# CCE Orchestration Windows OpenSSH の強化



## CCE Orchestration Windows OpenSSH の強化

Cloud Connect サーバが、オーケストレーション用の Windows ノード（ICM および CVP）へのパスワードレス セキュア シェル（SSH）接続を確立します。このセクションでは、CCE オーケストレーションの OpenSSH 強化について説明します。

Windows ノードの*%programdata%\ssh\sshd_config* にある OpenSSH サービス のデーモン設定ファイルで次の設定を変更し、OpenSSH サービスを再起動する必要があります。OpenSSH サービスの詳細については、『CCE のインストールとアップグレードガイド』の「オーケストレーション」のセクションを参照してください。

| 設定 | コンプライアンス設定 | 説明 |
|---|---|---|
| SSH 接続の制限 | `AllowUsers localuser@CloudConnectIP` | sshd_config の AllowUsers は、クラウド接続サーバホストだけが SSH 経由で Windows ユーザに接続できるようにします。<br>（注） 設定 `localuser@CloudConnectIP` とは、Cloud Connect IP で指定されているリモートクラウド接続ノードが、SSH 経由でローカルの Windows アカウントユーザに接続を許可することを意味します。クラウド接続のパブリッシャとサブスクライバの両方に、この設定のエントリが必要です。 |

| 設定 | コンプライアンス設定 | 説明 |
|---|---|---|
| DNS ホスト名チェックの有効化 | `UseDNS はい` | このフラグを [はい（Yes）] に設定すると、サーバは DNS サーバに対して接続されているクライアント（クラウド接続サーバ）のホスト名または IP アドレスの組み合わせを検証します。 |
| 認証試行の最大回数を設定する | `MaxAuthTries 3` | 推奨される MaxAuthTries は 3 です。 |
| 暗号化方式 | `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` | デフォルトでは、RSA がデフォルトの暗号として使用され、クラウド接続サーバと Windows ノード間で SSH 接続が確立されます。<br>顧客は ECDSA などの暗号を選択できます。ECDSA のコメントを解除し、RSA をコメントアウトします。<br>（注） 暗号タイプを変更した後、ユーザは、この特定の Windows ノードに対して、パブリッシャとサブスクライバの両方から、Cloud Connect CLI でコマンド `utils deployment test-connection` を実行し、新しい暗号がセキュリティハンドシェイクに使用されるのを確認する必要があります。CLI の詳細については、『CCE のインストールとアップグレードガイド』を参照してください。 |

# OpenSSH sshd_config へのアクセスの制限

当初、Windows ノードの Orchestration 用の Cloud Connect へのオンボードに使用される CVP または ICM の必須 ES のインストールを通じて、OpenSSH のインストール中に `sshd_config` に対して適切なユーザベースの権限が設定されています。

プラットフォームのオーケストレーション管理者ユーザが管理者によって変更された場合は、その権限を設定して、新しいユーザの `OpenSSH sshd_config` へのアクセス権を制限する必要があります。`OpenSSH sshd_config` へのアクセス権を制限するには、次の手順を実行します。

CCE Orchestration Windows OpenSSH の強化

### 手順

**ステップ 1** 新しいプラットフォームのオーケストレーション管理者ユーザを使用して Windows ノード（CVP または ICM）にログインします。

**ステップ 2** 管理者モードで PowerShell を起動します。

**ステップ 3** OpenSSH のデフォルトのインストールディレクトリに移動します（ICM の場合は `C:\icm\install\OpenSSH-Win64` など）。

**ステップ 4** コマンド `Repair-SshdConfigPermission -FilePath C:\ProgramData\ssh\sshd_config` を実行します。

**ステップ 5** **Enter** キーを押して、継承およびアクセス制限に関するクエリのデフォルトオプション「Y」を選択します。
上記のコマンドが正常に実行されると、*%programdata%\ssh\sshd_config* が制限付きアクセスで設定されます。

**ステップ 6** OpenSSH サービスを再起動します。OpenSSH サービスの詳細については、『CCE のインストールとアップグレードガイド』の「オーケストレーション」のセクションを参照してください。

**ステップ 7** この特定の Windows ノードに対して、パブリッシャとサブスクライバの両方から、Cloud Connect CLI でコマンド **utils deployment test-connection** を実行します。これは、Cloud Connect サーバが、オーケストレーションの Windows ノード（ICM および CVP）に対してパスワードレスのセキュアシェル（SSH）接続を確立できる状態を確保できるようにするために行ないます。

CCE Orchestration Windows OpenSSH の強化