CCE Orchestration Windows OpenSSH Hardening

CCE Orchestration Windows OpenSSH Hardening

Cloud Connect server establishes a password-less Secure Shell (SSH) connection to Windows nodes (ICM and CVP) for Orchestration. This section describes the OpenSSH hardening for CCE Orchestration.

Make the following configuration changes in the OpenSSH service daemon configuration file that is located at *%programdata%\ssh\sshd_config* on Windows nodes and restart the OpenSSH services. See the Orchestration section in the CCE Install and Upgrade Guide for details on the OpenSSH services.

Settings	**Compliance Configuration**	**Description**
Restrict SSH connection	`AllowUsers localuser@CloudConnectIP`	AllowUsers in sshd_config ensures that only the Cloud Connect server host can connect through the SSH to Windows user. **Note** Configuration `localuser@CloudConnectIP` allows the remote Cloud Connect node that is specified by Cloud Connect IP to connect through SSH to my local Windows account user. Both Publisher and Subscriber of Cloud Connect must have an entry for this configuration.
Enable DNS hostname check	`UseDNS yes`	Setting this flag to 'Yes' ensures that the server validates the hostname or IP address combination of the client (Cloud Connect server) that is connecting to it against the DNS server.
Set the maximum number of authentication attempts	`MaxAuthTries 3`	Recommended MaxAuthTries is 3.

Settings	Compliance Configuration	Description
Encryption Cipher	`HostKey` _PROGRAMDATA __/ssh/ssh_host_rsa_key #HostKey __PROGRAMDATA __/ssh/ssh_host_dsa_key #HostKey __PROGRAMDATA __/ssh/ssh_host_ecdsa_key #HostKey __PROGRAMDATA __/ssh/ssh_host_ed25519_key #HostKey	By default, RSA is used as the default cipher while establishing SSH connection between Cloud Connect server and Windows node. You can choose Cipher such as ECDSA. Uncomment the ECDSA and comment out RSA. **Note** After changing the Cipher type, users have to run the command `utils deployment test-connection` in the Cloud Connect CLI, from both publisher and subscriber against this particular Windows node to make sure that the new Cipher is used for the security handshake. See CCE Install and Upgrade Guide for details on the CLI. **Note** While you upgrade the ICM or Cisco Unified Customer Voice Portal, the latest version will not retain the custom configuration modified on the setting `%programdata%\ssh\sshd_config`. Back up the file `sshd_config` before the upgrade, and post upgrade restore the `sshd_config` file or redo the custom changes on `sshd_config` after upgrade. Restart the OpenSSH services after updating `sshd_config`, and run the command**utils deployment test-connection** from both publisher and subscriber nodes of Cloud Connect against the window node.

Settings	Compliance Configuration	Description
Common Vulnerability and Exposures (CVE-2023-48795) for OpenSSH	Use the following set of strong ciphers and MACs in the `sshd_config` file to avoid weak ciphers: **Note** You should use the below format. Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com MACs umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512 Below vulnerable ciphers can be disabled (either removed or commented) if the ciphers are present in the `%programdata%\ssh\sshd_config` file: chacha20-poly1305@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha1-etm@openssh.com hmac-md5-etm@openssh.com If these ciphers do not exist in the `sshd_config` file, you can ignore the change.	By default, OpenSSH services are enabled for ICM and CVP nodes. Hence, the following OpenSSH versions that are packaged with ICM and CVP are marked as affected versions: • OpenSSH 8.1.0.0 for Release 12.6(1) • OpenSSH 8.9.1.0 for Release 12.6(2) If the ciphers are not present in the `sshd_config` file, by default all the allowed ciphers are used. Hence, to avoid the weak ciphers, it is recommended to update the strong ciphers in the `sshd_config` file.

Restricting Access to OpenSSH sshd_config

Initially, appropriate user-based permissions have been configured for `sshd_config` during the installation of OpenSSH via the installation of CVP or ICM mandatory ES used for onboarding the Windows nodes to Cloud Connect for Orchestration.

In case if the platform Orchestration administrator user is changed by the administrator, then the permissions must be set to restrict access to `OpenSSH sshd_config` for the new user. To restrict the access to `OpenSSH sshd_config` perform the following steps:

Procedure

Step 1 Log in to Windows node (CVP or ICM) with new platform Orchestration administrator user.

Step 2 Launch PowerShell in administrator mode.

Step 3 Navigate to the default installation directory of OpenSSH (for example: `C:\icm\install\OpenSSH-Win64` in case of ICM).

Step 4 Run the command **Import-Module .\OpenSSHUtils.psd1 -Force**.

Step 5 Run the command **Repair-SshdConfigPermission -FilePath C:\ProgramData\ssh\sshd_config**.

Step 6 Press the **Enter** key to select the default option "Y" for queries on inheritance and access restriction.

On successful execution of the above command, *%programdata%\ssh\sshd_config* is set with restricted access.

Step 7 Restart the OpenSSH services. See the Orchestration section in CCE Install and Upgrade Guide for details on the OpenSSH services.

Step 8 Run the command **utils deployment test-connection** in Cloud Connect CLI, from both publisher and subscriber against this particular Windows node. This is to make sure the Cloud Connect server is able to establish password-less Secure Shell (SSH) connection to Windows nodes (ICM and CVP) for Orchestration.