to the the VNC viewer and complete the Windows installation. After the installation is complete, a VM will shut down and the VNC viewer will be disconnected automatically. Refer to "Connecting to VNC to Manage the Windows VM" on page 8 for instructions.
5. Open the PuTTy session and run the following command.

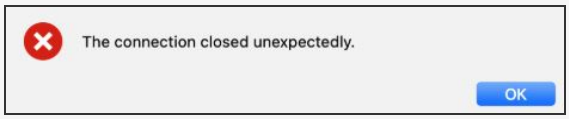
   ```
   virsh start WiNC_CHA_VM
   ```
6. Open the VNC viewer and PowerShell command-line editor. Refer to "Connecting to VNC to Manage the Windows VM" on page 8 for instructions.
7. Run the following command and copy the `.\arcmcConfig.ps1` Powershell script to the Windows VM:

   ```
   scp root@cha_ip:/scipt_path/arcmcConfig.ps1 c:\your_windows_path
   ```
8. Run the the `.\arcmcConfig.ps1` Powershell script to configure WinRM and add the required firewall polices.

Note: The `.\arcmcConfig.ps1` Powershell script enables WinRM and creates the required firewall policies to install the connector through ArcMC.

9. After creating an image, rerun the `./WiNC_CHA_Installer.sh` script and choose **option 7** to make a backup of the appliance image. The following backup file will be created:
   - WiNC_CHA_VM_Image.qcow2

Note: If you cannot connect to the VNC viewer and encounter the following error, run the `WiNC_CHA_VM` script with **option 6** that enabled VNC access mode of SElinux for Windows appliance. After running the script, connect through the VNC viewer and launch PowerShell.



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

Installing WiNC on the Windows Server 2019 VM

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

Installing WiNC Manually

1. Copy the WiNC Windows installer file into the /opt directory on CHA.
2. Open the VNC viewer and connect to the 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 on the Windows Server 2019 VM through a local ArcMC:

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 the Windows Server 2019 VM

The 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 a local ArcMC to manage the WiNC connector on the WiNC appliance.
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.
Enable VNC access in the Enforcing mode of SELinux for WiNC appliance	Configures SELinux to access VNC in the Enforcing mode.
Back up the WiNC appliance image, if you have set up 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.
Uninstall WiNC appliance	Uninstalls the WiNC appliance and deletes all the created files.
Exit	Terminates the installer script.

Replicating a VM in Other Systems

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

To prepare a 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 7** to make a back up of the VM. The backup VM image is created 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
   - arcmcConfig.ps1
   - WiNC_CHA_VM_Image.qcow2
3. Choose **option 9** to exit the script.
4. Create a zipped folder of the following files:
   - Dependencies
   - WiNC_CHA_Installer.sh
   - arcmcConfig.ps1
   - WiNC_CHA_VM_Image.qcow2

To replicate the VM in another G9 or G10 appliance:

1. Copy the zipped folder to any other ArcMC appliance.
2. Enable SSH on your appliance.
3. Connect to VNC to Manage the Installed Windows 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 8.1.0)

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!